Guida di amministrazione

AWS Directory Service

Version 1.0

AWS Directory Service: Guida di amministrazione

Table of Contents

Che cos'è AWS Directory Service?

AWS Directory Service offre diversi modi per utilizzare Microsoft Active Directory (AD) con altri AWS servizi. Le directory archiviano informazioni su utenti, gruppi e dispositivi e gli amministratori le utilizzano per gestire l'accesso a informazioni e risorse. AWS Directory Service offre diverse opzioni di directory per i clienti che desiderano utilizzare applicazioni compatibili con Microsoft AD o Lightweight Directory Access Protocol (LDAP) esistenti nel cloud. Inoltre, offre le stesse opzioni per gli sviluppatori che hanno bisogno di una directory per gestire utenti, gruppi, dispositivi e accesso.

AWS Directory Service opzioni

AWS Directory Service include diversi tipi di directory tra cui scegliere. Per ulteriori informazioni, seleziona una delle seguenti schede:

AWS Directory Service for Microsoft Active Directory

Conosciuto anche come AWS Managed Microsoft AD, AWS Directory Service for Microsoft Active Directory è basato su una vera e propria Microsoft Windows Server Active Directory (AD), gestita da AWS in the AWS Cloud. Consente di migrare un'ampia gamma di applicazioni compatibili con Active Directory sul cloud. AWS AWS Microsoft AD gestito funziona con Microsoft SharePoint Microsoft SQL Server Always On Availability Groups e molte applicazioni.NET. Supporta anche applicazioni e servizi AWS gestiti tra cui Amazon WorkSpaces, Amazon WorkDocs, Amazon Quick Suite, Amazon Chime, Amazon Connect e Amazon Relational Database Service per (Amazon RDS perSQL Server, Microsoft SQL Server Amazon RDS per e Amazon RDS Oracle per PostgreSQL).

AWS Managed Microsoft AD è approvato per le applicazioni nel AWS cloud soggette alla conformità allo U.S. Health Insurance Portability and Accountability Act (HIPAA) o al Payment Card Industry Data Security Standard (PCI DSS) quando abiliti la conformità per la tua directory.

Tutte le applicazioni compatibili funzionano con le credenziali utente archiviate in AWS Managed Microsoft AD oppure è possibile connettersi all'infrastruttura AD esistente con un trust e utilizzare le credenziali di un Active Directory in esecuzione in locale o su Windows. EC2 Se unisci EC2 istanze a AWS Managed Microsoft AD, i tuoi utenti possono accedere ai carichi di lavoro Windows nel AWS cloud con la stessa esperienza Windows Single Sign-On (SSO) di quando accedono ai carichi di lavoro nella tua rete locale.

AWS Microsoft AD gestito supporta anche casi d'uso federati che utilizzano credenziali di Active Directory. Da solo, AWS Managed Microsoft AD consente di accedere a Console di gestione AWS. Con AWS IAM Identity Center, puoi anche ottenere credenziali a breve termine da utilizzare con AWS SDK e CLI e utilizzare integrazioni SAML preconfigurate per accedere a molte applicazioni cloud. Aggiungendo Microsoft Entra Connect (in precedenza noto comeAzure Active Directory Connect) e facoltativamente Active Directory Federation Service (ADFS), è possibile accedere ad altre applicazioni cloud con credenziali archiviate in Managed AWS Microsoft AD. Microsoft Office 365

Il servizio include caratteristiche fondamentali che consentono di estendere lo schema, gestire le policy delle password e attivare la sicurezza delle comunicazioni LDAP tramite Secure Socket Layer (SSL)/Transport Layer Security (TLS). Puoi anche abilitare l'autenticazione a più fattori (MFA) per AWS Managed Microsoft AD per fornire un ulteriore livello di sicurezza quando gli utenti AWS accedono alle applicazioni da Internet. Poiché Active Directory è una directory LDAP, puoi anche utilizzare Microsoft AD gestito da AWS per l'autenticazione Linux Secure Shell (SSH) e per altre applicazioni abilitate per LDAP.

AWS fornisce monitoraggio, istantanee giornaliere e ripristino come parte del servizio: si aggiungono utenti e gruppi a Managed AWS Microsoft AD e si amministrano i Criteri di gruppo utilizzando gli strumenti familiari di Active Directory in esecuzione su un Windows computer unito al dominio Microsoft AD gestito AWS . Puoi anche ridimensionare la directory distribuendo ulteriori controller di dominio e migliorare così le prestazioni delle applicazioni distribuendo le richieste su un maggior numero di controller di dominio.

AWS Managed Microsoft AD è disponibile in due edizioni: Standard ed Enterprise.

- Standard Edition: Microsoft AD gestito da AWS (Standard Edition) è ottimizzato per essere una directory primaria per piccole e medie imprese con massimo 5.000 dipendenti. Fornisce una capacità di storage sufficiente per supportare fino a 30.000* oggetti di directory, come utenti, gruppi e computer.
- Enterprise Edition: Microsoft AD gestito da AWS (Enterprise Edition) è stato progettato per supportare le grandi organizzazioni con massimo 500.000* oggetti directory.

* I limiti sopra indicati sono approssimativi. La directory potrebbe supportare più o meno oggetti di directory a seconda della dimensioni degli oggetti e della necessità di prestazioni e comportamento delle applicazioni.

Quando usare

AWS Managed Microsoft AD è la scelta migliore se hai bisogno di funzionalità effettive di Active Directory per supportare AWS applicazioni o Windows carichi di lavoro, incluso Amazon Relational Database Service for. Microsoft SQL Server È anche la soluzione ideale se desideri una Active Directory autonoma nel AWS cloud che supporti Office 365 o se hai bisogno di una directory LDAP per supportare le tue applicazioni Linux. Per ulteriori informazioni, consulta AWSMicrosoft AD gestito.

AD Connector

AD Connector è un servizio proxy che offre un modo semplice per connettere AWS applicazioni compatibili, come Amazon WorkSpaces, Amazon Quick Suite e Amazon EC2 per Windows Server esempio, all'MicrosoftActive Directory locale esistente. Con il connettore AD puoi aggiungere semplicemente un account del servizio ad Active Directory. Il connettore AD, inoltre, elimina la necessità di sincronizzazione la directory o i costi e la complessità di ospitare un'infrastruttura di federazione.

Quando aggiungi utenti ad AWS applicazioni come Amazon Quick Suite, AD Connector legge l'Active Directory esistente per creare elenchi di utenti e gruppi tra cui scegliere. Quando gli utenti accedono alle AWS applicazioni, AD Connector inoltra le richieste di accesso ai controller di dominio Active Directory locali per l'autenticazione. AD Connector funziona con molte AWS applicazioni e servizi tra cui Amazon WorkSpaces, Amazon WorkDocs, Amazon Quick Suite, Amazon Chime, Amazon Connect e Amazon. WorkMail Puoi anche unire le tue EC2 Windows istanze al tuo dominio Active Directory locale tramite AD Connector utilizzando l'aggiunta al dominio senza interruzioni. AD Connector consente inoltre agli utenti di accedere Console di gestione AWS e gestire AWS le risorse accedendo con le credenziali di Active Directory esistenti. Il connettore AD non è compatibile con RDS SQL Server.

Puoi anche utilizzare AD Connector per abilitare l'autenticazione a più fattori (MFA) per gli utenti delle AWS tue applicazioni collegandola all'infrastruttura MFA esistente basata su RADIUS. Questo fornisce un ulteriore livello di sicurezza quando gli utenti accedono alle applicazioni AWS .

Con il connettore AD puoi continuare a gestire l'Active Directory allo stesso modo. Ad esempio, puoi aggiungere nuovi utenti e gruppi e aggiornare le password usando gli strumenti di amministrazione di Active Directory standard nell'Active Directory esistente. Ciò consente di applicare in modo coerente le politiche di sicurezza, come la scadenza delle password, la cronologia delle password e il blocco degli account, indipendentemente dal fatto che gli utenti accedano alle risorse in locale o nel cloud. AWS

Quando usare

AD Connector è la scelta migliore quando desideri utilizzare la tua directory locale esistente con AWS servizi compatibili. Per ulteriori informazioni, consulta AD Connector.

Simple AD

Simple AD è una Microsoft directory compatibile con Active Directory basata su Samba 4. AWS Directory Service Simple AD supporta le funzionalità di base di Active Directory come account utente, appartenenza a gruppi, accesso a un dominio Linux o a EC2 istanze Windows basate, SSO basato su Kerberos e politiche di gruppo. AWS fornisce monitoraggio, istantanee giornaliere e ripristino come parte del servizio.

Simple AD è una directory autonoma nel cloud in cui è possibile creare e gestire le identità degli utenti e l'accesso alle applicazioni. Puoi utilizzare molte applicazioni e strumenti comuni sensibili ad Active Directory che richiedono funzionalità di base di Active Directory. Simple AD è compatibile con le seguenti AWS applicazioni: Amazon WorkSpaces, Amazon WorkDocs, Amazon Quick Suite e Amazon WorkMail. Puoi anche accedere agli account utente Console di gestione AWS with Simple AD e gestire AWS le risorse.

Simple AD non supporta l'autenticazione a più fattori (MFA), le relazioni di trust, l'aggiornamento dinamico DNS, le estensioni dello schema, la comunicazione tramite PowerShell LDAPS, i cmdlet AD o il trasferimento di ruoli FSMO. Simple AD non è compatibile con RDS SQL Server. I clienti che richiedono le funzionalità di una vera Microsoft Active Directory o che intendono utilizzare la propria directory con RDS SQL Server dovrebbero invece utilizzare Managed AWS Microsoft AD. Verifica che le applicazioni necessarie siano completamente compatibili con Samba 4 prima di utilizzare Simple AD. Per ulteriori informazioni, consulta https://www.samba.org.

Quando usare

Puoi utilizzare Simple AD come directory autonoma nel cloud per supportare Windows carichi di lavoro che richiedono funzionalità di base di Active Directory, AWS applicazioni compatibili o per supportare carichi di lavoro Linux che richiedono il servizio LDAP. Per ulteriori informazioni, consulta Simple AD.

Consulta Disponibilità regionale per Directory Service per un elenco dei tipi di directory supportati per regione.

Quale scegliere

Puoi scegliere i servizi di directory con le caratteristiche e la scalabilità che meglio soddisfano le tue esigenze. Utilizza la tabella seguente per determinare quale opzione di AWS Directory Service directory è più adatta alla tua organizzazione.

Che cosa occorre fare?	AWS Directory Service Opzioni consigliate
Ho bisogno di Active Directory o LDAP per le applicazioni nel cloud	Usa AWS Directory Service for Microsoft Active Directory (Standard Edition o Enterprise Edition) se hai bisogno di una vera Microsoft Active Directory nel AWS cloud che supporti carichi di lavoro compatibili con Active Directory o AWS applicazioni e servizi come Amazon e WorkSpace s Amazon Quick Suite, oppure hai bisogno del supporto LDAP per applicazioni Linux. Usa AWS Directory Service per Microsoft Active Directory (Hybrid Edition) per estendere il tuo AD esistente autogesti to nel Cloud AWS AWS Directory Service Usa AD Connector se devi solo consentire agli utenti locali di accedere ad AWS applicazioni e servizi con le loro credenziali di Active Directory. Puoi anche utilizzare AD Connector per aggiungere EC2 istanze Amazon al tuo dominio Active Directory esistente. Utilizza Simple AD se hai bisogno di una directory a basso costo, su piccola scala con una compatibilità di base con Active Directory che supporti le applicazioni compatibili con Samba 4 o se hai bisogno della compatibilità LDAP per le applicazioni compatibili con LDAP.
Sviluppo applicazioni SaaS	Utilizza Amazon Cognito se sviluppi applicazioni SaaS su grande scala e hai bisogno di una directory scalabile per gestire e autenticare gli abbonati e che funzioni con le identità di social media.

Per ulteriori informazioni sulle opzioni di AWS Directory Service directory, consulta Come scegliere le soluzioni Active Directory su AWS.

Lavorare con Amazon EC2

Una conoscenza di base di Amazon EC2 è essenziale per l'utilizzo Directory Service. Consigliamo di iniziare leggendo gli argomenti seguenti:

- Che cos'è Amazon EC2? nella Amazon EC2 User Guide.
- Avvia un' EC2istanza Amazon nella Amazon EC2 User Guide.
- Gruppi EC2 di sicurezza Amazon per le tue EC2 istanze nella Amazon EC2 User Guide.
- Cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.
- Connetti il tuo VPC a reti remote utilizzando AWS Virtual Private Network la Amazon VPC User Guide.

AWSMicrosoft AD gestito

AWSDirectory Service for Microsoft Active Directory, noto anche come AWS Managed Microsoft AD, viene eseguito Microsoft Active Directory come un servizio gestito basato su Windows Server 2019. Crea una coppia di controller di dominio ad alta disponibilità nel tuo Amazon VPC in diverse zone di disponibilità, gestendo automaticamente il monitoraggio dell'host, AWS il ripristino, la replica dei dati, le istantanee e gli aggiornamenti software. Questo servizio ti consente di eseguire carichi di lavoro compatibili con le directory, gestire utenti e gruppi, fornire Single Sign-On, creare e applicare policy di gruppo e connetterti in modo sicuro alle istanze Amazon. EC2

Directory Serviceoffre due Microsoft Active Directory soluzioni: AWSDirectory Service per Microsoft Active Directory fornisce un servizio Active Directory completamente gestito nel AWS cloud, mentre AWSManaged Microsoft AD (Hybrid Edition) estende l'AD autogestito esistente aAWS.

AWSMicrosoft AD gestito (Standard Edition ed Enterprise Edition) crea nuovi domini AD gestiti su AWS cui gestire utenti, dispositivi e computer. Queste directory stabiliscono foreste di risorse che creano relazioni di fiducia con i domini AD esistenti in localeAWS, in o in ambienti multi-cloud. Gli utenti possono accedere alle AWS risorse con le credenziali esistenti dai domini AD correnti. Le identità degli utenti rimangono nei domini AD esistenti mentre la foresta di risorse gestisce le AWS risorse, mantenendo l'isolamento operativo tra gli ambienti e fornendo al contempo un single sign-on senza interruzioni.

AWSManaged Microsoft AD (Hybrid Edition) collega l'Active Directory autogestito con AWS Directory Service per Microsoft Active Directory, creando un ambiente di identità integrato che copre sia l'infrastruttura che il. Cloud AWS Questa soluzione estende i servizi di directory AWS senza sincronizzare le identità degli utenti, stabilisce relazioni di fiducia tra gli ambienti e fornisce un accesso senza interruzioni utilizzando le credenziali esistenti.

Con AWS Managed Microsoft AD, puoi eseguire carichi di lavoro compatibili con le directory nel AWS cloud, incluse applicazioni personalizzate basate su .NET Microsoft SharePoint e SQL Server. È inoltre possibile configurare relazioni di trust tra AWS Managed Microsoft AD e l'MicrosoftActive Directory autogestito esistente, fornendo a utenti e gruppi l'accesso alle risorse in entrambi i domini utilizzandoAWS IAM Identity Center.

Quale scegliere

Puoi scegliere tra due AWS Directory Service servizi con le funzionalità e la scalabilità più adatte alle tue esigenze. La tabella seguente consente di determinare l'Directory Serviceopzione più adatta alla propria organizzazione.

Caso d’uso	Soluzione consigliata
Esegui carichi di lavoro, AWS applicazioni o applicazioni Linux che richiedono il supporto LDAP	AWSMicrosoft AD gestito (Standard Edition ed Enterpris e Edition) crea nuovi domini AD gestiti su AWS cui gestire utenti, dispositivi e computer. Queste directory stabilisc ono foreste di risorse che creano relazioni di fiducia con i domini AD esistenti in localeAWS, in o in ambienti multi-cloud. Gli utenti possono accedere alle AWS risorse con le credenziali esistenti dai domini AD correnti. Le identità degli utenti rimangono nei domini AD esistenti mentre la foresta di risorse gestisce le AWS risorse, mantenend o l'isolamento operativo tra gli ambienti e fornendo al contempo un single sign-on senza interruzioni.
Estendi Active Directory esistente a AWS	AWSManaged Microsoft AD (Hybrid Edition) collega l'Active Directory autogestito con AWS Directory Service per Microsoft Active Directory, creando un ambiente di identità integrato che copre sia l'infrastruttura che il. Cloud AWS Questa soluzione estende i servizi di directory AWS senza sincronizzare le identità degli utenti, stabilisce relazioni di fiducia tra gli ambienti e fornisce un accesso senza interruzioni utilizzando le credenziali esistenti.

Argomenti

- Guida introduttiva a AWS Managed Microsoft AD
- Informazioni su AWS Managed Microsoft AD (Hybrid Edition)

Informazioni su AWS Managed Microsoft AD (Hybrid Edition)

AWSManaged Microsoft AD (Hybrid Edition) consente di estendere l'Active Directory esistente Cloud AWS con AWS Managed Microsoft AD. Questa funzionalità semplifica lo spostamento dei carichi di lavoro dipendenti dalla pubblicitàAWS, l'adozione di AWS servizi e l'aumento della ridondanza di Active Directory. AWSeseguirà periodicamente valutazioni delle directory sulla directory ibrida che è possibile visualizzare nella console. Directory Service

Una directory ibrida Directory Service collega l'utente esistente Microsoft Active Directorya AWSDirectory Service for Microsoft Active Directory (AWSManaged Microsoft AD). Questo crea un ambiente di identità integrato che comprende l'infrastruttura locale e multi-cloudAWS, che consente di mantenere un'unica fonte di identità estendendo al contempo i servizi di directory. AWS

Una configurazione di directory ibrida offre diverse funzionalità importanti:

- Estensione di AD autogestito a Cloud AWS senza la necessità di stabilire una relazione di fiducia
- Autenticazione e autorizzazione senza interruzioni in tutti gli ambienti utilizzando le credenziali Active Directory esistenti
- Credenziali utente e appartenenza ai gruppi coerenti in entrambi gli ambienti AD
- Gestione centralizzata delle politiche e delle autorizzazioni di accesso AD

Argomenti

Prerequisiti della directory ibrida

La directory ibrida estende la tua Active Directory autogestita a. Cloud AWS Prima di creare una directory ibrida, assicurati che il tuo ambiente soddisfi questi requisiti:

Microsoft Active Directoryrequisiti del dominio

Prima di creare una directory ibrida, assicurati che l'ambiente e l'infrastruttura AD autogestiti soddisfino i seguenti requisiti e raccogli le informazioni necessarie.

Requisiti del dominio

L'ambiente AD autogestito deve soddisfare i seguenti requisiti:

- Utilizza un livello 2016 funzionale Windows Server 2012 R2 or.
- Utilizza controller di dominio standard da valutare per la creazione di directory ibride. I controller di dominio di sola lettura (RODC) non possono essere utilizzati per la creazione di directory ibride.
- Dispone di due controller di dominio con tutti i servizi Active Directory in esecuzione.
- Il controller di dominio primario (PDC) deve essere sempre instradabile.

  In particolare, l'emulatore PDC e il RID Master IPs dell'AD autogestito devono rientrare in una di queste categorie:

  - Parte degli intervalli di indirizzi IP RFC1918 privati (10.0.0.0/8, 172.16.0.0/12 o 192.168.0.0/16)
  - All'interno della tua gamma VPC CIDR
  - Abbina il DNS IPs delle tue istanze autogestite alla directory

  È possibile aggiungere percorsi IP aggiuntivi per la directory dopo la creazione della directory ibrida.

Informazioni obbligatorie

Raccogli le seguenti informazioni sul tuo AD autogestito:

- Nome DNS directory
- Directory DNS IPs
- Credenziali dell'account di servizio con autorizzazioni di amministratore per il tuo AD autogestito
- AWSARN segreto per l'archiviazione delle credenziali dell'account di servizio (vedi) AWSARN segreto per directory ibrida

AWSARN segreto per directory ibrida

Per configurare una directory ibrida con il tuo AD autogestito, devi creare una chiave KMS per crittografare il AWS segreto e quindi creare il segreto stesso. Entrambe le risorse devono essere create nella stessa Account AWS che contiene la directory ibrida.

Crea una chiave KMS

La chiave KMS viene utilizzata per crittografare il tuo segreto. AWS

> **Important**
>
> In Chiave crittografia, non utilizzare la chiave KMS AWS predefinita. Assicurati di creare la chiave AWS KMS nella stessa Account AWS che contiene la directory ibrida che desideri creare per unirti al tuo AD autogestito.

Per creare una chiave KMS AWS

1. Nella AWS KMS console, scegli Crea chiave.
2. In Tipo di chiave, scegli Simmetrica.
3. In Utilizzo delle chiavi, scegli Crittografa e decrittografa.
4. In Advanced options (Opzioni avanzate):
    a. In Origine materiale chiave, scegli KMS.
    b. Per Regionalità, scegli la chiave Single-Region e scegli Avanti.
5. In Alias, fornisci un nome per la chiave KMS.
6. (Facoltativo) In Descrizione, immetti una descrizione per la chiave KMS.
7. (Facoltativo) Per i tag, aggiungi i tag per la chiave KMS e scegli Avanti.
8. Per gli amministratori chiave, seleziona un utente IAM.
9. Per l'eliminazione della chiave, mantieni la selezione predefinita per Consenti agli amministratori chiave di eliminare questa chiave e scegli Avanti.
10. Per gli utenti chiave, seleziona lo stesso utente IAM del passaggio precedente e scegli Avanti.
11. Riesamina la configurazione.
12. Per Key policy, aggiungi la seguente dichiarazione alla policy:

13. Scegli Fine.

Crea un AWS segreto

Crea un segreto in Secrets Manager per archiviare le credenziali del tuo account utente AD autogestito.

> **Important**
>
> Crea il segreto nella stessa Account AWS che contiene la directory ibrida a cui desideri unire con il tuo AD autogestito.

Per creare un segreto

- In Secrets Manager, scegli Archivia un nuovo segreto
- Per Tipo segreto, scegli Altro tipo di segreto
- In Coppie chiave/valore, aggiungi le due chiavi:

1. Aggiungi la chiave del nome utente
   a. Per la prima chiave, immetti `customerAdAdminDomainUsername`.
   b. Per il valore della prima chiave, immetti solo il nome utente (senza il prefisso di dominio) dell'utente AD. Non includere il nome di dominio in quanto impedisce la creazione dell'istanza.
2. Aggiungi la chiave della password
   a. Per la seconda chiave, immetti `customerAdAdminDomainPassword`.
   b. Per il valore della seconda chiave, immetti la password creata per l'utente AD nel dominio.

Completa la configurazione segreta

1. Per la chiave di crittografia, seleziona la chiave KMS che hai creato Crea una chiave KMS e scegli Avanti.
2. Per Nome segreto, inserisci una descrizione per il segreto.
3. (Facoltativo) In Descrizione, inserisci una descrizione per il segreto.

4. Scegli Next (Successivo).
5. In Configura impostazioni di rotazione, non modificare i valori predefiniti e scegli Avanti.
6. Controlla le impostazioni del segreto e scegli Store.
7. Scegli il segreto creato e copia il valore in ARN secreto. Utilizzerai questo ARN nel passaggio successivo per configurare la tua Active Directory autogestita.

Requisiti di infrastruttura

Prepara i seguenti componenti dell'infrastruttura:

- Due AWS Systems Manager nodi con privilegi di amministratore per gli agenti SSM
  - Se la tua Active Directory è gestita automaticamente all'esterno di Cloud AWS, avrai bisogno di due nodi Systems Manager per un ambiente ibrido e multicloud. Per ulteriori informazioni su come effettuare il provisioning di questi nodi, vedere Configurazione di Systems Manager per ambienti ibridi e multicloud.
  - Se Active Directory è gestita automaticamente all'interno diCloud AWS, saranno necessarie due EC2 istanze gestite da Systems Manager. Per ulteriori informazioni su come effettuare il provisioning di queste istanze, vedere Gestione delle EC2 istanze con Systems Manager.

Servizi Active Directory richiesti

Assicurati che i seguenti servizi siano in esecuzione sul tuo AD autogestito:

- Servizi di dominio Active Directory
- Servizio Web Active Directory (ADWS)
- Sistema di eventi COM+
- Distributed File System Replication (DFSR)
- Domain Name System (DNS)
- Server DNS
- Client di policy di gruppo
- Messaggistica tra siti
- Chiamata di procedura remota (RPC)
- Gestore degli account di sicurezza
- Time Server di Windows

> **Note**
>
> La directory ibrida richiede che sia la porta UDP 123 sia aperta sia che Windows Time Server sia abilitato e funzionante. Sincronizziamo l'ora con il controller di dominio per garantire che la replica delle directory ibride funzioni correttamente.

Requisiti di autenticazione Kerberos

I tuoi account utente devono avere la preautenticazione Kerberos abilitata. Per istruzioni dettagliate su come abilitare questa impostazione, consulta Assicurarsi che la preautenticazione Kerberos sia abilitata. Per informazioni generali su questa impostazione, vai a Preautenticazione attiva. Microsoft TechNet

Tipi di crittografia supportati

la directory ibrida supporta i seguenti tipi di crittografia durante l'autenticazione tramite Kerberos nei controller di dominio Active Directory:

- AES-256-HMAC

Requisiti delle porte di rete

AWSPer estendere i controller di dominio Active Directory autogestiti, il firewall della rete esistente deve avere le seguenti porte aperte CIDRs per entrambe le sottoreti del tuo Amazon VPC:

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticazione Kerberos
- UDP 123: server temporale
- TCP 135 - Chiamata di procedura remota
- TCP/UDP 389 - LDAP
- TCP 445 - SMB
- TCP 636 - Necessario solo per ambienti con Lightweight Directory Access Protocol Secure (LDAPS)
- TCP 49152-65535 - Porte TCP elevate allocate casualmente da RPC
- TCP 3268 e 3269 - Catalogo globale

- Servizi Web Active Directory (ADWS) TCP 9389

Queste sono le porte minime necessarie per creare una directory ibrida. La propria configurazione specifica potrebbe richiedere l'apertura di porte aggiuntive.

> **Note**
>
> Il DNS IPs fornito per i controller di dominio e i titolari di ruoli FSMO deve avere le porte di cui sopra aperte CIDRs per entrambe le sottoreti in Amazon VPC.

> **Note**
>
> La directory ibrida richiede che sia la porta UDP 123 sia aperta sia che Windows Time Server sia abilitato e funzionante. Sincronizziamo l'ora con il controller di dominio per garantire che la replica delle directory ibride funzioni correttamente.

Account AWSautorizzazioni

Avrai bisogno delle autorizzazioni per le seguenti azioni nel tuo: Account AWS

- ec2: AuthorizeSecurityGroupEgress
- ec2: AuthorizeSecurityGroupIngress
- ec2: CreateNetworkInterface
- ec2: CreateSecurityGroup
- ec2: DescribeNetworkInterfaces
- ec2: DescribeSubnets
- ec2: DescribeVpcs
- ec2: CreateTags
- ec2: CreateNetworkInterfacePermission
- ssm: ListCommands
- ssm: GetCommandInvocation
- ssm: GetConnectionStatus
- ssm: SendCommand

- gestore dei segreti: DescribeSecret
- gestore dei segreti: GetSecretValue
- sono: GetRole
- sono: CreateServiceLinkedRole

Requisiti di rete Amazon VPC

Un VPC con quanto segue:

- Almeno due sottoreti. Ciascuna sottorete deve trovarsi in una zona di disponibilità diversa
- Il VPC deve avere una locazione predefinita

Non è possibile creare una directory ibrida in un VPC utilizzando gli indirizzi nello spazio di indirizzi 198.18.0.0/15.

Directory Serviceutilizza una struttura a due VPC. Le EC2 istanze che compongono la tua directory vengono eseguite all'esterno della tua Account AWS e sono gestite da. AWS Hanno due schede di rete, `ETH0` e `ETH1`. `ETH0` è la scheda di gestione ed è al di fuori del tuo account. `ETH1` viene creata all'interno dell'account.

L'intervallo IP di gestione della rete ETH0 per la tua directory è. `198.18.0.0/15`

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di Amazon VPC:

- Cos'è Amazon VPC?
- Cos'è Amazon VPC?
- VPCs e sottoreti
- Che cos'è AWS Site-to-Site VPN?

Per ulteriori informazioni suAWS Direct Connect, consulta la sezione Cos'è? AWS Direct Connect

AWSconfigurazione del gruppo di sicurezza

Per impostazione predefinita, AWS collega un gruppo di sicurezza per consentire l'accesso di rete ai nodi AWS Systems Manager gestiti nel tuo VPC. Facoltativamente, puoi fornire il tuo gruppo di sicurezza che consente il traffico di rete da e verso i controller di dominio autogestiti al di fuori del tuo VPC.

Facoltativamente, puoi fornire il tuo gruppo di sicurezza che consente il traffico di rete da e verso i controller di dominio autogestiti al di fuori del tuo VPC. Se fornisci il tuo gruppo di sicurezza, devi:

- Consenti l'elenco dei tuoi VPC CIDR intervalli e degli intervalli autogestiti.
- Assicurati che questi intervalli non si sovrappongano agli intervalli IP riservati AWS

Considerazioni sulle valutazioni degli elenchi

Di seguito sono riportate le considerazioni da prendere in considerazione per la creazione di valutazioni relative agli elenchi e il numero di valutazioni che è possibile inserire nel proprio elenco: Account AWS

- Una valutazione delle directory viene creata automaticamente quando si crea una directory ibrida. Esistono due tipi di valutazioni: `CUSTOMER` e`SYSTEM`. Hai Account AWS un limite di 100 valutazioni nell'`CUSTOMER`elenco.
- Se si tenta di creare una directory ibrida e si dispone già di 100 valutazioni di `CUSTOMER` directory, si verificherà un errore. Elimina le valutazioni per liberare capacità prima di riprovare.
- Puoi richiedere un aumento della quota di valutazione dell'`CUSTOMER`elenco contattando Supporto o eliminando le valutazioni esistenti nell'elenco CUSTOMER per liberare spazio.

Creazione di una directory ibrida

Prima di creare una directory ibrida, è necessario creare e superare con successo una valutazione della directory che verifichi la connettività e l'interoperabilità con l'Active Directory autogestito

Creazione di una directory ibrida con AD autogestito

Segui questi passaggi per creare una directory ibrida con il tuo AD autogestito:

Per creare una directory ibrida

1. Apri la Directory Service console per la regione desiderata.
2. Nella pagina Seleziona il tipo di directory, scegli AWS Managed Microsoft AD.
3. In Guida introduttiva AWS a Managed Microsoft AD, seleziona Estendi il tuo dominio AD con una directory ibrida — new, quindi scegli Avanti. Verrai indirizzato alla pagina di valutazione Create directory.

4. Prima di poter creare una directory ibrida, è necessario creare e superare con successo una valutazione della directory. Per creare una valutazione delle directory, segui la procedura riportata di seguitoCreazione di valutazioni degli elenchi. Dopo aver superato con successo una valutazione delle directory, è possibile continuare con questa procedura.
5. Dopo aver superato con successo una valutazione delle directory, accedi alla pagina Elenchi.
6. Nella pagina Elenchi, in Trial hybrid directory assessments, scegli un ID di valutazione con uno stato di. SUCCESS Quindi seleziona Crea una directory ibrida, che ti indirizza alla pagina dei dettagli della valutazione
7. Nella pagina dei dettagli della valutazione, conferma questa azione selezionando Crea directory ibrida, che apre la pagina Crea directory ibrida utilizzando assessment-id.
8. Nella pagina Crea una directory ibrida utilizzando assessment-id, esamina le informazioni di Active Directory autogestita. Dopo aver confermato le informazioni, seleziona Crea directory ibrida.

   Dopo aver scelto Crea directory ibrida, AWS esegue un'altra valutazione della directory basata su queste informazioni per confermare che la configurazione AD autogestita è ancora valida. Se la valutazione della directory ha esito positivo, creiamo la directory ibrida.
9. Scegliendo Crea una directory ibrida si torna alla pagina Directory.

   a. Una volta creata correttamente la directory ibrida, verrà visualizzato un banner verde.

   b. Se la creazione della directory ibrida non riesce, verrà visualizzato un banner rosso. Risolvi gli errori di creazione della directory ibrida completando quanto segue:

      1. Eliminare la directory ibrida non riuscita nella console.
      2. Elimina eventuali AWS riserve rimanenti OUs nel tuo AD autogestito.

   Ulteriori informazioni

   - Eliminazione di una directory ibrida
   - Risoluzione dei problemi

Visualizzazione e modifica di una directory ibrida

Utilizza le seguenti procedure per visualizzare o modificare la tua directory ibrida.

Visualizzazione di una directory ibrida

È possibile visualizzare una directory ibrida nella Directory Service console.

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione Directory Service console, scegliere Directories (Directory).
2. Seleziona il collegamento dell'ID per la tua directory. Le informazioni sulla directory vengono visualizzate nella pagina dei dettagli della directory.

Informazioni su Active Directory gestite automaticamente

Questa sezione fornisce informazioni sull'Active Directory autogestito collegato all' AWS infrastruttura.

- Tipo di directory
- ID della directory
- Stato della directory
- Dettagli di rete per il tuo AD autogestito, ad esempio:
  - VPC
  - Sottoreti
  - Indirizzi DNS
- Nodi gestiti da Systems Manager

Schede di directory ibride

Puoi trovare le seguenti informazioni su AWS Managed Microsoft AD:

- Nella scheda Condividi e condividi, puoi condividere il tuo AWS Managed Microsoft AD con altri AWS account e visualizzare i dettagli di rete per i tuoi controller di dominio.
- Nella scheda Gestione applicazioni, puoi abilitare un URL di accesso all'applicazione per AWS Managed Microsoft AD e abilitare AWS applicazioni e servizi per AWS Managed Microsoft AD.
- Nella scheda Manutenzione, puoi consentire a SNS di ricevere notifiche sullo stato di AWS Managed Microsoft AD e rivedere le istantanee di Managed AWS Microsoft AD.
- Per ulteriori informazioni sul campo Status (Stato), consultare Informazioni sullo stato della directory AWS Managed Microsoft AD.

Aggiornamento di una directory ibrida

È possibile aggiornare una directory ibrida nella Directory Service console per modificare le impostazioni DNS o ripristinare l'accesso all'account amministratore.

Per aggiornare le informazioni sulla directory ibrida

1. Nel riquadro di navigazione Directory Service console, scegliere Directories (Directory).
2. Scegliete il collegamento all'ID della directory per aprire la pagina dei dettagli della directory.
3. Scegli Azioni, quindi scegli Aggiorna le informazioni della directory ibrida.
4. Nella pagina Aggiorna le informazioni della directory ibrida, puoi aggiornare le impostazioni DNS o ripristinare il tuo account amministratore.

   Aggiorna le impostazioni DNS (opzionale)

   In Informazioni su Active Directory autogestite, puoi modificare quanto segue:

   a. Nome DNS della directory
   b. Indirizzi IP DNS

   È possibile aggiornare entrambe le impostazioni insieme o singolarmente. È necessaria almeno una modifica per il processo di aggiornamento.
5. Recupera l'account dell'amministratore della directory ibrida

   Per ripristinare l'account di amministratore della directory ibrida, è necessario l'accesso temporaneo a un utente. Questo accesso viene fornito tramite un segreto di Secrets Manager. Utilizziamo queste credenziali solo una volta durante il ripristino e non le archiviamo. Se il tuo account di amministratore di Hybrid Directory esiste, non è necessario aggiornare questo segreto, anche se hai aggiornato l'utente amministratore di Active Directory autogestito.

   - Credenziali di amministratore segrete: creiamo un account amministratore di directory ibrida quando creiamo una directory ibrida. Se hai eliminato questo segreto, inserisci il tuo segreto di Secrets Manager per l'utente amministratore di AD autogestito.

Eliminazione di una directory ibrida

Quando si elimina una directory ibrida, tutti i dati e le istantanee della directory vengono eliminati e non possono essere recuperati. Dopo l'eliminazione della directory, tutte le istanze unite alla directory

rimangono intatte. Tuttavia, non è possibile utilizzare le credenziali della directory per accedere a queste istanze. È necessario accedere a queste istanze con un account utente locale.

Eliminazione di una directory

1. Nel riquadro di navigazione della console Directory Service, seleziona Directory. Assicurati di trovarti nel luogo in Regione AWS cui è distribuita la tua directory ibrida. Per ulteriori informazioni, consulta Scelta di una regione.
2. Assicurati che nessuna AWS applicazione sia abilitata per la directory che intendi eliminare. AWS Le applicazioni abilitate impediranno di eliminare la directory ibrida.
3. Nella pagina Directories (Directory), scegli l'ID della directory.
4. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione). Nella sezione AWS app e servizi, puoi vedere quali AWS applicazioni sono abilitate per la tua directory.

    a. Disabilita Console di gestione AWS l'accesso. Per ulteriori informazioni, vedere Disabilitazione dell'accesso alla console AWS di gestione.

    b. Per disabilitare Amazon FSx for Windows File Server, devi rimuovere il FSx file system Amazon dal dominio. Per ulteriori informazioni, consulta Working with Active Directory in FSx for Windows File Server nella Amazon FSx for Windows File Server User Guide.

    c. Per disabilitare Amazon Relational Database Service, devi rimuovere l'istanza Amazon RDS dal dominio. Per ulteriori informazioni, consulta Gestione di un'istanza database in un dominio nella Guida per l'utente di Amazon RDS.
5. Nel riquadro di navigazione, seleziona Directory.
6. Seleziona solo la directory da eliminare e scegli Elimina. Sono necessari alcuni minuti per l'eliminazione della directory. Una volta eliminata la directory, viene rimossa dal tuo elenco di directory.
7. Elimina manualmente tutti gli oggetti del controller di dominio rimanenti, inclusi eventuali oggetti AWS riservati OUs. È possibile eliminare l'intera directory AWS riservata per completare la pulizia dell'ambiente.

Valutazioni delle directory per directory ibride

Una valutazione delle directory esamina l'ambiente Active Directory autogestito per assicurarsi che soddisfi i requisiti per la creazione di una directory ibrida. Questa valutazione verifica la connettività di

rete, la configurazione dei controller di dominio e i servizi richiesti per aiutare a identificare e risolvere potenziali problemi prima di stabilire una connessione tra AD autogestito e. Directory Service

Esistono due tipi di valutazione delle directory:

- *CUSTOMER*valutazioni: avviate dall'utente nella console quando si inizia a configurare una directory ibrida. Puoi eliminare le valutazioni dell'elenco clienti, anche mentre sono in corso. Puoi avere fino a 100 valutazioni dei clienti.
- *SYSTEM*valutazioni: create automaticamente AWS ed eseguite periodicamente dopo una creazione riuscita. Non puoi eliminare le SYSTEM valutazioni.

Le valutazioni delle directory forniscono informazioni preziose sulla fattibilità dell'ambiente, tra cui:

- Connettività tra AD autogestito e AWS
- Disponibilità dei servizi richiesti sui controller di dominio
- Compatibilità della configurazione con i requisiti del AWS Directory Service
- Potenziali problemi che potrebbero impedire la corretta creazione di directory ibride

Prima di poter creare una directory ibrida, è necessaria una valutazione corretta (superata) della directory. Se una valutazione fallisce, puoi visualizzare il rapporto dettagliato per identificare e risolvere i problemi prima di riprovare. AWS elimina le SYSTEM valutazioni dopo 30 giorni.

Argomenti

- Creazione di valutazioni degli elenchi
- Visualizzazione delle valutazioni delle directory
- Eliminazione delle valutazioni delle directory

Creazione di valutazioni degli elenchi

È possibile creare una valutazione delle directory come parte della creazione di una directory ibrida oppure crearne una manualmente. Per creare una valutazione manualmente, apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/. Nella pagina Elenchi, nella sezione Valutazioni degli elenchi, scegli Crea valutazione.

Per creare una valutazione dell'elenco

1. Nella pagina di valutazione Create directory, per Directory DNS name, inserisci il tuo nome DNS Active Directory autogestito.
2. Per gli indirizzi IP DNS, inserisci due indirizzi IP DNS per il tuo AD autogestito.
3. La directory ibrida richiede un Amazon VPC con almeno due sottoreti. Se non li possiedi già, puoi crearli. Nella sezione Rete, fornisci quanto segue:

   a. Per VPC, scegli il tuo identificatore VPC.

   b. Per le sottoreti, scegli l'identificatore per ciascuna delle due sottoreti. Ogni sottorete deve trovarsi in zone di disponibilità diverse. Per ulteriori informazioni, consulta Requisiti di rete Amazon VPC.

   c. Per Gruppo di sicurezza, scegli l'identificatore del gruppo di sicurezza. Per impostazione predefinita, AWS collega un gruppo di sicurezza per consentire l'accesso di rete ai nodi Gestione dei segreti AWS gestiti nel tuo Amazon VPC. Facoltativamente, puoi fornire il tuo gruppo di sicurezza che consente il traffico di rete da e verso i controller di dominio autogestiti al di fuori del tuo Amazon VPC.
4. Nella sezione AWS Systems Manager nodi, scegli due nodi o istanze di Systems Manager in base ai seguenti requisiti:

   - Se la tua Active Directory è gestita automaticamente all'esterno di Cloud AWS, avrai bisogno di due nodi Systems Manager per un ambiente ibrido e multicloud. Per ulteriori informazioni su come effettuare il provisioning di questi nodi, vedere Configurazione di Systems Manager per ambienti ibridi e multicloud.
   - Se Active Directory è gestita automaticamente all'interno di Cloud AWS, saranno necessarie due EC2 istanze gestite di Systems Manager. Per ulteriori informazioni su come effettuare il provisioning di queste istanze, vedere Gestione delle EC2 istanze con Systems Manager.
5. Scegliete Avanti per aprire la pagina di valutazione Review and create directory.
6. Nella pagina Rivedi e crea una directory assessment, esamina le informazioni sulla valutazione della directory e apporta le modifiche necessarie. Quando le informazioni sono corrette, scegli Crea valutazione. La creazione della valutazione della directory richiede circa 30 minuti. Verrai reindirizzato alla pagina dei dettagli degli elenchi. Quando la valutazione della directory ha esito positivo, viene visualizzato un banner verde.

> **Warning**
>
> Per creare una directory ibrida, la valutazione della directory deve inserire lo stato SUCCESS. Non è possibile creare una directory ibrida senza aver prima superato con successo una valutazione della directory.

Visualizzazione delle valutazioni delle directory

È possibile visualizzare le valutazioni dell'elenco Console di gestione AWS per esaminare i risultati delle valutazioni e gestire i report di valutazione.

Per visualizzare una valutazione dell'elenco

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Elenchi, nella sezione Trial hybrid directory assessments, scegli la valutazione che desideri visualizzare. Verrà aperta la pagina dei dettagli della valutazione.
3. Nella pagina dei dettagli della valutazione, puoi scegliere:
   - Scarica per scaricare il rapporto di valutazione della directory come file CSV.
   - Elimina per eliminare il rapporto di valutazione della directory.
   - Crea valutazione per creare una nuova valutazione della directory.
4. Dalla pagina dei dettagli della valutazione, puoi visualizzare le seguenti informazioni:
   a. Informazioni sulla valutazione, come l'ID della valutazione, lo stato, se è stata creata dal cliente o dal sistema e quando è stata aggiornata l'ultima volta.
   b. Dettagli AD autogestiti come nome DNS, VPC e sottoreti.
   c. AWS Systems Manager gestiva le informazioni sui nodi, come l'indirizzo IP, lo stato di valutazione e il numero di test di valutazione superati e non riusciti.
   d. Stato di valutazione per i controller di dominio. È inoltre possibile esaminare i dettagli del test di valutazione scegliendo i controller di dominio. I codici di errore vengono visualizzati nella colonna Stato per i test di valutazione non riusciti.

Eliminazione delle valutazioni delle directory

È possibile eliminare le valutazioni delle directory create dal cliente in. Console di gestione AWS Non è possibile eliminare le valutazioni avviate dal sistema che vengono create automaticamente. AWS

Per eliminare una valutazione dell'elenco clienti

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Elenchi, nella sezione Valutazioni degli elenchi, scegli la valutazione dei clienti che desideri eliminare. In alternativa, puoi selezionare la casella di controllo accanto alle valutazioni della directory che desideri eliminare e quindi, dal menu Azioni, scegliere Elimina.
3. Verrai indirizzato alla pagina dei dettagli delle valutazioni. Scegli Azioni, quindi scegli Elimina valutazione. Viene visualizzata una finestra di dialogo per la valutazione dell'eliminazione della directory. Scegli Delete (Elimina).

Risoluzione dei problemi relativi alla directory ibrida e alla valutazione delle directory

È necessaria una valutazione della directory per creare una directory ibrida. I test di valutazione vengono eseguiti su ogni controller di dominio. I test di valutazione esaminano diverse aree e danno come risultato lo stato Superato o Fallito. Se la valutazione della directory ha esito negativo, è possibile visualizzare i test di valutazione dei controller di dominio per identificare i problemi che hanno causato l'errore.

> **Important**
>
> È possibile creare una directory ibrida quando lo stato della valutazione della directory viene superato con un avviso. Si consiglia di risolvere il problema che causa l'avviso prima di creare una directory ibrida

Argomenti

- Messaggi di errore del test di valutazione
- Messaggi di avviso relativi al test di valutazione

Risoluzione dei problemi di valutazione della directory ibrida non riuscita

È possibile risolvere i problemi relativi a una valutazione delle directory non riuscita dalla pagina Directory di. Console di gestione AWS

1. Accedi a Console di gestione AWS e apri la console all' Directory Service indirizzo. https://console.aws.amazon.com/directoryservicev2/
2. Nella sezione Directory assessment, seleziona la valutazione della directory ibrida non riuscita.
3. Nella pagina Dettagli della valutazione, esamina la valutazione della directory e identifica quali test non sono riusciti.
    - I test di valutazione del controller di dominio conterranno ulteriori informazioni su quali test hanno avuto esito positivo o negativo. La colonna Status fornisce ulteriori dettagli sulla causa del fallimento del test. Per visualizzare i test di valutazione del controller di dominio, consultaVisualizzazione delle valutazioni delle directory.
4. Risolvi i problemi che causano gli errori su Active Directory autogestito o AWS Microsoft AD gestito. Per ulteriori informazioni, consulta Messaggi di errore di valutazione della directory e Messaggi di errore del test di valutazione.
5. Torna alla valutazione non riuscita nella Directory Service console. Scegli Crea valutazione nel messaggio di avviso rosso. Creazione di una directory ibrida con AD autogestitoPer ulteriori informazioni sulla creazione di una valutazione della directory, consulta.

Errori di stato della directory

Directory Service le directory possono presentare diversi stati che indicano diversi tipi di problemi. La comprensione di questi stati consente di determinare i passaggi appropriati per la risoluzione dei problemi.

Tipi di stato delle directory

Status	Description	Operazione richiesta
Attivo	La creazione della directory è stata completata correttamente e funziona normalmente.	Nessuna operazione necessaria.
Impaired (Insufficiente)	La directory è stata creata correttamente, ma il controller di dominio ha riscontrato dei problemi in seguito. Il sistema tenta il ripristino automatico.	Monitora lo stato della directory. Se il problema persiste, contatta l' AWS assistenza.
Non riuscito	La creazione della directory non è riuscita ed è irreversibile.	Eliminare la directory danneggiata e crearne una nuova.
Non utilizzabile (solo Hybrid AD)	AWS ha rilevato un problema di sicurezza e ha isolato automaticamente la directory per motivi di protezione. La directory diventa completamente inutilizzabile fino al ripristino.	Contatta immediatamente il Supporto AWS Centro di contatto. Questo stato richiede un Supporto intervento per esaminare e ripristinare la directory.

Messaggi di errore di valutazione della directory

Per creare una directory ibrida, è necessaria una valutazione della directory superata. Le valutazioni delle directory possono avere esito negativo per vari motivi.

La tabella seguente mostra i messaggi di errore di valutazione delle directory e come risolverli.

Messaggi e risoluzioni di errore di valutazione delle directory

Messaggio di errore di valutazione della directory	Risoluzione
Questa valutazione non ha superato diversi test su entrambe le istanze gestite. Analizza i test non riusciti selezionando ogni	Uno o più test di valutazione della directory non sono riusciti per il tuo AD autogestito. Consulta la Messaggi di errore del test di valutazione

Messaggio di errore di valutazione della directory	Risoluzione
istanza gestita e risolvendoli nella directory locale. Quindi, crea una nuova valutazione.	pagina per ulteriori informazioni sugli errori di test specifici e sulle relative risoluzioni.
Questa valutazione non è riuscita a causa dell'eccezione del servizio interno. Riprova creando una nuova valutazione o contatta il servizio per la risoluzione dei problemi.	Prova a creare una nuova valutazione della directory. Se continui a riscontra re questo errore, contatta Supporto.
Questa valutazione non è riuscita a causa della mancanza dell'autorizzazione a eseguire un'azione come `ec2:Creat eSecurityGroup ec2:Delet eSecurityGroup ec2:CreateNetworkI nterface ,ec2:DeleteNetworkI nterface ,ec2:DescribeSubnets , eec2:DescribeNetworkInterface .`	Per creare una valutazione dell'elen co, è Account AWS necessario il necessarioAccount AWSautorizzazioni.
Questa valutazione non è riuscita a causa della mancanza dell'autorizzazione a eseguire un'azione come `ssm:GetCo nnectionStatus ssm:GetCo mmandInvocation ,,ssm:ListC ommands ,ssm:SendCommand .`	Per creare una valutazione delle directory, sono necessari due nodi Systems Manager con il necessarioAccount AWSautorizzazioni.
Questa valutazione non è riuscita perché è stato raggiunto il limite del numero di interfacce di rete che è possibile creare. Per ulteriori informazioni, consulta la pagina relativa alle quote di Amazon VPC.	Per creare una valutazione delle directory , è necessario creare un'interfaccia di rete e gruppi di sicurezza. Esistono dei limiti al numero di risorse VPC che puoi creare, tuttavia puoi modificare alcuni di questi limiti. Per ulteriori informazioni, consulta la pagina relativa alle quote di Amazon VPC.

Messaggio di errore di valutazione della directory	Risoluzione
Questa valutazione non è riuscita perché è stato raggiunto il limite del numero di gruppi di sicurezza che è possibile creare o assegnare a un'istanza. Per ulteriori informazioni, consulta la pagina relativa alle quote di Amazon VPC.	Per creare una valutazione delle directory , è necessario creare un'interfaccia di rete e gruppi di sicurezza. Esistono dei limiti al numero di risorse VPC che puoi creare, tuttavia puoi modificare alcuni di questi limiti. Per ulteriori informazioni, consulta la pagina relativa alle quote di Amazon VPC.
Questa valutazione non è riuscita. Impossibile connettersi alle istanze del cliente da AWS Systems Manager.	Per creare una valutazione della directory, sono necessari due AWS Systems Manager nodi con uno stato di connessione. Vedi Risoluzione dei problemi dell'agente SSM.
Questa valutazione non ha superato diversi test critici. Analizza i test non riusciti seleziona ndo ogni istanza gestita e risolvili nella directory locale. Quindi, crea una nuova valutazione.	Uno o più test di valutazione della directory non sono riusciti per il tuo AD autogesti to. Consulta il Messaggi di errore del test di valutazione per ulteriori informazioni.

Messaggi di errore del test di valutazione

La tabella seguente descrive i messaggi di errore che possono verificarsi durante i test di valutazione. Questi errori indicano problemi di blocco che devono essere risolti prima di procedere con la configurazione della directory ibrida.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Active Directory ServicesT est	`testActiv eDirector yServices`	`AD_CRITIC AL_SERVIC ES_NOT_RU NNING`	`Critical AD Services: [service_ list] not running on hostname.`	Si verifica se AD i servizi richiesti non sono in esecuzione nell'AD autogesti to.	ADI servizi specifici richiesti devono essere in esecuzione nell'AD autogesti to. Per ulteriori informazioni,

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
					consulta Servizi Active Directory richiesti.
Active Directory ServicesTest	`testActiveDirectoryServices`	`DOMAIN_CONTROLLER_NOT_FOUND`	`No domain controllers found for testActiveDirectoryServices.`	`Occurs if your self-managed AD domain controllers could not be both detected and queried during AD service validation.`	Assicurati che i controller di dominio AD autogestiti siano operativi e raggiungibili. Verifica la connettività e la DNS risoluzione di rete per i controller di dominio AD autogestiti.
ADTest della politica sulle password	`testPasswordPolicies`	`PASSWORD_POLICY_VIOLATIONS`	*`ErrorMessage`*	Si verifica se la politica di gestione automatica delle password di AD non soddisfa i requisiti di AWS Managed Microsoft AD.	La politica di gestione automatica delle password di AD deve soddisfare i requisiti relativi alle password di AWS Managed Microsoft AD. Per ulteriori informazioni, vedere Understanding AWS Managed Microsoft AD Password Policy.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test di esistenza degli utenti amministratori	`testAwsAdminUserExist`	`ADMINISTRATOR_ACCOUNT_MISSING`	`AWS Admin user not found or invalid.`	Si verifica se l'utente amministratore della directory ibrida non esiste nel file AWS Reserved OU on your AD autogestito.	Assicurati che l'utente amministratore della directory ibrida esista nella cartella AWS OU Riservata del tuo AD autogestito. Se l'utente non è presente, verifica che l'account sia stato creato correttamente durante il processo di configurazione della directory ibrida. Aggiornamento di una directory ibrida. Se lo stato della directory ibrida non è utilizzabile, contatta. Supporto

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test per utenti amministrativi SPN	`testNoSpnOnAwsAdminAccount`	`SPN_FOUND_ON_AWS_ADMIN`	`Found` *`spnCount`* `Service Principal Names (SPNs) set on AWS admin user` *`Username`*`. Please remove all SPNs from this account.`	Si verifica se l'utente amministratore della directory ibrida ne ha SPNs configurato uno sull'AD autogestito.	Rimuove tutti i Service Principal Names (SPNs) dall'account utente dell'amministratore della directory AWS ibrida. L'utente amministratore della directory ibrida non deve averne SPNs configurato nessuno perché può interferire con l'autenticazione della directory ibrida.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test del controller di dominio non FSMO del proprietario	`testAwsDcNotFsmoOwner`	`AWS_DC_HOLDS_FSMO_ROLE`	`AWS Domain Controller owns FSMO roles: rolesList . Please remove these roles.`	Si verifica se sono stati trasferiti FSMO ruoli (PDC EmulatorRID Master, oInfrastructure Master) dall'AD autogestito al controller di dominio della directory ibrida.	Trasferisci nuovamente tutti i FSMO ruoli (PDC Emulator, RID Master,Infrastructure Master) ai controller di dominio AD autogestiti prima di procedere. Per ulteriori informazioni, consulta la Microsoft documentazione sul trasferimento dei ruoli. FSMO
AWS Test di appartenenza a un gruppo riservato	`testValidateAwsReservedGroupMembership`	`AWS_RESERVED_OU_NOT_FOUND`	`AWS Reserved OU not found.`	Si verifica se l'opzione AWS OU Riservata sul tuo AD autogestito non esiste.	L'elemento AWS Riservato OU deve esistere nel tuo AD autogestito per convalidare l'appartenenza al gruppo. Contattare Supporto.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test di iscrizione al gruppo riservato	`testValidateAwsReservedGroupMembership`	`GROUP_MEMBERSHIP_MISMATCH`	`AWS Reserved OU Group [GroupNameA]: Missing User(s) [ Object1 ], [ Object2] and Extra user(s) [ Object3 ].`	Si verifica se i gruppi presenti nell' AWS area OU Riservata di AD autogestita contengono utenti non autorizzati.	Rimuovi tutti gli utenti non autorizzati dai OU gruppi AWS riservati sul tuo AD autogestito.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test riservato OU ACLs	`testReservedOuAclsPermissions`	`RESERVED_OU_NON_COMPLIANT_AC`	`AWS Reserved OU ACLs permissions are invalid.`	Si verifica se le impostazioni AWS riservate OU ACLs su AD autogestite non impongono autorizzazioni di sola lettura per le entità non gestite AWS e non impediscono l'accesso non autorizzato alle risorse gestite. AWS	Rivedi e correggi le autorizzazioni relative all'area Riservata del tuo AD autogestito. AWS OU ACLs Assicurati che le persone non AWS giuridiche dispongano solo delle autorizzazioni di lettura (`ListChildren` ,,,`ReadProperty` , `ListObject` `ReadControl` `GenericRead` ,`Synchronize`) e rimuovi le autorizzazioni eccessive.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test delle associazioni riservate OU GPO	`testReservedOuGPOs`	`AWS_RESERVED_OU_NON_RESERVED_GPO_FOUND`	`Found non-AWS GPOs attached to the AWS Reserved OU: AWS Reserved OU (`*`count`*` unauthorized). Allowed GPOs: [`*`allowedAwsGpos`*` ]. Domain Controllers OU (`*`count`*` unauthorized). Allowed GPOs: [`*`allowedDcGpos`*` ]. Please, remove extra GPOs from the AWS Reserved OU.`	Si verifica se i controller AWS riservati OU e di dominio dell'AD autogestito sono collegati a siti non autorizzati. GPOs	(A questi possono essere collegati solo gli oggetti di policy di gruppo AWS gestiti (GPOs). OUs Rimuovi tutti i GPOs collegamenti non autorizzati ai controller AWS OU riservati OU e di dominio dal tuo AD autogestito.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test delle risorse riservate OU	`testAwsReservedOUResources`	`AWS_RESERVED_OU_NOT_FOUND`	`The AWS Reserved OU does not exist. Please contact AWS Support.`	Si verifica se l' AWS elemento Riservato OU non esiste nell'AD autogestito, necessario per la funzionalità della directory AWS Managed Microsoft AD.	Il file AWS Reserved OU deve essere creato automaticamente durante la configurazione della directory ibrida e non deve essere eliminato. Se l'errore persiste, contatta Supporto.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test OU delle risorse riservate	`testAwsReservedOUResources`	`AWS_RESERVED_OU_RESOURCES_MISMATCH`	`The following required resources are missing from AWS Reserved OU - Objects: missing objects, GPOs: missing GPOs. The following resources should not exist but were found in AWS Reserved OU: Objects: unexpected objects , GPOs: unexpected GPOs`	Si verifica se il AWS Reserved OU creato nell'AD autogestito non contiene gli oggetti richiesti e GPOs consente il corretto funzionamento della directory ibrida.	Assicurati che nessuno modifichi il Reserved. AWS OU Deve contenere le risorse AWS gestite richieste . Rimuovi eventuali oggetti non autorizzati oppure GPOs contatta Supportose mancano le risorse necessarie.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
AWS Test riservato OU	`testCleanAwsReservedOU`	`AWS_RESERVED_RESOURCES_STILL_EXIST`	`AWS Reserved OU or AWS Reserved GPO still exists, please delete.`	Si verifica se esistono ancora risorse AWS riservate presenti nell'AD autogestito da una precedente configurazione di directory ibrida.	Elimina la directory ibrida esistente con errore dalla console. Quindi elimina tutte le informazioni AWS riservate OU e correlate GPOs dal tuo AD autogestito prima di procedere.
BridgeheadTest del contesto di denominazione	`testBridgeheadNamingContext`	`NAMING_CONTEXT_INCONSISTENT`	*`failureDetails`*	Si verifica se la replica AD autogestita tra siti utilizzati non Bridgehead funziona come previsto. Può verificarsi anche se i contesti di denominazione non sono sincronizzati tra i siti.	Il bridgehead sito AD autogestito deve avere successo. Puoi diagnosticare ulteriormente con:. `repadmin /bridgeheads /verbose` Risolvi i problemi di tale valutazione prima di continuare.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Child Domain Test	`testChildDomain`	`CHILD_DOMAIN_NOT_SUPPORTED`	`Child Domains are not supported for Hybrid Directory.`	Si verifica se la foresta AD autogestita contiene domini figlio, che non sono supportati con le directory gestite di AWS Microsoft AD.	AWS Le directory Microsoft AD gestite non supportano i domini secondari . È necessario utilizzare una foresta a dominio singolo per l'AD autogestito. Per ulteriori informazioni, consulta Microsoft Active Directoryrequisiti del dominio.
DcDiagTest	`testDcDiag`	`DCDIAG_TEST_FAILED`	`DCDiag test failed due to issue from [formatedFailedTests ].`	Si verifica se un Microsoft DCDiag test dell'AD autogestito ha esito negativo.	AWS viene utilizzato DCDiag per testare l'AD autogestito. In caso di errori, non è possibile creare una directory ibrida. Per ulteriori informazioni, consulta Microsoftla documentazione.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
DNSIP Match Test	`testDnsIpMatch`	`DNS_IP_MISMATCH`	`DNS IP address does not match expected IP addresses.`	Si verifica se gli indirizzi DNS IP forniti dell'AD autogestito non corrispondono agli indirizzi DNS IP dei controller di dominio AD autogestiti abilitati con. AWS Systems Manager	Fornisci gli indirizzi IP correttiDNS.
DNSTest di corrispondenza dei nomi	`testDnsNameMatch`	`DOMAIN_DNS_NAME_MISMATCH`	`DNS name does not match expected domain name.`	Si verifica se il DNS nome fornito per l'AD autogestito non corrisponde al DNS nome sui controller di dominio AD autogestiti abilitati con. AWS Systems Manager	Fornisci il nome corretto. DNS

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
DNSTest dei record	`testDnsRecords`	`DNS_RECORD_MISSING`	`Unable to resolve the following DNS queries: [`*`missingRecordsString`*` ]`.	Si verifica se Windows DNS i record non sono impostati per il tipo A NSSOA,, SRV e possono essere interrogati.	I DNS record per Address (A), Namespace (NS), State of Authority (SOA) e Service Record (SRV) devono essere impostati e possono essere interrogati. Per ulteriori informazioni, consulta la documentazione. Microsoft

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Test del livello funzionale di Domain Forest	`testDomainForestFunctionalLevel`	`UNSUPPORTED_FUNCTIONAL_LEVEL`	`Detected unsupported domain functional level: DomainFunctionalLevel , we require minimum of MinimumDomainMode . Detected unsupported forest functional level: ForestFunctionalLevel , we require minimum of MinimumForestMode .`	Si verifica se i livelli di funzionalità del dominio AD e della foresta autogestiti non soddisfano i requisiti minimi.	L'AD autogestito deve utilizzare il nostro Windows 2012 R2 livello 2016 funzionale. Per ulteriori informazioni, consulta la Microsoft documentazione.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Domain Health Tests	`testOnPremDcNumber`	`DC_NUMBER_BELOW_LIMIT`	`On-Prem DC count is lower than required number. DC count is` *`NumberOfDc`* `, AWS required number is` *`DcMinimum`* `.`	Si verifica se l'AD autogestito non dispone del numero minimo richiesto di controller di dominio.	Assicurati che il tuo AD autogestito abbia almeno due controller di dominio abilitati con. AWS Systems Manager Per ulteriori informazioni, consulta Microsoft Active Directoryrequisiti del dominio.
Test del dominio esistente	`testDomainAlreadyJoined`	`DOMAIN_ALREADY_JOINED`	`Instance is already joined to a domain.`	Si verifica se il dominio AD autogestito è già aggiunto a una directory ibrida esistente.	Il dominio AD autogestito è già aggiunto a una directory ibrida esistente. Ogni dominio AD autogestito unito a una directory ibrida deve essere unico. Crea un nuovo dominio AD autogestito o rimuovilo dalla configurazione di directory ibrida a cui è aggiunto.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
FSMOTest di connettività	`testFsmoConnectivity`	`FSMO_ROLE_HOLDER_NOT_ROUTABLE`	`(PDCEmulator Ip: 1.1.1.1, RIDMaster Ip: 1.1.1.1) is not in routable ranges: [2.2.0.0/16, 3.3.0.0/16, 4.4.0.0/16, 5.5.0.0/16, 6.6.0.0/16].`	Si verifica se FSMO i ruoliPDC Emulator, and/or RID Master IPs nell'AD autogestito non sono instradabili.	Il controller di dominio primario (PDC) deve essere instradabile in qualsiasi momento. In particolare, la fine RID Master IPs del PDC Emulator tuo AD autogestito. Per ulteriori informazioni, consulta Microsoft Active Directoryrequisiti del dominio.
FSMOTest di connettività	`testFsmoConnectivity`	`FSMO_ROLE_MISSING`	`FSMO role(s): [`*`missingRolesString`*` ] missing or DNS Record not found.`	Si verifica se i controller di dominio AD autogestiti non riescono ad accedere ai ruoli dell'utenteFSMO.	Il ruolo Flexible Single Master Operation (FSMO) nell'AD autogestito deve essere collegato ai controller di dominio AD autogestiti. Per ulteriori informazioni, consulta la documentazione. Microsoft

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Test di conflitto IP	`testIpConflict`	`IP_RANGE_CONFLICT`	`Conflicting IP address detected: ipOverlaps`	Si verifica se gli intervalli IP AD autogestiti si sovrappongono agli intervalli AWS riservati.	L'AD autogestito non può utilizzare un intervallo di indirizzi IP che si sovrappone agli intervalli IP riservati . AWS Per ulteriori informazioni, consulta Microsoft Active Directoryrequisiti del dominio.
KerberosTest	`testKerberos`	`KERBEROS_AUTHENTICATION_FAILED`	`Unable to get kerberos TGT.`	Si verifica se non Kerberos è configurato correttamente e in uso.	Kerberosdeve essere abilitato sul tuo AD autogestito. Per ulteriori informazioni, consulta la documentazione di Microsoft.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
LDAPTest di connettività	`testLdapConnectivity`	`LDAP_TEST_FAILED`	`Unable to query LDAP with rootDSE call.`	Si verifica se LDAP non funziona.	Lightweight Directory Access Protocol (LDAP) deve essere abilitato e funzionante su un AD autogestito. Per ulteriori informazioni, consulta la Microsoft documentazione.
Controller di dominio non di sola lettura per FSMO test	`testNotRodcForFsmo`	`FSMO_FOUND_ON_RODC`	`FSMO Role Found on RODC`	Si verifica se il FSMO ruolo di controller di dominio AD autogestito èRODC.	Il controller di dominio per l'AD autogestito non deve utilizzare un ruolo Flexible Single Master Operation (RODC) di tipo Controller di dominio in sola lettura (). FSMO Per ulteriori informazioni, consulta la documentazione. Microsoft

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Test di replica della password del controller di dominio in sola lettura	`testRodcPasswordReplication`	`RODC_REPLICATE_ADMIN_PASSWORD`	`ReadOnly Domain Controller password replication is not explicitly denied for following groups: [`*`missingGroupsString`*` ].`	Si verifica se RODC dispone dell'autorizzazione a replicare le password degli amministratori.	All'RODCAD autogestito deve essere esplicitamente negata l'autorizzazione a replicare le password di amministratore. Per ulteriori informazioni, consulta la documentazione. Microsoft
Test del controller di dominio in sola lettura	`testIsDCRodc`	`DC_READONLY_MODE`	`Provided Domain Controller is set to Read-Only mode.`	Si verifica se i controller di dominio AD autogestiti sono in ReadOnlyDC modalità.	I tuoi AD autogestiti devono essere controller di dominio di lettura e scrittura . Per ulteriori informazioni sui tipi di controller di dominio, consulta la documentazione. Microsoft

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Test di connettività delle porte remote	`testPortConnectivity`	`PORT_TEST_FAILED`	`Connection to` *`TargetDestination`* `failed for TCP ports [`*`failed TCP ports`*`]. UDP ports [`*`failed UDP ports`*`].`	Si verifica se le porte richieste sulla AWS sottorete e il controller di dominio AD autogestito non sono aperti.	Assicurati che tutte le porte richieste siano aperte tra la AWS sottorete e l'AD autogestito. Per ulteriori informazioni, consulta Requisiti delle porte di rete.
Test di replica	`testReplication`	`REPLICATION_FAILED`	`Replication failed for [`*`failedDSAsString`*` ].`	Si verifica se la replica dei controller di dominio AD autogestiti non è riuscita.	Lo stato di replica dei controller di dominio AD autogestiti deve avere esito positivo. Per ulteriori informazioni, consulta la documentazione. Microsoft
SMBV1Test	`testSMBV1`	`INSECURE_SETTING_SMB`	`SMBv1 is enabled on the system.`	Si verifica se AD autogestito viene attualmente utilizzato SMBv1 per l'autenticazione.	SMBv1è noto per non essere sicuro e deve essere disabilitato nell'AD autogestito. Per ulteriori informazioni, consulta Microsoft la documentazione.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
SSMTest delle autorizzazioni utente	`testSSMUserPermissions`	`INSUFFICIENT_PERMISSIONS`	`Systems Manager user does not have required elevated privileges.`	Si verifica se Windows l'utente utilizzato da non SSM dispone di privilegi sufficienti.	Avrai bisogno delle autorizzazioni di Windows amministratore per gli agenti di AWS System Manager (SSM) sul tuo AD autogestito. Per ulteriori informazioni, consulta Account AWSautorizzazioni.
SysvolTest di replica	`testSysvolReplication`	`DFSR_FAILURE_DETECTED`	`Failed DFSR event logs:` *`failedLogsString`* `.`	Si verifica se l'AD autogestito non utilizza il metodo di sysvol replica corretto (DFSR) e se uno di essi DCs non è riuscito durante l'DFSREvento di replica.	Il metodo di sysvol replica AD autogestito () DFSR deve avere esito positivo. Per ulteriori informazioni, consulta Microsoft la documentazione.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
GPOTest di alto livello	`testTopLevelEnforcedGPO`	`TOP_LEVEL_ENFORCED_GPO_FOUND`	`GroupPolicy cannot be set to Enforced at the Domain Root, Found GPOs: [`*`GposEnforced`*` ] set as Enforced.`	Si verifica se l'AD autogestito ha Top Level GPOs impostato su Enforced.	Assicurati che l'oggetto dei criteri di gruppo di primo livello del dominio AD autogestito (GPO) non sia impostato su Enforced. Per ulteriori informazioni, consulta Microsoft la documentazione.
Test dei tipi di fiducia	`testTrustTypes`	`INVALID_TRUST_TYPE`	`Invalid trust types detected: [`*`InvalidTrustString`*` ], only Uplevel (Microsoft AD) is currently supported.`	Si verifica se l'AD autogestito include tipi di trust non supportati.	Uplevelè l'unico tipo di trust supportato dalla directory ibrida. Il tuo AD autogestito non può avere i seguenti tipi di trust:DCE ,MIT,Down level. Per ulteriori informazioni sui tipi di trust, consulta Microsoftla documentazione.

Nome del test	Nome breve	Codice di errore	Messaggio di errore	Description	Risoluzione
Test valido del controller di dominio	`testValidDC`	`COMPUTER_NOT_DC`	`Provided instance is not a domain controller.`	Si verifica se le istanze AD autogestite fornite non sono controller di dominio o se fanno già parte di un'altra directory ibrida.	Fornisci controller di dominio AD autogestiti esclusivi per questa directory ibrida. Riprova con una nuova directory. Assicurati di aver eliminato la directory ibrida in cui si è verificato l'errore e tutte le cartelle presenti AWS OU nell'AD autogestito.

Messaggi di avviso relativi al test di valutazione

La tabella seguente descrive i messaggi di avviso che possono verificarsi durante i test di valutazione. Questi avvisi rappresentano consigli per una configurazione ottimale ma non impediscono la configurazione della directory ibrida.

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
Domain Health Tests	`testDisabledStaleUserNumber`	`STALE_USERS_FOUND`	*`StaleUserCount`* `users were found to be stale, they have not logged in for`	Si verifica se nel tuo AD autogestito sono presenti account utente che non hanno effettuato l'accesso	Pulisci gli account utente obsoleti.

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
			StaleThresholdInDays days.	per un periodo prolungato e che possono essere considerati obsoleti o inattivi.	
Test Time Source del controller di dominio	testDCTimeSource	DC_BAD_TIMESOURCE	Time sources not properly configured for PDC, should using an authoritative source. Time sources not properly configured for *dcHostName* , should using PDC as source	Si verifica se l'AD autogestito ha la corretta configurazione dell'origine temporale e se non vi è una grande asimmetria temporale rispetto a un' AWS origine temporale.	Il server orario del controller di dominio principale (PDC) è indirizzato a. 169.254.169.123 I controller di dominio non primari devono essere indicati PDC come origine. Per ulteriori informazioni, consulta Keeping time with. Amazon Time Sync Service

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
Test dello spazio libero	`testFreeSpace`	`DISK_SPACE_EXCEEDED`	`Supported service max capacity of 7 GB exceeded; SysVol + NTDS is currently using: 24 GB)`	Si verifica se AD Combined autogestito NTDS e Sysvol l'utilizzo superano la quota supportata.	L'AD autogestito deve disporre di 24 GB di spazio su disco per le directory ibride.

FSMO RolesTest	`testFSMORoles`	`FSMO_ROLE_TEST_FAILED`	`PDC Emulator (dc1.example.com ) is not among the provided domain controllers.`
			
			`RID Master (dc1.example.com ) is not among the provided domain controllers.`
				Si verifica se i ruoli FSMO (PDC Emulator e RID Master) non sono tra i due controller di dominio forniti quando si crea una directory ibrida.	La directory ibrida deve avere entrambi i ruoli FSMO (PDC Emulator e RID Master) tra i due controller di dominio forniti quando si crea una directory ibrida. Per ulteriori informazioni, consulta Come visualizzare e trasferire i ruoli. FSMO

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
SSPTest del canale S.	`testSchannelSSP`	`TLS_1_2_NOT_ENABLED`	`Disabled protocol` *`DisabledProtocol`* `is still enabled.`	Si verifica se un AD autogestito non utilizza TLS1.2 la AES256 crittografia.	L'AD autogestito deve utilizzare TLS 1.2 e AES256 per le directory ibride.
Test di danneggiamento del disco	`testDiskCorruption`	`DISK_CORRUPT`	`Disk corruption detected on` *`Drive`*`.`	Si verifica in caso di danneggiamento del disco nell'AD autogestito.	I dischi AD autogestiti non devono essere danneggiati.
Test delle specifiche del controller di dominio	`testDcSpecs`	`INSUFFICIENT_RESOURCES`	*`numAvailableCores`* `cores detected when` *`requiredCores`* `cores recommended.` *`gbAvailableRam`* `GB ram detected when` *`requiredRam`* `GB recommended.`	Si verifica se i controller di dominio AD autogestiti non soddisfano le specifiche richieste.	I controller di dominio AD autogestiti devono avere almeno 7 GB di RAM e 2 core CPU per la directory ibrida.

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
Test del plug-in a livello di server Dll	`testServerLevelPluginDll`	`SERVER_LEVEL_PLUGIN_DLL_IS_SET`	`ServerLevelPluginDll registry configuration is not permitted.`	Si verifica se ServerLevelPluginDll è impostato sui controller di dominio AD autogestiti.	I controller di dominio AD autogestiti non avrebbero dovuto essere configurati. ServerLevelPluginDll
Consenti NT4 Crypto Test	`testAllowNT4Crypto`	`NT4_CRYPTO_NOT_ALLOWED`	`Registry key AllowNt4Crypto is not allowed.`	Si verifica se AD autogestito consente la NT4 crittografia.	L'AD autogestito non deve utilizzare la crittografia. NT4 Per ulteriori informazioni, consultare la documentazione di Microsoft.
Test per utenti amministratori orfani	`testOrphanedAdminUsers`	`ORPHANED_ADMIN_USER_FOUND`	*`OrphanedUsersCount`* `Orphaned Admin Users Found: [`*`OrphanedUserNames`*` ].`	Si verifica se esistono utenti amministratori orfani nel tuo AD autogestito.	Rimuovi gli utenti orfani dal tuo AD autogestito prima di continuare.

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
Test del conteggio degli utenti privilegiati	`testPrivilegedUserCount`	`DOMAIN_ADMIN_COUNT_EXCEEDED`	`Number of Domain Admins (`*`daCount`*`) exceeded allowance of (`*`allowedDomainAdminCount`*` ).`	Si verifica se il conteggio totale degli amministratori integrati, degli amministratori di dominio e degli amministratori aziendali del sistema AD a autogestito è superiore a 5.	L'ambiente AD autogestito non dovrebbe avere più account privilegiati. È necessario rimuovere un numero eccessivo di account di amministrazione prima di continuare.
Test del conteggio degli utenti privilegiati	`testPrivilegedUserCount`	`ENTERPRISE_ADMIN_COUNT_EXCEEDED`	`Number of Enterprise Admins (`*`eaCount`*`) exceeded allowance of (`*`allowedEnterpriseAdminCount`*` ).`	Si verifica se il conteggio totale degli amministratori integrati, degli amministratori di dominio e degli amministratori aziendali del sistema AD a autogestito è superiore a 5.	L'ambiente AD autogestito non dovrebbe avere più account privilegiati. È necessario rimuovere un numero eccessivo di account di amministrazione prima di continuare.

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
Test del conteggio degli utenti privilegiati	`testPrivilegedUserCount`	`BUILTIN_ADMIN_COUNT_EXCEEDED`	`Number of Built-in Admins (baCount) exceeded allowance of (allowedAdminCount ).`	Si verifica se il conteggio totale degli amministratori integrati, degli amministratori di dominio e degli amministratori aziendali del sistema AD a autogestito è superiore a 5.	L'ambiente AD autogestito non dovrebbe avere più account privilegiati. È necessario rimuovere un numero eccessivo di account di amministrazione prima di continuare.
NTLMTest	`testNTLM`	`INSECURE_SETTING_NTLM`	`NTLMv1 is enabled.`	Si verifica se NTLMv1 è abilitata l'autenticazione sul tuo AD autogestito.	NT LAN Managerla versione 1 (NTLMv1) presenta vulnerabilità di sicurezza note e non deve essere utilizzata. NTLMv1Disabilitalo sul tuo AD autogestito. Per ulteriori informazioni, consulta la Microsoft documentazione.

Nome del test	Nome breve	Codice di avviso	Messaggio di avviso	Description	Risoluzione
Tombstone Lifetime Test	`testTombstoneLifetime`	`TOMBSTONE_LIFETIME_ABOVE_LIMIT`	`Tombstone Lifetime is too long. DC Tombstone Lifetime is` *`Tombstone LifeTime`* `, AWS suggested number is` *`Tombstone Maximum`* `days.`	Si verifica se la durata di vita di Tombstone sul tuo AD autogestito è superiore a 180 giorni.	La durata di Tombstone è il numero di giorni prima che un oggetto eliminato venga rimosso da. AD La durata di vita di Tombstone per il tuo AD autogestito dovrebbe essere pari o inferiore a 180 giorni. Per ulteriori informazioni, consulta la documentazione. Microsoft

Guida introduttiva a AWS Managed Microsoft AD

AWS Managed Microsoft AD crea un ambiente completamente gestito, Microsoft Active Directory integrato Cloud AWS e basato su Windows Server 2019 e opera ai livelli funzionali Forest e Domain di 2012 R2. Quando crei una directory con AWS Managed Microsoft AD, Directory Service crea due controller di dominio e aggiunge il servizio DNS per tuo conto. I controller di dominio vengono creati in diverse sottoreti in un Amazon VPC. Questa ridondanza aiuta a garantire che la directory rimanga accessibile anche in caso di errore. Se hai bisogno di più controller dei domini, puoi aggiungerli più tardi. Per ulteriori informazioni, consulta Implementazione di controller di dominio aggiuntivi per Managed AWS Microsoft AD.

Per una demo e una panoramica di AWS Managed Microsoft AD, guarda il YouTube video seguente.

AWS Demo e panoramica di Microsoft AD gestita

Argomenti

Prerequisiti per la creazione di un AWS Managed Microsoft AD

Per creare un Microsoft AD Active Directory AWS gestito, è necessario un Amazon VPC con quanto segue:

- Almeno due sottoreti. Ciascuna sottorete deve trovarsi in una zona di disponibilità diversa e deve appartenere allo stesso tipo di rete.

  Puoi usarlo IPv6 per il tuo VPC. Per ulteriori informazioni, consulta il IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
- Il VPC deve disporre di una tenancy hardware predefinita.
- Non è possibile creare un AWS Managed Microsoft AD in un VPC utilizzando gli indirizzi nello spazio degli indirizzi 198.18.0.0/15.

Se è necessario integrare il dominio Microsoft AD AWS gestito con un dominio Active Directory locale esistente, è necessario che i livelli di funzionalità Forest e Domain per il dominio locale siano impostati su Windows Server 2003 o versioni successive.

Directory Service utilizza una struttura a due VPC. Le EC2 istanze che compongono la directory vengono eseguite all'esterno dell' AWS account e sono gestite da. AWS Hanno due schede di rete, `ETH0` e `ETH1`. `ETH0` è la scheda di gestione ed è al di fuori del tuo account. `ETH1` viene creata all'interno dell'account.

L'intervallo IP di gestione della rete ETH0 della directory è 198.18.0.0/15.

Per un tutorial su come creare l' AWS ambiente e AWS Managed Microsoft AD, vediAWS Tutorial gestiti per laboratori di test Microsoft AD.

AWS IAM Identity Center prerequisiti

Se prevedi di utilizzare IAM Identity Center con AWS Managed Microsoft AD, devi assicurarti che quanto segue sia vero:

- La directory AWS Managed Microsoft AD è configurata nell'account di gestione dell' AWS organizzazione.
- L'istanza di IAM Identity Center si trova nella stessa regione in cui è configurata la directory AWS Managed Microsoft AD.

Per ulteriori informazioni, consulta i prerequisiti di IAM Identity Center nella Guida per l'AWS IAM Identity Center utente.

Prerequisiti dell'autenticazione a più fattori

Per supportare l'autenticazione a più fattori con la directory AWS Managed Microsoft AD, è necessario configurare il server RADIUS (Remote Authentication Dial-In User Service) locale o basato sul cloud nel modo seguente in modo che possa accettare le richieste dalla directory Managed AWS Microsoft AD in. AWS

1. Sul tuo server RADIUS, crea due client RADIUS per rappresentare entrambi i controller di dominio Microsoft AD AWS gestiti (DCs) in AWS. È necessario configurare entrambi i client utilizzando i seguenti parametri comuni (il tuo server RADIUS può variare):
   - Indirizzo (DNS o IP): è l'indirizzo DNS di uno dei Managed AWS Microsoft AD. DCs Entrambi gli indirizzi DNS sono disponibili nella AWS Directory Service Console nella pagina Dettagli della directory Microsoft AD AWS gestita in cui si prevede di utilizzare MFA. Gli indirizzi DNS visualizzati rappresentano gli indirizzi IP di entrambi i AWS Managed Microsoft AD DCs utilizzati da AWS.

     > **Note**
     >
     > Se il tuo server RADIUS supporta gli indirizzi DNS, è necessario creare solo una configurazione del client RADIUS. Altrimenti, è necessario creare una configurazione client RADIUS per ogni AWS Managed Microsoft AD DC.

   - Numero di porta: configura il numero di porta per la quale il server RADIUS accetta le connessioni ai client RADIUS. La porta RADIUS standard è 1812.

- Segreto condiviso: digita o genera un segreto condiviso che il server RADIUS utilizzerà per connettersi ai client RADIUS.
- Protocollo: potrebbe essere necessario configurare il protocollo di autenticazione tra AWS Managed Microsoft AD DCs e il server RADIUS. I protocolli supportati sono PAP, CHAP MS-CHAPv1 e MS-. CHAPv2 MS- CHAPv2 è consigliato perché offre il livello di sicurezza più elevato tra le tre opzioni.
- Nome dell'applicazione: questa operazione potrebbe essere facoltativa in alcuni server RADIUS e in genere identifica l'applicazione nei messaggi o nei report.

2. Configurate la rete esistente per consentire il traffico in entrata dai client RADIUS (indirizzi DCs DNS Microsoft AD AWS gestiti, vedere il passaggio 1) alla porta del server RADIUS.
3. Aggiungi una regola al gruppo di EC2 sicurezza Amazon nel tuo dominio Microsoft AD AWS gestito che consenta il traffico in entrata dall'indirizzo DNS e dal numero di porta del server RADIUS definiti in precedenza. Per ulteriori informazioni, consulta Aggiungere regole a un gruppo di sicurezza nella Guida per l'EC2 utente.

Per ulteriori informazioni sull'utilizzo di AWS Managed Microsoft AD con MFA, vedere. Abilitazione dell'autenticazione a più fattori per AWS Managed Microsoft AD

Creazione del tuo AWS Managed Microsoft AD

Per creare un nuovo AWS Managed Microsoft AD Active Directory, effettuare le seguenti operazioni. Prima di iniziare la procedura, assicurati di soddisfare i prerequisiti illustrati in Prerequisiti per la creazione di un AWS Managed Microsoft AD.

Per creare un AWS Managed Microsoft AD

1. Nel riquadro di navigazione della Console AWS Directory Service, scegli Directory, quindi seleziona Configura directory.
2. Nella pagina Seleziona il tipo di directory, scegli Microsoft AD gestito da AWS , quindi seleziona Successivo.
3. Nella pagina Enter directory information (Inserisci le informazioni sulla directory) inserisci le seguenti informazioni:

Edizione

Scegli tra la Standard Edition o l'Enterprise Edition di AWS Managed Microsoft AD. Per ulteriori informazioni sulle edizioni, consulta Servizio di directory AWS per Microsoft Active Directory.

Nome DNS directory

Il nome completo della directory, ad esempio `corp.example.com`.

> **Note**
>
> Se prevedi di utilizzare Amazon Route 53 for DNS, il nome di dominio del tuo AWS Managed Microsoft AD deve essere diverso dal nome di dominio Route 53. Possono verificarsi problemi di risoluzione DNS se Route 53 e AWS Managed Microsoft AD condividono lo stesso nome di dominio.

Nome NetBIOS della directory

Nome breve per la directory, ad esempio `CORP`.

Descrizione della directory

Descrizione opzionale della directory. Questa descrizione può essere modificata dopo aver creato AWS Managed Microsoft AD.

Password amministratore

La password dell'amministratore della directory. Con il processo di creazione della directory viene generato un account amministratore con nome utente `Admin` e questa password. Puoi modificare la password dell'amministratore dopo aver creato il tuo AWS Managed Microsoft AD.

Nella password non può essere inclusa la parola "admin".

La password dell'amministratore della directory applica la distinzione tra maiuscole e minuscole e deve contenere tra 8 e 64 caratteri. Deve anche contenere un carattere di almeno tre delle seguenti quattro categorie:

- Lettere minuscole (a-z)

- Lettere maiuscole (A-Z)
- Numeri (0-9)
- Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Conferma la password

Digitare di nuovo la password dell'amministratore.

(Facoltativo) Gestione di utenti e gruppi

Per abilitare AWS la gestione di utenti e gruppi di Microsoft AD gestita da Console di gestione AWS, selezionare Gestisci la gestione di utenti e gruppi in Console di gestione AWS. Per ulteriori informazioni su come utilizzare la gestione di utenti e gruppi, vederethe section called "Gestisci utenti e gruppi con la console, la CLI o PowerShell".

4. Nella pagina Choose VPC and subnets (Scegli VPC e sottoreti) fornire le seguenti informazioni, quindi selezionare Next (Successivo).

   VPC

   Selezionare il VPC per la directory.

   Tipo di rete

   Il sistema di indirizzamento IP (Internet Protocol) associato al VPC e alle sottoreti.

   Seleziona il blocco CIDR associato al tuo VPC esistente. Le risorse nella sottorete possono essere configurate per utilizzare IPv4 solo, IPv6 solo o entrambi IPv4 e IPv6 (dual-stack). Per ulteriori informazioni, consulta la sezione Confronta IPv4 e IPv6 nella Amazon Virtual Private Cloud User Guide.

   Sottoreti

   Seleziona le sottoreti per i controller di dominio. Le due sottoreti devono trovarsi in diverse zone di disponibilità.

5. Nella pagina Review & create (Rivedi e crea), esaminare le informazioni relative alla directory ed eseguire eventuali modifiche. Quando le informazioni sono corrette, scegli Create Directory (Crea directory). La creazione di una directory richiede dai 20 ai 40 minuti. Una volta creato, il valore Status cambia in Active (Attivo).

Per ulteriori informazioni su ciò che viene creato con AWS Managed Microsoft AD, consulta quanto segue:

- Cosa viene creato con AWS Managed Microsoft AD
- AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo

Articoli del blog AWS sulla sicurezza correlati

- Come delegare l'amministrazione della directory AWS Managed Microsoft AD agli utenti di Active Directory locali
- Come configurare politiche di password ancora più rigorose per soddisfare gli standard di sicurezza utilizzando Directory ServiceAWS Managed Microsoft AD
- Come aumentare la ridondanza e le prestazioni di Directory Service for Managed AWS Microsoft AD aggiungendo controller di dominio
- Come abilitare l'uso di desktop remoti implementando Microsoft Remote Desktop Licensing Manager su Managed Microsoft AD AWS
- Come accedere all' Console di gestione AWS utilizzo di AWS Managed Microsoft AD e alle credenziali locali
- Come abilitare l'autenticazione a più fattori per AWS i servizi utilizzando AWS Managed Microsoft AD e credenziali locali
- Come accedere facilmente ai AWS servizi utilizzando Active Directory locale

Cosa viene creato con AWS Managed Microsoft AD

Quando crei un Active Directory con AWS Managed Microsoft AD, Directory Service esegue le seguenti attività per tuo conto:

- crea e associa automaticamente una interfaccia di rete elastica (ENI) a ciascuno dei controller di dominio. Ciascuno di ENIs questi è essenziale per la connettività tra il VPC e i controller di Directory Service dominio e non deve mai essere eliminato. È possibile identificare tutte le interfacce di rete riservate all'uso Directory Service mediante la descrizione: "interfaccia di rete AWS creata per directory directory-id». Per ulteriori informazioni, consulta Elastic Network Interfaces nella Amazon EC2 User Guide. Il server DNS predefinito di AWS Managed Microsoft AD Active Directory è il server DNS VPC at Classless Inter-Domain Routing (CIDR) +2. Per ulteriori informazioni, consulta Amazon DNS server nella Amazon VPC User Guide.

> **Note**
>
> Per impostazione predefinita, i controller di dominio vengono distribuiti in due zone di disponibilità in una regione e collegati al tuo Amazon VPC (VPC). I backup vengono eseguiti automaticamente una volta al giorno e i volumi Amazon EBS (EBS) sono crittografati per garantire che i dati siano protetti anche quando sono inattivi. Iin caso di guasto, i controller di dominio vengono sostituiti automaticamente nella stessa zona di disponibilità utilizzando lo stesso indirizzo IP ed è possibile eseguire un ripristino di emergenza completo utilizzando il backup più recente.

- Effettua il provisioning di Active Directory all'interno del VPC in utilizzando due controller dei domini per la tolleranza ai guasti e un'alta disponibilità. È possibile eseguire il provisioning di più controller di dominio per una maggiore resilienza e prestazioni dopo che la directory è stata creata correttamente ed è attiva. Per ulteriori informazioni, consulta Implementazione di controller di dominio aggiuntivi per Managed AWS Microsoft AD.

  > **Note**
  >
  > AWSnon consente l'installazione di agenti di monitoraggio sui controller di dominio Microsoft AD AWS gestiti.

- Crea un gruppo AWS di sicurezza *sg-1234567890abcdef0* che stabilisce le regole di rete per il traffico in entrata e in uscita dai controller di dominio. La regola in uscita predefinita consente tutto il traffico verso tutti gli indirizzi. IPv4 Le regole in entrata predefinite consentono solo il traffico attraverso le porte richieste da Active Directory dal blocco IPv4 CIDR primario associato all'hosting VPC per il tuo Managed AWS Microsoft AD. Per una maggiore sicurezza, alle ENIs creazioni non è IPs associato Elastic e non sei autorizzato ad associare un IP elastico a tali elementi. ENIs Pertanto, per impostazione predefinita, l'unico traffico in entrata che può comunicare con AWS Managed Microsoft AD è il VPC locale. È possibile modificare le regole del gruppo di sicurezza per consentire sorgenti di traffico aggiuntive, ad esempio da altre fonti peer VPCs o CIDRs raggiungibili tramite VPN. Usa la massima cautela se tenti di modificare queste regole poiché potresti causare l'interruzione delle comunicazioni con i controller di dominio. Per ulteriori informazioni, consultare AWSBest practice gestite per Microsoft AD e Miglioramento della configurazione di sicurezza della rete AWS Managed Microsoft AD.

  Puoi utilizzare gli elenchi di prefissi per gestire i blocchi CIDR all'interno delle regole del gruppo di sicurezza. Gli elenchi di prefissi semplificano la gestione e la configurazione dei gruppi di sicurezza

e delle tabelle di routing. È possibile consolidare più blocchi CIDR con la stessa porta e gli stessi protocolli per scalare il traffico di rete.

- In un Windows ambiente, i client comunicano spesso tramite Server Message Block (SMB) o la porta 445. Questo protocollo facilita varie azioni come la condivisione di file e stampanti e la comunicazione generale di rete. Vedrai il traffico dei client sulla porta 445 verso le interfacce di gestione dei controller di dominio Microsoft AD AWS gestiti.

  Questo traffico si verifica quando i client SMB si affidano alla risoluzione dei nomi DNS (porta 53) e NetBIOS (porta 138) per individuare le risorse del dominio AWS Microsoft AD gestito. Questi client vengono indirizzati a qualsiasi interfaccia disponibile sui controller di dominio quando individuano le risorse del dominio. Questo comportamento è previsto e si verifica spesso in ambienti con più adattatori di rete e in cui SMB Multichannel consente ai client di stabilire connessioni tra diverse interfacce per migliorare le prestazioni e la ridondanza.

Le seguenti regole del gruppo di sicurezza vengono create per impostazione predefinita: AWS

Regole in entrata

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
ICMP	N/D	AWSCIDR Microsoft AD VPC IPv4 gestito	Ping	LDAP Keep Alive, DFS
TCP e UDP	53	AWSCIDR Microsoft AD VPC IPv4 gestito	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	AWSCIDR Microsoft AD VPC IPv4 gestito	Kerberos	Autentica zione utente e computer, trust a livello di foresta

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP e UDP	389	AWSCIDR Microsoft AD VPC IPv4 gestito	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	445	AWSCIDR Microsoft AD VPC IPv4 gestito	SMB/CIFS	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP e UDP	464	AWSCIDR Microsoft AD VPC IPv4 gestito	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	135	AWSCIDR Microsoft AD VPC IPv4 gestito	Replica	RPC, EPM
TCP	636	AWSCIDR Microsoft AD VPC IPv4 gestito	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	1024 - 65535	AWSCIDR Microsoft AD VPC IPv4 gestito	RPC	Replica, autentica zione utente e computer, policy di gruppo, trust

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP	3268 - 3269	AWSCIDR Microsoft AD VPC IPv4 gestito	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
UDP	123	AWSCIDR Microsoft AD VPC IPv4 gestito	Ora di Windows	Ora di Windows, trust
UDP	138	AWSCIDR Microsoft AD VPC IPv4 gestito	DFSN e NetLogon	DFS, policy di gruppo
Tutti	Tutti	AWSgruppo di sicurezza creato per i controlle r di dominio () *sg-123456 7890abcde f0*	All Traffic	

Regole in uscita

Protocollo	Intervallo porte	Destinazione	Tipo di traffico	Utilizzo di Active Directory
Tutti	Tutti	0.0.0.0/0	All Traffic	

- Per ulteriori informazioni sulle porte e i protocolli utilizzati da Active Directory, vedi Panoramica del servizio e requisiti delle porte di rete per Windows nella Microsoft documentazione.

- Crea un account amministratore della directory con nome utente Admin e la password specificata. Questo account si trova in Users OU (Ad esempio, Corp > Users). Utilizzi questo account per gestire la tua directory in. Cloud AWS Per ulteriori informazioni, consulta AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo.

> **Important**
>
> Assicurati di salvare questa password. Directory Servicenon memorizza questa password e non può essere recuperata. Tuttavia, è possibile reimpostare una password dalla Directory Service console o utilizzando l'ResetUserPasswordAPI.

- Crea le seguenti tre unità organizzative (OUs) nella radice del dominio:

Nome UO	Description
AWSDelegated Groups	Memorizza tutti i gruppi che è possibile utilizzare per delegare autorizzazioni AWS specifiche agli utenti.
AWSReserved	Memorizza tutti gli account specifici AWS di gestione.
<nomedominio>	Il nome di questa UO è basato sul nome NetBIOS digitato quando la directory è stata creata. Se non hai specificato un nome NetBIOS, per impostazione predefinita sarà la prima parte del nome DNS della directory (ad esempio, nel caso di corp.example.com, il nome NetBIOS sarebbe corp). Questa unità organizzativa è di proprietà AWS e contiene tutti gli oggetti di directory AWS correlati all'utente, sui quali è concesso il pieno controllo. Per impostazione predefinita, in questa unità organizzativa OUs esistono due figli: computer e utenti. Esempio: • Corp • Computer

Nome UO	Description
	• Utenti

- Crea i seguenti gruppi inAWSDelegated Groups OU:

Group name (Nome gruppo)	Description
AWSDelegated Account Operators	I membri di questo gruppo di sicurezza hanno limitate funzionalità di gestione dell'account, come la reimpostazione delle password
AWSDelegated Active Directory Based Activation Administrators	I membri di questo gruppo di sicurezza possono creare oggetti di attivazione licenza per volumi Active Directory, il che consente alle aziende di attivare i computer tramite una connessione al loro dominio.
AWSDelegated Add Workstations To Domain Users	I membri di questo gruppo di sicurezza possono aggiungere 10 computer a un dominio
AWSDelegated Administrators	I membri di questo gruppo di sicurezza possono gestire AWS Managed Microsoft AD, avere il pieno controllo di tutti gli oggetti dell'unità organizzativa e possono gestire i gruppi contenuti inAWS Delegated Groups OU.
AWSDelegated Allowed to Authenticate Objects	Ai membri di questo gruppo di sicurezza viene fornita la possibilità di autenticarsi su risorse informatiche in AWSReserved OU (necessar io solo per oggetti locali con autenticazione selettiva abilitata ai trust).
AWSDelegated Allowed to Authenticate to Domain Controllers	Ai membri di questo gruppo di sicurezza viene fornita la possibilità di autenticarsi su risorse informatiche in Domain Controllers

Group name (Nome gruppo)	Description
	OU (necessario solo per oggetti locali con autenticazione selettiva abilitata ai trust).
AWSDelegated Deleted Object Lifetime Administrators	I membri di questo gruppo di sicurezza possono modificare l'msDS-DeletedObje ctLifetimeoggetto, che definisce per quanto tempo un oggetto eliminato sarà disponibile per il ripristino dal Cestino di Active Directory.
AWSDelegated Distributed File System Administrators	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere i namespace FRS, DFS-R e DFS
AWSDelegated Domain Name System Administrators	I membri di questo gruppo di sicurezza possono gestire il DNS integrato con Active Directory.
AWSDelegated Dynamic Host Configuration Protocol Administrators	I membri di questo gruppo di sicurezza possono autorizzare i server Windows DHCP all'interno dell'azienda.
AWSDelegated Enterprise Certificate Authority Administrators	I membri di questo gruppo di sicurezza possono distribuire e gestire l'infrastruttura dell'autorità di certificazione aziendale di Microsoft.
AWSDelegated Fine Grained Password Policy Administrators	I membri di questo gruppo di sicurezza possono modificare le policy delle password fine-grained create in precedenza.
AWSDelegated FSx Administrators	Ai membri di questo gruppo di sicurezza viene fornita la possibilità di gestire FSx le risorse Amazon.

Group name (Nome gruppo)	Description
AWSDelegated Group Policy Administrators	I membri di questo gruppo di sicurezza possono eseguire attività di gestione delle policy di gruppo (creare, modificare, eliminare , collegare).
AWSDelegated Kerberos Delegation Administrators	I membri di questo gruppo di sicurezza possono abilitare la delega su oggetti di computer e account utenti.
AWSDelegated Managed Service Account Administrators	I membri di questo gruppo di sicurezza possono creare e cancellare account Managed Service.
AWSDelegated MS-NPRC Non-Compliant Devices	Ai membri di questo gruppo di sicurezza verrà fornita l'esclusione dalla richiesta di comunicazioni sicure tra canali con i controller di dominio. Questo gruppo è destinato agli account computer.
AWSDelegated Remote Access Service Administrators	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere server RAS dal gruppo Server RAS e IAS
AWSDelegated Replicate Directory Changes Administrators	I membri di questo gruppo di sicurezza possono sincronizzare le informazioni del profilo in Active Directory con SharePoint Server.
AWSDelegated Server Administrators	I membri di questo gruppo di sicurezza sono inclusi nel gruppo di amministratori locali in tutti i computer collegati al dominio
AWSDelegated Sites and Services Administrators	I membri di questo gruppo di sicurezza possono rinominare l' Default-First-Site -Nameoggetto in Siti e servizi di Active Directory.

Group name (Nome gruppo)	Description
AWSDelegated System Management Administrators	I membri di questo gruppo di sicurezza possono creare e gestire gli oggetti nel container System Management.
AWSDelegated Terminal Server Licensing Administrators	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere server Terminal Server License dal gruppo di server Terminal Server License
AWSDelegated User Principal Name Suffix Administrators	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere i suffissi nome principali degli utenti

> **Note**
>
> È possibile aggiungerliAWSDelegated Groups.

- Crea e applica i seguenti oggetti di policy di gruppo (GPOs):

> **Note**
>
> Non disponete delle autorizzazioni per eliminarli, modificarli o scollegarli. GPOs Ciò è dovuto alla progettazione in quanto sono riservati all'usoAWS. Se necessario, puoi collegarli a OUs ciò che controlli.

Nome policy di gruppo	Si applica a	Description
Default Domain Policy	Dominio	Include password di dominio e policy Kerberos.
ServerAdmins	Tutti gli account computer controller non di dominio	Aggiunge il 'AWSDelegated Server Administrators' come

Nome policy di gruppo	Si applica a	Description
		membro diBUILTIN\Administrators Group.
AWSReserved Policy:User	AWSReserved user accounts	Imposta le impostazioni di sicurezza consigliate per tutti gli account utente inAWS Reserved OU.
AWSManaged Active Directory Policy	Tutti i controller di dominio	Definisce le impostazioni di sicurezza consigliate su tutti i controller di dominio.
TimePolicyNT5DS	Tutti i controller non di PDCe dominio	Imposta la politica temporale di tutti i controller non di PDCe dominio per utilizzare Windows Time (NT5DS).
TimePolicyPDC	Il controller di PDCe dominio	Imposta la politica temporale del controller di PDCe dominio per utilizzare Network Time Protocol (NTP).
Default Domain Controllers Policy	Non utilizzato	Fornito durante la creazione del dominio, al suo posto viene utilizzato AWS Managed Active Directory Policy.

Per visualizzare le impostazioni di ciascun GPO, è possibile visualizzarle da un'istanza di Windows aggiunta a un dominio con la Console di gestione delle policy di gruppo (GPMC) attivata.

- Crea quanto segue default local accounts per la gestione di AWS Managed Microsoft AD:

> **Important**
>
> Assicurati di salvare la password dell'amministratore. Directory Servicenon memorizza questa password e non può essere recuperata. Tuttavia, è possibile reimpostare una password dalla Directory Service console o utilizzando l'ResetUserPasswordAPI.

Admin

Adminviene directory administrator account creato quando AWS Managed Microsoft AD viene creato per la prima volta. Fornisci una password per questo account quando crei un AWS Managed Microsoft AD. Questo account si trova sotto Users OU (ad esempio, Corp > Users). Questo account viene utilizzato per gestire Active Directory in. AWS Per ulteriori informazioni, consulta AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo.

AWS_***11111111111***

Qualsiasi nome di account che inizia con AWS seguito da un trattino basso e si trova in AWSReserved OU è un account gestito dal servizio. Questo account gestito dal servizio viene utilizzato da per interagire con Active AWS Directory. Questi account vengono creati quando AWS Directory Service Data è abilitato e con ogni nuova AWS applicazione autorizzata su Active Directory. Questi account sono accessibili solo dai AWS servizi.

krbtgt account

krbtgt accountSvolge un ruolo importante negli scambi di ticket Kerberos utilizzati dal tuo Managed AWS Microsoft AD. krbtgt accountSi tratta di un account speciale utilizzato per la crittografia Kerberos ticket-granting ticket (TGT) e svolge un ruolo cruciale nella sicurezza del protocollo di autenticazione Kerberos. Per ulteriori informazioni, consulta la documentazione Microsoft.

AWSruota automaticamente la krbtgt account password per AWS Managed Microsoft AD due volte ogni 90 giorni. C'è un periodo di attesa di 24 ore tra le due rotazioni consecutive ogni 90 giorni.

Per ulteriori informazioni sull'account amministratore e sugli altri account creati da Active Directory, consulta Microsoftla documentazione.

AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo

Quando si crea una AWS directory Directory Service per Microsoft Active Directory, AWS crea un'unità organizzativa (OU) per archiviare tutti i gruppi e gli account AWS correlati. Per ulteriori informazioni sull'UO, consulta Cosa viene creato con AWS Managed Microsoft AD. L'UO include l'account Admin. L'account Admin dispone delle autorizzazioni per eseguire le seguenti attività amministrative comuni per l'UO:

- aggiunta, aggiornamento o eliminazione di utenti, gruppi e computer; Per ulteriori informazioni, consulta Gestione di utenti e gruppi in AWS Managed Microsoft AD.
- Aggiunta di risorse al tuo dominio, come file o server di stampa, quindi assegnazione delle autorizzazioni per tali risorse a utenti e gruppi dell'UO;
- Crea contenitori aggiuntivi OUs e.
- Delega l'autorità dei contenitori aggiuntivi OUs e. Per ulteriori informazioni, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.
- creazione e collegamento policy di gruppo;
- ripristino degli oggetti eliminati dal cestino riciclaggio di Active Directory;
- Esegui i PowerShell moduli Active Directory e DNS sul servizio Web Active Directory.
- creazione e configurazione degli account del servizio gestito del gruppo; Per ulteriori informazioni, consulta Account del servizio gestito del gruppo.
- configurazione della delega vincolata Kerberos. Per ulteriori informazioni, consulta Delega vincolata Kerberos.

L'account Admin ha inoltre i diritti per eseguire le seguenti attività estese a tutto il dominio:

- gestione delle configurazioni DNS (aggiunta, eliminazione o aggiornamento di record, zone e server d'inoltro);
- visualizzazione di log di eventi DNS;
- visualizzazione di log di eventi di sicurezza.

Sono consentite all'account Admin solo le operazioni elencate di seguito. L'account Admin non dispone inoltre delle autorizzazioni per nessuna operazione relativa alla directory al di fuori dell'UO specifica, ad esempio la UO padre.

Considerazioni

- AWS Gli amministratori di dominio hanno accesso amministrativo completo a tutti i domini ospitati su. AWS Consulta il contratto AWS e le domande frequenti sulla protezione AWS dei dati per ulteriori informazioni su come vengono AWS gestiti i contenuti, incluse le informazioni sulle directory, archiviati sui AWS sistemi.
- Si consiglia di non eliminare o rinominare questo account. Se non desideri più utilizzare l'account, ti consigliamo di impostare una password lunga (al massimo 64 caratteri casuali) e quindi disabilitare l'account.

> **Note**
>
> AWS ha il controllo esclusivo degli utenti e dei gruppi con privilegi di Domain Administrator ed Enterprise Administrator. Ciò consente di AWS eseguire la gestione operativa della directory.

Account con privilegi Enterprise e Domain Administrator

AWS ruota automaticamente la password di amministratore integrata in una password casuale ogni 90 giorni. Ogni volta che viene richiesta la password di amministratore integrata per uso umano, viene creato un AWS ticket e registrato con il team. Directory Service Le credenziali dell'account sono crittografate e gestite su canali sicuri. Inoltre, le credenziali dell'account Administrator possono essere richieste solo dal team di gestione. Directory Service

Per eseguire la gestione operativa della directory, AWS ha il controllo esclusivo degli account con privilegi di amministratore aziendale e amministratore di dominio. Ciò include il controllo esclusivo dell'account amministratore di Active Directory. AWS protegge questo account automatizzando la gestione delle password tramite l'uso di un archivio di password. Durante la rotazione automatica della password dell'amministratore, AWS crea un account utente temporaneo e gli concede i privilegi di amministratore di dominio. Questo account temporaneo viene usato come un back-up in caso di errore nella rotazione delle password dell'account amministratore. Dopo aver ruotato AWS con successo la password dell'amministratore, AWS elimina l'account amministratore temporaneo.

Normalmente AWS gestisce la directory interamente tramite automazione. Nel caso in cui un processo di automazione non sia in grado di risolvere un problema operativo, AWS potrebbe essere necessario che un tecnico dell'assistenza acceda al controller di dominio (DC) per eseguire la diagnosi. In questi rari casi, AWS implementa un request/notification sistema per concedere

l'accesso. In questo processo, AWS l'automazione crea un account utente a tempo limitato nella directory con autorizzazioni di amministratore di dominio. AWS associa l'account utente al tecnico incaricato di lavorare sulla vostra rubrica. AWS registra questa associazione nel nostro sistema di log e fornisce all'ingegnere le credenziali da utilizzare. Tutte le azioni intrapreprese dall'ingegnere vengono registrate nel log di eventi di Windows. Quando trascorre l'intervallo di tempo allocato, l'automazione elimina l'account utente.

È possibile monitorare le operazioni di un account amministratore tramite la funzionalità di inoltro di log della directory. Questa funzionalità consente di inoltrare gli eventi di AD Security al CloudWatch sistema in cui è possibile implementare soluzioni di monitoraggio. Per ulteriori informazioni, consulta Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS.

Gli eventi di sicurezza IDs 4624, 4672 e 4648 vengono tutti registrati quando qualcuno accede a un DC in modo interattivo. È possibile visualizzare il registro degli eventi di Windows Security di ogni DC utilizzando il Visualizzatore eventi Microsoft Management Console (MMC) da un computer Windows aggiunto al dominio. Puoi anche Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS inviare tutti i registri degli eventi di sicurezza ai CloudWatch registri del tuo account.

Occasionalmente potresti vedere utenti creati ed eliminati all'interno dell'unità organizzativa AWS riservata. AWS è responsabile della gestione e della sicurezza di tutti gli oggetti in questa unità organizzativa e in qualsiasi altra unità organizzativa o contenitore a cui non abbiamo delegato le autorizzazioni di accesso e gestione dell'utente. Puoi visualizzare creazioni ed eliminazioni in quell'unità organizzativa. Questo perché Directory Service utilizza l'automazione per ruotare regolarmente la password dell'amministratore di dominio. Quando la password viene ruotata, viene creato un backup in caso di errore. Una volta completata la rotazione, l'account di backup viene eliminato automaticamente. Inoltre, nel raro caso in cui sia necessario un accesso interattivo DCs per la risoluzione dei problemi, viene creato un account utente temporaneo da utilizzare da un Directory Service tecnico. Una volta che un tecnico avrà completato il lavoro, l'account utente temporaneo verrà eliminato. Tieni presente che ogni volta che vengono richieste credenziali interattive per una directory, il team di Directory Service gestione viene avvisato.

Concetti chiave e best practice per AWS Managed Microsoft AD

Puoi ottenere di più da AWS Managed Microsoft AD acquisendo familiarità con i concetti chiave e le best practice. I concetti chiave aiutano a capire come funziona AWS Managed Microsoft AD. I concetti chiave includono ulteriori informazioni sullo schema di Active Directory, sulla pianificazione delle patch e sugli account dei servizi gestiti di gruppo. Lo schema di Active Directory include

elementi come attributi, classi e oggetti che costituiscono AWS Managed Microsoft AD. AWS aggiorna i controller di dominio Microsoft AD AWS gestiti con Microsoft aggiornamenti per tuo conto. Puoi anche saperne di più sugli account di servizio gestiti di gruppo (gMSAs) e utilizzarli con AWS Managed Microsoft AD.

È possibile evitare problemi con AWS Managed Microsoft AD prendendo in considerazione le best practice. Alcune di queste best practice includono:

- Quando configuri AWS Managed Microsoft AD, configuri i gruppi di sicurezza in base alle tue esigenze, ricorda l'ID e la password dell'account amministratore e abilita l'impostazione condizionale del forwarder.
- Quando utilizzi AWS Managed Microsoft AD, non modificare l'unità organizzativa AWS creata al momento della creazione della directory, monitora le prestazioni con strumenti come Amazon CloudWatch e Amazon SNS e utilizza client SMB 2.x.
- Quando si programmano applicazioni per l'utilizzo con AWS Managed Microsoft AD, è necessario utilizzare il servizio Windows DC Locator, caricare le modifiche dei test prima di implementarle negli ambienti di produzione e utilizzare query LDAP efficienti per evitare cicli significativi della CPU in un controller di dominio.

Argomenti

AWS Concetti chiave di Microsoft AD gestito

Otterrai il massimo da AWS Managed Microsoft AD se acquisirai familiarità con i seguenti concetti chiave.

Argomenti

Schema Active Directory

Uno schema è la definizione di attributi e classi che fanno parte di una directory distribuita ed è simile ai campi e alle tabelle in un database. Gli schemi includono un insieme di regole che determinano il tipo e il formato dei dati che possono essere aggiunti o inclusi nel database. La classe utente è un esempio di una classe archiviata nel database. Alcuni esempi di attributi della classe User possono includere il nome, il cognome, il numero di telefono dell'utente e così via.

Elementi dello schema

Attributi, classi e oggetti sono gli elementi fondamentali utilizzati per creare definizioni di oggetti nello schema. Di seguito vengono forniti dettagli sugli elementi dello schema che è importante conoscere prima di iniziare il processo di estensione dello schema AWS Managed Microsoft AD.

Attributes

Ogni attributo dello schema, simile a un campo in un database, presenta varie proprietà che definiscono le caratteristiche dell'attributo. Ad esempio, la proprietà utilizzata dai client LDAP per leggere e scrivere l'attributo è `LDAPDisplayName`. La proprietà `LDAPDisplayName` deve essere univoca all'interno di tutti gli attributi e le classi. Per un elenco completo delle caratteristiche di attributo, consulta la pagina relativa alle caratteristiche degli attributi sul sito Web MSDN. Per ulteriori istruzioni su come creare un nuovo attributo, consulta la pagina relativa alla definizione di un nuovo attributo sul sito Web MSDN.

Classi

Le classi sono analoghe alle tabelle di un database e presentano inoltre diverse proprietà da definire. Ad esempio, `objectClassCategory` definisce la categoria della classe. Per un elenco completo delle caratteristiche delle classi, consulta la pagina relativa alle caratteristiche delle classi di oggetto sul sito Web MSDN. Per ulteriori informazioni su come creare una nuova classe, consulta la pagina relativa alla definizione di una nuova classe sul sito Web MSDN.

Identificatore di oggetto (OID)

Ogni classe e attributo deve disporre di un OID univoco per tutti i tuoi oggetti. I fornitori di software devono ottenere il proprio OID per garantire l'univocità. L'univocità impedisce i conflitti quando lo stesso attributo viene utilizzato da più di un'applicazione per scopi differenti. Per garantire l'univocità, puoi ottenere un OID root da un'Autorità di registrazione nomi ISO. In alternativa, puoi ottenere un OID di base da Microsoft. Per ulteriori informazioni OIDs e su come ottenerli, vedere Identificatori di oggetti sul sito Web MSDN.

Attributi collegati allo schema

Alcuni attributi sono collegati tra due classi con collegamenti di inoltro e di ritorno. I gruppi sono l'esempio migliore. Esaminando un gruppo, vengono visualizzati i membri del gruppo. Esaminando un utente, puoi visualizzare i gruppi ai quali appartiene. Quando aggiungi un utente a un gruppo, Active Directory crea un link di inoltro al gruppo. Quindi Active Directory aggiunge un link di ritorno dal gruppo verso l'utente. È necessario generare un ID di collegamento univoco durante la creazione di un attributo che verrà collegato. Per ulteriori informazioni, consulta la pagina relativa agli attributi collegati sul sito Web MSDN.

Argomenti correlati

- Quando estendere lo schema AWS Managed Microsoft AD
- Tutorial: estensione dello schema AWS Managed Microsoft AD

Applicazione di patch e manutenzione per Microsoft AD gestito da AWS

AWS Directory Service for Microsoft Active Directory, noto anche come AWS DS for AWS Managed Microsoft AD, è in realtà Microsoft Active Directory Domain Services (AD DS), fornito come servizio gestito. Il sistema utilizza Microsoft Windows Server 2019 per i controller di dominio (DCs) e AWS aggiunge software DCs per la gestione dei servizi. AWS aggiornamenti (patch) DCs per aggiungere nuove funzionalità e mantenere aggiornato il software Microsoft Windows Server. Durante il processo di applicazione di patch, la directory rimane disponibile per essere utilizzata.

Verifica della disponibilità

Per impostazione predefinita, ogni directory è composta da due DCs, ciascuna installata in una zona di disponibilità diversa. A tua scelta, puoi aggiungere DCs per aumentare ulteriormente la disponibilità. Per ambienti critici che richiedono elevata disponibilità e tolleranza agli errori, consigliamo di installarne altri. DCs AWS esegue le patch DCs in modo sequenziale, durante il quale il DC che esegue attivamente le patch non è disponibile. AWS Nel caso in cui uno o più sistemi siano temporaneamente fuori servizio, AWS rimanda l' DCs applicazione delle patch fino a quando la directory non ne avrà almeno due operative. DCs Ciò consente di utilizzare l'altra unità operativa DCs durante il processo di patch, che in genere richiede dai 30 ai 45 minuti per DC, anche se questo periodo può variare. Per garantire che le applicazioni possano raggiungere un controller di dominio operativo nel caso in cui uno o più controller non DCs siano disponibili per qualsiasi motivo, inclusa l'applicazione di patch, le applicazioni devono utilizzare il servizio di localizzazione di Windows DC e non utilizzare indirizzi DC statici.

Comprendere la pianificazione dell'applicazione di patch

Per mantenere aggiornato il software Microsoft Windows Server DCs, AWS utilizza gli aggiornamenti Microsoft. Poiché Microsoft rende disponibili patch cumulative mensili per Windows Server, AWS si impegna al massimo per testare e applicare l'aggiornamento cumulativo a tutti i clienti DCs entro tre settimane di calendario. Inoltre, AWS esamina gli aggiornamenti che Microsoft rilascia al di fuori dell'aggiornamento cumulativo mensile in base all'applicabilità DCs e all'urgenza. Per le patch di sicurezza che Microsoft considera critiche o importanti e per le quali sono pertinenti DCs, AWS compie ogni sforzo per testare e distribuire la patch entro cinque giorni.

Account del servizio gestito del gruppo

Con Windows Server 2012, Microsoft ha introdotto un nuovo metodo che gli amministratori potevano utilizzare per gestire gli account di servizio denominato Account di servizio gestiti di gruppo (gMSAs). Utilizzando gMSAs, gli amministratori del servizio non avevano più bisogno di gestire manualmente la sincronizzazione delle password tra le istanze del servizio. Al contrario, un amministratore può semplicemente creare un account del servizio gestito del gruppo in Active Directory, quindi configurare più istanze del servizio per l'utilizzo di quell'unico account.

Per concedere le autorizzazioni in modo che gli utenti di AWS Managed Microsoft AD possano creare un gMSA, è necessario aggiungere i loro account come membri del gruppo di AWS sicurezza Delegated Managed Service Account Administrators. Per impostazione predefinita, l'account Admin è un membro di questo gruppo. Per ulteriori informazioni su gMSAs, vedere Panoramica degli account dei servizi gestiti di gruppo sul TechNet sito Web di Microsoft.

Post correlato sul blog AWS sulla sicurezza

- In che modo AWS Managed Microsoft AD aiuta a semplificare la distribuzione e migliorare la sicurezza delle applicazioni.NET integrate in Active Directory

Delega vincolata Kerberos

La delega vincolata Kerberos è una funzionalità di Windows Server. Questa funzionalità offre agli amministratori dei servizi la possibilità di specificare e far rispettare i limiti di fiducia delle applicazioni limitando l'ambito in cui i servizi applicativi possono agire per conto di un utente. Questo può essere utile quando è necessario configurare quali account di servizio front-end possono delegare ai propri servizi back-end. La delega vincolata Kerberos impedisce inoltre agli account del servizio gestito del gruppo di connettersi a qualsiasi o a tutti i servizi per conto degli utenti di Active Directory, riducendo la probabilità di un uso illecito da parte di sviluppatori non autorizzati.

Ad esempio, supponiamo che l'utente jsmith acceda a un'applicazione HR. Vuoi che SQL Server applichi le autorizzazioni del database di jsmith. Tuttavia, per impostazione predefinita, SQL Server apre la connessione al database utilizzando le credenziali dell'account di servizio che applicano le autorizzazioni hr-app-service di JSmith anziché le autorizzazioni configurate da jsmith. È necessario consentire all'applicazione HR Payroll di accedere al database SQL Server utilizzando le credenziali di jsmith. A tale scopo, abilita la delega vincolata Kerberos per l'account di hr-app-service servizio nella directory Managed AWS Microsoft AD in. AWS Quando jsmith esegue l'accesso, Active Directory fornisce un ticket Kerberos che Windows utilizzerà automaticamente al tentativo di jsmith di accedere ad altri servizi della rete. La delega Kerberos consente all' hr-app-serviceaccount di riutilizzare il ticket jsmith Kerberos per accedere al database, applicando così le autorizzazioni specifiche di jsmith all'apertura della connessione al database.

Per concedere le autorizzazioni che consentono agli utenti di AWS Managed Microsoft AD di configurare la delega vincolata Kerberos, è necessario aggiungere i relativi account come membri del gruppo di sicurezza AWS Delegated Kerberos Delegation Administrators. Per impostazione predefinita, l'account Admin è un membro di questo gruppo. Per ulteriori informazioni sulla delega vincolata Kerberos, vedere Panoramica sulla delega vincolata Kerberos sul sito Web Microsoft. TechNet

La delega vincolata basata su risorse è stata introdotta con Windows Server 2012. Fornisce all'amministratore del servizio back-end la possibilità di configurare la delega vincolata per il servizio.

AWSBest practice gestite per Microsoft AD

Di seguito sono riportati alcuni suggerimenti e linee guida da prendere in considerazione per evitare problemi e ottenere il massimo da AWS Managed Microsoft AD.

Argomenti

- Procedure consigliate per la configurazione di un AWS Managed Microsoft AD
- Procedure consigliate per l'utilizzo di una directory Microsoft AD AWS gestita
- Procedure consigliate per la programmazione delle applicazioni per un Microsoft AD AWS gestito

Procedure consigliate per la configurazione di un AWS Managed Microsoft AD

Ecco alcuni suggerimenti e linee guida per la configurazione di AWS Managed Microsoft AD:

Argomenti

- Prerequisiti
- Creazione del tuo AWS Managed Microsoft AD

Prerequisiti

Tieni presenti queste linee guida prima di creare la directory.

Verifica di avere il tipo di directory corretto

Directory Serviceoffre diverse modalità di utilizzo Microsoft Active Directory con altri AWS servizi. Puoi scegliere il servizio di directory con le caratteristiche di cui hai bisogno a un costo che si adatta al tuo budget:

- AWSDirectory Service per Microsoft Active Directory è un servizio gestito ricco di funzionalità Microsoft Active Directory ospitato sul AWS cloud. AWSMicrosoft AD gestito è la scelta migliore se hai più di 5.000 utenti e hai bisogno di impostare una relazione di fiducia tra una directory AWS ospitata e le directory locali.
- AD Connector collega semplicemente l'Active Directory locale esistente aAWS. Il connettore AD rappresenta la scelta migliore quando vuoi utilizzare la tua directory on-premise esistente tramite i servizi AWS.
- Simple AD è una directory a basso costo su scala ridotta con compatibilità di base con Active Directory. Supporta fino a 5.000 utenti, applicazioni compatibili con Samba 4 e compatibilità LDAP per applicazioni compatibili con LDAP.

Per un confronto più dettagliato delle Directory Service opzioni, consultaQuale scegliere.

Assicurati che le tue istanze VPCs e siano configurate correttamente

Per connetterti, gestire e utilizzare le tue directory, devi configurare correttamente le directory a VPCs cui sono associate. Consulta Prerequisiti per la creazione di un AWS Managed Microsoft AD, Prerequisiti di AD Connector o Prerequisiti di Simple AD per informazioni sulla sicurezza del VPC e sui requisiti di rete.

Se aggiungi un'istanza al dominio, assicurati di disporre della connessione e dell'accesso remoto all'istanza, come descritto in Modi per aggiungere un' EC2 istanza Amazon al tuo AWS Managed Microsoft AD.

Sii consapevole dei limiti

Scopri i vari limiti per il tuo tipo di directory specifico. Lo spazio di archiviazione disponibile e la dimensione aggregata degli oggetti sono le uniche limitazioni al numero di oggetti che puoi archiviare nella directory. Consulta, AWS Quote Microsoft AD gestite, Quote di AD Connector o Quote di Simple AD per maggiori dettagli sulla directory scelta.

Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory

AWSCrea un gruppo di sicurezza e lo collega alle interfacce di rete elastiche del controller di dominio della directory. Questo gruppo di sicurezza blocca il traffico non necessario verso il controller di dominio e consente il traffico necessario per le comunicazioni con Active Directory. AWSConfigura il gruppo di sicurezza per aprire solo le porte necessarie per le comunicazioni con Active Directory. Nella configurazione predefinita, il gruppo di sicurezza accetta il traffico verso queste porte dall'indirizzo IPv4 CIDR di AWS Managed Microsoft AD VPC. AWScollega il gruppo di sicurezza alle interfacce del controller di dominio accessibili dall'interno del dispositivo peerizzato o ridimensionato. VPCs Queste interfacce sono inaccessibili da Internet anche se modifichi le tabelle di routing, le connessioni di rete al VPC e configuri il servizio gateway NAT. In questo modo, solo le istanze e i computer che dispongono di un percorso di rete al VPC possono accedere alla directory. Questo semplifica la configurazione, evitando la necessità di configurare intervalli di indirizzi specifici. Al contrario, puoi configurare route e gruppi di sicurezza nel VPC che consentano il traffico solo da istanze e computer affidabili.

Modifica del gruppo di sicurezza della directory

Se desideri aumentare la sicurezza dei gruppi di sicurezza delle directory, puoi modificarli per accettare il traffico proveniente da un elenco di indirizzi IP più restrittivo. Ad esempio, è possibile modificare gli indirizzi accettati dall'intervallo IPv4 CIDR VPC a un intervallo CIDR specifico per una singola sottorete o computer. Analogamente, puoi scegliere di limitare gli indirizzi di destinazione con i quali i controller di dominio possono comunicare. Apporta tali modifiche solo se hai compreso a pieno come funziona il filtraggio del gruppo di sicurezza. Per ulteriori informazioni, consulta i gruppi EC2 di sicurezza Amazon per le istanze Linux nella Amazon EC2 User Guide. Modifiche improprie possono causare la perdita delle comunicazioni con i computer e le istanze previsti. AWSconsiglia di non tentare di aprire porte aggiuntive al controller di dominio in quanto ciò riduce la sicurezza della directory. Verifica attentamente il modello di responsabilità condivisa di AWS.

> **Warning**
>
> È tecnicamente possibile associare i gruppi di sicurezza utilizzati dalla directory ad altre EC2 istanze create dall'utente. Tuttavia, AWS sconsiglia questa pratica. AWSpuò avere motivi per modificare il gruppo di sicurezza senza preavviso per soddisfare le esigenze funzionali o di sicurezza della directory gestita. Tali modifiche coinvolgono tutte le istanze alle quali hai associato il gruppo di sicurezza della directory. Inoltre, l'associazione del gruppo di sicurezza della directory EC2 alle istanze crea un potenziale rischio per la EC2 sicurezza delle istanze. Il gruppo di sicurezza della directory accetta il traffico sulle porte Active Directory richieste dall'AWSindirizzo IPv4 CIDR VPC gestito di Microsoft AD. Se associ questo gruppo di sicurezza a un' EC2 istanza con un indirizzo IP pubblico collegato a Internet, qualsiasi computer su Internet può comunicare con l' EC2 istanza sulle porte aperte.

Creazione del tuo AWS Managed Microsoft AD

Di seguito sono riportati alcuni suggerimenti da prendere in considerazione durante la creazione di AWS Managed Microsoft AD.

Argomenti

- Ricorda l'ID amministratore e la password
- Creazione di un set di opzioni DHCP
- Abilita l'impostazione condizionale del forwarder
- Distribuzione di controller di dominio aggiuntivi
- Informazioni sulle limitazioni per il nome utente delle applicazioni AWS

Ricorda l'ID amministratore e la password

Quando configuri la directory, fornisci una password per l'account amministratore. L'ID dell'account è Admin for AWS Managed Microsoft AD. Ricorda la password creata per questo account; altrimenti sarai in grado di aggiungere oggetti alla directory.

Creazione di un set di opzioni DHCP

Ti consigliamo di creare un set di opzioni DHCP per la tua Directory Service directory e di assegnare le opzioni DHCP impostate al VPC in cui si trova la directory. Questo permette alle istanze in tale

VPC di puntare al dominio specificato, mentre i server DNS possono risolvere i propri nomi di dominio.

Per ulteriori informazioni sui set opzioni DHCP, consulta Creazione o modifica di un set di opzioni DHCP per AWS Managed Microsoft AD.

Abilita l'impostazione condizionale del forwarder

Le seguenti impostazioni di inoltro condizionale Archivia questo server d'inoltro condizionale in Active Directory, replicalo come segue: dovrebbe essere abilitato. L'attivazione di queste impostazioni garantirà che l'impostazione del forwarder condizionale sia persistente quando un nodo viene sostituito a causa di un guasto dell'infrastruttura o di un errore di sovraccarico.

I server d'inoltro condizionali devono essere creati su un controller di dominio con l'impostazione precedente abilitata. Ciò consentirà la replica su altri controller di dominio.

Distribuzione di controller di dominio aggiuntivi

Per impostazione predefinita, AWS crea due controller di dominio che esistono in zone di disponibilità separate. Ciò fornisce resilienza ai guasti durante l'applicazione di patch software e altri eventi che potrebbero rendere un controller di dominio irraggiungibile o non disponibile. Ti consigliamo di distribuire controller di dominio aggiuntivi per aumentare ulteriormente la resilienza e garantire prestazioni di scalabilità orizzontale in caso di un evento a lungo termine che influisce sull'accesso a un controller di dominio o a una zona di disponibilità.

Per ulteriori informazioni, consulta Utilizza il servizio di localizzazione Windows DC.

Informazioni sulle limitazioni per il nome utente delle applicazioni AWS

Directory Servicefornisce il supporto per la maggior parte dei formati di caratteri che possono essere utilizzati nella costruzione di nomi utente. Tuttavia, vengono applicate restrizioni sui caratteri ai nomi utente che verranno utilizzati per l'accesso ad AWS applicazioni WorkSpaces, come WorkDocs Amazon WorkMail o Quick Suite. Queste limitazioni richiedono che non vengano utilizzati i seguenti caratteri:

- Spazi
- Caratteri multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Il simbolo @ è consentito purché preceda un suffisso UPN.

Procedure consigliate per l'utilizzo di una directory Microsoft AD AWS gestita

Di seguito sono riportati alcuni suggerimenti da tenere a mente quando si utilizza AWS Managed Microsoft AD.

Argomenti

Non modificare utenti, gruppi e unità organizzative predefiniti

Quando si utilizza Directory Service per avviare una directory, AWS crea un'unità organizzativa (OU) che contiene tutti gli oggetti della directory. Questa unità organizzativa, che ha lo stesso nome NetBIOS che hai digitato al momento della creazione della directory, si trova nella radice del dominio. La radice del dominio è di proprietà e gestita daAWS. Vengono creati anche diversi gruppi e un utente amministrativo.

Non spostare, eliminare o modificare in qualsiasi altro modo questi oggetti predefiniti. In questo modo potresti rendere la tua directory inaccessibile sia a te che a. AWS Per ulteriori informazioni, consulta Cosa viene creato con AWS Managed Microsoft AD.

Unisci i domini automaticamente

Quando si avvia un'istanza di Windows che deve far parte di un Directory Service dominio, spesso è più semplice aggiungere l'istanza al dominio come parte del processo di creazione dell'istanza piuttosto che aggiungere manualmente l'istanza in un secondo momento. Per unire un dominio automaticamente, semplicemente seleziona la directory corretta in Domain join directory (Directory aggiunta dominio) quando avvii una nuova istanza. Puoi trovare i dettagli in Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory.

Configura i trust correttamente

Quando si imposta una relazione di trust tra la directory AWS Managed Microsoft AD e un'altra directory, è necessario tenere presenti queste linee guida:

- Il tipo di trust deve corrispondere su entrambi i lati (foresta o esterno)
- Assicurarsi che la direzione di trust sia impostata correttamente se si utilizza un trust unidirezionale (In uscita su dominio trusting, In entrata su dominio trusted)
- Sia i nomi di dominio completi (FQDNs) che i nomi NetBIOS devono essere univoci tra foreste/domini

Per ulteriori dettagli e istruzioni specifiche su come configurare una relazione di trust, consulta Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito.

Tieni traccia delle prestazioni del controller di dominio

Per ottimizzare le decisioni di scalabilità e migliorare la resilienza e le prestazioni delle directory, si consiglia di utilizzare le metriche. CloudWatch Per ulteriori informazioni, consulta Utilizzo CloudWatch per monitorare le prestazioni dei controller di dominio Microsoft AD AWS gestiti.

Per istruzioni su come configurare le metriche dei controller di dominio utilizzando la CloudWatch console, vedi Come automatizzare il ridimensionamento gestito di AWS Microsoft AD in base alle metriche di utilizzo nel Security Blog. AWS

Pianificazione delle estensioni dello schema

Applica con attenzione le estensioni dello schema per indicizzare le directory per le query importanti e frequenti. Ti consigliamo di non eseguire un numero eccessivo di indicizzazioni poiché gli indici occupano rapidamente lo spazio della directory e una modifica rapida dei valori indicizzati può essere la causa di eventuali problemi di prestazioni. Per aggiungere indici, è necessario creare un file a

LDIF (Directory Interchange Format) per LDAP (Lightweight Directory Access Protocol) ed estendere la modifica dello schema. Per ulteriori informazioni, consulta Estendi lo schema AWS Managed Microsoft AD.

Informazioni sui sistemi di bilanciamento del carico

Non utilizzare un sistema di bilanciamento del carico davanti agli endpoint Microsoft AD AWS gestiti. Microsoftha progettato Active Directory (AD) per l'uso con un algoritmo di rilevamento dei controller di dominio (DC) che trova il controller di dominio operativo più reattivo senza bilanciamento del carico esterno. I sistemi di bilanciamento del carico di rete esterni rilevano in modo errato i DCs sistemi attivi e possono comportare l'invio dell'applicazione a un controller di dominio imminente ma non pronto per l'uso. Per ulteriori informazioni, consulta Load balancer e Active Directory su Microsoft, TechNet che consiglia di correggere le applicazioni per utilizzare Active Directory correttamente anziché implementare bilanciamenti del carico esterni.

Fai un backup dell'istanza

Se decidi di aggiungere manualmente un'istanza a un Directory Service dominio esistente, esegui prima un backup o scatta un'istantanea di quell'istanza. Ciò è particolarmente importante quando aggiungi un'istanza Linux. Alcune delle procedure utilizzate per aggiungere un'istanza, se non vengono eseguite correttamente, possono rendere l'istanza non raggiungibile o inutilizzabile. Per ulteriori informazioni, consulta Ripristino di AWS Managed Microsoft AD con istantanee.

Configura la messaggistica SNS

Tramite Amazon Simple Notification Service (Amazon SNS), puoi ricevere messaggi e-mail o di testo (SMS) quando lo stato della directory cambia. Riceverai una notifica se la directory passa dallo stato Active (Attivo) agli stati Impaired (Insufficiente) o Inoperable (Inutilizzabile). Puoi anche ricevere una notifica quando la directory torna a uno stato Active (Attivo).

Ricorda inoltre che se hai un argomento SNS da cui riceve messaggiDirectory Service, prima di eliminarlo dalla console Amazon SNS, devi associare la tua directory a un argomento SNS diverso. In caso contrario, rischi di non ricevere importanti messaggi sullo stato della directory. Per informazioni su come configurare Amazon SNS, consulta Attivazione delle notifiche sullo stato della directory AWS Managed Microsoft AD con Amazon Simple Notification Service.

Applica le impostazioni del servizio di directory

AWSMicrosoft AD gestito consente di personalizzare la configurazione di sicurezza per soddisfare i requisiti di conformità e sicurezza. AWSMicrosoft AD gestito distribuisce e mantiene la configurazione

su tutti i controller di dominio nella directory, anche quando si aggiungono nuove aree o controller di dominio aggiuntivi. È possibile configurare e applicare queste impostazioni di sicurezza per tutte le directory nuove ed esistenti. Puoi eseguire questa operazione nella console seguendo i passaggi inclusi Modifica delle impostazioni di sicurezza della directory o tramite l'API. UpdateSettings

Per ulteriori informazioni, consulta Modifica delle impostazioni di sicurezza della directory Microsoft AD AWS gestita.

Rimozione delle applicazioni Amazon Enterprise prima di eliminare una directory

Prima di eliminare una directory associata a una o più applicazioni Amazon Enterprise come Amazon WorkSpaces Application Manager WorkSpaces WorkDocs, Amazon o Amazon WorkMail Relational Database Service (Amazon RDS), devi prima rimuovere ogni applicazione. Console di gestione AWS Per ulteriori informazioni su come rimuovere queste applicazioni, consulta Eliminazione di AWS Managed Microsoft AD.

Utilizzo dei client SMB 2.x quando si accede alle condivisioni SYSVOL e NETLOGON

I computer client utilizzano Server Message Block (SMB) per accedere alle condivisioni SYSVOL e NETLOGON sui controller di dominio AWS Microsoft AD gestiti per Criteri di gruppo, script di accesso e altri file. AWSMicrosoft AD gestito supporta solo la versione SMB 2.0 (SMBv2) e successive.

I SMBv2 protocolli della versione più recente aggiungono una serie di funzionalità che migliorano le prestazioni dei client e aumentano la sicurezza dei controller di dominio e dei client. Questa modifica segue le raccomandazioni del Computer Emergency Readiness Team degli Stati Uniti d'America e di Microsoft per SMBv1 la disattivazione.

> **Important**
>
> Se attualmente si utilizzano SMBv1 client per accedere alle condivisioni SYSVOL e NETLOGON del controller di dominio, è necessario aggiornare tali client per utilizzarli o versioni più recenti. SMBv2 La directory funzionerà correttamente, ma i SMBv1 client non riusciranno a connettersi alle condivisioni SYSVOL e NETLOGON dei controller di dominio AWS Microsoft AD gestiti e non saranno inoltre in grado di elaborare i criteri di gruppo.

SMBv1 i client funzioneranno con qualsiasi altro file server SMBv1 compatibile di cui disponi. Tuttavia, AWS consiglia di aggiornare tutti i server e client SMB a SMBv2 una versione più recente. Per ulteriori informazioni su come disabilitarlo SMBv1 e aggiornarlo alle versioni SMB più recenti sui tuoi sistemi, consulta questi post su Microsoft TechNet and Documentation. Microsoft

Monitoraggio delle connessioni remote SMBv1

È possibile esaminare il registro degli eventi Microsoft-Windows- SMBServer /Audit Windows in modalità remota quando si effettua la connessione al controller di dominio AWS Microsoft AD gestito. Tutti gli eventi in questo registro indicano connessioni. SMBv1 Di seguito è riportato un esempio delle informazioni che è possibile visualizzare in uno di questi log:

SMB1 accesso

Indirizzo client: ###.###.###.###

Linee guida:

Questo evento indica che un client ha tentato di accedere al server utilizzando SMB1.
Per interrompere il controllo dell' SMB1 accesso, utilizzare il PowerShell cmdlet Set-.
SmbServerConfiguration

Procedure consigliate per la programmazione delle applicazioni per un Microsoft AD AWS gestito

Prima di programmare le applicazioni per l'utilizzo con AWS Managed Microsoft AD, considera quanto segue:

Argomenti

- Utilizza il servizio di localizzazione Windows DC
- Esecuzione di test di caricamento prima della produzione
- Utilizzo delle query LDAP

Utilizza il servizio di localizzazione Windows DC

Durante lo sviluppo di applicazioni, utilizza il servizio di localizzazione Windows DC o il servizio DNS dinamico (DDNS) di Managed AWS Microsoft AD per individuare i controller di dominio (). DCs Non effettuare l'hard coding delle applicazioni con l'indirizzo di un DC. Il servizio di localizzazione DC garantisce che il carico della directory venga distribuito e ti consente di sfruttare i vantaggi della scalabilità orizzontale aggiungendo i controller dei domini alla distribuzione. Se colleghi l'applicazione a un DC fisso e il DC viene sottoposto a patch o ripristino, l'applicazione perderà l'accesso al DC anziché utilizzare uno dei controller rimanenti. DCs Inoltre, l'hard coding di un DC può provocare la creazione di "hot spot" su un solo DC. In casi gravi, gli hot spot possono provocare un blocco del

DC. In questi casi, inoltre, l'automazione delle AWS directory potrebbe contrassegnare la directory come danneggiata e avviare processi di ripristino che sostituiscono il controller di dominio che non risponde.

Esecuzione di test di caricamento prima della produzione

Assicurati di effettuare test di laboratorio con gli oggetti e le richieste più importanti del tuo carico di lavoro di produzione per confermare che la directory si adatti al carico dell'applicazione. Se hai bisogno di capacità aggiuntiva, esegui il test con quella aggiuntiva DCs distribuendo le richieste tra i. DCs Per ulteriori informazioni, consulta Implementazione di controller di dominio aggiuntivi per Managed AWS Microsoft AD.

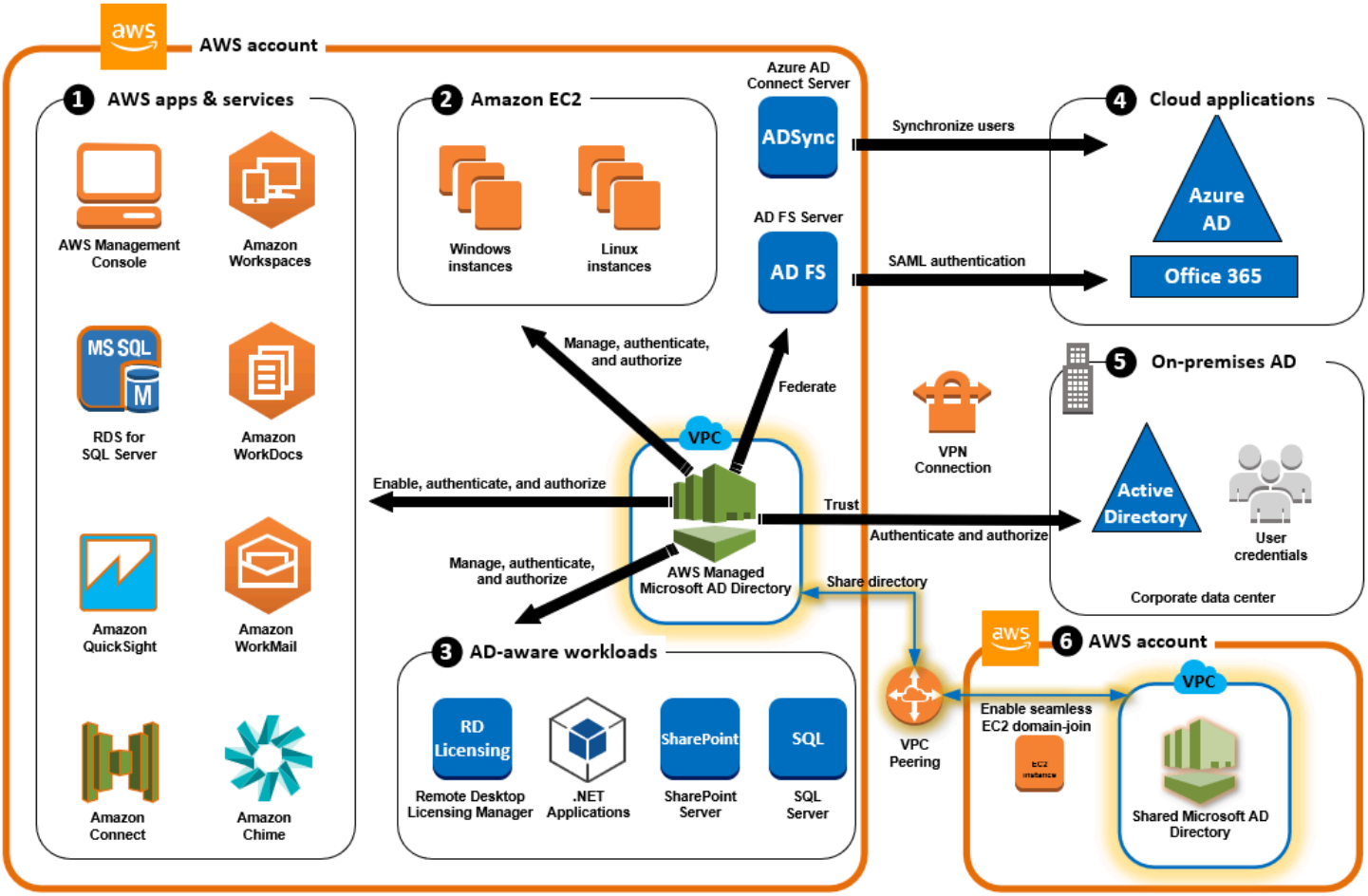
Utilizzo delle query LDAP

Query LDAP estese su un controller di dominio e decine di migliaia di oggetti possono consumare cicli di CPU significativi in un singolo DC e generare così hot spot. L'operazione potrebbe incidere sulle applicazioni che condividono lo stesso DC durante la query.

Casi d'uso per AWS Managed Microsoft AD

Con AWS Managed Microsoft AD, puoi condividere una singola directory per più casi d'uso. Ad esempio, puoi condividere una directory per autenticare e autorizzare l'accesso alle applicazioni .NET, Amazon RDS per SQL Server con l'autenticazione Windows abilitata e Amazon Chime per la messaggistica e le videoconferenze.

Il diagramma seguente mostra alcuni dei casi d'uso della directory AWS Managed Microsoft AD. Questi includono la possibilità di concedere agli utenti l'accesso ad applicazioni cloud esterne e consentire agli utenti di Active Directory locali di gestire e avere accesso alle risorse nel AWS cloud.



Utilizza AWS Managed Microsoft AD per uno dei seguenti casi d'uso aziendali.

Argomenti

- Caso d'uso 1: accesso ad AWS applicazioni e servizi con credenziali Active Directory
- Caso d'uso 2: gestione delle EC2 istanze Amazon
- Caso d'uso 3: Fornisci servizi di directory ai carichi di lavoro compatibili con Active Directory
- Caso d'uso 4: per Office 365 e altre applicazioni cloud AWS IAM Identity Center
- Caso d'uso 5: estendere Active Directory locale a Cloud AWS
- Caso d'uso 6: condividi la tua directory per unire senza problemi EC2 le istanze Amazon a un dominio tra più account AWS

Caso d'uso 1: accesso ad AWS applicazioni e servizi con credenziali Active Directory

Puoi abilitare più AWS applicazioni e servizi come Amazon Chime AWS Client VPNConsole di gestione AWSAWS IAM Identity Center, Amazon Connect, Amazon, Quick Suite FSx, Amazon RDS for SQL Server WorkDocs, WorkMailAmazon WorkSpacese utilizzare la tua directory AWS Managed Microsoft AD. Quando abiliti un'AWSapplicazione o un servizio nella tua directory, gli utenti possono accedere all'applicazione o al servizio con le proprie credenziali Active Directory.

Ad esempio, è possibile consentire agli utenti di accedere a Console di gestione AWS con le proprie credenziali di Active Directory. A tale scopo, abiliti l'applicazione Console di gestione AWS as a nella tua directory, quindi assegni gli utenti e i gruppi di Active Directory ai ruoli IAM. Quando i tuoi utenti accedono aConsole di gestione AWS, assumono un ruolo IAM per gestire AWS le risorse. In questo modo è più semplice concedere agli utenti l'accesso alla Console di gestione AWS, senza dover configurare e gestire un'infrastruttura SAML separata.

Per migliorare ulteriormente l'esperienza dell'utente finale, puoi abilitare le funzionalità Single Sign-on di WorkDocs, che offrono agli utenti la possibilità di accedere WorkDocs da un computer collegato alla directory senza dover inserire le proprie credenziali separatamente.

Puoi concedere l'accesso agli account utente nella tua directory o nell'Active Directory locale, in modo che possano accedere Console di gestione AWS o AWS CLI utilizzare le credenziali e le autorizzazioni esistenti per gestire le AWS risorse assegnando ruoli IAM direttamente agli account utente esistenti.

FSx per l'integrazione di Windows File Server con AWS Managed Microsoft AD

L'integrazione FSx per Windows File Server con AWS Managed Microsoft AD fornisce un file system con protocollo Server Message Block (SMB) nativo completamente gestito basato su Microsoft Windows che consente di spostare facilmente applicazioni e client basati su Windows (che utilizzano l'archiviazione di file condivisa) in. AWS Sebbene FSx per Windows File Server possa essere integrato con un Microsoft Active Directory autogestito, non discuteremo di questo scenario in questa sede.

Casi FSx d'uso e risorse comuni di Amazon

Questa sezione fornisce un riferimento alle risorse sui casi d' FSx uso comuni di Windows File Server con AWS Managed Microsoft AD. Ciascuno dei casi d'uso in questa sezione inizia con una

configurazione di base di AWS Managed Microsoft AD e FSx per Windows File Server. Per ulteriori informazioni su come creare queste configurazioni, consulta:

- Guida introduttiva a AWS Managed Microsoft AD
- Guida introduttiva ad Amazon FSx

FSx per Windows File Server come storage persistente su contenitori Windows

Amazon Elastic Container Service (ECS) supporta i container Windows in istanze di container avviate con l'AMI Windows ottimizzata per Amazon ECS. Le istanze di container Windows utilizzano la propria versione dell'agente del container Amazon ECS. Nell'AMI Windows ottimizzata per Amazon ECS l'agente del container di Amazon ECS viene eseguito come servizio sull'host.

Amazon ECS supporta l'autenticazione di Active Directory per i container Windows tramite un tipo speciale di account di servizio denominato account di servizio gestito di gruppo (gMSA, group Managed Service Account). Poiché i container Windows non possono essere aggiunti al dominio, è necessario configurare un container Windows per l'esecuzione con account gMSA.

Voci correlate

- Utilizzo FSx per Windows File Server come archiviazione persistente nei contenitori Windows
- Account del servizio gestito del gruppo

Supporto Amazon AppStream 2.0

Amazon AppStream 2.0 è un servizio di streaming di applicazioni completamente gestito. Fornisce agli utenti una gamma di soluzioni per il salvataggio e l'accesso ai dati tramite le proprie applicazioni. Amazon FSx with WorkSpaces Applications fornisce un'unità di archiviazione persistente personale tramite Amazon FSx e può essere configurata per fornire una cartella condivisa per accedere ai file comuni.

Voci correlate

- Procedura dettagliata 4: utilizzo di Amazon con FSx Amazon 2.0 AppStream
- Utilizzo di Amazon FSx con Amazon AppStream 2.0
- Utilizzo di Active Directory con WorkSpaces applicazioni

Supporto di Microsoft SQL Server

FSx per Windows File Server può essere utilizzato come opzione di archiviazione per Microsoft SQL Server 2012 (a partire dalla versione 11.x del 2012) e database di sistema più recenti (inclusi Master, Model, MSDB e TempDB) e per i database utente di Database Engine.

Voci correlate

- Installazione di SQL Server con archiviazione fileshare SMB
- Semplifica le distribuzioni ad alta disponibilità di Microsoft SQL Server utilizzando Windows FSx File Server
- Account del servizio gestito del gruppo

Supporto per cartelle home e profili utente in roaming

FSx per Windows File Server può essere utilizzato per archiviare i dati dalle home directory degli utenti di Active Directory e da My Documents in una posizione centrale. FSx per Windows File Server può essere utilizzato anche per archiviare dati dai profili utente mobili.

Voci correlate

- Le home directory di Windows semplificate con Amazon FSx
- Implementazione di profili utente in roaming
- Utilizzo FSx per Windows File Server con WorkSpaces

Supporto per la condivisione di file in rete

Le condivisioni di file in rete su un file server FSx per Windows forniscono una soluzione di condivisione di file gestita e scalabile. Un caso d'uso sono le unità mappate per i client che possono essere create manualmente o tramite policy di gruppo.

Voci correlate

- Procedura dettagliata 6: scalabilità orizzontale delle prestazioni con partizioni
- Mappatura dell'unità
- Utilizzo FSx per Windows File Server con WorkSpaces

Supporto per l'installazione di software con policy di gruppo

Poiché le dimensioni e le prestazioni della cartella SYSVOL sono limitate, è consigliabile evitare di archiviare dati come i file di installazione del software in tale cartella. Come possibile soluzione a questo problema, FSx per Windows File Server può essere configurato per archiviare tutti i file software installati utilizzando i Criteri di gruppo.

Voci correlate

- Utilizza i Criteri di gruppo per installare il software in remoto

Supporto per destinazioni Windows Server Backup

FSx per Windows File Server può essere configurato come unità di destinazione in Windows Server Backup utilizzando la condivisione di file UNC. In questo caso, è necessario specificare il percorso UNC del file server FSx per Windows anziché del volume EBS collegato.

Voci correlate

- Esecuzione del ripristino dello stato del sistema del server

Amazon supporta FSx anche la condivisione AWS gestita di Microsoft AD Directory. Per ulteriori informazioni, consulta:

- Condividi il tuo AWS Managed Microsoft AD
- Utilizzo di Amazon FSx con AWS Managed Microsoft AD in un altro VPC o account

Integrazione di Amazon RDS con AWS Managed Microsoft AD

Amazon RDS supporta l'autenticazione esterna degli utenti dei database con Kerberos e Microsoft Active Directory. Kerberos è un protocollo di autenticazione di rete che utilizza ticket e crittografia a chiave simmetrica eliminando la necessità di scambiare password sulla rete. Il supporto di Amazon RDS per Kerberos e Active Directory offre i vantaggi dell'autenticazione unica e centralizzata degli utenti dei database, in questo modo puoi mantenere le credenziali utente in Active Directory.

Per iniziare con questo caso d'uso, devi prima configurare una configurazione di base di AWS Managed Microsoft AD e Amazon RDS.

- Guida introduttiva a AWS Managed Microsoft AD

- Nozioni di base su Amazon RDS

Tutti i casi d'uso citati di seguito inizieranno con AWS Managed Microsoft AD e Amazon RDS di base e illustreranno come integrare Amazon RDS con Managed AWS Microsoft AD.

- Utilizzo dell'autenticazione Windows con un'istanza database di Amazon RDS per SQL Server
- Utilizzo dell'autenticazione Kerberos per MySQL
- Utilizzo dell'autenticazione Kerberos con Amazon RDS per Oracle
- Utilizzo dell'autenticazione Kerberos con Amazon RDS per PostgreSQL

Amazon RDS supporta anche la condivisione AWS gestita di Microsoft AD Directory. Per ulteriori informazioni, consulta:

- Condividi il tuo AWS Managed Microsoft AD
- Collegamento delle istanze DB Amazon RDS tra account in un singolo dominio condiviso

Per ulteriori informazioni sull'aggiunta di un Amazon RDS per SQL Server ad Active Directory, consulta Aggiunta di Amazon RDS per SQL Server all'Active Directory autogestita.

Applicazione .NET che utilizza Amazon RDS per SQL Server con account del servizio gestito del gruppo

Puoi integrare Amazon RDS for SQL Server con un'applicazione.NET di base e un gruppo di Managed Service Accounts (MSAsg). Per ulteriori informazioni, vedere In che modo AWS Managed Microsoft AD aiuta a semplificare la distribuzione e migliorare la sicurezza delle applicazioni.NET integrate in Active Directory

Caso d'uso 2: gestione delle EC2 istanze Amazon

Utilizzando i familiari strumenti di amministrazione di Active Directory, puoi applicare gli oggetti di policy di gruppo di Active Directory (GPOs) EC2 per gestire centralmente le tue istanze Amazon per Windows o Linux unendo le tue istanze al tuo dominio AWS Microsoft AD gestito.

Inoltre, i tuoi utenti possono accedere alle tue istanze con le proprie credenziali Active Directory. Ciò elimina la necessità di utilizzare le credenziali delle singole istanze o distribuire file di chiavi private (PEM). In questo modo è più semplice concedere o revocare istantaneamente l'accesso agli utenti utilizzando gli strumenti di amministrazione degli utenti di Active Directory che già utilizzi.

Caso d'uso 3: Fornisci servizi di directory ai carichi di lavoro compatibili con Active Directory

AWSManaged Microsoft AD è una vera e propria Microsoft Active Directory che consente di eseguire carichi di lavoro tradizionali compatibili con Active Directory come Remote Desktop Licensing Manager Microsoft SharePoint e Microsoft SQL Server Always On nel cloud. AWS AWSManaged Microsoft AD consente inoltre di semplificare e migliorare la sicurezza delle applicazioni.NET integrate in Active Directory utilizzando Managed Service Accounts (gMSAs) di gruppo e Kerberos Constrained Delegation (KCD).

Caso d'uso 4: per Office 365 e altre applicazioni cloud AWS IAM Identity Center

Puoi utilizzare AWS Managed Microsoft AD per fornire AWS IAM Identity Center servizi per applicazioni cloud. Puoi utilizzare Microsoft Entra Connect (precedentemente noto comeAzure Active Directory Connect) per sincronizzare gli utenti in Microsoft Entra (precedentemente noto come (AzureAD)) e quindi utilizzare Active Directory Federation Services Azure Active Directory (ADFS) in modo che gli utenti possano accedere a Microsoft Office 365 e ad altre applicazioni cloud SAML 2.0 utilizzando le proprie credenziali Active Directory.

L'integrazione di AWS Managed Microsoft AD con IAM Identity Center aggiunge funzionalità SAML a Managed AWS Microsoft AD e/o ai domini affidabili locali. Una volta integrato, gli utenti possono utilizzare IAM Identity Center con servizi che supportano SAML, incluse applicazioni cloud di terze parti come Office 365, Concur Console di gestione AWS e Salesforce senza dover configurare un'infrastruttura SAML. Per una dimostrazione sul processo per consentire agli utenti locali di utilizzare IAM Identity Center, guarda il seguente video. YouTube

> **Note**
>
> AWSSingle Sign-On è stato rinominato IAM Identity Center.

Caso d'uso 5: estendere Active Directory locale a Cloud AWS

Se disponi già di un'infrastruttura Active Directory e desideri utilizzarla per la migrazione di carichi di lavoro compatibili con Active Directory verso, Cloud AWS Managed AWS Microsoft AD può esserti utile. È possibile utilizzare i trust di Active Directory per connettere AWS Managed Microsoft AD all'Active Directory esistente. Ciò significa che gli utenti possono accedere alle AWS applicazioni e

alle applicazioni compatibili con Active Directory con le proprie credenziali di Active Directory locale, senza che sia necessario sincronizzare utenti, gruppi o password.

Ad esempio, i tuoi utenti possono accedere a Console di gestione AWS e Amazon WorkSpaces utilizzando i nomi utente e le password di Active Directory esistenti. Inoltre, quando si utilizzano applicazioni compatibili con Active Directory, ad esempio con SharePoint Managed AWS Microsoft AD, Windows gli utenti che hanno effettuato l'accesso possono accedere a queste applicazioni senza dover inserire nuovamente le credenziali.

È inoltre possibile migrare il dominio Active Directory locale per AWS liberarsi dal carico operativo dell'infrastruttura Active Directory utilizzando Active Directory Migration Toolkit (ADMT) insieme al Password Export Service (PES) per eseguire la migrazione.

Caso d'uso 6: condividi la tua directory per unire senza problemi EC2 le istanze Amazon a un dominio tra più account AWS

La condivisione della directory tra più AWS account consente di gestire EC2 facilmente AWS servizi come Amazon senza la necessità di gestire una directory per ogni account e ogni VPC. Puoi utilizzare la directory di qualsiasi account AWS e di qualsiasi Amazon VPC all'interno di una regione AWS. Questa funzionalità semplifica e rende più conveniente la gestione dei carichi di lavoro basati sulle directory con un'unica directory per più account e. VPCs Ad esempio, ora puoi gestire i carichi di lavoro Windows distribuiti in EC2 istanze su più account e VPCs facilmente utilizzando un'unica directory AWS Microsoft AD gestita.

Quando condividi la tua directory AWS Managed Microsoft AD con un altro AWS account, puoi utilizzare la EC2 console Amazon o AWS Systems Managerunire senza problemi le tue istanze da qualsiasi Amazon VPC all'interno dell'account e della regione. AWS Puoi distribuire rapidamente i carichi di lavoro compatibili con le directory sulle EC2 istanze eliminando la necessità di aggiungere manualmente le istanze a un dominio o di distribuire le directory in ogni account e VPC. Per ulteriori informazioni, consulta Condividi il tuo AWS Managed Microsoft AD.

Mantieni il tuo Microsoft AD AWS gestito

Puoi utilizzarlo Console di gestione AWS per gestire il tuo AWS Managed Microsoft AD e completare le attività day-to-day amministrative. I modi in cui è possibile gestire la directory includono:

- Visualizza i dettagli della tua directory AWS Managed Microsoft AD per conoscere il tipo di directory AWS Managed Microsoft AD, l'ID di directory, lo stato della directory e i dettagli di rete come Amazon VPC, sottoreti e zone di disponibilità.

- Ripristina il tuo AWS Managed Microsoft AD con istantanee. Puoi anche creare istantanee ed eliminare istantanee.
- Implementa controller di dominio aggiuntivi per migliorare le prestazioni e la AWS disponibilità di Managed Microsoft AD.
- Aggiorna AWS Managed Microsoft AD dall'edizione Standard all'edizione Enterprise che supporta più oggetti di directory.
- Aggiungi un nome utente principale alternativo (UPN) per migliorare l'esperienza di accesso dell'utente.
- Rinomina il nome del sito AWS Managed Microsoft AD per migliorare la capacità di AWS Managed Microsoft AD di trovare e autenticare gli utenti di Active Directory esistenti nella directory locale.
- Elimina AWS Managed Microsoft AD quando non ti serve più.

Visualizzazione delle informazioni sulla directory AWS Managed Microsoft AD

È possibile utilizzare il Console di gestione AWS per visualizzare i dettagli della directory AWS Managed Microsoft AD, ad esempio:

- Tipo di directory
- ID della directory
- Stato della directory
- Dettagli di rete per AWS Managed Microsoft AD come:
  - Amazon VPC
  - Sottoreti
  - Zone di disponibilità
  - Indirizzi DNS

Puoi trovare le seguenti informazioni su AWS Managed Microsoft AD:

- Nella scheda Condividi e condividi, puoi condividere il tuo AWS Managed Microsoft AD con altri Account AWS e conoscere i dettagli di rete per i tuoi controller di dominio.
- Nella scheda Gestione applicazioni, puoi abilitare un URL di accesso all'applicazione per AWS Managed Microsoft AD e abilitare AWS applicazioni e servizi per AWS Managed Microsoft AD.

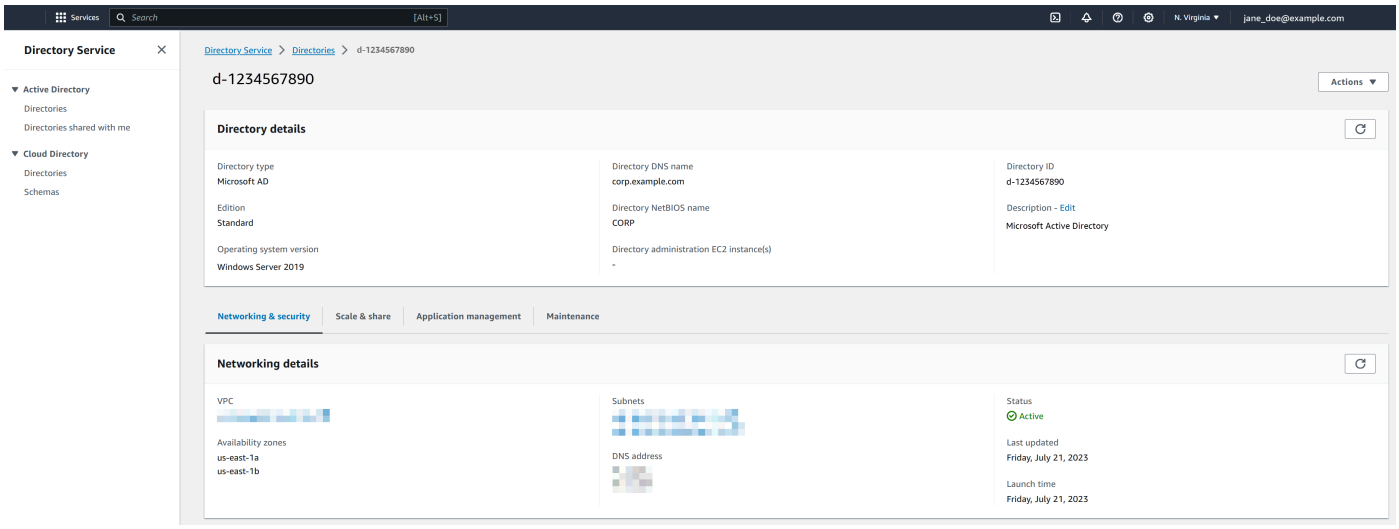
- Nella scheda Maintenance, puoi abilitare Amazon Simple Notification Service per ricevere notifiche sullo stato del tuo AWS Managed Microsoft AD e rivedere gli snapshot del tuo AWS Managed Microsoft AD.
- Per ulteriori informazioni sul campo Status (Stato), consultare Informazioni sullo stato della directory AWS Managed Microsoft AD.

È possibile visualizzare le informazioni sulla directory AWS Managed Microsoft AD utilizzando Console di gestione AWSAWS CLI, oPowerShell:

Console di gestione AWS

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory. Le informazioni sulla directory vengono visualizzate nella sezione Dettagli della directory.



AWS CLI

Per visualizzare informazioni dettagliate sulle directory con AWS CLI

- Aprire ilAWS CLI. Per visualizzare le informazioni sulla directory AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
aws ds describe-directories --directory-id d-1234567890 --output table
```

Per ulteriori informazioni, consulta describe-directories.

PowerShell

Per visualizzare informazioni dettagliate sulla directory con PowerShell

- Aprire PowerShell. Per visualizzare le informazioni sulla directory AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
(Get-DSDirectory -DirectoryId d-1234567890 |
    ForEach-Object {$_, $_.RegionsInfo, $_.VpcSettings}) |
Format-List *
```

Per ulteriori informazioni, consulta Get-DSDirectory.

Ripristino di AWS Managed Microsoft AD con istantanee

AWS Directory Serviceoffre istantanee giornaliere automatizzate e la possibilità di scattare istantanee manuali dei dati per il tuo AWS Microsoft AD Active Directory gestito. Queste istantanee possono essere utilizzate per eseguire un point-in-time ripristino di Active Directory. Hai un limite di cinque istantanee manuali per ogni AWS Managed Microsoft AD Active Directory. Se hai già raggiunto questo limite, devi eliminare una delle istantanee manuali esistenti prima di poterne creare un'altra. Non è possibile acquisire snapshot del connettore AD.

> **Note**
>
> Snapshot è una funzionalità globale di AWS Managed Microsoft AD. Se utilizzi Configurazione della replica multiarea per Managed AWS Microsoft AD, è necessario eseguire le seguenti procedure in Regione principale. Le modifiche verranno applicate automaticamente in tutte le Regioni replicate. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Argomenti

- Creazione di uno snapshot della directory
- Ripristino della directory da uno snapshot
- Eliminazione di uno snapshot

Creazione di uno snapshot della directory

Uno snapshot può essere utilizzato per riportare la tua directory a quello che era nel momento in cui è stato creato lo snapshot. Per creare uno snapshot manuale della tua directory, esegui la procedura seguente.

> **Note**
>
> Hai un limite di 5 snapshot manuali per ogni directory. Se hai già raggiunto questo limite, devi eliminare una delle istantanee manuali esistenti prima di poterne creare un'altra.

Utilizzare la procedura seguente per creare un'istantanea manuale di AWS Managed Microsoft AD con Console di gestione AWSAWS CLI, oPowerShell:

Console di gestione AWS

Per creare un'istantanea manuale in Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettagli della directory, scegli la scheda Manutenzione.
4. Nella sezione Snapshots (Snapshot) scegliere Actions (Operazioni), quindi selezionare Create snapshot (Crea snapshot).
5. Se lo si desidera, nella finestra di dialogo Create directory snapshot (Crea snapshot della directory) è possibile dare un nome allo snapshot. Quando pronto, scegli Create (Crea).

AWS CLI

Per creare un'istantanea manuale con AWS CLI

- Aprire il. AWS CLI Per creare un'istantanea del tuo AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory di Microsoft AD AWS gestito:

```
aws ds create-snapshot --directory-id d-1234567890 --name ManualSnapshot
```

Per ulteriori informazioni, consulta `create-snapshot`.

PowerShell

Per creare un'istantanea manuale con PowerShell

- Aprire PowerShell. Per creare un'istantanea del tuo AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory di Microsoft AD AWS gestito:

```
New-DSSnapshot -DirectoryId d-1234567890 -Name ManualSnapshot
```

Per ulteriori informazioni, consulta `New-DSSnapshot`.

A seconda delle dimensioni della directory, possono essere necessari alcuni minuti per creare lo snapshot. Quando lo snapshot è pronto, il valore Status (Stato) cambia in `Completed`.

Ripristino della directory da uno snapshot

Il ripristino di una directory da uno snapshot equivale a spostare la directory indietro nel tempo. Gli snapshot di directory sono univoci nella directory da cui sono stati creati. È possibile ripristinare uno snapshot solo nella directory da cui è stato creato. Inoltre, l'età massima supportata di un'istantanea manuale è di 180 giorni. Per ulteriori informazioni, vedi Durata utile di un backup dello stato del sistema di Active Directory sul sito Web. Microsoft

> **Warning**
>
> Consigliamo di contattare il centro del Supporto AWS prima che uno snapshot venga ripristinato, potremmo essere in grado di aiutarti per non dover ripristinare uno snapshot. Ogni ripristino da uno snapshot può risultare in perdita di dati come sono in un momento specifico. È importante comprendere che tutti i server DNS associati alla directory saranno offline fino al completamento dell'operazione di ripristino. DCs

Utilizzare la procedura seguente per ripristinare la directory da un'istantanea utilizzando Console di gestione AWSAWS CLI, o: PowerShell

Console di gestione AWS

Per ripristinare una directory da un'istantanea in Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettagli della directory, scegli la scheda Manutenzione.
4. Nella sezione Snapshots (Snapshot) selezionare uno snapshot dall'elenco, scegliere Actions (Operazioni), quindi selezionare Restore snapshot (Ripristina snapshot).
5. Verificare le informazioni nella finestra di dialogo Restore directory snapshot (Ripristina snapshot di directory), quindi scegliere Restore (Ripristina).

AWS CLI

Per ripristinare una directory da un'istantanea con AWS CLI

1. Aprire il. AWS CLI Per elencare le istantanee per il tuo AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory di Microsoft AD AWS gestito:

```
aws ds describe-snapshots --directory-id d-1234567890 \
  --query '(sort_by(Snapshots[*].
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \
  --output table
```

2. Per ripristinare AWS Managed Microsoft AD da un'istantanea, puoi usare il `restore-from-snapshot`comando. Assicurati di sostituire il `snapshot-id` parametro con l'ID snapshot che desideri utilizzare per ripristinare AWS Managed Microsoft AD:

```
aws ds restore-from-snapshot --snapshot-id s-1234567890
```

PowerShell

Per ripristinare una directory da un'istantanea con PowerShell

1. Aprire PowerShell. Per elencare le istantanee per il tuo AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory di Microsoft AD AWS gestito:

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. Per ripristinare AWS Managed Microsoft AD da un'istantanea, puoi usare il `Restore-DSFromSnapshot`comando. Assicurati di sostituire il `snapshot-id` parametro con l'ID snapshot che desideri utilizzare per ripristinare AWS Managed Microsoft AD:

```
Restore-DSFromSnapshot -SnapshotId s-1234567890
```

Per una directory Microsoft AD AWS gestita, il ripristino della directory può richiedere da due a tre ore. Una volta ripristinato correttamente, il valore Status (Stato) della directory passa a `Active`. Qualsiasi modifica apportata alla directory dopo la data di snapshot verrà sovrascritta.

Eliminazione di uno snapshot

Utilizza la procedura seguente per eliminare un'istantanea del tuo AWS Managed Microsoft AD con Console di gestione AWSAWS CLI, oPowerShell:

Console di gestione AWS

Per eliminare un'istantanea in Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.

3. Nella pagina Dettagli della directory, scegli la scheda Manutenzione.
4. Nella sezione Snapshots (Snapshot) scegliere Actions (Operazioni), quindi selezionare Delete snapshot (Elimina snapshot).
5. Verificare di voler eliminare lo snapshot, quindi scegliere Delete (Elimina).

AWS CLI

Per eliminare un'istantanea con AWS CLI

1. Aprire il. AWS CLI Per elencare le istantanee per il tuo AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory di Microsoft AD AWS gestito:

```
aws ds describe-snapshots --directory-id d-1234567890 \
  --query '(sort_by(Snapshots[*].
{ID:SnapshotId,Status:Status,Type:Type,StartTime:StartTime}, &StartTime))' \
  --output table
```

2. Per eliminare un'istantanea del tuo AWS Managed Microsoft AD, puoi usare il `delete-snapshot`comando. Assicurati di sostituire il `snapshot-id` parametro con l'ID dell'istantanea che desideri eliminare:

```
aws ds delete-snapshot --snapshot-id s-1234567890
```

PowerShell

Per eliminare un'istantanea con PowerShell

1. Aprire PowerShell. Per elencare le istantanee per il tuo AWS Managed Microsoft AD, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory di Microsoft AD AWS gestito:

```
Get-DSSnapshot -DirectoryId d-1234567890 | Sort-Object StartTime | Format-Table
```

2. Per ripristinare AWS Managed Microsoft AD da un'istantanea, puoi usare il `Remove-DSnapshot`comando. Assicurati di sostituire il `snapshot-id` parametro con l'ID dell'istantanea che desideri eliminare:

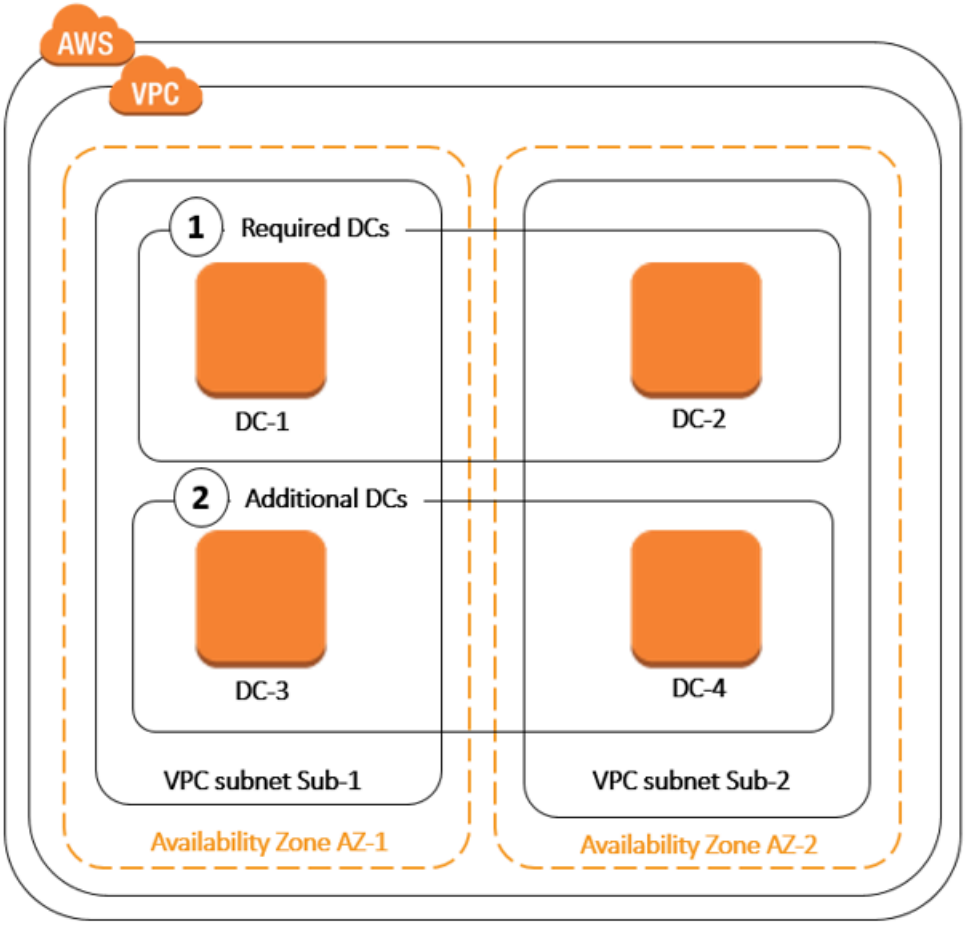
```
Remove-DSSnapshot -SnapshotId s-1234567890
```

Implementazione di controller di dominio aggiuntivi per Managed AWS Microsoft AD

L'implementazione di controller di dominio aggiuntivi per Managed AWS Microsoft AD aumenta la ridondanza, il che si traduce in una resilienza e una disponibilità ancora maggiori. Questo inoltre consente di migliorare le prestazioni della tua directory, sostenendo un maggior numero di richieste di Active Directory. Ad esempio, ora puoi utilizzare AWS Managed Microsoft AD per supportare più applicazioni.NET distribuite su grandi flotte di istanze Amazon EC2 e Amazon RDS for SQL Server.

Quando si crea la directory per la prima volta, AWS Managed Microsoft AD distribuisce due controller di dominio in più zone di disponibilità, il che è necessario per scopi di elevata disponibilità. Successivamente, è possibile distribuire facilmente controller di dominio aggiuntivi tramite la Directory Service console semplicemente specificando il numero totale di controller di dominio desiderati. AWSMicrosoft AD gestito distribuisce i controller di dominio aggiuntivi nelle zone di disponibilità e nelle sottoreti Amazon VPC su cui è in esecuzione la directory.

Ad esempio, nella seguente illustrazione, DC-1 e DC-2 rappresentano i due controller di dominio creati originariamente con la directory. La Directory Service console fa riferimento a questi controller di dominio predefiniti come obbligatori. AWSMicrosoft AD gestito colloca intenzionalmente ciascuno di questi controller di dominio in zone di disponibilità separate durante il processo di creazione della directory. In seguito, potresti decidere di aggiungere due ulteriori controller di dominio per aiutare a distribuire il carico di autenticazione su tempi di login di picco. DC-3 e DC-4 rappresentano il nuovo controller di dominio, a cui la console ora fa riferimento come Additional (Aggiuntivo). Come in precedenza, AWS Managed Microsoft AD colloca nuovamente automaticamente i nuovi controller di dominio in diverse zone di disponibilità per garantire l'elevata disponibilità del dominio.



Grazie a questo processo, non è più necessario configurare manualmente la replica della directory, gli snapshot automatizzati giornalieri o il monitoraggio dei dati della directory per i controller di dominio aggiuntivi. Inoltre, è più facile migrare ed eseguire carichi di lavoro mission critical integrati in Active Directory Cloud AWS senza dover implementare e mantenere la propria infrastruttura Active Directory.

Puoi utilizzare uno dei seguenti strumenti per distribuire o rimuovere controller di dominio aggiuntivi in Managed AWS Microsoft AD:

- `update-number-of-domain-controllers`AWS CLIcomando
- API UpdateNumberOfDomainControllers
- Aggiungere o rimuovere controller di dominio aggiuntivi con Console di gestione AWS

> **Note**
>
> I controller di dominio aggiuntivi sono una funzionalità regionale di AWS Managed Microsoft AD. Se si utilizza la replica multiregione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Aggiungere o rimuovere controller di dominio aggiuntivi con Console di gestione AWS

Puoi utilizzare il Console di gestione AWS per aggiungere o rimuovere controller di dominio aggiuntivi al tuo AWS Managed Microsoft AD.

Prerequisiti

Prima di aggiungere o rimuovere controller di dominio aggiuntivi a AWS Managed Microsoft AD, ecco ulteriori informazioni sui requisiti dei controller di dominio:

- Dopo la distribuzione dei controller di dominio aggiuntivi, puoi ridurre il numero di controller di dominio a due, ovvero al minimo necessario agli scopi di tolleranza ai guasti ed elevata disponibilità.
- I controller di dominio eliminati verranno eliminati dall'elenco dei controller di dominio aggiuntivi. I controller di dominio primario e secondario sono obbligatori e non possono essere eliminati.
- Se hai configurato AWS Managed Microsoft AD per abilitare LDAPS, anche tutti i controller di dominio aggiuntivi che aggiungi avranno LDAPS abilitato automaticamente. Per ulteriori informazioni, consulta Abilita Secure LDAP o LDAPS.

Procedura

Utilizza la procedura seguente per distribuire o rimuovere controller di dominio aggiuntivi nel tuo AWS Managed Microsoft AD con Console di gestione AWSAWS CLI, o. PowerShell

Console di gestione AWS

Per aggiungere o rimuovere controller di dominio aggiuntivi con Console di gestione AWS

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.

3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui desideri aggiungere o rimuovere i controller di dominio, quindi scegli la scheda Dimensiona e condividi. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Dimensiona e condividi.

4. Nella sezione Domain controllers (Controller dominio), seleziona Edit (Modifica).
5. Specifica il numero di controller di dominio da aggiungere o rimuovere dalla directory, quindi seleziona Modify (Modifica).
6. Quando AWS Managed Microsoft AD completa il processo di distribuzione, tutti i controller di dominio mostrano lo stato Attivo e vengono visualizzate sia la zona di disponibilità assegnata che le sottoreti Amazon VPC. I nuovi controller di dominio vengono distribuiti in modo uniforme tra le zone di disponibilità e le sottoreti in cui la directory è già stata distribuita.

AWS CLI

Per aggiungere o rimuovere controller di dominio aggiuntivi con AWS CLI

1. Aprire il. AWS CLI Per verificare il numero attuale di controller di dominio, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
aws ds describe-directories --directory-id d-1234567890 | grep
 DesiredNumberOfDomainControllers
```

2. Per aggiungere o rimuovere controller di dominio, puoi usare il `update-number-of-domain-controllers`comando. Ad esempio, è possibile utilizzare il comando seguente per impostare il numero totale di controller di dominio su 4. Assicurati di sostituire l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito e il `desired-number` parametro con il numero di controller di dominio che desideri distribuire.

```
aws ds update-number-of-domain-controllers --directory-id d-1234567890 --
desired-number 4
```

PowerShell

Per aggiungere o rimuovere controller di dominio aggiuntivi con PowerShell

1. Aprire PowerShell. Per verificare il numero attuale di controller di dominio, esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
Get-DSDirectory -DirectoryId d-1234567890 | Select-Object
 DesiredNumberOfDomainControllers
```

2. Per aggiungere o rimuovere controller di dominio, puoi usare il `Set-DSDomainControllerCount`comando. Ad esempio, è possibile utilizzare il comando seguente per impostare il numero totale di controller di dominio su 4. Assicurati di sostituire l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito e il `DesiredNumber` parametro con il numero di controller di dominio che desideri distribuire.

```
Set-DSDomainControllerCount -DirectoryId d-1234567890 -DesiredNumber 4
```

Articolo correlato del blog AWS sulla sicurezza

- Come aumentare la ridondanza e le prestazioni di Directory Service for Managed AWS Microsoft AD aggiungendo controller di dominio

Aggiornamento di Managed AWS Microsoft AD

Puoi aggiornare la tua edizione Standard AWS Managed Microsoft AD all'edizione Enterprise. Di seguito vengono descritte le differenze tra le edizioni Standard ed Enterprise:

- Standard Edition: Microsoft AD gestito da AWS (Standard Edition) è ottimizzato per essere una directory primaria per piccole e medie imprese con massimo 5.000 dipendenti. Fornisce una capacità di storage sufficiente per supportare fino a 30.000* oggetti di directory, come utenti, gruppi e computer.
- Enterprise Edition: Microsoft AD gestito da AWS (Enterprise Edition) è stato progettato per supportare le grandi organizzazioni con massimo 500.000* oggetti directory.

* I limiti sopra indicati sono approssimativi. La directory potrebbe supportare più o meno oggetti di directory a seconda della dimensioni degli oggetti e della necessità di prestazioni e comportamento delle applicazioni.

Per aggiornare l'edizione Standard AWS Managed Microsoft AD all'edizione Enterprise, UpdateDirectorySetuputilizzala dall'API, update-directory-setupda o DSDirectoryUpdate-Setup da AWS Strumenti per PowerShell. AWS CLI

API

Per aggiornare l'edizione Standard AWS Managed Microsoft AD all'edizione Enterprise:

```
{
   "DirectoryId": "d-1234567890",
   "UpdateType": "SIZE",
   "DirectorySizeUpdateSettings": {
      "DirectorySize": "Large"
   }
}
```

AWS CLI

Per aggiornare l'edizione Standard AWS Managed Microsoft AD all'edizione Enterprise:

```
aws ds update-directory-setup \
    --directory-id d-1234567890 \
    --update-type SIZE \
    --directory-size-update-settings DirectorySize=Large
```

PowerShell

Per aggiornare l'edizione Standard AWS Managed Microsoft AD all'edizione Enterprise:

```
Update-DSDirectorySetup `
    -DirectoryId d-9a676e4148 `
    -UpdateType SIZE `
    -DirectorySizeUpdateSettings_DirectorySize Large
```

Note

La replica multiarea è disponibile solo nell'edizione AWS Managed Microsoft AD Enterprise per le seguenti aree:

- Stati Uniti orientali (Ohio)
- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Asia Pacifico (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tailandia)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Cina (Pechino)
- Cina (Ningxia)
- Messico (centrale)
- Europa (Francoforte)
- Europa (Irlanda)
- Europe (London)
- Europe (Paris)
- Europa (Stoccolma)
- Sud America (San Paolo)
- AWS GovCloud (Stati Uniti occidentali)
- AWS GovCloud (Stati Uniti orientali)

Ci sono alcune limitazioni da tenere a mente quando si aggiorna Managed AWS Microsoft AD. Questi sono:

- L'aggiornamento comporterà costi aggiuntivi. Per ulteriori informazioni, consulta Prezzi di Directory Service.
- Una volta aggiornato, Active Directory non può essere ripristinato alla versione precedente.
- Le istantanee precedenti non possono essere utilizzate per ripristinare Active Directory dopo l'aggiornamento.
- Gli upgrade avvengono alla data e all'ora pianificate concordate con. Supporto Gli upgrade vengono effettuati dal lunedì al venerdì, dalle 9:00 alle 17:00 ora solare del Pacifico.
- Il processo di aggiornamento richiede da quattro a cinque ore.
- Durante il processo di aggiornamento, i controller di dominio di AWS Managed Microsoft AD vengono aggiornati uno alla volta. Ciò può influire negativamente sulle prestazioni e causare tempi di inattività durante la finestra di manutenzione.
- Il processo di aggiornamento modificherà il nome host di ogni istanza del controller di dominio, ma i relativi indirizzi IP rimarranno invariati.
- Se si utilizza LDAPS (Lightweight Directory Access Protocol over SSL), i controller di dominio avranno bisogno di nuovi certificati.

Aggiornamento del tipo di rete di directory

Puoi aggiornare il tipo di rete della tua Directory Service directory da IPv4 a Dual-stack (and). IPv4 IPv6 L'aggiornamento del tipo di rete per includere gli indirizzi IPv6 IP offre uno spazio di indirizzi più ampio di. IPv4 IPv4 e le IPv6 comunicazioni sono indipendenti l'una dall'altra.

Per i dettagli, consulta la sezione Confronta IPv4 e IPv6 nella Amazon Virtual Private Cloud User Guide.

> **Important**
>
> Si tratta di un'operazione unidirezionale che non può essere annullata. Esegui prima il test in un ambiente non di produzione.

Prerequisiti

Prima di aggiornare il tipo di rete di directory, assicuratevi che siano soddisfatti i seguenti requisiti:

- Il VPC e le sottoreti associate in cui esiste attualmente la directory devono essere configurati con intervalli CIDR. IPv6 Per maggiori dettagli, consulta il IPv6 supporto per il tuo VPC nella Amazon Virtual Private Cloud User Guide.
- Hai accesso amministrativo a. Console di gestione AWS
- La tua directory deve essere in stato attivo.
- Disponi delle autorizzazioni IAM appropriate per modificare Directory Service le impostazioni.

Per aggiornare il tipo di rete delle directory

Per aggiornare la directory alla rete dual-stack

> **Note**
>
> Se la directory viene replicata in più regioni, esegui questo aggiornamento in ciascuna regione.

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Seleziona la directory di destinazione.
3. Vai alla scheda Rete e sicurezza.
4. Scegli Aggiungi IPv6 supporto. Questa opzione è disponibile solo per le directory IPv4 -only.
5. Consulta le informazioni di aggiornamento e i dettagli sui prezzi.
6. Scegli Aggiungi per confermare l'aggiornamento.

Dopo aver avviato l'aggiornamento, lo stato della directory passa a Aggiornamento durante il processo di aggiornamento. Il completamento dell'aggiornamento richiede in genere 15-30 minuti. Una volta completato, lo stato della directory torna ad Attivo.

Aggiungere suffissi UPN alternativi a Managed Microsoft AD AWS

È possibile semplificare la gestione dei nomi di accesso di Active Directory (AD) e migliorare l'esperienza di accesso degli utenti aggiungendo suffissi UPN (User Principal Name) alternativi alla directory Managed AWS Microsoft AD. A tal fine, è necessario aver effettuato l'accesso all'account Amministratore o con un account membro del gruppo Amministratori delegati del suffisso del nome

utente principale AWS . Per ulteriori informazioni su questo gruppo, consulta Cosa viene creato con AWS Managed Microsoft AD.

Aggiunta di suffissi UPN alternativi

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Individua un' EC2 istanza Amazon aggiunta alla tua directory AWS Managed Microsoft AD. Seleziona l'istanza quindi scegli Connect (Connetti).
3. Nella finestra Server Manager, scegli Tools (Strumenti). Successivamente, scegli Domini e trust di Active Directory.
4. Nel riquadro a sinistra, fai clic su Domini e trust di Active Directory, quindi scegli Proprietà.
5. Nella scheda Suffissi UPN, digita un suffisso UPN alternativo (ad esempio **`sales.example.com`**). Scegli Add (Aggiungi) quindi scegli Apply (Applica).
6. Qualora fosse necessario aggiungere altri suffissi UPN alternativi, ripeti il passaggio 5 per il numero di volte necessario.

Ridenominazione del nome del sito della directory AWS Managed Microsoft AD

È possibile rinominare il nome del sito predefinito della directory AWS Managed Microsoft AD in modo che corrisponda ai nomi dei siti Microsoft Active Directory (AD) esistenti. Ciò consente AWS a Managed Microsoft AD di trovare e autenticare più rapidamente gli utenti AD esistenti nella directory locale. Il risultato è un'esperienza migliore quando gli utenti accedono a AWS risorse come Amazon EC2 e Amazon RDS per le istanze di SQL Server che hai aggiunto alla tua directory AWS Managed Microsoft AD.

Per farlo, è necessario essere connessi con l'account Admin o con un account membro del gruppo AWS Delegated Sites and Services Administrators (Amministratori di siti e servizi delegati). Per ulteriori informazioni su questo gruppo, consulta Cosa viene creato con AWS Managed Microsoft AD.

Per ulteriori vantaggi sulla rinominazione del sito in relazione ai trust, consulta Domain Locator Across a Forest Trust nel sito Web di Microsoft.

Per rinominare il nome del sito AWS Managed Microsoft AD

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.

2. Individua un' EC2 istanza Amazon aggiunta alla tua directory AWS Managed Microsoft AD. Seleziona l'istanza quindi scegli Connect (Connetti).
3. Nella finestra Server Manager, scegli Tools (Strumenti). Quindi scegli Active Directory Sites and Services (Servizi e siti Active Directory).
4. Nel riquadro sinistro, espandi la cartella Sites (Siti), fai clic con il pulsante destro del mouse sul nome del sito (l'impostazione predefinita è Default-Site-Name) quindi scegli Rename (Rinomina).
5. Digita il nuovo nome del sito quindi scegli Enter (Invio).

Eliminazione di AWS Managed Microsoft AD

Quando si elimina una directory AWS Managed Microsoft AD, Simple AD o ibrida, tutti i dati e le istantanee della directory vengono eliminati e non possono essere recuperati. Dopo l'eliminazione della directory, tutte le istanze collegate alla directory rimangono intatte. Tuttavia, non puoi utilizzare le credenziali della directory per accedere a queste istanze. È necessario accedere a queste istanze con un account utente che è in locale all'istanza.

Quando una directory del connettore AD viene eliminata, quella on-premise rimane intatta. Anche tutte le istanze collegate alla directory rimangono intatte e collegate alla tua directory on-premise. Puoi, tuttavia, utilizzare le credenziali della directory per accedere a queste istanze.

Eliminazione di una directory

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory. Assicurati di trovarti nel Regione AWS luogo in cui è distribuito Active Directory. Per ulteriori informazioni, consulta Scelta di una regione.
2. Assicurati che nessuna AWS applicazione sia abilitata per la directory che intendi eliminare. AWSLe applicazioni abilitate impediranno l'eliminazione di AWS Managed Microsoft AD o Simple AD.

    a. Nella pagina Directories (Directory), scegli l'ID della directory.

    b. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione). Nella sezione AWSapp e servizi, puoi vedere quali AWS applicazioni sono abilitate per la tua directory.

        - Disabilita Console di gestione AWS l'accesso. Per ulteriori informazioni, consulta Disabilitazione dell'accesso Console di gestione AWS.

- Per disabilitare Amazon WorkSpaces, devi annullare la registrazione del servizio dalla directory nella WorkSpaces console. Per ulteriori informazioni, consulta Eliminare una directory nella Amazon WorkSpaces Administration Guide.
- Per disabilitarlo WorkDocs, devi eliminare il WorkDocs sito nella WorkDocs console. Per ulteriori informazioni, consulta Eliminare un sito nella Amazon WorkDocs Administration Guide.
- Per disabilitare Amazon WorkMail, devi rimuovere l' WorkMail organizzazione Amazon dalla WorkMail console Amazon. Per ulteriori informazioni, consulta Rimuovere un'organizzazione nella Amazon WorkMail Administrator Guide.
- Per disabilitare Amazon FSx for Windows File Server, devi rimuovere il FSx file system Amazon dal dominio. Per ulteriori informazioni, consulta Working with Active Directory in FSx for Windows File Server nella Amazon FSx for Windows File Server User Guide.
- Per disabilitare Amazon Relational Database Service, devi rimuovere l'istanza Amazon RDS dal dominio. Per ulteriori informazioni, consulta Gestione di un'istanza database in un dominio nella Guida per l'utente di Amazon RDS.
- Per disabilitare AWS Client VPN il servizio, è necessario rimuovere il servizio di directory dall'endpoint Client VPN. Per ulteriori informazioni, consulta Work with Client VPN nella AWS Client VPNAdministrator Guide.
- Per disabilitare Amazon Connect, è necessario eliminare l'istanza di Amazon Connect. Per ulteriori informazioni, consulta Eliminare l'istanza Amazon Connect nella Amazon Connect Administration Guide.
- Per disabilitare Amazon Quick Suite, devi annullare l'iscrizione ad Amazon Quick Suite. Per ulteriori informazioni, consulta Chiusura Amazon Quick Suite dell'account nella Guida per l'utente di Amazon Quick Suite.

> **Note**
>
> Se la utilizzi AWS IAM Identity Center e la hai precedentemente connessa alla directory AWS Managed Microsoft AD che intendi eliminare, devi prima modificare l'origine dell'identità prima di poterla eliminare. Per ulteriori informazioni, consulta Modifica della fonte di identità nella Guida per l'utente del Centro identità IAM.

3. Nel riquadro di navigazione, seleziona Directory.

4. Seleziona solo la directory da eliminare, quindi fai clic su Elimina. Sono necessari alcuni minuti per l'eliminazione della directory. Una volta eliminata la directory, viene rimossa dal tuo elenco di directory.

Proteggi il tuo AWS Managed Microsoft AD

Puoi utilizzare criteri di password, funzionalità come l'autenticazione a più fattori (MFA) e impostazioni per proteggere il tuo AWS Managed Microsoft AD. I modi per proteggere la tua directory includono:

- Scopri come funzionano le politiche relative alle password in Active Directory in modo che possano essere applicate agli utenti di AWS Managed Microsoft AD. Puoi anche delegare quale utente può gestire le policy relative alle password di AWS Managed Microsoft AD.
- Abilita l'MFA per aumentare la sicurezza di AWS Managed Microsoft AD.
- >Abilita Lightweight Directory Access Protocol over Secure Socket Layer (SSL) /Transport Layer Security (TLS) (LDAPS) in modo che le comunicazioni su LDAP siano crittografate e migliorino la sicurezza.
- Gestisci la conformità di AWS Managed Microsoft AD con standard come Federal Risk and Authorization Management Program (FedRAMP) e Payment Card Industry (PCI) Data Security Standard (DSS).
- Migliora la configurazione di sicurezza della rete AWS Managed Microsoft AD> modificando AWS Security Group per soddisfare le esigenze del tuo ambiente.
- Modifica le impostazioni di sicurezza della directory AWS Managed Microsoft AD come Certificate Base Authentication, Secure Channel Cipher e Protocol per soddisfare le tue esigenze.
- Configura AWS Autorità di certificazione privata Connector for AD in modo da poter emettere e gestire certificati per AWS Managed Microsoft AD con AWS Private CA.

Informazioni sui criteri di AWS gestione delle password di Microsoft AD

AWS Managed Microsoft AD consente di definire e assegnare diversi criteri di blocco delle password e degli account (denominati anche criteri granulari per le password) per i gruppi di utenti gestiti nel dominio Microsoft AD gestito AWS . Quando si crea una directory Microsoft AD AWS gestita, viene creata e applicata una politica di dominio predefinita ad Active Directory. Questa policy include le seguenti impostazioni:

Policy	Impostazione
Applica la cronologia delle password	24 password ricordate
Durata massima delle password	42 giorni *
Durata minima delle password	1 giorno
Lunghezza minima delle password	7 caratteri
Le password devono soddisfare i requisiti di complessità	Abilitato
Archivia le password utilizzando una crittografia reversibile	Disabilitato

> **Note**
>
> * La durata massima della password di 42 giorni include la password di amministratore.

Ad esempio, puoi assegnare un'impostazione di policy meno rigida per i dipendenti che hanno accesso solo a informazioni a bassa sensibilità. Per i responsabili senior che accedono regolarmente a informazioni riservate puoi applicare impostazioni più rigide.

Le seguenti risorse forniscono ulteriori informazioni sulle politiche granulari in materia di password e sulle politiche di sicurezza di Microsoft Active Directory:

- Configurare le impostazioni dei criteri di sicurezza
- Requisiti di complessità delle password
- Complessità delle password: considerazioni sulla sicurezza

AWS fornisce una serie di criteri granulari per le password in Managed AWS Microsoft AD che puoi configurare e assegnare ai tuoi gruppi. Per configurare le politiche, è possibile utilizzare strumenti di Microsoft policy standard come il Centro di amministrazione di Active Directory. Per iniziare a utilizzare gli strumenti relativi alle Microsoft policy, consultaInstallazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.

Come vengono applicate le politiche relative alle password

Esistono differenze nel modo in cui vengono applicate le politiche granulari in materia di password a seconda che la password sia stata reimpostata o modificata. Gli utenti del dominio possono modificare la propria password. Un amministratore o un utente di Active Directory con le autorizzazioni necessarie può reimpostare le password degli utenti. Per ulteriori informazioni, consulta la tabella seguente.

Policy	Reimpostazione della password	Modifica della password
Applica la cronologia delle password	 No	 Sì
Durata massima delle password	 Sì	 Sì
Durata minima delle password	 No	 Sì
Lunghezza minima delle password	 Sì	 Sì
Le password devono soddisfare i requisiti di complessità	 Sì	 Sì

Queste differenze hanno implicazioni in termini di sicurezza. Ad esempio, ogni volta che la password di un utente viene reimpostata, le politiche relative all'applicazione della cronologia delle password e all'età minima della password non vengono applicate. Per ulteriori informazioni, consulta la documentazione Microsoft sulle considerazioni di sicurezza relative all'applicazione della cronologia delle password e dei criteri relativi all'età minima delle password.

Impostazioni delle policy supportate

AWS Microsoft AD gestito include cinque policy dettagliate con un valore di precedenza non modificabile. Le policy dispongono di una serie di proprietà che puoi configurare per applicare la forza della password e delle operazioni di blocco account in caso di errori di login. Puoi assegnare le policy per zero o più gruppi di Active Directory. Se un utente finale è un membro di più gruppi e riceve più di una policy di password, Active Directory applica la policy con il valore di priorità più basso.

AWS politiche predefinite in materia di password

Nella tabella seguente sono elencate le cinque politiche incluse nella directory AWS Managed Microsoft AD e il valore di precedenza assegnato. Per ulteriori informazioni, consulta Priorità.

Nome policy	Priorità
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

Proprietà delle policy sulle password

Puoi modificare le seguenti proprietà nelle tue policy sulle password per conformarti allo standard di conformità che meglio soddisfa le tue esigenze aziendali.

- Nome policy
- Applica la cronologia delle password
- Lunghezza minima delle password

- Durata minima delle password
- Durata massima delle password
- Archivia le password utilizzando una crittografia reversibile
- Le password devono soddisfare i requisiti di complessità

Non puoi modificare i valori di priorità di queste policy. Per ulteriori dettagli su come queste impostazioni influiscono sull'applicazione delle password, consulta AD DS: criteri granulari per le password sul sito Web Microsoft. TechNet Per informazioni generali su questi criteri, vedere Criteri relativi alle password sul TechNet sito Web di Microsoft.

Policy sul blocco degli account

Puoi anche modificare le seguenti proprietà delle tue policy sulle password per specificare se e come Active Directory debba bloccare un account dopo errori di accesso:

- Numero di tentativi di accesso non riusciti permesso
- Durata del blocco di un account
- Reimposta tentativi di accesso non riusciti dopo un certo periodo di tempo

Per informazioni generali su questi criteri, vedere Criteri di blocco degli account sul TechNet sito Web di Microsoft.

Priorità

Le policy con un valore di priorità inferiore hanno maggiore priorità. Assegna le policy sulle password ai gruppi di sicurezza di Active Directory. Mentre è necessario applicare una singola policy a un gruppo di sicurezza, un singolo utente può ricevere più di una policy sulle password. Ad esempio, supponiamo che `jsmith` sia un membro del gruppo HR e anche membro del gruppo MANAGER. Se assegni CustomerPSO-05 (che ha una priorità di 50) al gruppo HR e CustomerPSO-04 (che ha una priorità di 40) ai MANAGER, CustomerPSO-04 ha la priorità più alta e Active Directory applica tale policy a `jsmith`.

Se assegni più policy a un utente o gruppo, Active Directory determina la policy risultante come segue:

1. Si applica una policy che assegni direttamente all'oggetto utente.
2. Se nessuna policy viene assegnata direttamente all'oggetto utente, viene applicata la policy con la priorità più bassa di tutte le policy ricevute dall'utente in virtù dell'appartenenza al gruppo.

Per ulteriori dettagli, consulta AD DS: politiche granulari per le password sul sito Web di Microsoft. TechNet

Argomenti

- Assegnazione di criteri di password agli utenti di Microsoft AD AWS gestiti
- Delegare chi può gestire le policy relative alle password di AWS Managed Microsoft AD

Articolo correlato AWS del blog sulla sicurezza

- Come configurare politiche di password ancora più rigorose per soddisfare gli standard di sicurezza utilizzando Directory ServiceAWS Managed Microsoft AD

Assegnazione di criteri di password agli utenti di Microsoft AD AWS gestiti

Gli account utente che sono membri del gruppo di sicurezza degli Amministratori delegati AWS per le policy granulari sulle password possono utilizzare la procedura seguente per assegnare le policy agli utenti e ai gruppi di sicurezza.

Assegnazione delle policy sulle password ai tuoi utenti

1. Avvia il centro amministrativo di Active Directory (ADAC) da qualsiasi EC2 istanza gestita a cui hai aggiunto il tuo dominio Microsoft AD AWS gestito.
2. Passa alla Visualizzazione ad albero e vai a System\Password Settings Container (Sistema \Contenitore delle impostazioni delle password).
3. Fai doppio clic sulla policy fine-grained che desideri modificare. Fai clic su Add (Aggiungi) per modificare le proprietà della policy e aggiungi gli utenti o i gruppi di sicurezza alla policy. Per ulteriori informazioni sulle policy granulari predefinite fornite da Microsoft AD gestito da AWS , consulta AWS politiche predefinite in materia di password.
4. Per verificare che la politica in materia di password sia stata applicata, esegui il PowerShell comando seguente:

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

> **Note**
>
> Evita di utilizzare il comando `net user` poiché i risultati potrebbero essere imprecisi.

Se non si configura nessuna delle cinque politiche relative alle password nella directory AWS gestita di Microsoft AD, Active Directory utilizza la politica di gruppo di domini predefinita. Per ulteriori informazioni sull'utilizzo del Password Settings Container (Contenitore delle impostazioni delle password), consulta questo post del blog Microsoft.

Delegare chi può gestire le policy relative alle password di AWS Managed Microsoft AD

È possibile delegare le autorizzazioni per la gestione delle policy relative alle password a specifici account utente creati in Managed AWS Microsoft AD aggiungendo gli account al gruppo di sicurezza AWS Delegated Fine Grained Password Policy Administrators. Quando un account diventa un membro di questo gruppo, l'account dispone di autorizzazioni per modificare e configurare una qualsiasi delle policy sulle password elencate in precedenza.

Delega di chi può gestire le tue policy sulle password

1. Avvia il centro amministrativo di Active Directory (ADAC) da qualsiasi EC2 istanza gestita a cui hai aggiunto il tuo dominio Microsoft AD AWS gestito.
2. Passa alla Visualizzazione ad albero e naviga fino all'UO di Gruppi delegati AWS . Per ulteriori informazioni sull'UO, consulta Cosa viene creato con AWS Managed Microsoft AD.
3. Cerca il gruppo utenti di Amministratori delegati AWS per le policy granulari sulle password. Aggiungi utenti o gruppi dal tuo dominio a questo gruppo.

Abilitazione dell'autenticazione a più fattori per AWS Managed Microsoft AD

Puoi abilitare l'autenticazione a più fattori (MFA) per la tua directory AWS Managed Microsoft AD per aumentare la sicurezza quando gli utenti specificano le proprie credenziali AD per accedere alle applicazioni Amazon Enterprise supportate. Quando si abilita la MFA, gli utenti inseriscono i propri nome utente e password (primo fattore) come di consueto, quindi devono inserire anche un codice di autenticazione (secondo fattore), fornito dalla soluzione MFA virtuale o dell'hardware. Tutti questi fattori forniscono maggiore sicurezza impedendo l'accesso alle applicazioni Amazon Enterprise, a meno che gli utenti non forniscano credenziali valide e un codice MFA valido.

Per abilitare MFA, è necessario disporre di una soluzione MFA che funge da server Remote Authentication Dial-In User Service (RADIUS) oppure disporre di un plug-in MFA per un server RADIUS già implementato nell'infrastruttura on-premise. La soluzione MFA deve implementare i codici d'accesso monouso (OTP, One Time Passcode) che gli utenti ottengono da un dispositivo hardware o dal software in esecuzione su un dispositivo, ad esempio un telefono cellulare.

RADIUS è un client/server protocollo standard del settore che fornisce l'autenticazione, l'autorizzazione e la gestione contabile per consentire agli utenti di connettersi ai servizi di rete. AWS Microsoft AD gestito include un client RADIUS che si connette al server RADIUS su cui è stata implementata la soluzione MFA. Il server RADIUS convalida il nome utente e il codice OTP. Se il server RADIUS convalida correttamente l'utente, AWS Managed Microsoft AD autentica l'utente con Active Directory. Una volta completata l'autenticazione con Active Directory, gli utenti possono quindi accedere all'applicazione. AWS La comunicazione tra il client Microsoft AD RADIUS AWS gestito e il server RADIUS richiede la configurazione di gruppi AWS di sicurezza che abilitano la comunicazione sulla porta 1812.

È possibile abilitare l'autenticazione a più fattori per la directory AWS Managed Microsoft AD eseguendo la procedura seguente. Per ulteriori informazioni su come configurare il server RADIUS per il funzionamento con Directory Service e MFA, consulta Prerequisiti dell'autenticazione a più fattori.

Considerazioni

Di seguito sono riportate alcune considerazioni sull'autenticazione a più fattori per Managed AWS Microsoft AD:

- L'autenticazione a più fattori non è disponibile per Simple AD. Tuttavia, MFA può essere abilitato per la directory AD Connector. Per ulteriori informazioni, consulta Abilitazione dell'autenticazione a più fattori per AD Connector.
- MFA è una funzionalità regionale di Managed AWS Microsoft AD. Se si utilizza la replica multiarea, sarà possibile utilizzare l'autenticazione a più fattori solo nell'area principale di Managed Microsoft AD AWS .
- Se intendi utilizzare AWS Managed Microsoft AD per comunicazioni esterne, ti consigliamo di configurare un gateway Internet NAT (Network Address Translation) o un gateway Internet esterno alla AWS rete per queste comunicazioni.
  - Se desideri supportare le comunicazioni esterne tra il tuo AWS Managed Microsoft AD e il tuo server RADIUS ospitato sulla AWS rete, contatta Supporto.

- Tutte le applicazioni IT di Amazon Enterprise WorkSpaces WorkDocs, tra cui Amazon WorkMail, Amazon Quick Suite, e l'accesso AWS IAM Identity Center e Console di gestione AWS sono supportati quando si utilizza AWS Managed Microsoft AD e AD Connector con MFA. Queste AWS applicazioni che utilizzano MFA non sono supportate in più aree.

  Per ulteriori informazioni, vedere Come abilitare l'autenticazione a più fattori per AWS i servizi utilizzando AWS Managed Microsoft AD e credenziali locali.

  - Per informazioni su come configurare l'accesso utente di base alle applicazioni Amazon Enterprise, AWS Single Sign-On e l' Console di gestione AWS utilizzo Directory Service, consulta Accesso ad AWS applicazioni e servizi dal tuo AWS Managed Microsoft AD e. Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite
  - Consulta il seguente post sul AWS Security Blog per scoprire come abilitare l'autenticazione a più fattori per WorkSpaces gli utenti Amazon su Managed AWS Microsoft AD, come abilitare l'autenticazione a più fattori per AWS i servizi utilizzando Managed AWS Microsoft AD e credenziali locali

Abilitazione dell'autenticazione a più fattori per Microsoft AD gestito da AWS

La procedura seguente mostra come abilitare l'autenticazione a più fattori per AWS Managed Microsoft AD.

1. Identifica l'indirizzo IP del tuo server RADIUS MFA e della tua directory AWS Managed Microsoft AD.
2. Modifica i gruppi di sicurezza Virtual Private Cloud (VPC) per abilitare le comunicazioni sulla porta 1812 tra gli endpoint IP AWS Microsoft AD gestiti e il server MFA RADIUS.
3. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
4. Scegli il link ID della directory per la tua directory AWS Managed Microsoft AD.
5. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi abilitare MFA, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
6. Nella sezione Multi-factor authentication (Autenticazione a più fattori) selezionare Actions (Operazioni), quindi Enable (Abilita).

7. Fornire i seguenti valori nella pagina Enable multi-factor authentication (MFA) (Abilita l'autenticazione a più fattori (MFA)):

   Display label (Visualizza etichetta)

   Indicare un nome per l'etichetta.

   RADIUS server DNS name or IP addresses (Indirizzi IP o nome DNS del server RADIUS)

   Gli indirizzi IP degli endpoint del server RADIUS o l'indirizzo IP del sistema di bilanciamento del carico del server RADIUS. Puoi inserire più indirizzi IP separandoli con una virgola, ad esempio `192.0.0.0,192.0.0.12`.

   > **Note**
   >
   > RADIUS MFA è applicabile solo per autenticare l'accesso a o ad applicazioni e servizi Amazon Enterprise come Amazon Quick Suite o WorkSpaces Amazon Chime. Console di gestione AWS Le applicazioni e i servizi Amazon Enterprise sono supportati nella regione principale solo se la replica multiregione è configurata per Managed AWS Microsoft AD. Non fornisce MFA ai carichi di lavoro Windows in esecuzione su EC2 istanze o per l'accesso a un'istanza. EC2 Directory Service non supporta l'autenticazione RADIUS Challenge/Response.
   > Quando inseriscono nome utente e password, gli utenti devono disporre del proprio codice MFA. In alternativa, è necessario utilizzare una soluzione che esegua l'autenticazione a più fattori, out-of-band ad esempio notifiche push o password monouso (OTP) di autenticazione per l'utente. Nelle soluzioni out-of-band MFA, è necessario assicurarsi di impostare il valore di timeout RADIUS in modo appropriato per la soluzione in uso. Quando si utilizza una soluzione out-of-band MFA, la pagina di accesso richiederà all'utente un codice MFA. In questo caso, gli utenti devono inserire la loro password nel campo password e nel campo MFA.

   Porta

   La porta utilizzata dal server RADIUS per le comunicazioni. La rete locale deve consentire il traffico in entrata attraverso la porta server RADIUS predefinita (UDP:1812) dai server. Directory Service

Shared secret code (Codice segreto condiviso)

Il codice segreto condiviso specificato quando sono stati creati gli endpoint RADIUS.

Confirm shared secret code (Conferma codice segreto condiviso)

Conferma il codice segreto condiviso per gli endpoint RADIUS.

Protocollo

Seleziona il protocollo specificato quando sono stati creati gli endpoint RADIUS.

Server timeout (in seconds) (Timeout del server (in secondi))

Il periodo di tempo, in secondi, per cui il server RADIUS attende una risposta. Il valore deve essere compreso tra 1 e 50.

> **Note**
>
> Ti consigliamo di configurare il timeout del server RADIUS su un massimo di 20 secondi. Se il timeout supera i 20 secondi, il sistema non può riprovare con un altro server RADIUS e potrebbe causare un errore di timeout.

Max RADIUS request retries (Numero massimo di tentativi di richieste RADIUS)

Il numero di volte per cui viene tentata la comunicazione con il server RADIUS. Il valore deve essere compreso tra 0 e 10.

L'autenticazione a più fattori è disponibile se RADIUS Status (Stato RADIUS) viene modificato in Enabled (Abilitato).

8. Scegli Abilita .

Abilita Secure LDAP o LDAPS

Lightweight Directory Access Protocol (LDAP) è un protocollo di comunicazioni standard utilizzato per leggere e scrivere dati in e da Active Directory. Alcune applicazioni utilizzano LDAP per aggiungere, eliminare o cercare utenti e gruppi in Active Directory o per il trasferimento delle credenziali per l'autenticazione degli utenti in Active Directory. Ogni comunicazione LDAP include un client (ad esempio un'applicazione) e un server (ad esempio Active Directory).

Per impostazione predefinita, le comunicazioni tramite LDAP non sono crittografate. Ciò permette a un utente malintenzionato di utilizzare software di monitoraggio delle reti per visualizzare i pacchetti di dati trasmessi in rete. È per questo motivo che molte policy di sicurezza aziendale tipicamente richiedono che le organizzazioni eseguano la crittografia della comunicazione LDAP.

Per mitigare questa forma di esposizione dei dati, AWS Managed Microsoft AD offre un'opzione: è possibile abilitare LDAP su Secure Sockets Layer (SSL) /Transport Layer Security (TLS), noto anche come LDAPS. Con LDAPS, è possibile migliorare la sicurezza attraverso il cavo. È inoltre possibile soddisfare i requisiti di conformità crittografando tutte le comunicazioni tra le applicazioni abilitate per LDAP e Managed Microsoft AD AWS .

AWS Microsoft AD gestito fornisce supporto per LDAPS nei seguenti scenari di distribuzione:

- LDAPS lato server crittografa le comunicazioni LDAP tra le applicazioni LDAP commerciali o homegrown (che agiscono come client LDAP) e Microsoft AD gestito da AWS (che agisce come server LDAP). Per ulteriori informazioni, consulta Abilitazione del protocollo LDAPS lato server utilizzando Managed Microsoft AD AWS.
- Il protocollo LDAPS lato client crittografa le comunicazioni LDAP tra AWS applicazioni quali WorkSpaces (che fungono da client LDAP) e l'Active Directory autogestito (locale) (che funge da server LDAP). Per ulteriori informazioni, consulta Abilitazione del protocollo LDAPS lato client utilizzando Managed Microsoft AD AWS.

Per ulteriori informazioni sulle best practice relative alla protezione dell'implementazione di Active Directory, consulta la documentazione. MicrosoftCertificate ServicesMicrosoft

Argomenti

- Abilitazione del protocollo LDAPS lato server utilizzando Managed Microsoft AD AWS
- Abilitazione del protocollo LDAPS lato client utilizzando Managed Microsoft AD AWS

Abilitazione del protocollo LDAPS lato server utilizzando Managed Microsoft AD AWS

Il Lightweight Directory Access Protocol Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) supporto lato server crittografa LDAP le comunicazioni tra le applicazioni commerciali o sviluppate internamente e la directory LDAP Managed Microsoft AD. AWS Questo aiuta a migliorare la sicurezza su tutta la rete e a soddisfare i requisiti di conformità utilizzando il protocollo crittografico. Secure Sockets Layer (SSL)

Abilita LDAPS lato server utilizzando AWS Autorità di certificazione privata

Per istruzioni dettagliate su come impostare e configurare il protocollo LDAPS lato server e l'utilizzo AWS Private CA del server dell'autorità di certificazione (CA), consulta. Configurazione di AWS Private CA Connector for AD per AWS Managed Microsoft AD

Abilitare il protocollo LDAPS lato server utilizzando CA Microsoft

Per istruzioni dettagliate su come impostare e configurare LDAPS lato server e il server dell'autorità di certificazione (CA), vedi Come abilitare LDAPS lato server per la directory AWS gestita di Microsoft AD sul blog sulla sicurezza. AWS

Devi eseguire la maggior parte della configurazione dall' EC2 istanza Amazon che usi per gestire i controller di dominio Microsoft AD AWS gestiti. I seguenti passaggi ti guidano nell'attivazione di LDAPS per il tuo dominio in. Cloud AWS

Se desideri utilizzare l'automazione per configurare la tua PKI infrastruttura, puoi utilizzare MicrosoftPublic Key Infrastructure on AWS QuickStart Guide. In particolare, ti consigliamo di seguire le istruzioni nella guida per caricare il modello per Deploy MicrosoftPKI in un account esistente VPC. AWS Una volta caricato il modello, assicurati di scegliere **`AWSManaged`** quando accedi all'opzione Tipo di Active Directory Domain Services. Se hai usato la QuickStart guida, puoi passare direttamente aFase 3: creazione di un modello di certificato.

Argomenti

- Fase 1: delega per l'abilitazione di LDAPS
- Fase 2: configurazione dell'autorità di certificazione
- Fase 3: creazione di un modello di certificato
- Fase 4: aggiungere regole per i gruppi di sicurezza

Fase 1: delega per l'abilitazione di LDAPS

Per abilitare LDAPS lato server, è necessario essere un membro del gruppo Admins o AWS Delegated Enterprise Certificate Authority Administrators nella directory Managed Microsoft AD. AWS In alternativa, è possibile essere l'utente amministrativo predefinito (account amministratore). Se si preferisce, è possibile avere un utente diverso dall'impostazione dell'account Admin LDAPS. In tal caso, aggiungi quell'utente al gruppo Admins o AWS Delegated Enterprise Certificate Authority Administrators nella directory Managed AWS Microsoft AD.

Fase 2: configurazione dell'autorità di certificazione

Prima di abilitare LDAPS lato server, è necessario creare un certificato. Questo certificato deve essere emesso da un Microsoft Enterprise CA server che fa parte del tuo dominio Microsoft AD AWS gestito. Una volta creato, il certificato deve essere installato su ciascuno dei controller di dominio appartenenti a quel dominio. Questo certificato consente al LDAP servizio sui controller di dominio di ascoltare e accettare automaticamente SSL le connessioni dai LDAP client.

> **Note**
>
> Il protocollo LDAPS lato server con Managed AWS Microsoft AD non supporta i certificati emessi da una CA autonoma. Inoltre, non supporta i certificati emessi da un'autorità di certificazione di terze parti.

A seconda delle esigenze aziendali, puoi disporre delle seguenti opzioni di configurazione o connessione a una CA nel dominio:

- Crea un server subordinato Microsoft Enterprise CA: (consigliato) Con questa opzione, puoi implementare un server subordinato nel cloud. Microsoft Enterprise CA AWS Il server può utilizzare Amazon EC2 in modo che funzioni con la tua Microsoft CA principale esistente. Per ulteriori informazioni su come configurare un subordinato MicrosoftEnterprise CA, vedere Passaggio 4: Aggiungere un file alla AWS Microsoft AD directory in Come Microsoft Enterprise CA abilitare il protocollo LDAPS lato server per la directory gestita di AWS Microsoft AD.
- Crea una radice Microsoft Enterprise CA: con questa opzione, puoi creare una radice Microsoft Enterprise CA nel AWS cloud utilizzando Amazon EC2 e aggiungerla al tuo dominio Microsoft AD AWS gestito. Questa CA di root può emettere il certificato per i controller di dominio. Per ulteriori informazioni sulla configurazione di una nuova CA principale, vedere Passaggio 3: Installazione e configurazione di una CA offline in Come abilitare LDAPS lato server per la directory gestita di AWS Microsoft AD.

Per ulteriori informazioni su come aggiungere l' EC2 istanza al dominio, consulta. Modi per aggiungere un' EC2 istanza Amazon al tuo AWS Managed Microsoft AD

Fase 3: creazione di un modello di certificato

Dopo aver Enterprise CA configurato il tuo, puoi configurare il modello di certificato di Kerberos autenticazione.

Creazione di un modello di certificato

1. Avvia Server Manager di Microsoft Windows. Seleziona Strumenti > Autorità di certificazione.
2. Nella finestra Autorità di certificazione, espandi l'albero Autorità di certificazione nel riquadro a sinistra. Fai clic con il pulsante destro del mouse su Modelli di certificazione, quindi scegli Gestisci.
3. Nella finestra Console dei modelli di certificazione, fai clic con il pulsante destro del mouse su Autenticazione Kerberos, quindi scegli Duplica dominio.
4. Verrà visualizzata la finestra pop-up Proprietà del nuovo modello.
5. Nella finestra Proprietà del nuovo modello, vai alla scheda Compatibilità, quindi procedi come segue:

   a. Cambia l'Autorità di certificazione con OS quella corrispondente alla tua CA.

   b. Se viene visualizzata la finestra pop-up Modifiche risultanti, seleziona OK.

   c. Cambia il destinatario della certificazione in Windows 10/Windows Server 2016.

      > **Note**
      >
      > AWS Managed Microsoft AD è fornito daWindows Server 2019.

   d. Se viene visualizzata la finestra pop-up Modifiche risultanti, seleziona OK.
6. Fai clic sulla scheda Generale e modifica il nome visualizzato del modello in LDAPOverSSL o in qualsiasi altro nome che preferisci.
7. Fai clic sulla scheda Sicurezza e scegli Controller di dominio nella sezione Nomi gruppi o utenti. Nella sezione Autorizzazioni per i controller di dominio, verifica che le caselle di controllo Consenti per Lettura, Registrazione e Registrazione automatica siano selezionate.
8. Scegli OK per creare il modello di certificato LDAPOverSSL (o il nome specificato sopra). Chiudi la finestra Console dei modelli di certificato.
9. Nella finestra Autorità di certificazione, fai clic con il pulsante destro del mouse su Modelli di certificazione e scegli Nuovo > Modello di certificazione da emettere.
10. Nella finestra Abilita modelli di certificato, scegli LDAPOverSSL (o il nome specificato sopra), quindi scegli OK.

Fase 4: aggiungere regole per i gruppi di sicurezza

Nel passaggio finale, devi aprire la EC2 console Amazon e aggiungere le regole del gruppo di sicurezza. Queste regole consentono ai controller di dominio di connettersi al tuo Enterprise CA per richiedere un certificato. A tale scopo, aggiungi regole in entrata in modo da Enterprise CA poter accettare il traffico in entrata dai controller di dominio. Quindi aggiungi regole in uscita per consentire il traffico dai controller di dominio a. Enterprise CA

Una volta configurate entrambe le regole, i controller di dominio richiedono Enterprise CA automaticamente un certificato e abilitano LDAPS per la directory. Il LDAP servizio sui controller di dominio è ora pronto per accettare connessioni LDAPS.

Configurazione delle regole per i gruppi di sicurezza

1. Accedi alla tua EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2 e accedi con le credenziali di amministratore.
2. Nel riquadro a sinistra, scegli Security Groups (Gruppi di sicurezza) in Network & Security (Rete e sicurezza).
3. Nel riquadro principale, scegli il gruppo di AWS sicurezza per la tua CA.
4. Seleziona la scheda Inbound (In entrata), quindi seleziona Edit (Modifica).
5. Nella finestra di dialogo Edit inbound rules (Modifica regole in entrata) esegui queste operazioni:
   - Selezionare Add Rule (Aggiungi regola).
   - Scegli All traffic (Tutto il traffico) in Type (Tipo) e Custom (Personalizzato) in Source (Origine).
   - Inserisci il gruppo AWS di sicurezza (ad esempio,`sg-123456789`) per la tua directory nella casella accanto a Source.
   - Scegli Save (Salva).
6. Ora scegli il gruppo di AWS sicurezza della tua directory AWS Managed Microsoft AD. Seleziona la scheda Outbound (In uscita), quindi seleziona Edit (Modifica).
7. Nella finestra di dialogo Edit outbound rules (Modifica regole in uscita) esegui queste operazioni:
   - Selezionare Add Rule (Aggiungi regola).
   - Scegli All traffic (Tutto il traffico) in Type (Tipo) e Custom (Personalizzato) in Destination (Destinazione).
   - Inserisci il gruppo AWS di sicurezza per la tua CA nella casella accanto a Destinazione.
   - Scegli Save (Salva).

È possibile testare la connessione LDAPS alla directory AWS Managed Microsoft AD utilizzando lo LDP strumento. Lo LDP strumento viene fornito con. Active Directory Administrative Tools Per ulteriori informazioni, consulta Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.

> **Note**
>
> Prima di verificare la connessione LDAPS, è necessario attendere fino a 30 minuti affinché la CA subordinata emetta un certificato ai controller di dominio.

Per ulteriori dettagli sul protocollo LDAPS lato server e per vedere un esempio di utilizzo su come configurarlo, vedi Come abilitare il protocollo LDAPS lato server per la directory AWS gestita di Microsoft AD nel blog sulla sicurezza. AWS

Abilitazione del protocollo LDAPS lato client utilizzando Managed Microsoft AD AWS

Il supporto Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) sul lato client in AWS Managed Microsoft AD crittografa le comunicazioni tra Microsoft Active Directory (AD) autogestita (locale) e le applicazioni. AWS Esempi di tali applicazioni includono WorkSpaces AWS IAM Identity Center, Quick Suite e Amazon Chime. Questa crittografia ti aiuta a proteggere meglio i dati di identità della tua organizzazione e a soddisfare i tuoi requisiti di sicurezza.

Prerequisiti

Prima di abilitare LDAPS lato client, è necessario soddisfare i seguenti requisiti.

Argomenti

- Crea una relazione di fiducia tra AWS Managed Microsoft AD e Microsoft Active Directory autogestito
- Distribuire certificati server in Active Directory
- Requisiti dei certificati dell'Autorità di certificazione
- Requisiti di rete

Crea una relazione di fiducia tra AWS Managed Microsoft AD e Microsoft Active Directory autogestito

Innanzitutto, è necessario stabilire una relazione di fiducia tra Microsoft AD AWS gestito e Microsoft Active Directory autogestito per abilitare il protocollo LDAPS lato client. Per ulteriori informazioni, consulta the section called “Creazione di una relazione di trust”.

Distribuire certificati server in Active Directory

Per abilitare LDAPS lato client, è necessario ottenere e installare i certificati server per ogni controller di dominio in Active Directory. Questi certificati verranno utilizzati dal servizio LDAP per ascoltare e accettare automaticamente connessioni SSL dai client LDAP. È possibile utilizzare certificati SSL emessi da una distribuzione interna di Active Directory Certificate Services (ADCS) o acquistati da un’emittente commerciale. Per ulteriori informazioni sui requisiti dei certificati server Active Directory, vedere il certificato LDAP su SSL (LDAPS) sul sito Web Microsoft.

Requisiti dei certificati dell'Autorità di certificazione

Un certificato di autorità di certificazione (CA), che rappresenta l'emittente dei certificati server, è necessario per l'operazione LDAPS lato client. I certificati CA sono abbinati ai certificati server presentati dai controller di dominio Active Directory per crittografare le comunicazioni LDAP. Tenere presenti i seguenti requisiti del certificato CA:

- L'Enterprise Certification Authority (CA) è necessaria per abilitare il protocollo LDAPS lato client. È possibile utilizzare Active Directory Certificate Service, un'autorità di certificazione commerciale di terze parti oppure. AWS Certificate Manager Per ulteriori informazioni su Microsoft Enterprise Certificate Authority, consulta Microsoftla documentazione.
- Per registrare un certificato, sono necessari più di 90 giorni dalla scadenza.
- I certificati devono essere in formato PEM (Privacy-Enhanced Mail). Se si esportano certificati CA da Active Directory, scegliere il formato di file di esportazione con codifica Base64 X.509 (.CER).
- È possibile archiviare un massimo di cinque (5) certificati CA per directory Microsoft AD AWS gestita.
- I certificati che utilizzano l'algoritmo di firma RSASSA-PSS non sono supportati.
- I certificati CA che concatenano ogni certificato server a ogni dominio trusted devono essere registrati.

Requisiti di rete

AWS il traffico LDAP dell'applicazione verrà eseguito esclusivamente sulla porta TCP 636, senza alcun fallback sulla porta LDAP 389. Tuttavia, le comunicazioni LDAP di Windows che supportano replica, trust e altro ancora continueranno a utilizzare la porta LDAP 389 con protezione nativa di Windows. Configura i gruppi AWS di sicurezza e i firewall di rete per consentire le comunicazioni TCP sulla porta 636 in Managed AWS Microsoft AD (in uscita) e Active Directory autogestita (in entrata). Lascia aperta la porta LDAP 389 tra Microsoft AD gestito da AWS e Active Directory autogestita.

Abilita LDAPS lato client

Per abilitare LDAPS lato client, è possibile importare il certificato di autorità di certificazione (CA) in Microsoft AD gestito da AWS e quindi abilitare LDAPS nella directory. All'attivazione, tutto il traffico LDAP tra applicazioni AWS e l'AD gestita dal cliente verranno trasmessi con crittografia del canale Secure Sockets Layer (SSL).

Sono disponibili due metodi diversi per abilitare LDAPS lato client per la directory. È possibile utilizzare il metodo o il metodo. Console di gestione AWS AWS CLI

> **Note**
>
> LDAPS lato client è una funzionalità regionale di Managed AWS Microsoft AD. Se si utilizza la replica multiarea, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Argomenti

Fase 1: Registrare un certificato in Directory Service

Utilizza uno dei seguenti metodi per registrare un certificato in Directory Service.

Metodo 1: Per registrare il certificato in Directory Service (Console di gestione AWS)

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.

2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi registrare il certificato, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Client-side LDAPS (LDAPS lato client) selezionare il menu Actions (Operazioni) e quindi selezionare Register certificate (Registra certificato).
5. Nella finestra di dialogo Register a CA certificate (Registra un certificato CA) selezionare Browse (Sfoglia), quindi selezionare il certificato e scegliere Open (Apri).
6. Scegliere Register certificate (Registra certificato).

Metodo 2: registrare il certificato in Directory Service (AWS CLI)

- Esegui il comando seguente. Per i dati del certificato, scegliere il percorso del file del certificato CA. Nella risposta verrà fornito un ID certificato.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Fase 2: controllare lo stato della registrazione

Per visualizzare lo stato di una registrazione di certificati o di un elenco di certificati registrati, utilizzare uno dei seguenti metodi.

Metodo 1: controllare lo stato di registrazione del certificato in Directory Service (Console di gestione AWS)

1. Andare alla sezione Client-side LDAPS (LDAPS lato client) nella pagina dei Directory details (Dettagli della directory).
2. Esaminare lo stato di registrazione del certificato corrente visualizzato nella colonna Registration status (Stato registrazione). Quando il valore dello stato di registrazione cambia in Registered (Registrato), il certificato è stato registrato.

Metodo 2: Per controllare lo stato di registrazione del certificato in Directory Service (AWS CLI)

- Esegui il comando seguente. Se il valore dello stato restituisce `Registered`, il certificato è stato registrato.

```
aws ds list-certificates --directory-id your_directory_id
```

Fase 3: abilitare LDAPS lato client

Utilizzate uno dei seguenti metodi per abilitare l'accesso LDAPS lato client. Directory Service

> **Note**
>
> Devi aver registrato almeno un certificato prima di poter abilitare LDAPS lato client.

Metodo 1: Per abilitare LDAPS lato client in () Directory ServiceConsole di gestione AWS

1. Andare alla sezione Client-side LDAPS (LDAPS lato client) nella pagina dei Directory details (Dettagli della directory).
2. Scegli Abilita . Se questa opzione non è disponibile, verificare che un certificato valido sia stato registrato e riprovare.
3. Nella finestra di dialogo Enable client-side LDAPS (Abilita LDAPS lato client) scegliere Enable (Abilita).

Metodo 2: Per abilitare LDAPS lato client in () Directory ServiceAWS CLI

- Esegui il comando seguente.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Fase 4: controllare lo stato LDAPS

Utilizzate uno dei seguenti metodi per verificare lo stato del protocollo LDAPS. Directory Service

Metodo 1: per controllare lo stato LDAPS in Directory Service ()Console di gestione AWS

1. Andare alla sezione Client-side LDAPS (LDAPS lato client) nella pagina dei Directory details (Dettagli della directory).
2. Se il valore dello stato visualizzato è Enabled (Abilitato), LDAPS è stato configurato.

Metodo 2: Per controllare lo stato LDAPS in Directory Service ()AWS CLI

- Esegui il comando seguente. Se il valore di stato restituisce `Enabled`, LDAPS è stato configurato.

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

Gestire LDAPS lato client

Utilizzare questi comandi per gestire la configurazione LDAPS.

Sono disponibili due metodi diversi per gestire le impostazioni LDAPS lato client. È possibile utilizzare il Console di gestione AWS metodo o il AWS CLI metodo.

Visualizzare i dettagli del certificato

Utilizza uno dei seguenti metodi per vedere quando scade un certificato.

Metodo 1: per visualizzare i dettagli del certificato in Directory Service (Console di gestione AWS)

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi visualizzare il certificato, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Client-side LDAPS (LDAPS lato client), le informazioni sul certificato verranno visualizzate in CA certificates (Certificati CA).

Metodo 2: Per visualizzare i dettagli del certificato in Directory Service (AWS CLI)

- Esegui il comando seguente. Per l'ID del certificato, utilizzare l'identificatore restituito da `register-certificate` o `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Annullare la registrazione di un certificato

Utilizza uno dei seguenti metodi per annullare la registrazione di un certificato.

> **Note**
>
> Se è registrato un solo certificato, è necessario disabilitare LDAPS prima di poter annullare la registrazione del certificato.

Metodo 1: annullare la registrazione di un certificato in Directory Service ()Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi annullare la registrazione di un certificato, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Client-side LDAPS (LDAPS lato client) selezionare il menu Actions (Operazioni) e quindi selezionare Deregister certificate (Annulla registrazione certificato).
5. Nella finestra di dialogo Deregister a CA certificate (Annulla la registrazione di un certificato CA) scegliere Deregister (Annulla registrazione).

Metodo 2: annullare la registrazione di un certificato in () Directory ServiceAWS CLI

- Esegui il comando seguente. Per l'ID del certificato, utilizzare l'identificatore restituito da `register-certificate` o `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Disabilitare LDAPS lato client

Utilizza uno dei seguenti metodi per disabilitare LDAPS lato client.

Metodo 1: disabilitare LDAPS lato client in () Directory ServiceConsole di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi disabilitare LDAPS lato client, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Client-side LDAPS (LDAPS lato client) scegliere Disable (Disabilita).
5. Nella finestra di dialogo Disable client-side LDAPS (Disabilita LDAPS lato client) scegliere Disable (Disabilita).

Metodo 2: disabilitare LDAPS lato client in () Directory ServiceAWS CLI

- Esegui il comando seguente.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Problemi relativi alla registrazione dei certificati

Il processo di registrazione dei controller di dominio Microsoft AD AWS gestiti con i certificati CA può richiedere fino a 30 minuti. Se riscontri problemi con la registrazione del certificato e desideri riavviare

i controller di dominio AWS Microsoft AD gestiti, puoi contattare. Supporto Per creare un caso di supporto, vedi Creazione di casi di supporto e gestione dei casi.

Gestisci la conformità per AWS Managed Microsoft AD

Puoi utilizzare AWS Managed Microsoft AD per supportare le tue applicazioni compatibili con Active Directory, nel AWS cloud, soggette ai seguenti requisiti di conformità. Tuttavia, le tue applicazioni non saranno conformi ai requisiti di conformità se usi Simple AD.

Standard di conformità supportati

AWS Managed Microsoft AD 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 Managed Microsoft AD soddisfa i requisiti di sicurezza del Federal Risk and Authorization Management Program (FedRAMP) e ha ricevuto la Provisional Authority to Operate (P-ATO) del FedRAMP Joint Authorization Board (JAB) al FedRAMP Moderate and High Baseline. Per ulteriori informazioni su FedRAMP, consulta la sezione relativa alla Conformità al programma FedRAMP.
	AWS Managed Microsoft AD dispone di un attestato di conformità per lo standard di sicurezza dei dati (DSS) PCI (Payment Card Industry) versione 3.2 al livello 1 del provider di servizi. I clienti che utilizzano AWS prodotti e servizi per archiviare, elaborare o trasmettere i dati dei titolari di carte possono utilizzare AWS Managed Microsoft AD per gestire la propria certificazione di conformità PCI DSS. Per ulteriori informazioni su PCI DSS, incluso come richiedere una copia del PCI AWS Compliance Package, vedere PCI DSS livello 1. È importante sottolineare che

	è necessario configurare policy granulari per le password in Managed AWS Microsoft AD per garantire la coerenza con gli standard PCI DSS versione 3.2. Per informazioni dettagliate sulle politiche da applicare, consulta la sezione seguente intitolata Abilita la conformità PCI per la tua directory gestita di AWS Microsoft AD.
	AWS ha ampliato il suo programma di conformità all'Health Insurance Portability and Accountability Act (HIPAA) per includere Managed AWS Microsoft AD come servizio idoneo all'HIPAA. Se hai sottoscritto un Business Associate Agreement (BAA) con AWS, puoi utilizzare AWS Managed Microsoft AD per aiutarti a creare le tue applicazioni conformi allo standard HIPAA. AWS offre un white paper incentrato sull'HIPAA per i clienti interessati a saperne di più su come sfruttare per l'elaborazione e l'archiviazione delle informazioni sanitarie. AWS Per ulteriori informazioni, consulta Compliance HIPAA.

Responsabilità condivisa

La sicurezza, inclusa la conformità con FedRAMP, HIPAA e PCI, è una responsabilità condivisa. È importante comprendere che lo stato di conformità di AWS Managed Microsoft AD non si applica automaticamente alle applicazioni eseguite nel AWS cloud. È necessario assicurarsi che l'utilizzo dei AWS servizi sia conforme agli standard.

Per un elenco completo di tutti i vari programmi di AWS conformità supportati da AWS Managed Microsoft AD, consulta la sezione AWS Servizi rientranti nell'ambito del programma di conformità.

Abilita la conformità PCI per la tua directory AWS Managed Microsoft AD

Per abilitare la conformità PCI per la directory AWS Managed Microsoft AD, è necessario configurare politiche granulari in materia di password come specificato nel documento di attestazione di conformità (AOC) e riepilogo delle responsabilità PCI DSS fornito da. AWS Artifact

Per ulteriori informazioni sull'utilizzo di policy di password fine-grained, consulta Informazioni sui criteri di AWS gestione delle password di Microsoft AD.

Miglioramento della configurazione di sicurezza della rete AWS Managed Microsoft AD

Il gruppo AWS di sicurezza fornito per la directory AWS Managed Microsoft AD è configurato con le porte di rete in entrata minime necessarie per supportare tutti i casi d'uso noti per la directory Managed AWS Microsoft AD. Per ulteriori informazioni sul gruppo di AWS sicurezza fornito, vedere. Cosa viene creato con AWS Managed Microsoft AD

Per migliorare ulteriormente la sicurezza di rete della directory AWS Managed Microsoft AD, è possibile modificare il gruppo AWS di sicurezza in base ai seguenti scenari comuni.

Controller di dominio del cliente CIDR: in questo blocco CIDR risiedono i controller di dominio locali del dominio.

Client cliente CIDR: questo blocco CIDR è il luogo in cui i tuoi client, come computer o utenti, si autenticano sul tuo Managed AWS Microsoft AD. Anche i controller di dominio Microsoft AD AWS gestiti risiedono in questo blocco CIDR.

Scenari

- AWS le applicazioni supportano solo
- AWS applicazioni solo con supporto affidabile
- AWS applicazioni e supporto nativo per i carichi di lavoro di Active Directory
- AWS supporto per applicazioni e carichi di lavoro nativi di Active Directory con supporto affidabile

AWS le applicazioni supportano solo

Tutti gli account utente vengono forniti solo nel tuo AWS Managed Microsoft AD per essere utilizzati con AWS le applicazioni supportate, come le seguenti:

- Amazon Chime
- Amazon Connect
- Quick Suite
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail

- AWS Client VPN
- Console di gestione AWS

È possibile utilizzare la seguente configurazione del gruppo AWS di sicurezza per bloccare tutto il traffico non essenziale verso i controller di dominio Microsoft AD AWS gestiti.

> **Note**
>
> - Quanto segue non è compatibile con questa configurazione del gruppo AWS di sicurezza:
>   - EC2 Istanze Amazon
>   - Amazon FSx
>   - Amazon RDS per MySQL
>   - Amazon RDS per Oracle
>   - Amazon RDS per PostgreSQL
>   - Amazon RDS per SQL Server
>   - WorkSpaces
>   - Trust di Active Directory
>   - Client o server aggiunti al dominio

Regole in entrata

Nessuna.

Regole in uscita

Nessuna.

AWS applicazioni solo con supporto affidabile

Tutti gli account utente vengono forniti nel tuo AWS Managed Microsoft AD o in Active Directory affidabile per essere utilizzati con AWS le applicazioni supportate, come le seguenti:

- Amazon Chime
- Amazon Connect

- Quick Suite
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- Console di gestione AWS

È possibile modificare la configurazione del gruppo AWS di sicurezza fornita per bloccare tutto il traffico non essenziale verso i controller di dominio AWS Microsoft AD gestiti.

> **Note**
>
> - Quanto segue non è compatibile con questa configurazione del gruppo AWS di sicurezza:
>   - EC2 Istanze Amazon
>   - Amazon FSx
>   - Amazon RDS per MySQL
>   - Amazon RDS per Oracle
>   - Amazon RDS per PostgreSQL
>   - Amazon RDS per SQL Server
>   - WorkSpaces
>   - Trust di Active Directory
>   - Client o server aggiunti al dominio
> - Questa configurazione richiede che la rete CIDR dei «controller di dominio del cliente» sia sicura.
> - TCP 445 viene utilizzato solo per la creazione di trust e può essere rimosso dopo che il trust è stato stabilito.
> - TCP 636 è richiesto solo quando LDAP su SSL è in uso.

Regole in entrata

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP e UDP	53	Controller di dominio del cliente CIDR	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	Controller di dominio del cliente CIDR	Kerberos	Autentica zione utente e computer, trust a livello di foresta
TCP e UDP	389	Controller di dominio del cliente CIDR	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	464	Controller di dominio del cliente CIDR	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	445	Controller di dominio del cliente CIDR	SMB/CIFS	Replica, autentica zione utente e computer, trust di policy di gruppo
TCP	135	Controller di dominio del cliente CIDR	Replica	RPC, EPM

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP	636	Controller di dominio del cliente CIDR	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	Controller di dominio del cliente CIDR	RPC	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	Controller di dominio del cliente CIDR	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
UDP	123	Controller di dominio del cliente CIDR	Ora di Windows	Ora di Windows, trust

Regole in uscita

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
Tutti	Tutti	Controller di dominio del cliente CIDR	Tutto il traffico	

AWS applicazioni e supporto nativo per i carichi di lavoro di Active Directory

Gli account utente vengono forniti solo in AWS Managed Microsoft AD per essere utilizzati con AWS applicazioni supportate, come le seguenti:

- Amazon Chime
- Amazon Connect
- EC2 Istanze Amazon
- Amazon FSx
- Suite rapida
- Amazon RDS per MySQL
- Amazon RDS per Oracle
- Amazon RDS per PostgreSQL
- Amazon RDS per SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- Console di gestione AWS

È possibile modificare la configurazione del gruppo AWS di sicurezza fornita per bloccare tutto il traffico non essenziale verso i controller di dominio AWS Microsoft AD gestiti.

> **Note**
>
> - I trust di Active Directory non possono essere creati e AWS gestiti tra la directory gestita di Microsoft AD e i controller di dominio del cliente CIDR.
> - Richiede che tu assicuri che la rete CIDR del «client cliente cliente» sia sicura.
> - TCP 636 è richiesto solo quando LDAP su SSL è in uso.
> - Se desideri utilizzare una CA Enterprise con questa configurazione, dovrai creare una regola in uscita «TCP, 443, CA CIDR».

Regole in entrata

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP e UDP	53	Cliente cliente CIDR	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	Cliente cliente CIDR	Kerberos	Autentica zione utente e computer, trust a livello di foresta
TCP e UDP	389	Cliente cliente CIDR	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	445	Cliente cliente CIDR	SMB/CIFS	Replica, autentica zione utente e computer, trust di policy di gruppo
TCP e UDP	464	Cliente cliente CIDR	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	135	Cliente cliente CIDR	Replica	RPC, EPM

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP	636	Cliente cliente CIDR	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	Cliente cliente CIDR	RPC	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	Cliente cliente CIDR	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	9389	Cliente cliente CIDR	SOAP	Servizi Web DS AD
UDP	123	Cliente cliente CIDR	Ora di Windows	Ora di Windows, trust
UDP	138	Cliente cliente CIDR	DFSN e NetLogon	DFS, policy di gruppo

Regole in uscita

Nessuna.

AWS supporto per applicazioni e carichi di lavoro nativi di Active Directory con supporto affidabile

Tutti gli account utente vengono forniti nel tuo AWS Managed Microsoft AD o in Active Directory affidabile per essere utilizzati con AWS le applicazioni supportate, come le seguenti:

- Amazon Chime
- Amazon Connect
- EC2 Istanze Amazon
- Amazon FSx
- Suite rapida
- Amazon RDS per MySQL
- Amazon RDS per Oracle
- Amazon RDS per PostgreSQL
- Amazon RDS per SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- Console di gestione AWS

È possibile modificare la configurazione del gruppo AWS di sicurezza fornita per bloccare tutto il traffico non essenziale verso i controller di dominio AWS Microsoft AD gestiti.

> **Note**
>
> - È necessario garantire che le reti «customer domain controllers CIDR» e «customer client CIDR» siano sicure.
> - Il protocollo TCP 445 con i «controller di dominio del cliente CIDR» viene utilizzato solo per creare fiducia e può essere rimosso dopo che la fiducia è stata stabilita.
> - Il protocollo TCP 445 con il «client-client CIDR» deve essere lasciato aperto in quanto è necessario per l'elaborazione dei criteri di gruppo.

- TCP 636 è richiesto solo quando LDAP su SSL è in uso.
- Se desideri utilizzare una CA aziendale con questa configurazione, dovrai creare una regola in uscita «TCP, 443, CA CIDR».

Regole in entrata

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP e UDP	53	Controller di dominio del cliente (CIDR)	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	Controller di dominio del cliente CIDR	Kerberos	Autentica zione utente e computer, trust a livello di foresta
TCP e UDP	389	Controller di dominio del cliente CIDR	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	464	Controller di dominio del cliente CIDR	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	445	Controller di dominio del cliente CIDR	SMB/CIFS	Replica, autentica zione utente e computer,

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
				trust di policy di gruppo
TCP	135	Controller di dominio del cliente CIDR	Replica	RPC, EPM
TCP	636	Controller di dominio del cliente CIDR	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	Controller di dominio del cliente CIDR	RPC	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	Controller di dominio del cliente CIDR	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
UDP	123	Controller di dominio del cliente CIDR	Ora di Windows	Ora di Windows, trust

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP e UDP	53	Controller di dominio del cliente CIDR	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	Controller di dominio del cliente CIDR	Kerberos	Autentica zione utente e computer, trust a livello di foresta
TCP e UDP	389	Controller di dominio del cliente CIDR	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	445	Controller di dominio del cliente CIDR	SMB/CIFS	Replica, autentica zione utente e computer, trust di policy di gruppo
TCP e UDP	464	Controller di dominio del cliente CIDR	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	135	Controller di dominio del cliente CIDR	Replica	RPC, EPM

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP	636	Controller di dominio del cliente CIDR	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	Controller di dominio del cliente CIDR	RPC	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	Controller di dominio del cliente CIDR	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	9389	Controller di dominio del cliente CIDR	SOAP	Servizi Web DS AD
UDP	123	Controller di dominio del cliente CIDR	Ora di Windows	Ora di Windows, trust
UDP	138	Controller di dominio del cliente CIDR	DFSN e NetLogon	DFS, policy di gruppo

Regole in uscita

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
Tutti	Tutti	Controller di dominio del cliente CIDR	Tutto il traffico	

Modifica delle impostazioni di sicurezza della directory Microsoft AD AWS gestita

Puoi configurare impostazioni di directory granulari per il tuo Managed AWS Microsoft AD per soddisfare i requisiti di conformità e sicurezza senza alcun aumento del carico di lavoro operativo. Nelle impostazioni della directory, puoi aggiornare la configurazione del canale sicuro per i protocolli e i codici utilizzati nella tua directory. Ad esempio, hai la flessibilità di disabilitare singoli cifrari legacy, come RC4 o DES, e protocolli, come SSL 2.0/3.0 e TLS 1.0/1.1. AWS Microsoft AD gestito distribuisce quindi la configurazione su tutti i controller di dominio nella directory, gestisce i riavvii dei controller di dominio e mantiene questa configurazione man mano che si esegue la scalabilità orizzontale o ne vengono distribuiti altri. Regioni AWS Per tutte le impostazioni disponibili, consulta Elenco delle impostazioni di sicurezza della directory.

Modifica delle impostazioni di sicurezza della directory

Puoi configurare e modificare le impostazioni per tutte le tue directory.

Per modificare le impostazioni delle directory

1. Accedi alla console di AWS gestione e apri la console all'indirizzo. Directory Service https://console.aws.amazon.com/directoryservicev2/
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. In Rete e sicurezza, trova Impostazioni della directory, quindi scegli Modifica impostazioni.
4. In Modifica impostazioni, modifica Valore nelle impostazioni che desideri modificare. Quando modifichi un'impostazione, il suo stato cambia da Predefinito a Pronto per l'aggiornamento. Se l'impostazione è stata modificata in precedenza, il suo stato cambia da Aggiornato a Pronto per l'aggiornamento. Scegli quindi Rivedi.
5. In Rivedi e aggiorna le impostazioni, consulta Impostazioni della directory e assicurati che i nuovi valori siano tutti corretti. Se desideri apportare altre modifiche alle impostazioni, scegli Modifica

impostazioni. Quando sei soddisfatto delle modifiche e pronto a implementare i nuovi valori, scegli Aggiorna impostazioni. Quindi, verrai reindirizzato alla pagina dell'ID della directory.

> **Note**
>
> In Impostazioni della directory, puoi visualizzare lo Stato delle impostazioni aggiornate. Mentre le impostazioni vengono implementate, lo Stato è su Aggiornamento in corso. Non è possibile modificare altre impostazioni se ce n'è una con Aggiornamento in corso come Stato. Lo Stato diventa Aggiornato se l'impostazione viene aggiornata correttamente con la modifica. Lo Stato diventa Non riuscito se l'impostazione non viene aggiornata con la modifica.

Impostazioni di sicurezza della directory non riuscite

Se si verifica un errore durante l'aggiornamento delle impostazioni, lo Stato visualizzato è Non riuscito. In questo caso, le impostazioni non vengono aggiornate ai nuovi valori e vengono mantenuti i valori originali. Puoi riprovare ad aggiornare queste impostazioni o ripristinarle ai valori precedenti.

Per risolvere le impostazioni di aggiornamento non riuscite

- In Impostazioni della directory, scegli Risolvi impostazioni non riuscite. Effettua quindi una delle seguenti operazioni:
  - Per ripristinare le impostazioni al valore originale precedente all'errore, scegli Ripristina impostazioni non riuscite. Quindi, scegli Ripristina nel pop-up.
  - Per riprovare ad aggiornare le impostazioni della directory, scegli Riprova impostazioni non riuscite. Se desideri apportare ulteriori modifiche alle impostazioni della directory prima di riprovare gli aggiornamenti non riusciti, scegli Continua a modificare. In Verifica e riprova gli aggiornamenti non riusciti, scegli Aggiorna impostazioni.

Elenco delle impostazioni di sicurezza della directory

L'elenco seguente mostra il tipo, il nome, il nome API, i valori potenziali e la descrizione delle impostazioni per tutte le impostazioni di sicurezza delle directory disponibili.

TLS 1.2 e AES 256/256 sono le impostazioni di sicurezza delle directory predefinite se tutte le altre impostazioni di sicurezza sono disabilitate. Queste impostazioni non possono essere disabilitate.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
Autenticazione basata su certificati	Compensazione del backdating del certificato	COMPENSAZIONE_BACKDATING_CERTIFICATO	Anni: da 0 a 50 Mesi: da 0 a 11 Giorni: da 0 a 30 Ore: da 0 a 23 Minuti: da 0 a 59 Secondi: da 0 a 59	Specifica un valore per indicare per quanto tempo un certificato può essere anteriore a un utente in Active Directory e continuare a essere utilizzato per l'autenticazione in Active Directory. Il valore predefinito è di 10 minuti. Puoi configurare questo valore da 1 secondo a 50 anni. Per configurare questa impostazione, devi selezionare il tipo di Compatibilità per Strong Certifica

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				te Binding Enforcement. Per ulteriori informazioni, vedere KB5014754 — Modifiche all'autenticazione basata su certificati nei controller di dominio Windows nella documentazione di Microsoft Support.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
	Applicazione avanzata del certificato	APPLICAZIONE_AVANZATA_CERTIFICATO	Compatibilità, applicazione avanzata	Specifica uno dei seguenti tipi di applicazione: • Compatibilità: l'autenticazione è consentita se un certificato non può essere mappato in modo sicuro a un utente. Se il certificato è precedente all'account utente in Active Directory, devi anche impostare Compensazione del backdating del certificato, altrimenti l'autenticazione avrà esito negativo.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				• Applicazione completa (impostazione predefinita): l'autenticazione non è consentita se un certificato non può essere mappato in modo sicuro a un utente. Se scegli questo tipo di applicazione, Compensazione del backdating del certificato non può essere configurato. Per ulteriori informazioni, vedere KB5014754 — Modifiche

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				all'autenticazione basata su certificati nei controller di dominio Windows nella documentazione di Microsoft Support.
Canale sicuro: crittografia	AES 128/128	AES_128_128	Abilita, disabilita	Abilita o disabilita l'algoritmo di crittografia AES 128/128 per comunicazioni sicure tra i controller di dominio nella tua directory.
	DES 56/56	DES_56_56	Abilita, disabilita	Abilita o disabilita l'algoritmo di crittografia DES 56/56 per comunicazioni sicure tra i controller di dominio nella tua directory.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
	RC2 40/128	RC2_40_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC2 40/128 per comunicazioni sicure tra i controller di dominio nella tua directory.
	RC2 56/128	RC2_56_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC2 56/128 per comunicazioni sicure tra i controller di dominio nella tua directory.
	RC2 128/128	RC2_128_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC2 128/128 per comunicazioni sicure tra i controller di dominio nella tua directory.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
	RC4 40/128	RC4_40_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC4 40/128 per comunicazioni sicure tra i controller di dominio nella tua directory.
	RC4 56/128	RC4_56_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC4 56/128 per comunicazioni sicure tra i controller di dominio nella tua directory.
	RC4 64/128	RC4_64_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC4 64/128 per comunicazioni sicure tra i controller di dominio nella tua directory.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
	RC4 128/128	RC4_128_128	Abilita, disabilita	Abilita o disabilita il codice di crittografia RC4 128/128 per comunicazioni sicure tra i controller di dominio nella tua directory.
	Triple DES 168/168	3DES_168_168	Abilita, disabilita	Abilita o disabilita l'algoritmo di crittografia Triple DES 168/168 per comunicazioni sicure tra i controller di dominio nella tua directory.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
Canale sicuro: protocollo	PCT 1.0	PCT_1_0	Abilita, disabilita	Abilita o disabilita il protocollo PCT 1.0 per comunicazioni sicure tra canali (server e client) sui controller di dominio nella tua directory.
	SSL 2.0	SSL_2_0	Abilita, disabilita	Abilita o disabilita il protocollo SSL 2.0 per comunicazioni sicure tra canali (server e client) sui controller di dominio nella tua directory.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
	SSL 3.0	SSL_3_0	Abilita, disabilita	Abilita o disabilita il protocollo SSL 3.0 per comunicazioni sicure tra canali (server e client) sui controller di dominio nella tua directory.
	TLS 1.0	TLS_1_0	Abilita, disabilita	Abilita o disabilita il protocollo TLS 1.0 per comunicazioni sicure tra canali (server e client) sui controller di dominio nella tua directory.

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
	TLS 1.1	TLS_1_1	Abilita, disabilita	Abilita o disabilita il protocollo TLS 1.1 per comunicazioni sicure tra canali (server e client) sui controller di dominio nella tua directory.

Abilita la crittografia a chiave pubblica per l'autenticazione iniziale (PKINIT) per gli utenti di AWS Microsoft AD gestito

AWS Le directory Microsoft AD gestite utilizzano l'associazione avanzata dei certificati per impostazione predefinita, che richiede una mappatura esplicita tra certificati e oggetti AD. Le seguenti mappature sono considerate affidabili per Managed AWS Microsoft AD:

- `altSecurityIdentities`Emittente e numero di serie
- `altSecurityIdentities`Identificatore chiave del soggetto
- `altSecurityIdentities` SHA1 Hash della chiave pubblica

Questi attributi consentono una mappatura avanzata dei certificati, che fornisce una maggiore sicurezza per l'autenticazione basata su certificati richiedendo certificate-to-user relazioni esplicite definite in Active Directory. Questo aiuta a prevenire gli attacchi di escalation dei privilegi basati sui certificati

È possibile utilizzare questa procedura per configurare solide associazioni di certificati per prevenire gli attacchi di escalation dei privilegi mantenendo al contempo la funzionalità di autenticazione dei certificati.

Per ulteriori informazioni, vedere Microsoft KB5 014754: modifiche all'autenticazione basata su certificati nei controller di dominio Windows

Prerequisiti

- Una directory Microsoft AD AWS gestita con autorità di certificazione configurata
- Accesso amministrativo all'ambiente Active Directory
- PowerShell con il modulo Active Directory installato
- Il certificato che desideri mappare all'oggetto AD

AltSecurityIdentityAttributo della mappa

1. Scegli uno dei seguenti metodi di `AltSecurityIdentity` mappatura in base alle informazioni del certificato:
   - SHA1 hash: utilizza l' SHA1 hash della chiave pubblica del certificato

     Per la mappatura SHA1 hash, estrai l'hash del certificato e applicalo all'oggetto utente:

     ```
     $Username = 'YourUsername'
     $cert = certutil -dump "YourCertificate.cer"
     $certHash = ($cert | Select-String -Pattern "(sha1):*" |
         Select-String -Pattern "Cert").ToString().TrimStart('Cert Hash(sha1):
      ').Replace(' ','')
     Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<SHA1-
     PUKEY>$CertHash"}
     ```

   - Emittente e numero di serie: utilizza il nome e il numero di serie dell'emittente del certificato

     Per la mappatura dell'emittente e del numero di serie, utilizza l'emittente e il numero di serie del certificato:

     ```
     $Username = 'YourUsername'
     $IssuerName = 'YourCertificateIssuer'
     $SerialNumber = 'YourCertificateSerialNumber'
     Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<I>
     $IssuerName<SR>$SerialNumber"}
     ```

   - Identificatore chiave dell'oggetto: utilizza l'estensione dell'identificatore della chiave dell'oggetto del certificato

Per la mappatura dell'identificatore della chiave dell'oggetto, utilizza l'identificatore della chiave oggetto del certificato:

```
$Username = 'YourUsername'
$SubjectKeyIdentifier = 'YourSubjectKeyIdentifier'
Set-ADUser -Identity $Username -Add @{'altSecurityIdentities'="X509:<SKI>
$SubjectKeyIdentifier"}
```

2. Verifica che la mappatura sia stata applicata correttamente:

```
Get-ADUser -Identity $Username -Properties altSecurityIdentities |
    Select-Object -ExpandProperty altSecurityIdentities
```

3. Attendi il completamento della replica di Active Directory (in genere 15-30 secondi) prima di testare l'autenticazione del certificato.

Esempio: mappatura in blocco dell'attributo da parte di un certificato AltSecurityIdentity

L'esempio seguente mostra come mappare l'`AltSecurityIdentity`attributo per più certificati utente di un'autorità di certificazione:

```
$CertificateTemplateName = 'User'
$Now = $((Get-Date).ToString($(Get-culture).DateTimeFormat.ShortDatePattern))
$Restrict = "Disposition=20,NotAfter>=$Now,Certificate Template=
$CertificateTemplateName"
$Out = "SerialNumber,Certificate Hash,User Principal
 Name,RequesterName,CommonName,CertificateTemplate,NotBefore,NotAfter"
$Certs = certutil -view -restrict $Restrict -out $Out csv | ConvertFrom-CSV
$UserSha1HashMapping = @{}

ForEach ($Cert in $Certs) {
    $UPN = $Cert.'User Principal Name'
    $Username, $Domain = $UPN.Split('@')
    $CertificateThumbprint = ($Cert.'Certificate Hash').Replace(' ','')
    $AdUserObject = Get-ADUser -Identity $Username
    If ($AdUserObject -And $AdUserObject.Count -gt 1) {
        Write-Output "Unable to map user: $Username, multiple user objects found"
        Continue
    }
    If ($AdUserObject) {
        If ($UserSha1HashMapping.Keys -Contains $Username) {
```

```
            $UserSha1HashMapping[$Username] += $CertificateThumbprint
        } Else {
            $UserSha1HashMapping[$Username] = @($CertificateThumbprint)
        }
    }
}

ForEach ($User in $UserSha1HashMapping.Keys) {
    Write-Output "Mapping altSecurityIdentity for $User"
    $UserObject = Get-ADUser -Identity $User | Get-ADObject -Properties
 'altSecurityIdentities'
    $altSecurityIdentities = $UserObject.altSecurityIdentities
    ForEach ($thumbprint in $UserSha1HashMapping[$User]) {
        $SHA1PUKEY = "X509:<SHA1-PUKEY>$thumbprint"
        If ($altSecurityIdentities -Contains $SHA1PUKEY) {
            Write-Output "Skipping $thumbprint, already mapped."
            Continue
        }
        Write-Output "Adding $thumbprint to $User as altSecurityIdentity"
        Set-ADUser -Identity $User -Add @{'altSecurityIdentities'=$SHA1PUKEY}
    }
}
```

Passaggi successivi

- Verifica l'autenticazione basata sui certificati con i tuoi certificati mappati
- Configura le tue applicazioni per utilizzare i certificati mappati per l'autenticazione
- Monitora il tuo AWS Managed Microsoft ADper eventi di autenticazione

Configurazione di AWS Private CA Connector for AD per AWS Managed Microsoft AD

Puoi integrare AWS Managed Microsoft AD con AWS Autorità di certificazione privata (CA) per emettere e gestire certificati per i controller di dominio Active Directory, gli utenti aggiunti al dominio, i gruppi e i computer. AWS Private CA Connector for Active Directory ti consente di utilizzare un sostituto AWS Private CA drop-in completamente gestito per la tua azienda autogestita CAs senza la necessità di distribuire, applicare patch o aggiornare agenti locali o server proxy.

Puoi configurare AWS Private CA l'integrazione con la tua directory tramite la Directory Service console, la console AWS Private CA Connector for Active Directory o chiamando l'API.

`CreateTemplate` Per configurare l'integrazione di Private CA tramite la console AWS Private CA Connector for Active Directory, vedi Creazione di un modello di connettore. Consulta i seguenti passaggi su come configurare questa integrazione dalla Directory Service console.

Configurazione di AWS Private CA Connector for AD

Per creare un connettore CA privato per Active Directory

1. Accedi a Console di gestione AWS e apri la Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella scheda Gestione delle AWS applicazioni e nella sezione App e servizi, scegli AWS Private CA Connector for AD.
4. Nella pagina Crea certificato CA privato per Active Directory, completa i passaggi per creare il connettore CA privata per Active Directory.

Per ulteriori informazioni, consulta Creazione di un connettore.

Visualizzazione di AWS Private CA Connector for AD

Per visualizzare i dettagli del connettore CA privato

1. Accedi Console di gestione AWS e apri la Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella scheda Gestione delle AWS applicazioni e nella sezione app e servizi, visualizza i connettori CA privati e la CA privata associata. Vengono visualizzati i seguenti campi:

    a. AWS Private CA ID connettore: l'identificatore univoco di un AWS Private CA connettore. Sceglilo per visualizzare la pagina dei dettagli.

    b. AWS Private CA oggetto: informazioni relative al nome distinto della CA. Sceglilo per visualizzare la pagina dei dettagli.

    c. Status: risultati del controllo dello stato del AWS Private CA Connector e AWS Private CA:

    - Attivo: entrambi i controlli vengono superati
    - 1/2 controlli non riusciti: un controllo fallisce
    - Fallito: entrambi i controlli hanno esito negativo

Per informazioni sullo stato dell'errore, passa il mouse sul collegamento ipertestuale per vedere quale controllo non è riuscito.

d. Stato di registrazione dei certificati DC: verifica dello stato dello stato del certificato del controller di dominio:

   - Abilitato: la registrazione dei certificati è abilitata
   - Disabilitata: la registrazione dei certificati è disabilitata

e. Data di creazione: quando è stato creato il AWS Private CA connettore.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli del connettore.

La tabella seguente mostra i diversi stati per la registrazione dei certificati dei controller di dominio per Managed AWS Microsoft AD con. AWS Private CA

Stato della registrazione DC	Descrizione	Azione richiesta
Abilitato	I certificati dei controller di dominio sono stati registrati correttamente nella directory.	Nessuna operazione necessaria.
Non riuscito	L'attivazione o la disabilitazione della registrazione dei certificati del controller di dominio non è riuscita per la tua directory.	Se l'operazione di attivazione fallisce, riprova disattivando i certificati del controller di dominio e riaccende ndendoli. Se l'azione di disabilit azione fallisce, riprova attivando i certificati dei controller di dominio e quindi disattivando nuovamente. Se il nuovo tentativo fallisce, contatta l' AWS assistenza.
Impaired (Insuffic iente)	I controller di dominio presentano problemi di connettività di rete nella comunicazione con gli endpoint. AWS Private CA	Controlla le policy degli endpoint AWS Private CA VPC e dei bucket S3 per consentire la connettività di rete con la tua directory. Per ulteriori informazioni, consulta Risoluzione

Stato della registrazione DC	Descrizione	Azione richiesta
		dei messaggi di eccezione dell'Autorità di certificazione AWS privata e Risoluzione dei problemi di revoca dei certificati. AWS Private CA
Disabilitato	La registrazione dei certificati del controller di dominio è stata disattivata correttamente per la tua directory.	Nessuna operazione necessaria.
Disabilitazione	La disabilitazione della registrazione dei certificati del controller di dominio è in corso.	Nessuna operazione necessaria.
Abilitazione	L'attivazione della registrazione dei certificati del controller di dominio è in corso.	Nessuna operazione necessaria.

Configurazione delle politiche AD

AWS Private CA Connector for AD deve essere configurato in modo che i controller di dominio e gli oggetti di Microsoft AD AWS gestiti possano richiedere e ricevere certificati. Configura il tuo oggetto di policy di gruppo (GPO) in modo da AWS Private CA poter emettere certificati per oggetti Microsoft AD AWS gestiti.

Configurazione delle politiche di Active Directory per i controller di dominio

Attiva i criteri di Active Directory per i controller di dominio

1. Apri la scheda Rete e sicurezza.
2. Scegli AWS Private CA Connettori.
3. Scegli un connettore collegato all' AWS Private CA oggetto che rilascia i certificati del controller di dominio nella tua directory.
4. Scegli Azioni, Abilita i certificati del controller di dominio.

> **Important**
>
> Configura un modello di controller di dominio valido prima di attivare i certificati dei controller di dominio per evitare aggiornamenti ritardati.

Dopo aver attivato la registrazione dei certificati dei controller di dominio, i controller di dominio della directory richiedono e ricevono certificati da AWS Private CA Connector for AD.

Per modificare l'emissione dei certificati dei controller di dominio, collega innanzitutto i nuovi certificati AWS Private CA alla directory utilizzando un nuovo AWS Private CA Connector AWS Private CA for AD. Prima di attivare la registrazione dei certificati su quello nuovo AWS Private CA, disattiva la registrazione dei certificati su quello esistente:

Disattiva i certificati del controller di dominio

1. Apri la scheda Rete e sicurezza.
2. Scegli AWS Private CA Connettori.
3. Scegli un connettore collegato all' AWS Private CA oggetto che rilascia i certificati del controller di dominio nella tua directory.
4. Scegli Azioni, Disabilita i certificati del controller di dominio.

Configurazione delle politiche di Active Directory per utenti, computer e macchine aggiunti al dominio

Configura gli oggetti delle politiche di gruppo

1. Connect all'istanza di amministrazione di Microsoft AD AWS Managed e apri Server Manager dal menu Start.
2. In Strumenti, scegli Gestione dei criteri di gruppo.
3. In Foresta e domini, individua l'unità organizzativa (OU) del sottodominio (ad esempio, `corp` è l'unità organizzativa del sottodominio se hai seguito le procedure descritte inCreazione del tuo AWS Managed Microsoft AD) e fai clic con il pulsante destro del mouse sull'unità organizzativa del sottodominio. Scegli Crea un GPO in questo dominio, collegalo qui e inserisci PCA GPO come nome. Scegli OK.
4. Il GPO appena creato viene visualizzato dopo il nome del sottodominio. Fai clic con il pulsante destro del mouse su **`PCA GPO`** e scegli Modifica. Se si apre una finestra di dialogo con un messaggio di avviso che indica che si tratta di un collegamento e che le modifiche vengono

propagate a livello globale, confermate il messaggio scegliendo OK per continuare. Viene visualizzata la finestra Group Policy Management Editor.

5. Nella finestra Group Policy Management Editor, vai a Configurazione computer > Criteri > Impostazioni di Windows > Impostazioni di sicurezza > Politiche a chiave pubblica (scegli la cartella).
6. In Tipo di oggetto, scegli Certificate Services Client - Certificate Enrollment Policy.
7. Nella finestra Certificate Services Client - Certificate Enrollment Policy, modificate il modello di configurazione su Abilitato.
8. Conferma che la politica di registrazione di Active Directory sia selezionata e abilitata. Scegli Aggiungi.
9. Viene visualizzata la finestra di dialogo Certificate Enrollment Policy Server. Immettete l'endpoint del server della politica di iscrizione del certificato generato al momento della creazione del connettore nel campo Enter enrollment Server Policy URI. Lascia che il tipo di autenticazione sia integrato in Windows.
10. Scegli Convalida. Una volta completata la convalida, scegli Aggiungi.
11. Tornate alla finestra di dialogo Certificate Services Client - Certificate Enrollment Policy e selezionate la casella accanto al connettore appena creato per assicurarvi che il connettore sia la politica di registrazione predefinita.
12. Scegli Active Directory Enrollment Policy e scegli Rimuovi.
13. Nella finestra di dialogo di conferma, scegli Sì per eliminare l'autenticazione basata su LDAP.
14. Scegli Applica e quindi OK nella finestra Certificate Services Client - Certificate Enrollment Policy. Quindi chiudi la finestra.
15. In Tipo di oggetto per la cartella Public Key Policies, scegli Certificate Services Client - Auto-Enrollment.
16. Modificate l'opzione Modello di configurazione su Abilitato.
17. Conferma che le opzioni Rinnova certificati scaduti e Aggiorna certificati siano entrambe selezionate. Lascia le altre impostazioni così come sono.
18. Scegliete Applica, quindi OK e chiudete la finestra di dialogo.

Quindi, configura le politiche a chiave pubblica per la configurazione dell'utente ripetendo i passaggi 6-17 nella sezione Configurazione utente > Criteri > Impostazioni di Windows > Impostazioni di sicurezza > Politiche a chiave pubblica.

Dopo aver completato la configurazione GPOs e le politiche a chiave pubblica, gli oggetti del dominio richiedono i certificati da AWS Private CA Connector for AD e ricevono i certificati emessi da. AWS Private CA

Conferma dell'emissione di un AWS Private CA certificato

Il processo di aggiornamento AWS Private CA per l'emissione di certificati per AWS Managed Microsoft AD può richiedere fino a 8 ore.

Puoi effettuare una delle seguenti operazioni:

- Puoi aspettare questo periodo di tempo.
- È possibile riavviare i computer collegati al dominio Microsoft AD AWS gestito che erano configurati per ricevere certificati da AWS Private CA. Puoi quindi confermare che i certificati sono AWS Private CA stati emessi per i membri del tuo dominio Microsoft AD AWS gestito seguendo la procedura riportata nella Microsoftdocumentazione.
- È possibile utilizzare il PowerShell comando seguente per aggiornare i certificati per AWS Managed Microsoft AD:

```
certutil -pulse
```

Monitora il tuo AWS Managed Microsoft AD

Puoi ottenere il massimo da AWS Managed Microsoft AD scoprendo di più sui diversi stati di AWS Managed Microsoft AD e sul loro significato per AWS Managed Microsoft AD. Puoi anche utilizzare AWS servizi come Amazon Simple Notification Service e Amazon CloudWatch per monitorare il tuo AWS Managed Microsoft AD. Amazon Simple Notification Service può inviarti notifiche sullo stato della tua directory AWS Managed Microsoft AD. Amazon CloudWatch può monitorare le prestazioni dei tuoi controller di dominio Microsoft AD AWS gestiti.

Attività per monitorare il tuo AWS Managed Microsoft AD

- Informazioni sullo stato della directory AWS Managed Microsoft AD
- Attivazione delle notifiche sullo stato della directory AWS Managed Microsoft AD con Amazon Simple Notification Service
- Comprensione dei log delle directory di Microsoft AD AWS gestite
- Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS

- Utilizzo CloudWatch per monitorare le prestazioni dei controller di dominio Microsoft AD AWS gestiti
- Disattivazione dell'inoltro dei CloudWatch log di Amazon per Managed Microsoft AD AWS
- Monitoraggio del server DNS con Microsoft Event Viewer

Informazioni sullo stato della directory AWS Managed Microsoft AD

Di seguito sono elencati i diversi stati per una directory.

Active (Attivo)

La directory funziona normalmente. Nessun problema è stato rilevato da Directory Service per la directory.

Creating (Creazione in corso)

La directory è attualmente in fase di creazione. Solitamente la creazione di una directory può richiedere da 20 a 45 minuti, ma può variare in base al carico di sistema.

Deleted (Eliminato)

La directory è stata eliminata. Tutte le risorse per la directory sono state rilasciate. Una volta che una directory entra in questo stato, non può essere ripristinata.

Deleting (Eliminazione in corso)

La directory è attualmente in fase di eliminazione. La directory rimarrà in questo stato finché non sarà completamente eliminata. Una volta che una directory entra in questo stato, l'operazione di eliminazione non può essere annullata e la directory non può essere ripristinata.

Failed (Non riuscito)

Impossibile creare la directory. Elimina questa directory. Se questo problema persiste, contatta il Centro Supporto AWS.

Impaired (Insufficiente)

La directory è in esecuzione in uno stato danneggiato. Uno o più problemi sono stati rilevati e non tutte le operazioni di directory potrebbero lavorare alla massima capacità operativa. Ci sono molti motivi per cui la directory può trovarsi in questo stato. Queste includono le normali attività di manutenzione operativa, ad esempio l'applicazione di patch o la rotazione delle EC2 istanze, l'hot spotting temporaneo da parte di un'applicazione su uno dei controller di dominio o le modifiche apportate alla rete che interrompono inavvertitamente le comunicazioni tra gli elenchi.

Per ulteriori informazioni, consulta Risoluzione dei problemi relativi AWS a Managed Microsoft AD, Risoluzione dei problemi di AD Connector, Risoluzione dei problemi di Simple AD. Per i normali problemi relativi alla manutenzione, AWS risolve questi problemi entro 40 minuti. Se dopo aver esaminato l'argomento di risoluzione dei problemi, la directory è in stato Danneggiato per più di 40 minuti, consigliamo di contattare il Centro Supporto AWS.

> **Important**
>
> Non ripristinare uno snapshot mentre la directory è in stato danneggiato. Raramente è necessario ripristinare uno snapshot per risolvere dei danni. Per ulteriori informazioni, consulta Ripristino di AWS Managed Microsoft AD con istantanee.

Requested (Richiesta)

Una richiesta di creazione della directory è attualmente in sospeso.

RestoreFailed

Ripristino della directory da uno snapshot non riuscito. Riprova l'operazione di ripristino. Se il problema persiste, prova un altro snapshot oppure contatta il Centro Supporto AWS.

Restoring (Ripristino)

La directory è attualmente in corso di ripristino da uno snapshot automatico o manuale. Il ripristino da uno snapshot richiede solitamente alcuni minuti, a seconda delle dimensioni dei dati della directory nello snapshot.

Attivazione delle notifiche sullo stato della directory AWS Managed Microsoft AD con Amazon Simple Notification Service

Tramite Amazon Simple Notification Service (Amazon SNS), puoi ricevere messaggi e-mail o di testo (SMS) quando lo stato della directory cambia. Riceverai una notifica se la tua directory passa da uno stato Attivo a uno Non funzionante. Puoi anche ricevere una notifica quando la directory torna a uno stato Active (Attivo).

Come funziona

Amazon SNS utilizza «argomenti» per raccogliere e distribuire messaggi. Ogni argomento ha uno o più abbonati che ricevono i messaggi che sono stati pubblicati su quell'argomento. Utilizzando i

passaggi seguenti puoi aggiungere Directory Service come editore a un argomento di Amazon SNS. Quando Directory Service rileva una modifica nello stato della tua directory, pubblica un messaggio su quell'argomento, che viene quindi inviato ai sottoscrittori dell'argomento.

Puoi associare più directory come editori a un singolo argomento. Puoi anche aggiungere messaggi sullo stato della directory agli argomenti che hai creato in precedenza in Amazon SNS. Hai un controllo dettagliato su chi può pubblicare ed effettuare la sottoscrizione a un argomento. Per informazioni complete su Amazon SNS, consulta Cos'è Amazon SNS?.

> **Note**
>
> Le notifiche sullo stato delle directory sono una funzionalità regionale di AWS Managed Microsoft AD. Se si utilizza la replica multiregione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Abilitazione di Amazon SNS

Di seguito viene illustrato come abilitare Amazon SNS per Managed AWS Microsoft AD:

1. Accedi a Console di gestione AWS e apri la Directory Serviceconsole.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi abilitare la messaggistica SNS, quindi scegli la scheda Manutenzione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Manutenzione.
4. Nella sezione Monitoraggio delle directory, scegli Operazioni, quindi seleziona Crea notifica.
5. Nella pagina Crea notifica, seleziona Scegli un tipo di notifica, quindi scegli Crea una nuova notifica. In alternativa, se disponi già di un argomento SNS, puoi scegliere Associa ad argomento SNS esistente per l'invio di messaggi di stato da questa directory a tale argomento.

> **Note**
>
> Se scegli Crea una nuova notifica, ma utilizzerai lo stesso nome dell'argomento per un argomento SNS già esistente, Amazon SNS non crea un nuovo argomento, ma aggiunge semplicemente le nuove informazioni di abbonamento a quello esistente.
> Se scegli Associa ad argomento SNS esistente, potrai solo scegliere un argomento SNS presente nella stessa regione della directory.

6. Scegli il Tipo di destinatario e inserisci le informazioni di contatto del Destinatario. Se inserisci un numero di telefono per SMS, utilizza solo numeri. Non includere trattini, spazi o parentesi.
7. (Facoltativo) Fornisci un nome per l'argomento SNS e un relativo nome visualizzato. Il nome visualizzato è un nome breve di massimo 10 caratteri incluso in tutti i messaggi SMS di questo argomento. Quando utilizzi l'opzione SMS, il nome visualizzato è obbligatorio.

> **Note**
>
> Se hai effettuato l'accesso utilizzando un utente o un ruolo IAM con solo la policy DirectoryServiceFullAccessgestita, il nome dell'argomento deve iniziare con "DirectoryMonitoring». Se desideri personalizzare ulteriormente il nome dell'argomento, avrai bisogno di privilegi aggiuntivi per SNS.

8. Scegli Create (Crea).

Se desideri designare abbonati SNS aggiuntivi, ad esempio un indirizzo e-mail aggiuntivo, code Amazon SQS oppureAWS Lambda, puoi farlo dalla console Amazon SNS.

Rimuovere i messaggi di stato della directory da un argomento di Amazon SNS

Di seguito viene illustrato come rimuovere i messaggi di stato della directory AWS Managed Microsoft AD da un argomento di Amazon SNS:

1. Accedi a Console di gestione AWS e apri la Directory Serviceconsole.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

- Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi rimuovere i messaggi dello stato, quindi scegli la scheda Manutenzione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Manutenzione.

4. Nella sezione Monitoraggio delle directory, seleziona il nome di un argomento SNS nell'elenco, scegli Operazioni, quindi seleziona Rimuovi.
5. Scegli Rimuovi.

Questa operazione rimuove la directory come editore per l'argomento SNS selezionato.

Eliminazione di un argomento di Amazon SNS

Se desideri eliminare l'intero argomento, puoi farlo dalla console Amazon SNS.

Prima di eliminare un argomento Amazon SNS tramite la console di SNS, devi accertarti che una directory non stia inviando messaggi di stato a tale argomento.

Se elimini un argomento Amazon SNS tramite la console di SNS, questa modifica non si rifletterà immediatamente nella console Servizio di directory. Riceverai una notifica solo la prossima volta che una directory pubblicherà una notifica sull'argomento eliminato, nel qual caso vedrai uno stato aggiornato nella scheda Monitoraggio della directory che indica che l'argomento non è stato trovato.

Pertanto, per evitare di perdere importanti messaggi sullo stato della directory, prima di eliminare qualsiasi argomento da cui vengono ricevuti messaggiDirectory Service, associa la directory a un argomento Amazon SNS diverso.

Per ulteriori informazioni su come eliminare un argomento e un abbonamento Amazon SNS, consulta Eliminazione di un argomento e di un abbonamento ad Amazon SNS.

Comprensione dei log delle directory di Microsoft AD AWS gestite

I log di sicurezza delle istanze del controller di dominio Microsoft AD AWS gestito vengono archiviati per un anno. Puoi anche configurare la tua directory AWS Managed Microsoft AD per inoltrare i log dei controller di dominio ad Amazon CloudWatch Logs quasi in tempo reale. Per ulteriori informazioni, consulta Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS.

AWS registra i seguenti eventi per verificarne la conformità.

Categoria di monitoraggio	Impostazione di policy	Stato di audit
Accesso account	Convalida delle credenziali di audit	Successo, fallimento
	Audit di altri eventi di accesso di account	Successo, fallimento
	Verifica il servizio di autentica zione Kerberos	Successo, fallimento
Gestione dell'account	Audit della gestione dell'acco unt computer	Successo, fallimento
	Audit di altri eventi di gestione account	Successo, fallimento
	Audit della gestione dei gruppi di sicurezza	Successo, fallimento
	Audit della gestione dell'acco unt utente	Successo, fallimento
Monitoraggio dettagliato	Audit attività DPAPI	Successo, fallimento
	Audit attività PNP	Riuscito
	Audit della creazione dei processi	Successo, fallimento
Accesso a DS	Audit dell'accesso a Directory Service	Successo, fallimento
	Audit delle modifiche a Directory Service	Successo, fallimento
Accesso/Disconnessione	Audit blocco account	Successo, fallimento

Categoria di monitoraggio	Impostazione di policy	Stato di audit
	Audit della disconnessione	Riuscito
	Audit dell'accesso	Successo, fallimento
	Audit di altri eventi di accesso/ disconnessione	Successo, fallimento
	Audit dell'accesso speciale	Successo, fallimento
Accesso agli oggetti	Audit di altri eventi di accesso a oggetti	Successo, fallimento
	Audit degli archivi rimovibili	Successo, fallimento
	Audit della gestione temporanea policy di accesso centrale	Successo, fallimento
Modifiche di policy	Audit delle modifiche di policy	Successo, fallimento
	Audit delle modifiche delle policy di autenticazione	Successo, fallimento
	Audit delle modifiche delle policy di autorizzazione	Successo, fallimento
	Audit modifica policy a livello di regola MPSSVC	Riuscito
	Audit altri eventi di modifica policy	Errore
Uso dei privilegi	Audit dell'uso di privilegi sensibili	Successo, fallimento
System (Sistema)	Driver di controllo IPsec	Successo, fallimento
	Audit di altri eventi di sistema	Successo, fallimento

Categoria di monitoraggio	Impostazione di policy	Stato di audit
	Audit della modifica stato sicurezza	Successo, fallimento
	Audit dell'estensione del sistema di sicurezza	Successo, fallimento
	Audit dell'integrità del sistema	Successo, fallimento

Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS

Puoi utilizzare la Directory Service console o APIs inoltrare i registri degli eventi di sicurezza dei controller di dominio ad Amazon CloudWatch Logs per Managed AWS Microsoft AD. Questo consente di soddisfare i requisiti di monitoraggio di sicurezza, audit e policy di retention di log offrendo trasparenza degli eventi di sicurezza nella directory.

CloudWatch I log possono anche inoltrare questi eventi ad altri AWS account, AWS servizi o applicazioni di terze parti. Ciò semplifica il monitoraggio e la configurazione centralizzata degli avvisi che consentono di rilevare, in modo proattivo, attività insolite e rispondere a esse in tempo reale.

Una volta abilitato, puoi utilizzare la console CloudWatch Logs per recuperare i dati dal gruppo di log specificato quando hai abilitato il servizio. Questo gruppo di log contiene i log di sicurezza dei controller di dominio.

Per ulteriori informazioni sui gruppi di log e su come leggerne i dati, consulta Working with log groups and log stream nella Amazon CloudWatch Logs User Guide.

> **Note**
>
> L'inoltro dei log è una funzionalità regionale di Managed AWS Microsoft AD. Se si utilizza la replica multiregione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.
> Una volta abilitata, la funzionalità di inoltro dei log inizierà a trasmettere i log dai controller di dominio al gruppo di log specificato. CloudWatch Tutti i log creati prima che l'inoltro dei log sia abilitato non verranno trasferiti al gruppo di log. CloudWatch

Argomenti

Utilizzo di Console di gestione AWS per abilitare l'inoltro dei log di Amazon CloudWatch Logs

Puoi abilitare l'inoltro CloudWatch dei log di Amazon Logs per il tuo Managed AWS Microsoft AD nel. Console di gestione AWS

1. Nel riquadro di navigazione Directory Service console, scegliere Directories (Directory).
2. Scegli l'ID della directory AWS Managed Microsoft AD che desideri condividere.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi abilitare l'inoltro dei log, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Log forwarding (Inoltro dei log), scegliere Enable (Abilita).
5. Nella finestra di CloudWatch dialogo Abilita l'inoltro dei log a, scegli una delle seguenti opzioni:
   a. Seleziona Crea un nuovo gruppo di CloudWatch log, in Nome gruppo di CloudWatch log, specifica un nome a cui puoi fare riferimento in CloudWatch Logs.
   b. Seleziona Scegli un gruppo di CloudWatch log esistente e in Gruppi di CloudWatch log esistenti seleziona un gruppo di log dal menu.
6. Esaminare le informazioni sui prezzi e il collegamento e quindi scegliere Enable (Abilita).

Utilizzando la CLI o PowerShell per abilitare l'inoltro dei log di Amazon CloudWatch Logs

Prima di poter utilizzare il `ds create-log-subscription`comando, devi prima creare un gruppo di CloudWatch log Amazon e quindi creare una policy delle risorse IAM che conceda le autorizzazioni necessarie a quel gruppo. Per abilitare l'inoltro dei log utilizzando la CLI oppure PowerShell, completare i seguenti passaggi.

Passaggio 1: creare un gruppo di log in Logs CloudWatch

Creare un gruppo di log che verrà utilizzato per ricevere i log di sicurezza dai controller di dominio. Consigliamo di aggiungere `/aws/directoryservice/` prima del nome, ma non è obbligatorio. Esempio:

CLI Command

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-1111111111'
```

PowerShell Command

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-1111111111'
```

Per istruzioni su come creare un gruppo di CloudWatch log, consulta Creare un gruppo di log in CloudWatch Logs nella Amazon CloudWatch Logs User Guide.

Fase 2: Creare una politica delle risorse CloudWatch Logs in IAM

Crea una politica delle risorse CloudWatch Logs che conceda Directory Service i diritti di aggiungere log nel nuovo gruppo di log che hai creato nel passaggio 1. È possibile specificare l'ARN esatto per il gruppo di log per limitare l'accesso ad altri gruppi Directory Service di log o utilizzare una wild card per includere tutti i gruppi di log. La seguente policy di esempio utilizza il metodo wild card per identificare che verranno inclusi tutti i gruppi di log che iniziano con `/aws/directoryservice/` l'AWSaccount in cui risiede la directory.

Dovrai salvare questa policy in un file di testo (ad esempio DSPolicy .json) sulla tua workstation locale poiché dovrai eseguirla dalla CLI. Esempio:

CLI Command

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document
          file://DSPolicy.json
```

PowerShell Command

```
$PolicyDocument = Get-Content .\DSPolicy.json -Raw
```

```
Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument
 $PolicyDocument
```

Fase 3: Creare un abbonamento di registro Directory Service

In questa fase finale è possibile abilitare l'inoltro di log creando la sottoscrizione di log. Esempio:

CLI Command

```
aws ds create-log-subscription --directory-id 'd-1111111111' --log-group-name '/aws/
directoryservice/d-1111111111'
```

PowerShell Command

```
New-DSLogSubscription -DirectoryId 'd-1111111111' -LogGroupName '/aws/
directoryservice/d-1111111111'
```

Utilizzo CloudWatch per monitorare le prestazioni dei controller di dominio Microsoft AD AWS gestiti

Directory Service si integra con Amazon CloudWatch per aiutarti a fornire importanti metriche prestazionali per ogni controller di dominio in Active Directory. Ciò significa che puoi monitorare i contatori delle prestazioni dei controller di dominio, come l'utilizzo della CPU e della memoria. Puoi inoltre configurare allarmi e avviare azioni automatiche per rispondere a periodi di utilizzo elevato. Ad esempio, puoi configurare un allarme per un utilizzo della CPU del controller di dominio superiore al 70% e creare un argomento SNS per avvisare l'utente quando ciò si verifica. Puoi utilizzare questo argomento SNS per avviare l'automazione, ad esempio AWS Lambda le funzioni, per aumentare il numero di controller di dominio in Active Directory.

Per ulteriori informazioni sul monitoraggio dei controller di dominio, consulta Determinare quando aggiungere controller di dominio con metriche CloudWatch .

Sono previste commissioni associate ad Amazon CloudWatch. Per ulteriori informazioni, consulta la sezione CloudWatchFatturazione e costi.

> **Important**
>
> Le metriche delle prestazioni dei controller di dominio con non CloudWatch sono disponibili nella regione Canada occidentale (Calgary).
> Per abilitarlo CloudWatch, consulta. Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS

Ricerca delle metriche delle prestazioni dei controller di dominio in CloudWatch

Nella CloudWatch console Amazon, le metriche per un determinato servizio vengono raggruppate innanzitutto in base allo spazio dei nomi del servizio. Puoi aggiungere filtri per i parametri subordinati a quel namespace. Utilizzare la procedura seguente per individuare lo spazio dei nomi e la metrica subordinata corretti necessari per configurare le metriche del controller di dominio AWS Microsoft AD gestito in. CloudWatch

Per trovare le metriche dei controller di dominio nella console CloudWatch

1. Accedi a Console di gestione AWS e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Dall'elenco dei parametri, seleziona lo spacename di Directory Service, quindi dall'elenco seleziona il parametro Microsoft AD gestito da AWS .

Per istruzioni su come configurare le metriche dei controller di dominio utilizzando la CloudWatch console, vedi Come automatizzare il ridimensionamento gestito di AWS Microsoft AD in base alle metriche di utilizzo nel Security Blog. AWS

Determinare quando aggiungere controller di dominio con metriche CloudWatch

Il bilanciamento del carico su tutti i controller di dominio è importante per la resilienza e le prestazioni di Active Directory. Per aiutarti a ottimizzare le prestazioni dei controller di dominio in AWS Managed Microsoft AD, ti consigliamo innanzitutto di monitorare le metriche importanti CloudWatch per formare una linea di base. Durante questo processo, analizzi Active Directory nel tempo per identificare l'utilizzo medio e massimo di Active Directory. Dopo aver determinato la linea di base, puoi monitorare queste metriche regolarmente per determinare quando aggiungere un controller di dominio ad Active Directory.

È importante monitorare regolarmente i seguenti parametri. Per un elenco completo delle metriche dei controller di dominio disponibili in CloudWatch, consulta. AWS Contatori delle prestazioni Microsoft AD gestiti

- Parametri specifici del controller di dominio, come:
  - Processore
  - Memoria
  - Disco logico
  - Interfaccia di rete
- AWS Metriche gestite specifiche della directory Microsoft AD, come:
  - Ricerche LDAP
  - Associazioni
  - Query DNS
  - Letture della directory
  - Scritture della directory

Per istruzioni su come configurare le metriche dei controller di dominio utilizzando la CloudWatch console, vedi Come automatizzare il ridimensionamento gestito di AWS Microsoft AD in base alle metriche di utilizzo nel Security Blog. AWS Per informazioni generali sui parametri in CloudWatch, consulta Using Amazon CloudWatch metrics nella Amazon CloudWatch User Guide.

Per informazioni generali sulla pianificazione dei controller di dominio, consulta Pianificazione della capacità per i servizi di dominio di Active Directory sul sito Web Microsoft.

AWS Contatori delle prestazioni Microsoft AD gestiti

La tabella seguente elenca tutti i contatori delle prestazioni disponibili in Amazon CloudWatch per tracciare le prestazioni dei controller di dominio e delle directory in AWS Managed Microsoft AD.

Categoria parametro	Nome parametro
Database ==> Istanze (NTDSA)	%Hit della cache del database
	Latenza media delle letture del database I/O
	I/O Database Reads/sec

Categoria parametro	Nome parametro
	Latenza media delle scritture dei log I/O
DirectoryServices (NTDS)	Tempo di associazione LDAP
	Operazioni di replica in attesa di DRA
	Sincronizzazioni di replica in attesa di DRA
DNS	Query ricorsive/sec
	Errore di query ricorsive/sec
	Query TCP ricevute/sec
	Query totali ricevute/sec
	Risposta totale inviata/sec
	Query UDP ricevute/sec
LogicalDisk	Media Lunghezza coda disco
	% spazio libero
Memoria	% byte impegnati in uso
	Durata media della cache in standby a lungo termine (sec)
Interfaccia di rete	Byte inviati/sec
	Byte ricevuti/sec
	Larghezza di banda attuale
NTDS	Ritardo di coda stimato ATQ
	Latenza delle richieste ATQ
	Letture della directory DS/sec

Categoria parametro	Nome parametro
	Ricerche nella directory DS/sec
	Scritture directory DS/sec
	Sessioni client LDAP
	Ricerche LDAP/sec
	Associazioni LDAP completate/sec
Processore	% tempo del processore
Statistiche di sicurezza a livello di sistema	Autenticazioni Kerberos
	Autenticazioni NTLM

Disattivazione dell'inoltro dei CloudWatch log di Amazon per Managed Microsoft AD AWS

Puoi disabilitare l'inoltro CloudWatch dei log dei log per il tuo Managed AWS Microsoft AD in. Console di gestione AWS Per ulteriori informazioni sull'inoltro dei log, vedere. the section called “Utilizzato CloudWatch per monitorare la directory”

1. Nel riquadro di navigazione Directory Service console, scegliere Directories (Directory).
2. Scegli l'ID della directory AWS Managed Microsoft AD che desideri condividere.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi disabilitare l'inoltro dei log, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Log forwarding (Inoltro dei log), scegliere Disable (Disabilita).
5. Dopo aver letto le informazioni nella finestra di dialogo Disabilita l'inoltro dei log, scegli Disabilita.

Monitoraggio del server DNS con Microsoft Event Viewer

Puoi controllare gli eventi di AWS Managed Microsoft AD DNS, semplificando l'identificazione e la risoluzione dei problemi DNS. Ad esempio, se manca un record DNS, puoi usare il log di eventi di audit DNS per individuare la causa e risolvere il problema. Puoi usare i log di eventi di audit DNS per potenziare la sicurezza rilevando e bloccando le richieste provenienti da indirizzi IP sospetti.

A tal fine, è necessario aver effettuato l'accesso all'account Amministratore o con un account membro del gruppo Amministratori del sistema del nome di dominio AWS . Per ulteriori informazioni su questo gruppo, consulta Cosa viene creato con AWS Managed Microsoft AD.

Per accedere a Event Viewer per il tuo DNS Microsoft AD AWS gestito

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Istanze.
3. Individua un' EC2 istanza Amazon aggiunta alla tua directory AWS Managed Microsoft AD. Seleziona l'istanza quindi scegli Connect (Connetti).
4. Una volta connesso all' EC2 istanza Amazon, apri il menu Start e seleziona la cartella Strumenti di amministrazione di Windows. All'interno della cartella Strumenti di amministrazione, seleziona Event Viewer.
5. Nella finestra Event Viewer (Visualizzatore eventi), scegli Action (Operazione) quindi Connect to Another Computer (Collega a un altro computer).
6. Seleziona Altro computer, digita il nome o l'indirizzo IP di uno dei tuoi server Microsoft AD DNS AWS gestiti e scegli OK.
7. Nel riquadro di sinistra, passa a Applications and Services Logs>Microsoft>Windows>DNS-Server, quindi seleziona Audit.

Accesso ad AWS applicazioni e servizi dal tuo AWS Managed Microsoft AD

Puoi concedere l'accesso agli utenti di AWS Managed Microsoft AD per accedere ad AWS applicazioni e servizi. Alcune di queste AWS applicazioni e servizi includono:

- Amazon Chime
- Amazon EC2

- Suite rapida
- Console di gestione AWS
- Amazon WorkSpaces

Puoi anche utilizzare l'accesso URLs e il Single Sign-On con Managed AWS Microsoft AD.

Attività per accedere ad AWS applicazioni e servizi da AWS Managed Microsoft AD

- Compatibilità delle applicazioni per AWS Managed Microsoft AD
- Consentire l'accesso ad AWS applicazioni e servizi per AWS Managed Microsoft AD
- Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite
- Creazione di un URL di accesso per AWS Managed Microsoft AD
- Abilitazione del Single Sign-On per Managed AWS Microsoft AD

Compatibilità delle applicazioni per AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) è compatibile con più AWS servizi e applicazioni di terze parti.

Di seguito è riportato un elenco di AWS applicazioni e servizi compatibili:

- Amazon Chime
- Amazon Connect
- Amazon EC2
- Suite rapida
- Amazon RDS
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS IAM Identity Center
- AWS License Manager
- Console di gestione AWS
- FSx per Windows File Server
- WorkSpaces

Per ulteriori informazioni, consulta Consentire l'accesso ad AWS applicazioni e servizi per AWS Managed Microsoft AD.

A causa della vastità delle off-the-shelf applicazioni personalizzate e commerciali che utilizzano Active Directory, non esegue e AWS non può eseguire verifiche formali o ampie della compatibilità delle applicazioni di terze parti con AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD). Sebbene AWS collabori con i clienti nel tentativo di superare eventuali problemi di installazione delle applicazioni che potrebbero incontrare, non siamo in grado di garantire che qualsiasi applicazione sia o continuerà a essere compatibile con AWS Managed Microsoft AD.

Le seguenti applicazioni di terze parti sono compatibili con AWS Managed Microsoft AD:

- Attivazione basata su Active Directory (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- Application Server (.NET)
- Microsoft Entra(precedentemente noto come Azure Active Directory (AzureAD))
- Microsoft Entra Connect(precedentemente noto come) Azure Active Directory Connect
- Distributed File System Replication (DFSR)
- Distributed File System Namespaces (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(inclusi i gruppi di disponibilità Always On di SQL Server)
- Microsoft System Center Configuration Manager(SCCM) - L'utente che implementa SCCM deve essere un membro del gruppo AWS Delegated System Management Administrators.
- Microsoft Windows and Windows Server OS
- Office 365

Tenere presente che alcune configurazioni di queste applicazioni potrebbero non essere supportate.

Linee guida per la compatibilità

Sebbene le applicazioni possano avere configurazioni incompatibili, spesso le configurazioni di distribuzione delle applicazioni possono superare l'incompatibilità. Di seguito sono descritti i motivi

più comuni per l'incompatibilità delle applicazioni. I clienti possono utilizzare queste informazioni per analizzare le caratteristiche di compatibilità di un'applicazione desiderata e identificare le potenziali modifiche di distribuzione.

- Amministratore di dominio o altre autorizzazioni con privilegi – Alcune applicazioni richiedono di essere installate dall'utente amministratore di dominio. Poiché è AWS necessario mantenere il controllo esclusivo di questo livello di autorizzazione per fornire Active Directory come servizio gestito, non è possibile agire come amministratore di dominio per installare tali applicazioni. Tuttavia, spesso è possibile installare tali applicazioni delegando autorizzazioni specifiche, meno privilegiate e AWS supportate alla persona che esegue l'installazione. Per ulteriori dettagli sulle precise autorizzazioni richieste da un'applicazione, rivolgiti al fornitore dell'applicazione. Per ulteriori informazioni sulle autorizzazioni che AWS consentono di delegare, vedere. Cosa viene creato con AWS Managed Microsoft AD
- Accesso a contenitori Active Directory privilegiati: all'interno della directory, AWS Managed Microsoft AD fornisce un'unità organizzativa (OU) sulla quale hai il pieno controllo amministrativo. Non disponi di autorizzazioni di creazione o scrittura e potresti avere autorizzazioni in lettura limitate per i container che si trovano in una posizione nella struttura dell'Active Directory superiore rispetto alla tua unità organizzativa. Le applicazioni che creano o accedono ai container per i quali non si dispone di autorizzazioni potrebbero non funzionare. Tuttavia, tali applicazioni spesso hanno la possibilità di utilizzare un container che puoi creare nella tua unità organizzativa come alternativa. Verifica con il provider di applicazioni i diversi modi disponibili per creare e utilizzare un container nella tua unità organizzativa come alternativa. Per ulteriori informazioni sull'unità organizzativa, vedereCosa viene creato con AWS Managed Microsoft AD.
- Modifiche allo schema durante il flusso di lavoro di installazione - Alcune applicazioni Active Directory richiedono delle modifiche allo schema predefinito di Active Directory e potrebbero tentare di installare tali modifiche durante il flusso di lavoro di installazione delle applicazioni. Grazie alla natura privilegiata delle estensioni dello schema, AWS rende possibile tutto ciò importando file LDIF (Lightweight Directory Interchange Format) solo tramite console Directory Service , CLI o SDK. Tali applicazioni sono spesso dotate di un file LDIF che è possibile applicare alla directory tramite il processo di aggiornamento dello schema. Directory Service Per ulteriori informazioni su come funziona il processo di importazione LDIF, consulta Tutorial: estensione dello schema AWS Managed Microsoft AD. Puoi installare l'applicazione in modo da evitare l'installazione dello schema durante il processo di installazione.

Applicazioni sicuramente incompatibili

Di seguito sono elencate le off-the-shelf applicazioni commerciali più richieste per le quali non è stata trovata una configurazione compatibile con AWS Managed Microsoft AD. AWS aggiorna questo elenco di tanto in tanto a sua esclusiva discrezione a titolo di cortesia per aiutarti a evitare sforzi improduttivi. AWS fornire queste informazioni senza garanzie o reclami riguardanti la compatibilità attuale o futura.

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

Consentire l'accesso ad AWS applicazioni e servizi per AWS Managed Microsoft AD

Gli utenti possono autorizzare AWS Managed Microsoft AD a fornire ad AWS applicazioni e servizi, come Amazon WorkSpaces, l'accesso al tuo Active Directory. Le seguenti AWS applicazioni e servizi possono essere abilitati o disabilitati per funzionare con AWS Managed Microsoft AD.

AWS applicazione/servizio	Ulteriori informazioni…
Amazon Chime	Per ulteriori informazioni, vedere Connessione ad Active Directory.
Amazon Connect	Per ulteriori informazioni, consulta la Guida all'amministrazione di Amazon Connect.
Amazon EC2	Per ulteriori informazioni, consulta Modi per aggiungere un' EC2 istanza Amazon al tuo AWS Managed Microsoft AD.
File server Amazon FSx per Windows	Per ulteriori informazioni, consulta Usare Amazon FSx with AWS Directory Service per Microsoft Active Directory.

AWS applicazione/servizio	Ulteriori informazioni…
Quick Suite	Per ulteriori informazioni, consulta l'edizione Utilizzo di Active Directory con Quick Suite Enterprise.
Amazon Relational Database Service	Per ulteriori informazioni, consulta gli argomenti seguenti: • Utilizzo dell'autenticazione Kerberos per MySQL • Utilizzo dell'autenticazione Kerberos con Amazon RDS for Oracle • Utilizzo dell'autenticazione Kerberos con Amazon RDS for PostgreSQL • Utilizzo di AWS Managed Microsoft AD con Amazon RDS for SQL Server
Amazon WorkDocs	Per ulteriori informazioni, consulta Enable Amazon WorkDocs for AWS Managed Microsoft AD.
Amazon WorkMail	Per ulteriori informazioni, consulta la sezione Creazione di un'organizzazione.
Amazon WorkSpaces	Puoi creare un Simple AD, AWS Managed Microsoft AD o AD Connector direttamente da WorkSpaces. È sufficiente avviare Advanced Setup (Impostazioni avanzate) durante la creazione del Workspace. Per ulteriori informazioni, consulta Registrare una Directory Service directory esistente con WorkSpaces Personal.
AWS Client VPN	Per ulteriori informazioni, consulta l'autenticazione Active Directory in Client VPN.

AWS applicazione/servizio	Ulteriori informazioni…
AWS IAM Identity Center	Per ulteriori informazioni, consulta Connect to a Microsoft AD directory.
AWS License Manager	Per ulteriori informazioni, consulta la sezione Gestione degli abbonamenti basati sugli utenti in License Manager.
Console di gestione AWS	Per ulteriori informazioni, consulta Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite.
AWS Autorità di certificazione privata	Per ulteriori informazioni, consulta Configurazione di AWS Private CA Connector per Active Directory.
AWS Transfer Family	Per ulteriori informazioni, consulta Configurazione di un endpoint server SFTP, FTPS o FTP.

Una volta abilitato, puoi gestire l'accesso alle directory nella console dell'applicazione o del servizio a cui intendi consentire l'accesso alla directory.

Trova applicazioni e servizi AWS

Per trovare le AWS applicazioni e i servizi descritti in precedenza nella Directory Service console, procedi nel seguente modo.

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Consulta l'elenco nella sezione app e servizi AWS .

Per ulteriori informazioni su come autorizzare o rimuovere l'autorizzazione all'utilizzo Directory Service di AWS applicazioni e servizi, vedere. Autorizzazione per l'AWSutilizzo di applicazioni e servizi Directory Service

Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite

Directory Service consente di concedere ai membri della directory l'accesso a Console di gestione AWS. Per impostazione predefinita, i membri della directory non hanno accesso ad alcuna AWS risorsa. Assegni ruoli IAM ai membri della tua directory per consentire loro di accedere ai vari AWS servizi e risorse. Il ruolo IAM definisce i servizi, le risorse e il livello di accesso dei membri della directory.

Prima di poter concedere l'accesso alla console ai membri della directory, la directory deve disporre di un URL di accesso. Per ulteriori informazioni su come visualizzare i dettagli della directory e ottenere l'URL di accesso, consulta Visualizzazione delle informazioni sulla directory AWS Managed Microsoft AD. Per ulteriori informazioni su come creare un URL di accesso, consulta Creazione di un URL di accesso per AWS Managed Microsoft AD.

Per ulteriori informazioni su come creare e assegnare ruoli IAM ai membri della directory, consulta Concedere agli utenti e ai gruppi di AWS Managed Microsoft AD l'accesso alle AWS risorse con ruoli IAM.

Argomenti

- Abilitazione dell'accesso Console di gestione AWS
- Disabilitazione dell'accesso Console di gestione AWS
- Impostazione della durata della Console di gestione AWS sessione di accesso

Articolo correlato del blog AWS sulla sicurezza

- Come accedere all' Console di gestione AWS utilizzo di Microsoft AD AWS gestito e alle credenziali locali

Articolo correlato AWS re:Post

- Come posso concedere l'accesso a un Console di gestione AWS utente di Active Directory locale?

> **Note**
>
> L'accesso a Console di gestione AWS è una funzionalità regionale di AWS Managed Microsoft AD. Se si utilizza la replica multiregione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Abilitazione dell'accesso Console di gestione AWS

Per impostazione predefinita, l'accesso alla console non è abilitato per tutte le directory. Per abilitare l'accesso alla console dei membri e dei gruppi della directory, segui la procedura indicata:

Abilitazione dell'accesso alla console

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiarea sono visualizzate più regioni, seleziona la regione a cui desideri abilitare l'accesso Console di gestione AWS, quindi scegli la scheda Gestione delle applicazioni. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
4. Nella sezione Console di gestione AWS, scegli Abilita. Ora l'accesso alla console è abilitato per la tua directory.

> **Important**
>
> Prima che gli utenti possano accedere alla console con il tuo URL di accesso, devi prima aggiungere gli utenti al ruolo IAM. Per ulteriori informazioni sull'assegnazione di ruoli IAM agli utenti, consulta Assegnazione di utenti o gruppi a un ruolo IAM esistente. Dopo l'assegnazione dei ruoli IAM, gli utenti possono accedere alla console utilizzando l'URL di accesso. Ad esempio, se l'URL di accesso alla directory è`example-corp.awsapps.com`, l'URL per accedere alla console è`https://example-corp.awsapps.com/console/`.

Disabilitazione dell'accesso Console di gestione AWS

Per disabilitare Console di gestione AWS l'accesso per gli utenti e i gruppi della directory AWS Managed Microsoft AD, procedi nel seguente modo:

Disabilitare l'accesso alla console

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiarea sono visualizzate più regioni, seleziona la regione a cui desideri disabilitare l'accesso Console di gestione AWS, quindi scegli la scheda Gestione delle applicazioni. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
4. Nella sezione Console di gestione AWS, scegli Disabilita. Ora l'accesso alla console è disabilitato per la tua directory.
5. Se nella directory sono stati assegnati ruoli IAM a utenti o gruppi, il pulsante Disabilita potrebbe non essere disponibile. In questo caso, devi rimuovere tutte le assegnazioni dei ruoli IAM per la directory prima di procedere, tra cui quelle per gli utenti o i gruppi della directory che sono stati eliminati, che saranno visualizzati come Utente eliminato o Gruppo eliminato.

   Una volta rimosse tutte le assegnazioni dei ruoli IAM, ripeti le fasi indicate precedentemente.

Impostazione della durata della Console di gestione AWS sessione di accesso

Per impostazione predefinita, gli utenti hanno a disposizione 1 ora per utilizzare la sessione dopo aver effettuato correttamente l'accesso Console di gestione AWS prima di disconnettersi. Successivamente, gli utenti devono accedere nuovamente per avviare la prossima sessione di 1 ora prima che venga effettuato nuovamente il logout. Puoi utilizzare la procedura seguente per modificare il periodo di tempo fino a 12 ore per ogni sessione.

Per impostare la durata della sessione di Console di gestione AWS accesso

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.

3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi impostare il periodo di sessione del login, quindi scegli la scheda Gestione dell'applicazione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.

4. Nella sezione App e servizi AWS , scegli Console di gestione AWS .
5. Nella finestra di dialogo Gestisci l'accesso alle AWS risorse, scegli Continua.
6. Nella pagina Assign users and groups to IAM roles (Assegna utenti e gruppi a ruoli IAM), in Set login session length (Imposta periodo di sessione di login) modifica il valore numerato, quindi seleziona Save (Salva).

Creazione di un URL di accesso per AWS Managed Microsoft AD

Un URL di accesso viene utilizzato con AWS applicazioni e servizi, come Amazon WorkDocs, per raggiungere una pagina di accesso associata alla tua directory. Puoi creare un URL di accesso per la tua directory eseguendo la procedura seguente.

Considerazioni

- L'URL deve essere univoco a livello globale.
- L'URL di accesso può essere configurato solo dalla regione principale quando si utilizzano directory multiregionali.
- Una volta creato, l'URL di accesso all'applicazione per questa directory non potrà essere modificato. Dopo aver creato un URL di accesso, non può essere utilizzato da altri utenti. Se cancelli la tua directory, anche l'URL di accesso viene eliminato e può quindi essere utilizzato da qualsiasi altro account.

Per creare un URL di accesso

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

- Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona la regione primaria, quindi scegli la scheda Gestione dell'applicazione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.

4. Nella sezione URL di accesso all'applicazione, se un URL di accesso non è stato assegnato alla directory, viene visualizzato il pulsante Crea. Inserisci un alias di directory e scegli Crea. Se viene restituito un errore Entità già esistente, l'alias di directory specificato è già stato allocato. Scegli un altro alias e ripeti questa procedura.

   L'URL di accesso viene visualizzato nel formato *<alias>* .awsapps.com. Per impostazione predefinita, questo URL ti porterà alla pagina di accesso per. WorkDocs

Abilitazione del Single Sign-On per Managed AWS Microsoft AD

AWS Directory Service offre la possibilità di consentire agli utenti di accedere WorkDocs da un computer aggiunto alla directory senza dover inserire le proprie credenziali separatamente.

Prima di abilitare l'accesso single sign-on, è necessario eseguire operazioni aggiuntive per abilitare il browser Web dei tuoi utenti a supportare l'accesso single sign-on. Gli utenti potrebbero dover modificare le proprie impostazioni del browser Web per abilitare l'accesso single sign-on.

> **Note**
>
> L'accesso single sign-on funziona solo quando viene utilizzato su un computer collegato alla directory Directory Service e non può essere utilizzato sui computer che non sono collegati alla directory.

Se la directory è una directory del connettore AD e l'account del servizio Connettore AD non dispone dell'autorizzazione per aggiungere o rimuovere l'attributo nome dell'entità servizio, per i passaggi 5 e 6 seguenti sono disponibili due opzioni:

1. È possibile procedere e verrà richiesto il nome utente e la password per un utente di directory che dispone di questa autorizzazione per aggiungere o rimuovere l'attributo nome dell'entità servizio nell'account del servizio Connettore AD. Queste credenziali vengono utilizzate solo per abilitare

l'accesso single sign-on e non vengono archiviate dal servizio. Le autorizzazioni dell'account del servizio Connettore AD non vengono modificate.

2. Puoi delegare le autorizzazioni per consentire all'account del servizio AD Connector di aggiungere o rimuovere l'attributo del nome principale del servizio su se stesso, puoi eseguire i PowerShell comandi seguenti da un computer aggiunto al dominio utilizzando un account che dispone delle autorizzazioni per modificare le autorizzazioni sull'account del servizio AD Connector. Il comando seguente darà all'account del servizio Connettore AD la possibilità di aggiungere e rimuovere un attributo nome dell'entità servizio solo per se stesso.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Per abilitare o disabilitare il single sign-on con WorkDocs

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).

4. Nella sezione URL di accesso all'applicazione, scegli Abilita per abilitare il single sign-on per. WorkDocs

   Se non visualizzi il pulsante Enable (Abilita), potresti dover creare un URL di accesso prima che questa opzione venga visualizzata. Per ulteriori informazioni su come creare un URL di accesso, consulta Creazione di un URL di accesso per AWS Managed Microsoft AD.
5. Nella finestra di dialogo Enable Single Sign-On for this directory (Abilita accesso single sign-on per questa directory) scegli Enable (Abilita). L'accesso single sign-on è abilitato per la directory.
6. Se in seguito desiderate disabilitare il Single Sign-On con WorkDocs, scegliete Disabilita, quindi nella finestra di dialogo Disabilita il Single Sign-On per questa directory, scegliete nuovamente Disabilita.

Argomenti

- Accesso con autenticazione unica per IE e Chrome
- Accesso con autenticazione unica per Firefox

Accesso con autenticazione unica per IE e Chrome

Per permettere ai browser Internet Explorer (IE) e Google Chrome di Microsoft di supportare l'accesso single sign-on, è necessario eseguire le attività seguenti sul computer client:

- Aggiungi il tuo URL di accesso (ad esempio, https://*<alias>*.awsapps.com) all'elenco dei siti approvati per il Single Sign-On.
- Abilita lo scripting attivo (). JavaScript
- Permetti l'accesso automatico.
- Abilita l'autenticazione integrata.

Tu o i tuoi utenti potete eseguire queste attività manualmente oppure potete modificare queste impostazioni usando le impostazioni delle policy di gruppo.

Argomenti

- Aggiornamento manuale per l'accesso con autenticazione unica su Windows
- Aggiornamento manuale per l'accesso con autenticazione unica su OS X
- Impostazioni delle policy di gruppo per l'accesso con autenticazione unica

Aggiornamento manuale per l'accesso con autenticazione unica su Windows

Per abilitare manualmente l'accesso single sign-on su un computer Windows, esegui la procedura seguente sul computer client. Alcune di queste impostazioni possono essere già impostate correttamente.

Abilitazione manuale dell'accesso single sign-on per Internet Explorer e Chrome su Windows

1. Per aprire la finestra di dialogo Internet Properties (Proprietà Internet), seleziona il menu Start, digita `Internet Options` nella casella di ricerca e seleziona Internet Options (Opzioni Internet).
2. Aggiungi il tuo URL di accesso all'elenco dei siti approvati per l'accesso single sign-on eseguendo le fasi seguenti:
    a. Nella finestra di dialogo Internet Properties (Proprietà Internet), seleziona la scheda Security (Sicurezza).
    b. Seleziona Local Intranet (Intranet locale) e scegli Sites (Siti).
    c. Nella finestra di dialogo Local intranet (Intranet locale) scegli Advanced (Opzioni avanzate).
    d. Aggiungi il tuo URL di accesso all'elenco di siti Web e scegli Close (Chiudi).
    e. Nella finestra di dialogo Local intranet (Intranet locale) scegli OK.
3. Per abilitare lo scripting attivo, segui la procedura seguente:
    a. Nella scheda Security (Sicurezza) della finestra di dialogo Internet Properties (Proprietà Internet), scegli Custom level (Livello personalizzato).
    b. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale), scorri verso il basso a Scripting e seleziona Enable (Abilita) sotto Active scripting (Scripting attivo).
    c. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale) scegli OK.
4. Per abilitare l'accesso automatico, segui la procedura seguente:
    a. Nella scheda Security (Sicurezza) della finestra di dialogo Internet Properties (Proprietà Internet), scegli Custom level (Livello personalizzato).
    b. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale), scorri verso il basso a User Authentication (Autenticazione utenti) e seleziona Automatic logon only in Intranet zone (Accesso automatico solo in area intranet) sotto Logon (Accesso).

c. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale) scegli OK.

d. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale) scegli OK.

5. Per abilitare l'autenticazione integrata, segui la procedura seguente:

   a. Nella finestra di dialogo Internet Properties (Proprietà Internet), seleziona la scheda Advanced (Opzioni avanzate).

   b. Scorri verso il basso a Security (Sicurezza) e seleziona Enable Integrated Windows Authentication (Abilita autenticazione di Windows integrata).

   c. Nella finestra di dialogo Internet Properties (Proprietà Internet) scegli OK.

6. Chiudi e riapri il browser perché queste modifiche diventino effettive.

Aggiornamento manuale per l'accesso con autenticazione unica su OS X

Per abilitare manualmente l'accesso single sign-on a Chrome su OS X, esegui la procedura seguente sul computer client. Dovrai disporre di diritti di amministratore sul tuo computer per completare questa procedura.

Abilitazione manuale dell'accesso single sign-on a Chrome su OS X

1. Aggiungete l'URL di accesso alla AuthServerAllowlistpolicy eseguendo il comando seguente:

   ```
   defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
   ```

2. Apri System Preferences (Preferenze di sistema), vai al pannello Profiles (Profili) ed elimina il profilo `Chrome Kerberos Configuration`.

3. Riavvia Chrome e apri chrome://policy in Chrome per confermare che le nuove impostazioni siano effettive.

Impostazioni delle policy di gruppo per l'accesso con autenticazione unica

L'amministratore di dominio può implementare le impostazioni delle policy di gruppo per effettuare le modifiche dell'accesso single sign-on su computer client collegati al dominio.

> **Note**
>
> Se gestisci i browser web Chrome sui computer del tuo dominio con i criteri di Chrome, devi aggiungere il tuo URL di accesso alla AuthServerAllowlistpolitica. Per ulteriori informazioni su come impostare le policy di Chrome, vai all'argomento relativo alle Impostazioni delle policy in Chrome.

Abilitazione manuale dell'accesso single sign-on per Internet Explorer e Chrome utilizzando le impostazioni delle policy di gruppo

1. Crea un nuovo oggetto Group Policy seguendo questa procedura:

   a. Apri lo strumento di gestione di Group Policy, vai al tuo dominio e seleziona Group Policy Objects (Oggetti Group Policy).

   b. Dal menu principale, seleziona Action (Operazione) e quindi New (Nuovo).

   c. Nella finestra di dialogo New GPO (Nuovo GPO) digita un nome descrittivo per l'oggetto Group Policy, ad esempio `IAM Identity Center Policy` e lascia Source Starter GPO (GPO Starter di origine) impostato su (none) (nessuno). Fai clic su OK.

2. Aggiungi l'URL di accesso all'elenco dei siti approvati per l'accesso single sign-on eseguendo la procedura seguente:

   a. Nello strumento di gestione di policy di gruppo, vai al tuo dominio, seleziona Oggetti di policy di gruppo, apri il menu contestuale (pulsante destro del mouse) per la tua policy Centro identità IAM e scegli Modifica.

   b. Nella struttura della policy, seleziona User Configuration (Configurazione utente) > Preferences (Preferenze) > Windows Settings (Impostazioni di Windows).

   c. Nell'elenco Windows Settings (Impostazioni di Windows), apri il menu contestuale (pulsante destro del mouse) per Registry (Registro di sistema) e seleziona New registry item (Nuovo elemento di registro di sistema).

   d. Nella finestra di dialogo New Registry Properties (Nuove proprietà di registro di sistema), inserisci le impostazioni seguenti e scegli OK:

      Azione

      ```
      Update
      ```

Hive

```
HKEY_CURRENT_USER
```

Path

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

Il valore per *<alias>* è derivato dal tuo URL di accesso. Se il tuo URL di accesso è `https://examplecorp.awsapps.com`, l'alias è `examplecorp` e la chiave di registro sarà `Software\Microsoft\Windows\CurrentVersion\Internet Settings \ZoneMap\Domains\awsapps.com\examplecorp`.

Value name (Nome valore)

```
https
```

Value type (Tipo di valore)

```
REG_DWORD
```

Value data (Dati valore)

```
1
```

3. Per abilitare lo scripting attivo, segui la procedura seguente:

   a. Nello strumento di gestione di policy di gruppo, vai al tuo dominio, seleziona Oggetti di policy di gruppo, apri il menu contestuale (pulsante destro del mouse) per la tua policy Centro identità IAM e scegli Modifica.

   b. Nella struttura della policy, passa a Computer Configuration (Configurazione computer) > Policies (Policy) > Administrative Templates (Modelli amministrativi) > Windows Components (Componenti di Windows) > Internet Explorer > Internet Control Panel (Pannello di controllo Internet) > Security Page (Pagina protezione) > Intranet Zone (Area Intranet).

   c. Nell'elenco Intranet Zone (Area Intranet), apri il menu contestuale (pulsante destro del mouse) per Allow active scripting (Consenti scripting attivo) e scegli Modifica (Edit).

   d. Nella finestra di dialogo Allow active scripting (Consenti scripting attivo), inserisci le impostazioni seguenti e scegli OK:

      - Seleziona il pulsante di opzione Enabled (Abilitato).

- In Options (Opzioni) imposta Allow active scripting (Consenti scripting attivo) su Enable (Abilita).

4. Per abilitare l'accesso automatico, segui la procedura seguente:

   a. Nello strumento di gestione di Group Policy, passa al tuo dominio, seleziona Group Policy Objects (Oggetti Group Policy), apri il menu contestuale (pulsante destro del mouse) della policy SSO e scegli Edit (Modifica).

   b. Nella struttura della policy, passa a Computer Configuration (Configurazione computer) > Policies (Policy) > Administrative Templates (Modelli amministrativi) > Windows Components (Componenti di Windows) > Internet Explorer > Internet Control Panel (Pannello di controllo Internet) > Security Page (Pagina protezione) > Intranet Zone (Area Intranet).

   c. Nell'elenco Intranet Zone (Area Intranet), apri il menu contestuale (pulsante destro del mouse) per Logon options (Opzioni di accesso) e scegli Modifica (Edit).

   d. Nella finestra di dialogo Logon options (Opzioni di accesso), inserisci le impostazioni seguenti e scegli OK:

      - Seleziona il pulsante di opzione Enabled (Abilitato).
      - In Options (Opzioni) imposta Logon options (Opzioni di accesso) su Automatic logon only in Intranet zone (Accesso automatico solo nell'area Intranet).

5. Per abilitare l'autenticazione integrata, segui la procedura seguente:

   a. Nello strumento di gestione di policy di gruppo, vai al tuo dominio, seleziona Oggetti di policy di gruppo, apri il menu contestuale (pulsante destro del mouse) per la tua policy Centro identità IAM e scegli Modifica.

   b. Nella struttura della policy, seleziona User Configuration (Configurazione utente) > Preferences (Preferenze) > Windows Settings (Impostazioni di Windows).

   c. Nell'elenco Windows Settings (Impostazioni di Windows), apri il menu contestuale (pulsante destro del mouse) per Registry (Registro di sistema) e seleziona New registry item (Nuovo elemento di registro di sistema).

   d. Nella finestra di dialogo New Registry Properties (Nuove proprietà di registro di sistema), inserisci le impostazioni seguenti e scegli OK:

      Azione

      ```
      Update
      ```

Hive

```
HKEY_CURRENT_USER
```

Path

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Value name (Nome valore)

```
EnableNegotiate
```

Value type (Tipo di valore)

```
REG_DWORD
```

Value data (Dati valore)

```
1
```

6. Chiudi la finestra Group Policy Management Editor (Editor gestione di Group Policy) se è ancora aperta.
7. Assegna la nuova policy al tuo dominio seguendo questa procedura:
   a. Nella struttura di gestione di Group Policy, apri il menu contestuale (pulsante destro del mouse) del tuo dominio e scegli Link an Existing GPO (Collega un GPO esistente).
   b. Nell'elenco Oggetti policy di gruppo, seleziona la policy Centro identità IAM e scegli OK.

Queste modifiche diventeranno effettive dopo l'aggiornamento successivo della policy di gruppo sul client, oppure all'accesso successivo da parte dell'utente.

Accesso con autenticazione unica per Firefox

Per consentire al browser Mozilla Firefox di supportare il single sign-on, aggiungi il tuo URL di accesso (ad esempio, https://*<alias>*.awsapps.com) all'elenco dei siti approvati per il Single Sign-On. Puoi eseguire questa operazione manualmente oppure in maniera automatizzata con uno script.

Argomenti

- Aggiornamento manuale dell'accesso con autenticazione unica
- Aggiornamento automatico dell'accesso con autenticazione unica

Aggiornamento manuale dell'accesso con autenticazione unica

Per aggiungere manualmente l'URL di accesso all'elenco dei siti approvati in Firefox, esegui la seguente procedura sul computer client.

Aggiunta manuale dell'URL di accesso all'elenco dei siti approvati in Firefox

1. Apri Firefox e apri la pagina `about:config`.
2. Apri la preferenza `network.negotiate-auth.trusted-uris` e aggiungi il tuo URL di accesso all'elenco dei siti. Utilizza una virgola (,) per separare più voci.

Aggiornamento automatico dell'accesso con autenticazione unica

In qualità di amministratore di dominio, puoi utilizzare uno script per aggiungere l'URL di accesso alla preferenza utente `network.negotiate-auth.trusted-uris` di Firefox su tutti i computer della rete. Per ulteriori informazioni, visita https://support.mozilla. org/en-US/questions/939037.

Concedere agli utenti e ai gruppi di AWS Managed Microsoft AD l'accesso alle AWS risorse con ruoli IAM

AWS Directory Serviceoffre la possibilità di fornire agli utenti e ai gruppi di AWS Managed Microsoft AD l'accesso a AWS servizi e risorse, come l'accesso alla EC2 console Amazon. Analogamente alla concessione agli utenti IAM dell'accesso alla gestione delle directory come descritto inPolicy basate su identità (policy IAM), affinché gli utenti della tua directory abbiano accesso ad altre AWS risorse, come Amazon, EC2 devi assegnare ruoli e policy IAM a tali utenti e gruppi. Per ulteriori informazioni, consulta Ruoli IAM nella Guida per l'utente IAM.

Per informazioni su come concedere agli utenti l'accesso a, consultaConsole di gestione AWS. Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite

Argomenti

- Creazione di un nuovo ruolo IAM
- Modifica della relazione di fiducia per un ruolo IAM esistente
- Assegnazione di utenti o gruppi a un ruolo IAM esistente
- Visualizzazione di utenti e gruppi assegnati a un ruolo
- Rimuovere un utente o un gruppo da un ruolo IAM

- Utilizzo di politiche AWS gestite con Directory Service

Creazione di un nuovo ruolo IAM

Se devi creare un nuovo ruolo IAM da utilizzare conDirectory Service, devi crearlo utilizzando la console IAM. Una volta creato il ruolo, devi quindi impostare una relazione di fiducia con quel ruolo prima di poterlo vedere nella Directory Service console. Per ulteriori informazioni, consulta Modifica della relazione di fiducia per un ruolo IAM esistente.

> **Note**
>
> L'utente che esegue questa operazione deve disporre dell'autorizzazione a eseguire le seguenti operazioni IAM. Per ulteriori informazioni, consulta Policy basate su identità (policy IAM).
>
> - Io sono: PassRole
> - Io sono: GetRole
> - Io sono: CreateRole
> - Io sono: PutRolePolicy

Per creare un nuovo ruolo nella console IAM

1. Nel pannello di navigazione della console IAM seleziona Ruoli. Per ulteriori informazioni, consulta la pagina Creazione di un ruolo (Console di gestione AWS) nella Guida per l'utente di IAM.
2. Scegli Crea ruolo.
3. In Choose the service that will use this role (Scegli il servizio che utilizzerà questo ruolo), scegliere Directory Service, quindi Next (Successivo).
4. Seleziona la casella di controllo accanto alla politica (ad esempio Amazon EC2 FullAccess) che desideri applicare agli utenti della tua directory, quindi scegli Avanti.
5. Se necessario, aggiungere un tag al ruolo, quindi scegliere Next (Successivo).
6. Specificare un Role name (Nome ruolo) e una Description (Descrizione) opzionale, quindi scegliere Create role (Crea ruolo).

Esempio: creazione di un ruolo per abilitare l'accesso a Console di gestione AWS

La seguente lista di controllo fornisce un esempio delle attività da completare per creare un nuovo ruolo IAM che consenta a specifici utenti di AWS Managed Microsoft AD l'accesso alla EC2 console Amazon.

1. Creare un ruolo con la console IAM utilizzando la procedura descritta sopra. Quando ti viene richiesta una politica, scegli Amazon EC2 FullAccess.
2. Utilizzare le istruzioni riportate nelle fasi Modifica della relazione di fiducia per un ruolo IAM esistente per modificare il ruolo creato, quindi aggiungere le informazioni sulla relazione di trust al documento della policy. Questo passaggio è necessario affinché il ruolo sia visibile immediatamente dopo aver abilitato l'accesso a Console di gestione AWS nel passaggio successivo.
3. Segui le istruzioni fornite nelle fasi Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite per configurare l'accesso generale alla Console di gestione AWS.
4. Segui i passaggi indicati Assegnazione di utenti o gruppi a un ruolo IAM esistente per aggiungere al nuovo ruolo gli utenti che necessitano dell'accesso completo alle EC2 risorse.

Modifica della relazione di fiducia per un ruolo IAM esistente

Puoi assegnare i ruoli IAM esistenti a Directory Service utenti e gruppi. Per fare ciò, tuttavia, il ruolo deve avere un rapporto di fiducia conDirectory Service. Quando si utilizza Directory Service per creare un ruolo utilizzando la procedura inCreazione di un nuovo ruolo IAM, questa relazione di fiducia viene impostata automaticamente.

> **Note**
>
> È necessario solo stabilire questa relazione di attendibilità per i ruoli IAM che non sono stati creati da Directory Service.

Stabilire una relazione di fiducia per un ruolo IAM esistente Directory Service

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione della console IAM, in Gestione degli accessi, scegli Ruoli.

   La console visualizza i ruoli del tuo account.

3. Seleziona il nome del ruolo che intendi modificare e, nella pagina del ruolo, seleziona la scheda Relazioni di attendibilità .
4. Seleziona Modifica policy di attendibilità.
5. In Modifica policy di attendibilità, incolla quanto indicato di seguito, quindi seleziona Aggiorna policy.

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

È inoltre possibile aggiornare questo documento di policy utilizzando la AWS CLI. Per ulteriori informazioni, consulta update-trust in Riferimento ai comandi AWS CLI.

Assegnazione di utenti o gruppi a un ruolo IAM esistente

Puoi assegnare un ruolo IAM esistente a un utente o gruppo di AWS Managed Microsoft AD. A tale scopo, assicurati di aver completato quanto segue.

Prerequisiti

- Crea un Microsoft AD AWS gestito.
- Crea un utente IAM o crea un gruppo IAM.
- Crea un ruolo con cui instaurare un rapporto di fiduciaDirectory Service. Per i ruoli IAM esistenti, dovrai modificare la relazione di fiducia per un ruolo esistente.

> **Important**
>
> L'accesso per gli utenti di AWS Managed Microsoft AD in gruppi nidificati all'interno della directory non è supportato. I membri del gruppo padre hanno accesso alla console, diversamente dai membri dei gruppi figli.

Per assegnare utenti o gruppi di AWS Managed Microsoft AD a un ruolo IAM esistente

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   a. Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
   b. Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi effettuare le assegnazioni, quindi scegli la scheda Gestione dell'applicazione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
4. Scorri verso il basso fino alla Console di gestione AWSsezione, scegli Azioni e Abilita.
5. Nella sezione Accesso delegato alla console, scegli il nome del ruolo IAM per il ruolo IAM esistente a cui desideri assegnare gli utenti.
6. Nella pagina Ruolo selezionato, in Manage users and groups for this role (Gestione di utenti e gruppi per questo ruolo), scegliere Aggiungi.
7. Nella pagina Aggiungi utenti e gruppi al ruolo, in Seleziona la foresta Active Directory, seleziona la foresta Microsoft AD gestito da AWS (questa foresta) oppure quella on-premise (foresta trusted), a seconda di quale contiene gli account che necessitano dell'accesso alla Console di gestione AWS. Per ulteriori informazioni su come configurare una foresta affidabile, consulta Tutorial: creazione di una relazione di trust tra il tuo Microsoft AD gestito da AWS e il dominio di Active Directory autogestito.
8. In Specify the users or groups to add (Specifica quali utenti o gruppi aggiungere), selezionare Find by user (Cerca per utente) o Find by group (Cerca per gruppo), quindi digitare il nome dell'utente o del gruppo. Nell'elenco di corrispondenze possibili, seleziona l'utente o il gruppo che intendi aggiungere.
9. Selezionare Add (Aggiungi) per terminare l'assegnazione di utenti e gruppi al ruolo.

Visualizzazione di utenti e gruppi assegnati a un ruolo

Per visualizzare gli utenti e i gruppi di AWS Managed Microsoft AD assegnati a un ruolo IAM, procedi nel seguente modo.

Prerequisiti

- Crea un Microsoft AD AWS gestito.
- Crea un utente IAM o crea un gruppo IAM.
- Crea un ruolo con cui instaurare un rapporto di fiduciaDirectory Service. Per i ruoli IAM esistenti, dovrai modificare la relazione di fiducia per un ruolo esistente.
- Assegna i tuoi utenti o gruppi a un ruolo IAM esistente.

Per visualizzare gli utenti e i gruppi di AWS Managed Microsoft AD assegnati a un ruolo IAM

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

    a. Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi visualizzare le assegnazioni, quindi scegli la scheda Gestione dell'applicazione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.

    b. Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
4. Scorri verso il basso fino Console di gestione AWSalla sezione. Lo stato deve essere abilitato. In caso contrario, scegli Azioni e Abilita. Per ulteriori informazioni, consulta Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite.

    > **Note**
    >
    > Non vedrai alcun gruppo o utente se Console di gestione AWS è disabilitato.
5. Nella sezione Delegate Console Access, seleziona il collegamento ipertestuale del ruolo IAM che desideri visualizzare. In alternativa, puoi selezionare Visualizza la policy in IAM per visualizzare la policy IAM nella console IAM.

6. Nella pagina Ruolo selezionato, nella sezione Gestisci utenti e gruppi per questo ruolo, puoi visualizzare gli utenti e i gruppi assegnati al ruolo IAM.

Rimuovere un utente o un gruppo da un ruolo IAM

Per rimuovere un utente o un gruppo di AWS Managed Microsoft AD da un ruolo IAM, procedi nel seguente modo.

Per rimuovere un utente o un gruppo da un ruolo IAM

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

    a. Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi rimuovere le assegnazioni, quindi scegli la scheda Gestione dell'applicazione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.

    b. Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
4. Nella Console di gestione AWSsezione, scegli il ruolo IAM da cui desideri rimuovere utenti e gruppi.
5. Nella pagina Selected role (Ruolo selezionato), in Manage users and groups for this role (Gestione utenti e gruppi per questo ruolo), seleziona gli utenti o i gruppi da cui rimuovere il ruolo e scegli Remove (Rimuovi). Il ruolo viene rimosso dagli utenti e dai gruppi specificati, ma non viene rimosso dal tuo account.

> **Note**
>
> Se desideri eliminare un ruolo, consulta Eliminare ruoli o profili di istanza.

Utilizzo di politiche AWS gestite con Directory Service

Directory Servicefornisce le seguenti politiche AWS gestite per consentire a utenti e gruppi di accedere a AWS servizi e risorse, come l'accesso alla EC2 console Amazon. È necessario accedere alla Console di gestione AWS prima di poter visualizzare queste policy.

- Accesso in sola lettura
- Accesso utenti avanzati
- Directory Serviceaccesso completo
- Directory Serviceaccesso in sola lettura
- AWSAccesso completo ai dati del Directory Service
- AWSAccesso in sola lettura ai dati del Directory Service
- Accesso completo alla directory del cloud Amazon
- Accesso in sola lettura alla directory del cloud Amazon
- Accesso EC2 completo ad Amazon
- Accesso in sola EC2 lettura ad Amazon
- Accesso completo ad Amazon VPC
- Accesso in sola lettura ad Amazon VPC
- Accesso completo ad Amazon RDS
- Accesso in sola lettura ad Amazon RDS
- Accesso completo ad Amazon DynamoDB
- Accesso in sola lettura ad Amazon DynamoDB
- Accesso completo ad Amazon S3
- Accesso in sola lettura ad Amazon S3
- AWS CloudTrailaccesso completo
- AWS CloudTrailaccesso in sola lettura
- Accesso CloudWatch completo ad Amazon
- Accesso in sola CloudWatch lettura ad Amazon
- Accesso completo ad Amazon CloudWatch Logs
- Accesso in sola lettura CloudWatch ad Amazon Logs

Per ulteriori informazioni su come creare le tue policy, consulta Example policies for administration AWS resources nella IAM User Guide.

Configurazione della replica multiarea per Managed AWS Microsoft AD

La replica multiregione può essere utilizzata per replicare automaticamente i dati della directory AWS Microsoft AD gestita su più siti. Regioni AWS Questa replica può migliorare le prestazioni di utenti e applicazioni in aree geografiche dislocate. AWS Microsoft AD gestito utilizza la replica nativa di Active Directory per replicare i dati della directory in modo sicuro nella nuova regione.

La replica multiregione è supportata solo per l'Enterprise Edition di Managed AWS Microsoft AD.

È possibile utilizzare la replica automatica in più regioni nella maggior parte delle regioni in cui è AWS disponibile Managed Microsoft AD.

Important

La replica in più regioni non è disponibile nelle regioni opzionali. Le seguenti sono regioni opzionali:

- Africa (Città del Capo) (af-south-1)
- Asia Pacifico (Hong Kong) ap-east-1
- Asia Pacifico (Hyderabad) ap-south-2
- Asia Pacific (Giacarta) ap-southeast-3
- Asia Pacifico (Melbourne) ap-southeast-4
- Asia Pacifico (Tailandia) ap-southeast-7
- Canada occidentale (Calgary) ca-west-1
- Europa (Milano) eu-south-1
- Europa (Spagna) eu-south-2
- Europa (Zurigo) eu-central-2
- Israele (Tel Aviv) il-central-1
- Medio Oriente (Bahrein) me-south-1
- Medio Oriente (EAU) me-central-1
- Messico (Centrale) mx-central-1

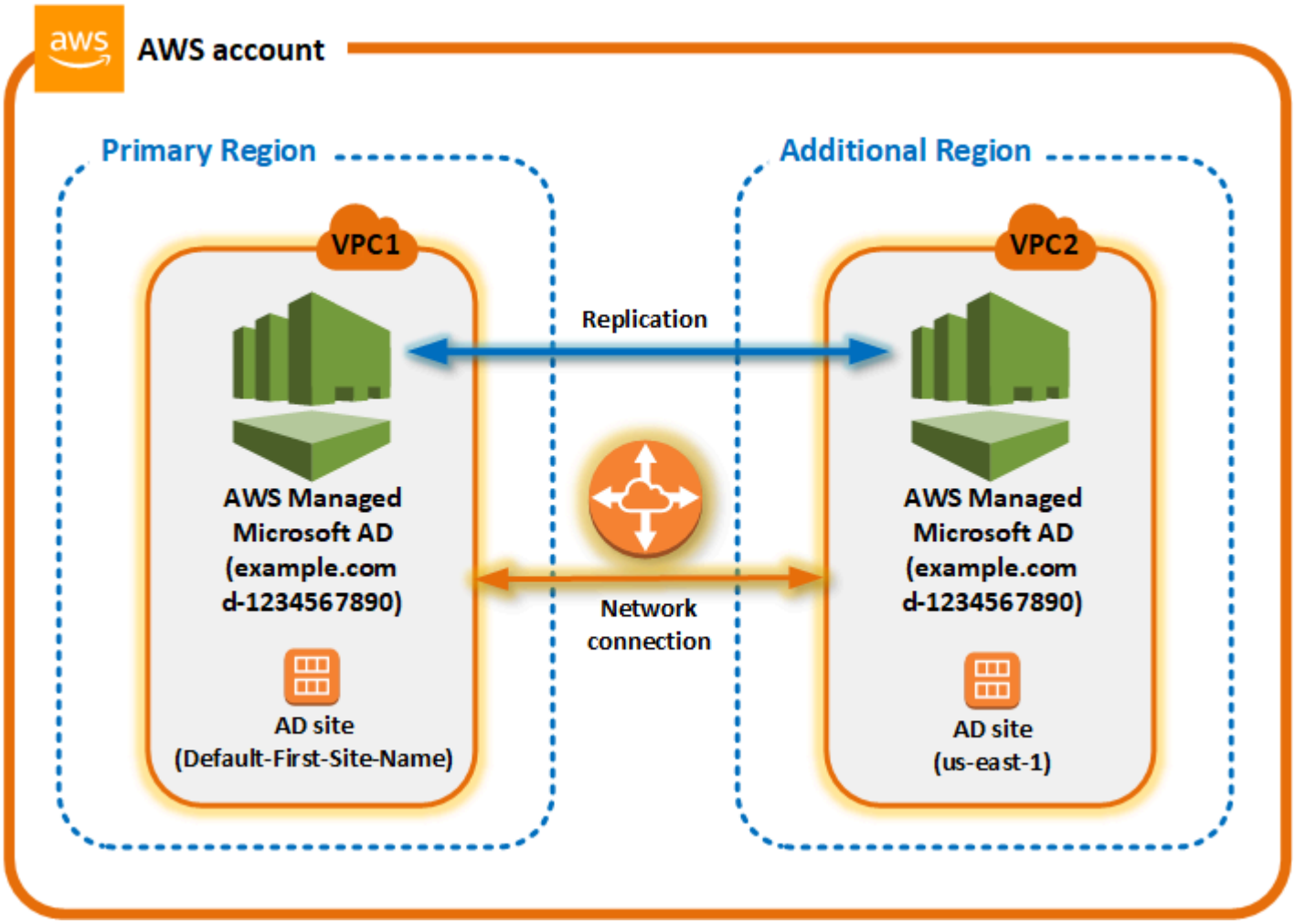
Per ulteriori informazioni sulle regioni con consenso esplicito e su come abilitarle, consulta Specifica quali Regioni AWS possono essere utilizzate dall'account nella Guida di Gestione dell'account AWS .

Come funziona la replica multiregionale

Con la funzionalità di replica multiregionale, Managed AWS Microsoft AD elimina il peso indifferenziato della gestione di un'infrastruttura Active Directory globale. Una volta configurato, AWS replica tutti i dati dell'elenco clienti, inclusi utenti, gruppi, politiche di gruppo e schemi, su più pagine. Regioni AWS

Una volta aggiunta una nuova regione, vengono eseguite automaticamente le seguenti operazioni, come mostrato nell'illustrazione:

- AWS Microsoft AD gestito crea due controller di dominio nel VPC selezionato e li distribuisce nella nuova regione con lo stesso account. AWS L'identificatore della directory (`directory_id`) rimane lo stesso in tutte le Regioni. È possibile aggiungere ulteriori controller di dominio in un secondo momento, se lo si desidera.
- AWS Microsoft AD gestito configura la connessione di rete tra la regione principale e la nuova regione.
- AWS Microsoft AD gestito crea un nuovo sito Active Directory e gli assegna lo stesso nome della regione, ad esempio us-east-1. È possibile anche rinominarlo in un secondo momento utilizzando lo strumento Siti e servizi di Active Directory.
- AWS Microsoft AD gestito replica tutti gli oggetti e le configurazioni di Active Directory nella nuova regione, inclusi utenti, gruppi, policy di gruppo, trust di Active Directory, unità organizzative e schema di Active Directory. I collegamenti ai siti di Active Directory sono configurati per utilizzare Notifica di modifiche. Con la notifica delle modifiche tra i siti abilitata, le modifiche si propagano al sito remoto con la stessa frequenza con cui vengono propagate all'interno del sito di origine, comprese le modifiche che richiedono una replica urgente.
- Se questa è la prima regione che aggiungi, AWS Managed Microsoft AD rende tutte le funzionalità compatibili con più aree geografiche. Per ulteriori informazioni, consulta Funzionalità globali e regionali.



Siti Active Directory

La replica multiregione supporta più siti di Active Directory (un sito Active Directory per regione). Quando viene aggiunta una nuova regione, gli viene assegnato lo stesso nome della regione, ad esempio us-east-1. È possibile anche rinominarla in un secondo momento utilizzando Siti e servizi di Active Directory.

AWS servizi

AWS servizi come Amazon RDS for SQL Server e FSx Amazon si connettono alle istanze locali della directory globale. Ciò consente agli utenti di accedere una sola volta alle applicazioni compatibili con Active Directory eseguite in locale e a AWS servizi AWS come Amazon RDS for SQL Server in qualsiasi regione. AWS A tale scopo, gli utenti hanno bisogno delle credenziali di AWS Managed Microsoft AD o di Active Directory locale quando si dispone di un trust con Managed AWS Microsoft AD.

È possibile utilizzare i seguenti AWS servizi con la funzionalità di replica multiregionale.

- Amazon EC2
- File server Amazon FSx per Windows
- Amazon Relational Database Service per SQL Server
- Amazon RDS per Oracle
- Amazon RDS per MySQL
- Amazon RDS per PostgreSQL
- Amazon RDS per MariaDB
- Amazon Aurora per MySQL
- Amazon Aurora per PostgreSQL

Failover

Nel caso in cui tutti i controller di dominio in una regione siano inattivi, AWS Managed Microsoft AD ripristina i controller di dominio e replica automaticamente i dati della directory. Nel frattempo, i controller di dominio in altre regioni rimangono attivi e funzionanti.

Vantaggi della replica in più aree

Con la replica multiarea in Managed AWS Microsoft AD, le applicazioni compatibili con Active Directory utilizzano la directory localmente per prestazioni elevate e la funzionalità multiarea per la resilienza. Puoi utilizzare la replica multiregionale con applicazioni compatibili con Active Directory come SQL Server Always On, nonché AWS servizi come Amazon RDS per SQL Server SharePoint e per Windows File Server. FSx Di seguito sono riportati i vantaggi aggiuntivi della replica multi regione.

- Consente di distribuire una singola istanza AWS Managed Microsoft AD a livello globale, in modo rapido ed elimina il pesante compito di gestire autonomamente un'infrastruttura Active Directory globale.
- Rende più semplice ed economica la distribuzione e la gestione dei carichi di lavoro Windows e Linux in più regioni. AWS La replica automatizzata in più regioni consente prestazioni ottimali nelle applicazioni globali compatibili con Active Directory. Tutte le applicazioni distribuite in istanze Windows o Linux utilizzano Managed AWS Microsoft AD localmente nella regione, il che consente di rispondere alle richieste degli utenti dalla regione più vicina possibile.
- Fornisce resilienza multi regione. Implementato nell'infrastruttura AWS gestita ad alta disponibilità, AWS Managed Microsoft AD gestisce gli aggiornamenti software automatici, il monitoraggio, il

ripristino e la sicurezza dell'infrastruttura Active Directory sottostante in tutte le regioni. In questo modo, puoi concentrarti sulla creazione delle tue applicazioni.

Argomenti

Funzionalità globali e regionali

Quando si aggiunge una AWS regione alla directory utilizzando la replica multiarea, viene Directory Service migliorato l'ambito di tutte le funzionalità in modo che diventino consapevoli della regione. Queste funzionalità sono elencate in varie schede della pagina dei dettagli che viene visualizzata quando si sceglie l'ID di una directory nella console Directory Service . Ciò significa che tutte le funzionalità sono abilitate, configurate o gestite in base alla regione selezionata nella sezione Replica multi regione della console. Le modifiche apportate alle funzionalità in ciascuna regione vengono applicate a livello globale o per regione.

La replica multiregione è supportata solo per l'Enterprise Edition di Managed AWS Microsoft AD.

Funzionalità globali

Qualsiasi modifica apportata alle funzionalità globali mentre Regione principale è selezionata verrà applicata in tutte le regioni.

È possibile identificare le funzionalità utilizzate a livello globale nella pagina Dettagli della directory, in quanto accanto viene visualizzata la dicitura Applicato a tutte le Regioni replicate. In alternativa, se nell'elenco hai selezionato un'altra regione che non è la regione primaria, puoi identificare le funzionalità utilizzate a livello globale perché mostrano la dicitura Ereditato dalla regione primaria.

Funzionalità regionali

Qualsiasi modifica apportata a una funzionalità in una Regione aggiuntiva verrà applicata solo a quella regione.

È possibile identificare le funzionalità regionali nella pagina Dettagli della directory, in quanto accanto non viene visualizzata la dicitura Applicato a tutte le Regioni replicate o Ereditato dalla regione primaria.

Regioni primarie e regioni aggiuntive

Con la replica multiarea, AWS Managed Microsoft AD utilizza i seguenti due tipi di aree per differenziare il modo in cui le funzionalità globali o regionali devono essere applicate nella directory.

Regione principale

La regione iniziale in cui è stata creata la directory per la prima volta viene definita regione primaria. È possibile eseguire solo operazioni a livello di directory globale, come la creazione di attendibilità di Active Directory e l'aggiornamento dello schema AD dalla regione primaria.

La regione primaria può sempre essere identificata come la prima regione visualizzata nella parte superiore dell'elenco nella sezione Replica multi regione e termina con - Primaria. Ad esempio Stati Uniti orientali (Virginia settentrionale) - Primaria.

Qualsiasi modifica apportata alla Funzionalità globali mentre la regione primaria è selezionata verrà applicata in tutte le regioni.

Puoi aggiungere regioni solo mentre è selezionata la regione primaria. Per ulteriori informazioni, consulta Aggiungere una regione replicata per AWS Managed Microsoft AD.

Regione aggiuntiva

Tutte le regioni che hai aggiunto alla tua directory vengono chiamate Regioni aggiuntive.

Sebbene alcune funzionalità possano essere gestite a livello globale per tutte le regioni, altre sono gestite individualmente per regione. Per gestire una funzionalità per una regione aggiuntiva (Regione non primaria), è necessario innanzitutto selezionare la regione aggiuntiva dall'elenco nella sezione Replica multi regione nella pagina Dettagli della directory. È quindi possibile procedere alla gestione della funzionalità.

Qualsiasi modifica apportata alla Funzionalità regionali mentre è selezionata una regione aggiuntiva verrà applicata solo a quella regione.

Aggiungere una regione replicata per AWS Managed Microsoft AD

Quando aggiungi una regione utilizzando la Configurazione della replica multiarea per Managed AWS Microsoft AD funzionalità, AWS Managed Microsoft AD crea due controller di dominio nella AWS

regione selezionata, Amazon Virtual Private Cloud (VPC) e subnet. AWS Managed Microsoft AD crea anche i gruppi di sicurezza correlati che consentono ai carichi di lavoro Windows di connettersi alla directory nella nuova regione. Inoltre, crea queste risorse utilizzando lo stesso account AWS in cui è già implementata la directory. Puoi farlo scegliendo la regione, specificando il VPC e fornendo le configurazioni per la nuova regione.

La replica multiregione è supportata solo per l'Enterprise Edition di Managed AWS Microsoft AD.

Prerequisiti

Prima di procedere con la procedura per aggiungere una nuova regione di replica, si consiglia di esaminare le seguenti attività prerequisite.

- Verifica di disporre delle autorizzazioni AWS Identity and Access Management (IAM) necessarie, della configurazione di Amazon VPC e della configurazione della sottorete nella nuova regione in cui desideri replicare la directory.
- Se desideri utilizzare le credenziali di Active Directory esistenti in locale per accedere e gestire carichi di lavoro compatibili con Active Directory in AWS, devi creare un trust Active Directory tra Managed AWS Microsoft AD e l'infrastruttura AD locale. Per ulteriori informazioni sulle attendibilità, consulta Connect AWS Managed Microsoft AD all'infrastruttura Active Directory esistente.
- Se esiste una relazione di trust tra il tuo Active Directory locale e desideri aggiungere una regione replicata, devi verificare di disporre della configurazione Amazon VPC e della sottorete necessarie nella nuova regione in cui desideri replicare la directory.

Puoi anche creare un rapporto di fiducia tra la tua infrastruttura Microsoft AD AWS gestita e l'infrastruttura AD locale, in modo da poter utilizzare le credenziali di Active Directory locali esistenti per gestire i carichi di lavoro Ad-aware. Per ulteriori informazioni, consulta Connect AWS Managed Microsoft AD all'infrastruttura Active Directory esistente.

Aggiungere una regione

Utilizzare la procedura seguente per aggiungere una regione replicata per la directory Microsoft AD AWS gestita.

Per aggiungere una regione replicata

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.

3. Nella pagina Dettagli della directory, in Replica multi regione, scegli la regione primaria dall'elenco, quindi scegli Aggiungi regione.

> **Note**
>
> Puoi aggiungere Regioni solo mentre è selezionata la regione primaria. Per ulteriori informazioni, consulta Regione principale.

4. Nella pagina Aggiungi regione, in regione, scegli quella che desideri aggiungere dall'elenco.
5. In VPC, scegli il VPC da usare per questa regione.

> **Note**
>
> Il VPC non deve avere un routing interdominio senza classi (CIDR) che si sovrappone a un VPC utilizzato da questa directory in un'altra regione.

6. In Sottoreti, scegli la sottorete da utilizzare per questa regione.
7. Controlla le informazioni in Prezzi, quindi scegli Aggiungi.
8. Quando AWS Managed Microsoft AD completa il processo di distribuzione del controller di dominio, la regione mostrerà lo stato Attivo. Ora puoi apportare aggiornamenti a questa regione in base alle esigenze.

Passaggi successivi

Dopo aver aggiunto una nuova regione, è consigliabile proseguire con le seguenti fasi successive:

- Se necessario, implementa controller di dominio aggiuntivi (fino a 20) nella nuova regione. Il numero di controller di dominio quando aggiungi una nuova regione è 2 per impostazione predefinita, che è il minimo richiesto per scopi di tolleranza agli errori e alta disponibilità. Per ulteriori informazioni, consulta Aggiungere o rimuovere controller di dominio aggiuntivi con Console di gestione AWS.

> **Note**
>
> Quando si aggiunge un replicato Regione AWS a AWS Managed Microsoft AD, per impostazione predefinita vengono creati due controller di dominio, ovvero il numero minimo di controller di dominio richiesto per la tolleranza agli errori e l'elevata disponibilità.

- Condividi la tua directory con più account per regione. AWS Le configurazioni di condivisione delle directory non vengono replicate automaticamente dalla regione primaria. Per ulteriori informazioni, consulta Condividi il tuo AWS Managed Microsoft AD.

  > **Note**
  >
  > Le configurazioni di condivisione delle directory non vengono replicate automaticamente nella versione principale. Regione AWS

- Abilita l'inoltro dei log per recuperare i log di sicurezza della tua directory utilizzando CloudWatch Amazon Logs dalla nuova regione. Quando abiliti l'inoltro dei log, devi fornire un nome per il gruppo di log in ogni regione in cui hai replicato la directory. Per ulteriori informazioni, consulta Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS.

  > **Note**
  >
  > Quando abiliti l'inoltro dei log, devi fornire un nome per il gruppo di log in ognuno dei luoghi in cui hai replicato la tua directory. Regione AWS

- Abilita il monitoraggio Amazon Simple Notification Service (Amazon SNS) per la nuova regione per monitorare lo stato di integrità della directory per regione. Per ulteriori informazioni, consulta Attivazione delle notifiche sullo stato della directory AWS Managed Microsoft AD con Amazon Simple Notification Service.

Eliminazione di una regione replicata per Managed AWS Microsoft AD

Utilizzare la procedura seguente per eliminare una regione dalla directory Microsoft AD AWS gestita. Prima di eliminare una regione, assicurati che non presenti nessuno dei seguenti elementi:

- Applicazioni autorizzate ad essa allegate.
- Directory condivise ad essa associate.

Per eliminare una regione replicata

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella barra di navigazione, scegli il selettore Regioni e seleziona la regione in cui è archiviata la directory.

3. Nella pagina Directories (Directory), scegli l'ID della directory.
4. Nella pagina Dettagli della directory, in Replica multi regione, scegli Elimina regione.
5. Nella finestra di dialogo Elimina regione, rivedi le informazioni, quindi inserisci il nome della regione per confermare. Scegli Elimina.

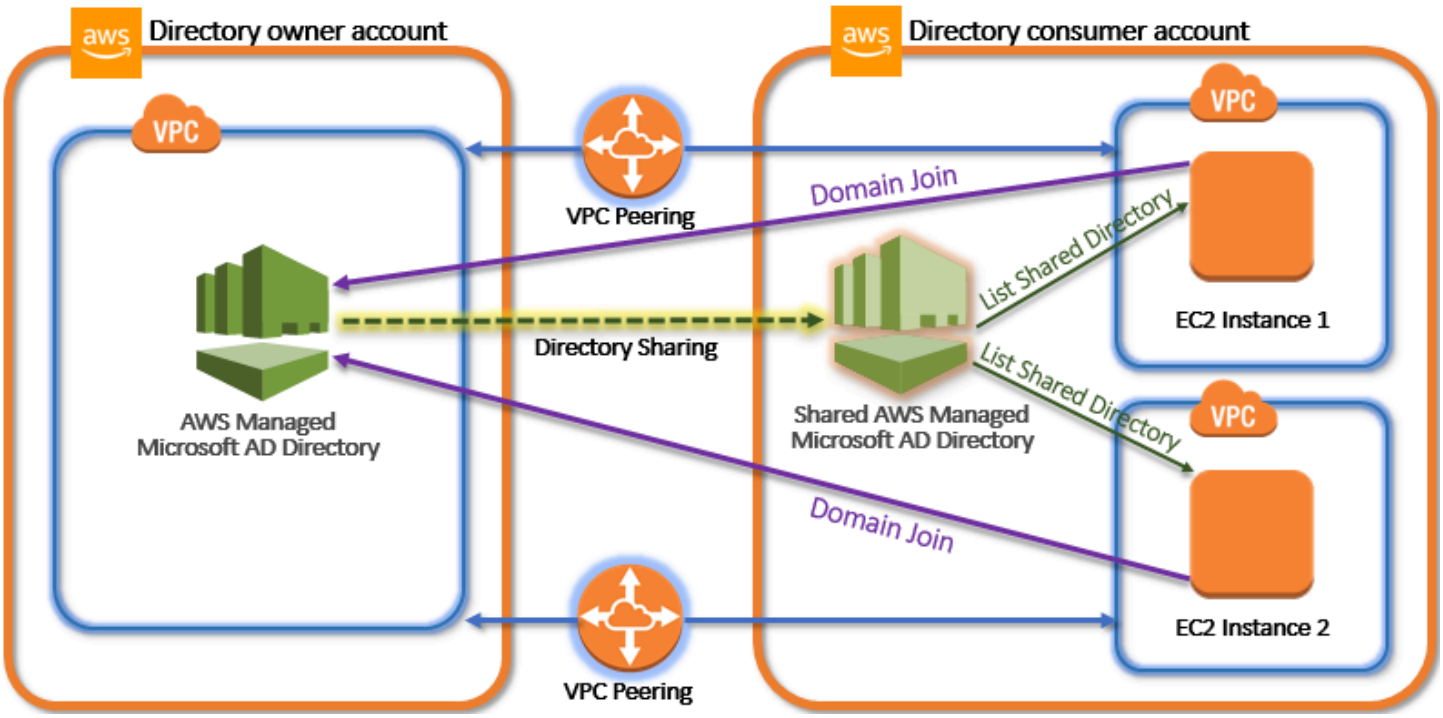
> **Note**
>
> Non puoi aggiornare la regione mentre è in corso di eliminazione.

Condividi il tuo AWS Managed Microsoft AD

AWS Microsoft AD gestito si integra perfettamente con AWS Organizations per consentire la condivisione di directory senza interruzioni tra più utenti. Account AWSÈ possibile condividere una singola directory con altre persone affidabili Account AWS all'interno della stessa organizzazione o condividere la directory con altre persone Account AWS esterne all'organizzazione. Puoi anche condividere la tua rubrica quando non sei attualmente membro di un'organizzazione. Account AWS

Concetti chiave sulla condivisione di directory

Otterrete il massimo dalla funzionalità di condivisione delle directory se acquisirete familiarità con i seguenti concetti chiave.



Account del proprietario della directory

Il proprietario della directory è il Account AWS proprietario della directory di origine nella relazione di directory condivisa. Un amministratore di questo account avvia il flusso di lavoro di condivisione delle directory specificando con chi Account AWS condividere la propria directory. I proprietari di directory possono vedere con chi hanno condiviso una directory utilizzando la scheda Scale & Share (Dimensiona e condividi) per una directory specificata nella console Directory Service .

Account dell'utilizzatore della directory

In una relazione directory condivisa, un utilizzatore della directory rappresenta l' Account AWS con cui il proprietario della directory ha condiviso la directory. A seconda del metodo di condivisione utilizzato, è possibile che un amministratore in questo account debba accettare un invito inviato dal proprietario della directory prima di iniziare a utilizzare la directory condivisa.

Il processo di condivisione directory crea una directory condivisa nell'account dell'utilizzatore della directory. Questa directory condivisa contiene i metadati che consentono all' EC2 istanza di unirsi senza problemi al dominio, che individua la directory di origine nell'account del proprietario della directory. Ogni directory condivisa nell'account dell'utilizzatore della directory dispone di un identificatore univoco (Shared directory ID (ID directory condivisa)).

Metodi di condivisione

AWS Microsoft AD gestito offre i due metodi di condivisione delle directory seguenti:

- AWS Organizations: questo metodo consente di semplificare la condivisione della directory all'interno dell'organizzazione perché permette di individuare e convalidare gli account dell'utilizzatore della directory. Per utilizzare questa opzione, Tutte le funzionalità deve essere abilitato nell'organizzazione e la directory deve trovarsi nell'account principale di quest'ultima. Questo metodo di condivisione semplifica la configurazione perché non richiede che gli account utente della directory accettino la richiesta di condivisione della directory. Nella console, questo metodo è denominato Share this directory with Account AWS inside your organization.
- Handshake: questo metodo consente la condivisione della directory quando non si utilizza AWS Organizations. Il metodo di handshake richiede che l'account dell'utilizzatore della directory accetti la richiesta di condivisione della directory. Nella console, questo metodo è denominato Condividi questa directory con altri Account AWS.

Connettività di rete

La connettività di rete è un prerequisito per utilizzare una relazione di condivisione di directory tra di loro. Account AWS AWS supporta molte soluzioni per connettere il tuo VPCs, alcune di queste includono peering VPC, Transit Gateway e VPN. Per iniziare, consulta Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2 .

Considerazioni

Di seguito sono riportate alcune considerazioni relative all'utilizzo della condivisione di directory con AWS Managed Microsoft AD:

Prezzi

- AWS addebita un costo aggiuntivo per la condivisione della directory. L'account Account AWS che utilizza il AWS Managed Microsoft AD condiviso è l'account a cui vengono addebitate le commissioni di condivisione. Per ulteriori informazioni, consulta la pagina dei prezzi sul Directory Service sito Web.
- La condivisione di directory rende AWS Managed Microsoft AD un modo più conveniente per l'integrazione con Amazon EC2 in più account e. VPCs

Disponibilità nelle regioni

- La condivisione delle directory è disponibile in tutte le AWS regioni in cui viene offerto AWS Managed Microsoft AD.
- In AWS Cina (Ningxia), questa funzionalità è disponibile solo quando si utilizza AWS Systems Manager(SSM) per unire senza problemi le istanze Amazon. EC2

Per ulteriori informazioni sulla condivisione delle directory e su come estendere la portata della directory di Microsoft AD AWS gestita oltre i limiti degli AWS account, consulta i seguenti argomenti.

Argomenti

- Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2
- Annullamento della condivisione della rubrica

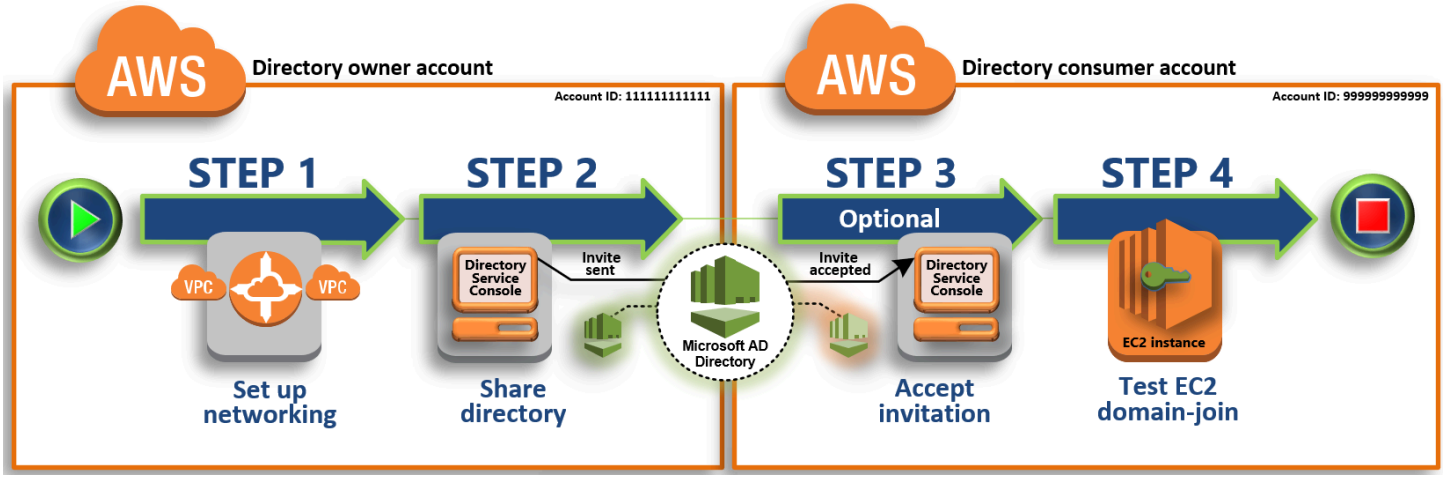
Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2

Questo tutorial mostra come condividere la directory AWS Managed Microsoft AD (l'account del proprietario della directory) con un'altra Account AWS (l'account utente della directory). Una volta completati i prerequisiti di rete, condividerai una directory tra dueAccount AWS. Quindi imparerai come aggiungere senza problemi un' EC2 istanza a un dominio nella directory dell'account consumer.

Ti consigliamo di rivedere innanzitutto i concetti chiave di condivisione di directory e utilizzare il contenuto del caso d'uso prima di iniziare a utilizzare questo tutorial. Per ulteriori informazioni, consulta Concetti chiave sulla condivisione di directory.

Il processo di condivisione della directory varia a seconda che la si condivida con un altro Account AWS membro della stessa AWS organizzazione o con un account esterno all'organizzazione. AWS Per ulteriori informazioni sul funzionamento della condivisione, consulta Metodi di condivisione.

Questo flusso di lavoro ha quattro fasi di base.



Fase 1: configurazione dell'ambiente di rete

Nell'account del proprietario della directory, configura tutti i prerequisiti di rete necessari per il processo di condivisione della directory.

Fase 2: condivisione della directory

Dopo aver effettuato l'accesso con le credenziali di amministratore del proprietario della directory, apri la console Directory Service e avvia il flusso di lavoro di condivisione directory, che invia un invito all'account dell'utilizzatore della directory.

Passaggio 3: Accetta l'invito alla directory condivisa - Facoltativo

Dopo aver effettuato l'accesso con le credenziali di amministratore della directory, apri la Directory Service console e accetti l'invito alla condivisione della directory.

Passaggio 4: Prova a unire senza problemi un' EC2 istanza di Windows Server a un dominio

Infine, in qualità di amministratore dei consumatori di directory, tenti di aggiungere un' EC2istanza al tuo dominio e verificarne il funzionamento.

Altre risorse

- Caso d'uso: condividi la tua directory per unire senza problemi EC2 le istanze Amazon a un dominio su Account AWS
- AWSArticolo del blog sulla sicurezza: Come unire EC2 istanze Amazon da più account e VPCs a un'unica directory Microsoft AD AWS gestita

Fase 1: configurazione dell'ambiente di rete

Dovrai stabilire una connessione peering Amazon VPC per condividere la tua directory AWS Microsoft AD gestita (proprietario dell'account di directory) con un'altra Account AWS (account utente della directory). Consulta le seguenti procedure per i passaggi per configurare l'ambiente di rete per un Microsoft AD AWS gestito condiviso.

Prerequisiti

Prima di iniziare le fasi in questo tutorial, è necessario, innanzitutto, eseguire le operazioni seguenti:

- Creane due nuovi Account AWS a scopo di test nella stessa regione. Quando ne crei unoAccount AWS, viene creato automaticamente un cloud privato virtuale (VPC) dedicato in ogni account. Prendi nota dell'ID VPC in ogni account. Saranno necessari in seguito.
- Crea un Microsoft AD AWS gestito.
- Quando si crea una connessione peering VPC, sia il proprietario dell'account di directory che l'account consumatore della directory avranno bisogno delle autorizzazioni necessarie per creare e accettare la connessione peering. Per ulteriori informazioni, consulta Esempio: creazione di una connessione peering VPC e Esempio: accettazione di una connessione peering VPC.

> **Note**
>
> Sebbene esistano molti modi per connettere il proprietario di Directory e l'account utente di Directory VPCs, questo tutorial utilizzerà il metodo di peering VPC. Per ulteriori opzioni di connettività VPC, consulta Connettività di rete.

Configurazione di una connessione peering VPC tra il proprietario della directory e l'account dell'utilizzatore della directory

La connessione peering VPC che creerai è tra l'utente della directory e il proprietario della directory. VPCs Segui queste fasi per configurare una connessione peering di VPC per la connettività con l'account dell'utilizzatore della directory. Con questa connessione è possibile instradare il traffico tra i due VPCs utilizzando indirizzi IP privati.

Per creare una connessione peering di VPC tra l'account del proprietario della directory e l'account dell'utilizzatore della directory

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Si assicura di accedere come utente con credenziali di amministratore nell'account del proprietario della directory con le autorizzazioni necessarie per creare una connessione peering VPC. Per ulteriori informazioni, consulta Prerequisiti.
2. Nel riquadro di navigazione, scegliere Peering Connections (Connessioni peering). Quindi scegliere Create Peering Connection (Crea connessione peering).
3. Configurare le seguenti informazioni:
   - Peering connection name tag (Tag del nome della connessione peering): fornire un nome che identifica chiaramente questa connessione con il VPC nell'account dell'utilizzatore della directory.
   - VPC (Requester) (VPC (richiedente)): selezionare l'ID VPC per l'account del proprietario della directory.
   - In Select another VPC to peer with (Seleziona un altro VPC da collegare in peering), accertarsi che My account (Il mio account) e This region (Questa regione) siano entrambe selezionate.
   - VPC (Requester) (VPC (accettante)): selezionare l'ID VPC per l'account dell'utilizzatore della directory.

4. Scegliere Create Peering Connection (Crea connessione peering). Nella finestra di dialogo di conferma, scegliere OK.

Per accettare la richiesta di peering per conto dell'account dell'utilizzatore della directory

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Si assicura di accedere come utente con le autorizzazioni necessarie per accettare la richiesta di peering. Per ulteriori informazioni, consulta Prerequisiti.
2. Nel riquadro di navigazione, scegliere Peering Connections (Connessioni peering).
3. Selezionare la connessione peering di VPC in attesa. Il suo stato è Accettazione in sospeso. Scegliere Actions (Azioni), Accept Request (Accetta richiesta).
4. Nella finestra di dialogo di conferma, scegliere Yes, Accept (Sì, accetta). Nella finestra di dialogo di conferma successiva, scegliere Modify my route tables now (Modifica le tabelle di routing ora) per accedere direttamente alla pagina delle tabelle di routing.

A questo punto, la connessione peering di VPC è attiva e devi quindi aggiungere una voce alla tabella di routing VPC nell'account del proprietario della directory. Questo consente di indirizzare il traffico al VPC nell'account dell'utilizzatore della directory.

Per aggiungere una voce alla tabella di routing VPC nell'account del proprietario della directory

1. Nella sezione Tabelle di routing della console Amazon VPC, seleziona la tabella di routing per il VPC del proprietario della directory.
2. Scegli la scheda Routing, quindi Modifica route e Aggiungi instradamento.
3. Nella colonna Destination (Destinazione), immettere il blocco CIDR per il VPC dell'utilizzatore della directory.
4. Nella colonna Target (Destinazione), immettere l'ID connessione peering di VPC (ad esempio **`pcx-123456789abcde000`**) per la connessione peering creata in precedenza nell'account del proprietario della directory.
5. Scegli Save changes (Salva modifiche).

Per aggiungere una voce alla tabella di routing VPC nell'account dell'utilizzatore della directory

1. All'interno della sezione Tabelle di routing della console Amazon VPC, seleziona la tabella di routing per il VPC dell'utilizzatore della directory.

2. Scegli la scheda Routing, quindi Modifica route e Aggiungi instradamento.
3. Nella colonna Destination (Destinazione), immettere il blocco CIDR per il VPC del proprietario della directory.
4. Nella colonna Target (Destinazione), digitare l'ID connessione peering di VPC (ad esempio **`pcx-123456789abcde001`**) per la connessione peering creata in precedenza nell'account dell'utilizzatore della directory.
5. Scegli Save changes (Salva modifiche).

Aggiungi i protocolli e le porte di Active Directory alle regole in uscita per i gruppi di sicurezza in Directory Consumer. VPCs Per ulteriori informazioni, consulta Gruppi di sicurezza per il VPC e Prerequisiti di Microsoft AD gestito da AWS.

Fase successiva

Fase 2: condivisione della directory

Fase 2: condivisione della directory

Utilizza le seguenti procedure per avviare il flusso di lavoro di condivisione directory dall'account del proprietario della directory.

> **Note**
>
> La condivisione delle directory è una funzionalità regionale di AWS Managed Microsoft AD. Se si utilizza la replica multiregione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per condividere la directory dall'account del proprietario della directory

1. Accedi Console di gestione AWS con le credenziali di amministratore nell'account del proprietario della directory e apri la console all'AWS Directory Serviceindirizzo. https://console.aws.amazon.com/directoryservicev2/
2. Nel riquadro di navigazione, seleziona Directory.
3. Scegli l'ID della directory AWS Managed Microsoft AD che desideri condividere.

4. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella in cui desideri condividere la directory, quindi scegli la scheda Dimensiona e condividi. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Dimensiona e condividi.

5. Nella sezione Shared directories (Directory condivise), scegliere Actions (Operazioni), quindi selezionare Create new shared directory (Crea nuova directory condivisa).

6. Nella pagina Scegli con quale Account AWS condividere, scegli uno dei seguenti metodi di condivisione in base alle tue esigenze aziendali:

   a. Condividi questa rubrica con l'Account AWSinterno dell'organizzazione: con questa opzione puoi selezionare la persona con Account AWS cui vuoi condividere la rubrica da un elenco che mostra tutte le informazioni Account AWS all'interno AWS dell'organizzazione. È necessario abilitare l'accesso affidabile con Directory Service prima di condividere una directory. Per ulteriori informazioni, consulta Come abilitare o disabilitare l'accesso attendibile.

      > **Note**
      >
      > Per utilizzare questa opzione, Tutte le funzionalità deve essere abilitato nell'organizzazione e la directory deve trovarsi nell'account principale di quest'ultima.

      i. In Account AWSNella tua organizzazione, seleziona la Account AWS persona con cui vuoi condividere la directory e fai clic su Aggiungi.

      ii. Esaminare i dettagli prezzi e quindi scegliere Share (Condividi).

      iii. Continuare con la fase 4 in questa guida. Poiché tutti Account AWS fanno parte della stessa organizzazione, non è necessario seguire la Fase 3.

   b. Condividi questa directory con altri Account AWS: con questa opzione, puoi condividere una directory con account interni o esterni all'AWSorganizzazione. Puoi utilizzare questa opzione anche quando la tua rubrica non è membro di un'AWSorganizzazione e desideri condividerla con un'altraAccount AWS.

      i. In Account AWSID, inserisci tutti gli identificativi con Account AWS IDs cui vuoi condividere la directory, quindi fai clic su Aggiungi.

ii. In Invia una nota, digita un messaggio per l'amministratore nell'altro Account AWS.

iii. Esaminare i dettagli prezzi e quindi scegliere Share (Condividi).

iv. Continuare con la fase 3.

Fase successiva

Passaggio 3: Accetta l'invito alla directory condivisa - Facoltativo

Passaggio 3: Accetta l'invito alla directory condivisa - Facoltativo

Se nella procedura precedente è stata selezionata l'opzione Condividi questa directory con altri Account AWS (metodo handshake), utilizza questa procedura per terminare il flusso di lavoro della directory condivisa. Se hai scelto l'opzione Condividi questa directory con l'Account AWSinterno dell'organizzazione, salta questo passaggio e procedi al Passaggio 4.

Per accettare l'invito directory condivisa

1. Accedi all'account consumer della directory Console di gestione AWS con le credenziali di amministratore e apri la AWS Directory Serviceconsole all'indirizzo. https://console.aws.amazon.com/directoryservicev2/
2. Nel riquadro di navigazione, scegliere Directories shared with me (Directory condivise).
3. Nella colonna Shared directory ID (ID directory condivisa), scegliere l'ID della directory che si trova nello stato Pending acceptance (Accettazione in sospeso).
4. Nella pagina Shared directory details (Visualizza dettagli della directory), scegliere Review (Revisione).
5. Nella finestra di dialogo Pending shared directory invitation (Invito directory condivisa in sospeso), rivedere la nota, i dettagli del proprietario della directory e le informazioni relative la prezzo. Se si accetta, scegliere Accept (Accetta) per iniziare a utilizzare la directory.

Fase successiva

Passaggio 4: Prova a unire senza problemi un' EC2 istanza di Windows Server a un dominio

Passaggio 4: Prova a unire senza problemi un' EC2 istanza di Windows Server a un dominio

Puoi utilizzare uno dei due metodi seguenti per testare l'aggiunta senza problemi di un' EC2istanza a un dominio.

Metodo 1: verifica l'accesso al dominio utilizzando la EC2 console Amazon

Utilizza questi passaggi nell'account dell'utilizzatore della directory.

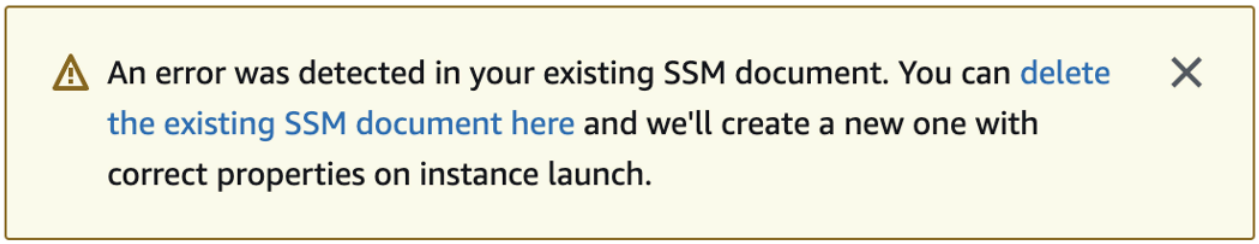
1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nella EC2 Dashboard, nella sezione Launch instance, scegli Launch instance.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per l' EC2 istanza di Windows.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivi per aggiungere una o più coppie chiave-valore di tag per organizzare, tracciare o controllare l'accesso per questa EC2 istanza.
6. Nella sezione Applicazione e immagine del sistema operativo (Amazon Machine Image), scegli Windows nel riquadro Guida rapida. Puoi modificare l'Amazon Machine Image (AMI) di Windows dall'elenco a discesa Amazon Machine Image (AMI).
7. Nella sezione Tipo di istanza, scegli il tipo di istanza che desideri utilizzare dall'elenco a discesa Tipo di istanza.
8. Nella sezione Coppia di chiavi (accesso), puoi scegliere se creare una nuova coppia di chiavi o selezionare una coppia di chiavi esistente.
    a. Per creare una nuova coppia di chiavi, scegli Crea nuova coppia di chiavi.
    b. Inserisci un nome per la coppia di chiavi e seleziona un'opzione per il Tipo di coppia di chiavi e il Formato del file della chiave privata.
    c. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegli .pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegli .ppk.
    d. Scegli crea coppia di chiavi.
    e. Il file della chiave privata viene automaticamente scaricato dal browser. Salvare il file della chiave privata in un luogo sicuro.

> **Important**
>
> Questo è l'unico momento in cui salvare il file della chiave privata.

9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto il traffico esterno instradato a un gateway Internet. In caso contrario, non potrai connetterti in remoto all'istanza.

    Per ulteriori informazioni su come connettersi a un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta l'indirizzo IP delle EC2 istanze Amazon nella Amazon EC2 User Guide.
12. Nelle impostazioni Firewall (gruppi di sicurezza), puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
13. Nelle impostazioni Configurazione dell'archiviazione, puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
14. Seleziona la sezione Dettagli avanzati, scegli il tuo dominio dall'elenco a discesa Directory di aggiunta al dominio.

> **Note**
>
> Dopo aver scelto la directory di accesso al dominio, potresti vedere:
>
> 
>
>
> Questo errore si verifica se la procedura guidata di EC2 avvio identifica un documento SSM esistente con proprietà impreviste. Puoi effettuare una delle seguenti operazioni:
>
> - Se in precedenza hai modificato il documento SSM e le proprietà sono previste, scegli chiudi e procedi all'avvio dell' EC2 istanza senza modifiche.

- Seleziona qui il link Elimina il documento SSM esistente per eliminare il documento SSM. Ciò consentirà la creazione di un documento SSM con le proprietà corrette. Il documento SSM verrà creato automaticamente all'avvio dell' EC2 istanza.

15. In Profilo dell'istanza IAM, puoi selezionare un profilo dell'istanza IAM esistente o crearne uno nuovo. Seleziona un profilo di istanza IAM a cui sono SSMDirectory ServiceAccess associate le policy AWS gestite Amazon SSMManaged InstanceCore e Amazon dall'elenco a discesa del profilo dell'istanza IAM. Per crearne uno nuovo, scegli il link Crea nuovo profilo IAM, quindi procedi come segue:

    1. Scegli Crea ruolo.
    2. In Seleziona entità attendibile, scegli Servizio AWS.
    3. In Use case (Caso d'uso), scegli EC2.
    4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le SSMDirectory ServiceAccess politiche di Amazon SSMManaged InstanceCore e Amazon. Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Scegli Next (Successivo).

    > **Note**
    >
    > Amazon SSMDirectory ServiceAccess fornisce le autorizzazioni per unire le istanze a un Active Directory gestito da. Directory Service Amazon SSMManaged InstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il AWS Systems Manager servizio. Per ulteriori informazioni sulla creazione di un ruolo con queste autorizzazioni e per informazioni su altre autorizzazioni e policy che puoi assegnare al tuo ruolo IAM, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager.

    5. Nella pagina Denomina, rivedi e crea inserisci un Nome ruolo. Avrai bisogno di questo nome di ruolo da associare all' EC2istanza.
    6. (Facoltativo) Puoi fornire una descrizione del profilo dell'istanza IAM nel campo Descrizione.
    7. Scegli Crea ruolo.
    8. Torna alla pagina Avvia un'istanza e scegli l'icona di aggiornamento accanto al profilo dell'istanza IAM. Il tuo nuovo profilo dell'istanza IAM dovrebbe essere visibile nell'elenco a discesa Profilo dell'istanza IAM. Scegli il nuovo profilo e lascia il resto delle impostazioni con i valori predefiniti.

16. Scegliere Launch Instance (Avvia istanza).

Metodo 2: test dell'aggiunta del dominio utilizzando AWS Systems Manager

Utilizza questi passaggi nell'account dell'utilizzatore della directory. Per completare questa procedura, sono necessarie alcune informazioni sull'account del proprietario della directory, come l'ID della directory, il nome della directory e gli indirizzi IP DNS.

Prerequisiti

- ConfigurazioneAWS Systems Manager.
  - Per ulteriori informazioni su Systems Manager, consulta la Configurazione generale per AWS Systems Manager.
- Le istanze a cui desideri aderire al dominio AWS Managed Microsoft Active Directory devono avere un ruolo IAM associato contenente le policy SSMDirectory ServiceAccess gestite da Amazon SSMManaged InstanceCore e Amazon.
  - Per ulteriori informazioni su queste regole gestite e altre policy che è possibile collegare a un profilo di istanza IAM per Systems Manager, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager. Per ulteriori informazioni sulle policy, consulta Policy gestite da AWS nella Guida per l'utente IAM.

Per ulteriori informazioni sull'utilizzo di Systems Manager per aggiungere EC2 istanze a un dominio Microsoft Active Directory AWS gestito, vedi Come si usa AWS Systems Manager per aggiungere un'istanza EC2 Windows in esecuzione al mio dominio AWS Directory Service? .

1. Apri la AWS Systems Manager console all'indirizzohttps://console.aws.amazon.com/systems-manager/.
2. Nel riquadro di navigazione, in Gestione dei nodi, scegli Esegui comando.
3. Seleziona Esegui comando.
4. Nella pagina Esegui un comando, cerca `AWS-JoinDirectoryServiceDomain`. Quando viene visualizzata nei risultati di ricerca, seleziona l'opzione `AWS-JoinDirectoryServiceDomain`.
5. Scorri verso il basso fino alla sezione Command parameters (Parametri comando). Occorre fornire i seguenti parametri:

   > **Note**
   >
   > Puoi individuare l'ID della directory, il nome della directory e gli indirizzi IP DNS tornando alla Directory Service console, selezionando Directory shared with me e selezionando la tua directory. Il tuo ID directory è disponibile nella sezione Dettagli della directory

condivisa. Puoi individuare i valori per Nome directory e Indirizzi IP DNS nella sezione Dettagli della directory del proprietario.

- In ID directory, inserisci il nome di Microsoft Active Directory gestita daAWS.
- In Nome directory, inserisci il nome di Microsoft Active Directory gestita da AWS (per l'account del proprietario della directory).
- Per gli indirizzi IP DNS, immettere gli indirizzi IP dei server DNS nella directory AWS Microsoft Active Directory gestita (per l'account del proprietario della directory).

6. In Destinazioni, scegli Scegli istanze manualmente, quindi seleziona le istanze a cui desideri aggiungere al dominio.
7. Lascia il resto del modulo impostato sui valori predefiniti, scorri la pagina verso il basso e quindi scegli Run (Esegui).
8. Lo stato del comando passerà da In sospeso a Eseguito correttamente una volta che le istanze saranno entrate a far parte del dominio correttamente. È possibile visualizzare l'output del comando selezionando l'ID istanza che è entrata a far parte del dominio e Visualizza output.

Dopo aver completato uno di questi passaggi, ora dovresti essere in grado di aggiungere la tua EC2 istanza al dominio. Dopo averlo fatto, puoi accedere all'istanza utilizzando un client RDP (Remote Desktop Protocol) con le credenziali del tuo account utente AWS Microsoft AD gestito.

Annullamento della condivisione della rubrica

Utilizzare la procedura seguente per annullare la condivisione di una directory Microsoft AD AWS gestita.

Per annullare la condivisione della directory

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Scegli l'ID della directory AWS Managed Microsoft AD che desideri annullare la condivisione.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

   - Se nella sezione Replica multi regione sono visualizzate più Regioni, seleziona quella in cui desideri annullare la condivisione della directory, quindi scegli la scheda Dimensiona e condividi. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.

- Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Dimensiona e condividi.

4. Nella sezione Shared directories (Directory condivise), selezionare la directory condivisa di cui annullare la condivisione e scegliere Actions (Operazioni), Unshare (Annulla condivisione).
5. Nella finestra di dialogo Unshare directory (Annulla condivisione directory), scegliere Unshare (Annulla condivisione).

Altre risorse

- Caso d'uso: condividi la tua directory per unire senza problemi EC2 le istanze Amazon a un dominio tra più account AWS
- AWS articolo del blog sulla sicurezza: Come unire EC2 istanze Amazon da più account e VPCs in un'unica directory Microsoft AD AWS gestita
- Collegamento delle istanze DB Amazon RDS tra account in un singolo dominio condiviso

Migrazione degli utenti di Active Directory a AWS Managed Microsoft AD

È possibile utilizzare Active Directory Migration Toolkit (ADMT) insieme al Password Export Service (PES) per migrare gli utenti da Active Directory autogestita alla directory Managed AWS Microsoft AD. Ciò consente di migrare più facilmente gli oggetti di Active Directory e le password crittografate per gli utenti.

Per istruzioni dettagliate, consulta Come migrare il dominio locale a Managed AWS Microsoft AD utilizzando ADMT sul Security Blog.AWS

Connect AWS Managed Microsoft AD all'infrastruttura Active Directory esistente

Questa sezione descrive come configurare le relazioni di trust tra AWS Managed Microsoft AD e l'infrastruttura Active Directory esistente.

Attività per connettere AWS Managed Microsoft AD all'Active Directory esistente:

- Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito

- Aggiungere percorsi IP quando si utilizzano indirizzi IP pubblici con AWS Managed Microsoft AD
- Tutorial: creazione di una relazione di trust tra il tuo Microsoft AD gestito da AWS e il dominio di Active Directory autogestito
- Tutorial: creazione di una relazione di trust tra due domini Microsoft AD gestito da AWS

Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito

È possibile configurare relazioni di trust esterne e forestali unidirezionali tra il AWS Directory Service per Microsoft Active Directory e le directory autogestite (locali), nonché tra più directory AWS Microsoft AD gestite nel cloud. AWS AWSMicrosoft AD gestito supporta tutte e tre le direzioni delle relazioni di trust: in entrata, in uscita e bidirezionale (bidirezionale).

Per ulteriori informazioni sulla relazione di trust, vedi Tutto quello che volevi sapere sui trust con AWS Managed Microsoft AD.

> **Note**
>
> Quando si impostano relazioni di trust, è necessario assicurarsi che la directory autogestita sia e rimanga compatibile con Directory Service s. Per ulteriori informazioni sulle proprie responsabilità, consultare il nostro modello sulla responsabilità condivisa.

AWSMicrosoft AD gestito supporta trust sia esterni che forestali. Per esaminare uno scenario di esempio che mostra come creare un trust tra foreste, consulta Tutorial: creazione di una relazione di trust tra il tuo Microsoft AD gestito da AWS e il dominio di Active Directory autogestito.

È richiesta una fiducia bidirezionale per app AWS aziendali come Amazon Chime, Amazon Connect, Quick SuiteAWS IAM Identity Center, WorkDocs, Amazon WorkMail, WorkSpaces Amazon e. Console di gestione AWS AWSMicrosoft AD gestito deve essere in grado di interrogare gli utenti e i gruppi nell'Active Directory autogestito.

È possibile abilitare l'autenticazione selettiva in modo che solo l'account del servizio specifico dell'AWSapplicazione possa interrogare l'Active Directory autogestito. Per ulteriori informazioni, vedi Migliorare la sicurezza dell'integrazione delle AWS app con AWS Managed Microsoft AD.

Amazon EC2, Amazon RDS e Amazon FSx funzioneranno con un trust unidirezionale o bidirezionale.

Prerequisiti

La creazione di un trust richiede solo pochi passaggi, ma è necessario completare diverse fasi preliminari prima di configurare il trust.

> **Note**
>
> AWSMicrosoft AD gestito non supporta l'attendibilità con domini a etichetta singola.

Connettiti a VPC

Se stai creando una relazione di fiducia con la tua directory autogestita, devi prima connettere la tua rete autogestita ad Amazon VPC contenente il tuo Managed Microsoft ADAWS. Il firewall per le reti Microsoft AD AWS gestite e autogestite deve avere aperte le porte di rete elencate nella Microsoft documentazione di WindowsServer 2008 e versioni successive.

Per utilizzare il nome NetBIOS anziché il nome di dominio completo per l'autenticazione con AWS applicazioni come Amazon o WorkDocs Amazon Quick Suite, devi consentire la porta 9389. Per ulteriori informazioni sulle porte e i protocolli di Active Directory, consulta Panoramica del servizio e requisiti delle porte di rete nella documentazione. Windows Microsoft

Queste sono le porte minime necessarie per riuscire a connettersi alla directory. La propria configurazione specifica potrebbe richiedere l'apertura di porte aggiuntive.

Configura il VPC

Il VPC che contiene Managed AWS Microsoft AD deve avere le regole in uscita e in entrata appropriate.

Configurazione delle regole in uscita del VPC

1. Nella AWS Directory Serviceconsole, nella pagina Dettagli della directory, annota l'ID della directory Microsoft AD AWS gestita.
2. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Scegli i Security Groups (Gruppi di sicurezza).
4. Cerca il tuo ID di directory AWS Managed Microsoft AD. Nei risultati della ricerca, seleziona l'elemento con la descrizione "gruppo di sicurezza AWS creato per i controller di directory ID delle directory».

> **Note**
>
> Il gruppo di sicurezza selezionato è un gruppo di sicurezza che viene creato in modo automatico quando crei la directory inizialmente.

5. Vai alla scheda Outbound Rules (Regole in uscita) di tale gruppo di sicurezza. Seleziona Edit (Modifica), quindi seleziona Add another rule (Aggiungi un'altra regola). Inserisci i valori seguenti per la nuova regola:

   - Type (Tipo): tutto il traffico
   - Protocol (Protocol): tutti
   - Destinazione determina il traffico che può lasciare i controller di dominio e dove può andare all'interno della rete autogestita. Specifica un singolo indirizzo IP o un intervallo di indirizzi IP nella notazione CIDR (ad esempio, 203.0.113.5/32). Puoi specificare anche il nome o l'ID di un altro gruppo di sicurezza nella stessa regione. Per ulteriori informazioni, consulta Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory.

6. Seleziona Salva.

Abilitazione della preautenticazione Kerberos

Gli account utente devono avere la preautenticazione Kerberos abilitata. Per ulteriori informazioni su questa impostazione, consulta Preauthentication on Microsoft TechNet.

Configurazione dei server d'inoltro condizionale DNS sul dominio autogestito

È necessario configurare i server d'inoltro condizionale DNS sul dominio autogestito. Per informazioni dettagliate sui server d'inoltro condizionali, consulta Assegnazione di un server d'inoltro condizionale TechNet per un nome di dominio su Microsoft.

Per eseguire la procedura seguente, devi disporre dell'accesso ai seguenti strumenti di Windows Server nel dominio autogestito:

- Strumenti AD DS e AD LDS
- DNS

Configurazione dei server d'inoltro condizionale sul dominio autogestito

1. Innanzitutto è necessario ottenere alcune informazioni su AWS Managed Microsoft AD. Accedi alla Console di gestione AWS e apri la console AWS Directory Service.
2. Nel riquadro di navigazione seleziona Directories (Directory).
3. Scegli l'ID della directory del tuo AWS Managed Microsoft AD.
4. Annota il nome di dominio completo (FQDN) e l'indirizzo DNS della tua directory.
5. Ora torna al controller di dominio autogestito. Aprire Server Manager.
6. Nel menu Tools (Strumenti), seleziona DNS.
7. Nella struttura della console, espandi il server DNS del dominio per il quale configuri il trust.
8. Nella struttura della console, scegli Conditional Forwarders (Serve d'inoltro condizionale).
9. Nel menu Action (Operazione), scegli New conditional forwarder (Nuovo server d'inoltro condizionale).
10. Nel dominio DNS, digita il nome di dominio completo (FQDN) del tuo Managed AWS Microsoft AD, come indicato in precedenza.
11. Scegli gli indirizzi IP dei server primari e digita gli indirizzi DNS della directory AWS Managed Microsoft AD, che hai annotato in precedenza.

    Dopo aver inserito l'indirizzo DNS, potresti ricevere un errore "timeout" o "unable to resolve" ("impossibile risolvere"). In genere, puoi ignorare questi errori.
12. Seleziona Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain (Memorizza questo server d'inoltro condizionale in Active Directory e replica come segue: tutti i server DNS in questo dominio). Scegli OK.

Password della relazione di trust

Se crei una relazione di trust con un dominio esistente, configurala su tale dominio utilizzando gli strumenti di Windows Server Administration. Nel farlo, annota la password di trust utilizzata. È necessario utilizzare la stessa password per configurare la relazione di trust su AWS Managed Microsoft AD. Per ulteriori informazioni, vedi Managing Trust on Microsoft TechNet.

Ora sei pronto per creare la relazione di trust sul tuo AWS Managed Microsoft AD.

NetBIOS e nomi di dominio

Il NetBIOS e i nomi di dominio devono essere univoci e non possono essere gli stessi per stabilire una relazione di trust.

Creazione, verifica o eliminazione di una relazione di trust

> **Note**
>
> Le relazioni di fiducia sono una funzionalità globale di AWS Managed Microsoft AD. Se utilizzi Configurazione della replica multiarea per Managed AWS Microsoft AD, è necessario eseguire le seguenti procedure in Regione principale. Le modifiche verranno applicate automaticamente in tutte le Regioni replicate. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per creare una relazione di fiducia con AWS Managed Microsoft AD

1. Apri la AWS Directory Service console.
2. Nella pagina Directory, scegli il tuo ID Microsoft AD AWS gestito.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), scegli Actions (Azioni), quindi seleziona Add trust relationship (Aggiungi relazione di trust).
5. Nella pagina Add a trust relationship (Aggiungi una relazione di trust), fornisci le informazioni necessarie, tra cui il tipo di trust, il nome dominio completo (FQDN) del dominio trusted, la password di trust e la direzione di trust.
6. (Facoltativo) Se desideri consentire solo agli utenti autorizzati di accedere alle risorse nella tua directory Microsoft AD AWS gestita, puoi facoltativamente scegliere la casella di controllo Autenticazione selettiva. Per informazioni generali sull'autenticazione selettiva, vedere Considerazioni sulla sicurezza per i trust su Microsoft. TechNet

7. In Server d'inoltro condizionale, digita l'indirizzo IP del server DNS autogestito. Se in precedenza hai creato server d'inoltro condizionale, puoi digitare il nome di dominio completo (FQDN) del dominio autogestito, invece dell'indirizzo IP DNS.
8. (Facoltativo) Scegli Aggiungi un altro indirizzo IP e digita l'indirizzo IP di un server DNS autogestito aggiuntivo. Puoi ripetere questa fase per ogni indirizzo del server DNS applicabile, per un totale di quattro indirizzi.
9. Scegliere Aggiungi.
10. Se il server DNS o la rete del dominio autogestito utilizza un spazio di indirizzi IP pubblici (al di fuori dello spazio RFC 1918), accedi alla sezione Instradamento IP), scegli Operazioni, quindi seleziona Aggiungi instradamento. Digita il blocco dell'indirizzo IP del server DNS o della rete autogestita tramite il formato CIDR, ad esempio 203.0.113.0/24. Questa fase non è necessaria se sia il server DNS che la rete autogestita utilizzano spazi di indirizzi IP RFC 1918.

    > **Note**
    >
    > Quando utilizzi uno spazio di indirizzi IP pubblici, assicurati di non utilizzare nessuno degli intervalli di indirizzi IP AWS, in quanto questi non possono essere utilizzati.

11. (Facoltativo) Quando sei sulla pagina Add routes (Aggiungi instradamento), ti consigliamo di selezionare anche Add routes to the security group for this directory's VPC (Aggiungi instradamenti al gruppo di sicurezza del VPC di questa directory). Ciò permetterà la configurazione dei gruppi di sicurezza, come descritto sopra nella sezione "Configura VPC". Queste regole di sicurezza incidono su un'interfaccia di rete interna che non viene esposta pubblicamente. Se questa opzione non è disponibile, visualizzerai un messaggio che indica che hai già personalizzato i gruppi di sicurezza.

È necessario configurare la relazione di trust su entrambi i domini. Le relazioni devono essere complementari. Ad esempio, nel caso di creazione di un trust in uscita su un dominio, sarà necessario creare un trust in entrata sull'altro.

Se crei una relazione di trust con un dominio esistente, configurala su tale dominio utilizzando gli strumenti di Windows Server Administration.

Puoi creare più trust tra il tuo AWS Managed Microsoft AD e vari domini Active Directory. Tuttavia, può esistere solo una relazione di fiducia per coppia alla volta. Ad esempio, se si dispone di un trust unidirezionale esistente nella «Direzione in entrata» e si desidera impostare un'altra relazione di

trust nella «direzione in uscita», sarà necessario eliminare la relazione di trust esistente e creare una nuova relazione di trust «bidirezionale».

Verifica di una relazione di trust in uscita

1. Apri la AWS Directory Service console.
2. Nella pagina Directory, scegli il tuo ID Microsoft AD AWS gestito.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), seleziona il trust da verificare, scegli Actions (Operazioni), quindi seleziona Verify trust relationship (Verifica relazione di trust).

Questo processo verifica solo la direzione in uscita di un trust bidirezionale. AWSnon supporta la verifica di un trust in entrata. Per ulteriori informazioni su come verificare l'attendibilità da o verso l'Active Directory autogestito, consulta Verify a Trust on Microsoft TechNet.

Eliminazione di una relazione di trust esistente

1. Apri la AWS Directory Service console.
2. Nella pagina Directory, scegli il tuo ID Microsoft AD AWS gestito.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), seleziona il trust da eliminare, scegli Actions (Operazioni), quindi seleziona Delete trust relationship (Elimina relazione di trust).
5. Scegli Delete (Elimina).

Aggiungere percorsi IP quando si utilizzano indirizzi IP pubblici con AWS Managed Microsoft AD

È possibile utilizzare AWS Directory Service per Microsoft Active Directory per sfruttare molte potenti funzionalità di Active Directory, inclusa la creazione di trust con altre directory. Tuttavia, se i server DNS per le reti delle altre directory utilizzano indirizzi IP, pubblici (al di fuori dello spazio RFC 1918), è necessario specificare tali indirizzi IP come parte della configurazione della fiducia. Le istruzioni necessarie per eseguire questa operazione sono disponibili in Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito.

Allo stesso modo, è necessario inserire le informazioni sull'indirizzo IP anche quando si instrada il traffico da AWS Managed Microsoft AD AWS a un VPC peer, se il AWS VPC utilizza intervalli di IP pubblici.

Quando aggiungi gli indirizzi IP come descritto in Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito, puoi selezionare Add routes to the security group for this directory's VPC (Aggiungi instradamenti al gruppo di sicurezza per il VPC di questa directory). Questa opzione dovrebbe essere selezionata a meno che tu non abbia precedentemente personalizzato il gruppo di sicurezza per consentire il traffico necessario come illustrato di seguito. Per ulteriori informazioni, consulta Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory.

Tutorial: creazione di una relazione di trust tra il tuo Microsoft AD gestito da AWS e il dominio di Active Directory autogestito

Questo tutorial illustra tutti i passaggi necessari per impostare una relazione di fiducia tra AWS Directory Service per Microsoft Active Directory e Active Directory autogestito (locale)Microsoft. Sebbene la creazione di trust comprenda poche fasi, è necessario prima completare le seguenti fasi preliminari.

Argomenti

- Prerequisiti
- Fase 1: Preparazione del dominio di AD autogestito
- Fase 2: preparazione di Microsoft AD gestito da AWS
- Fase 3: creazione della relazione di trust

Vedi anche

Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito

Prerequisiti

Questo tutorial presuppone che tu abbia già:

> **Note**
>
> AWS Microsoft AD gestito non supporta l'attendibilità con domini Single label.

- Una directory Microsoft AD AWS gestita creata su AWS. Se hai bisogno di aiuto per eseguire questa operazione, consulta Guida introduttiva a AWS Managed Microsoft AD.
- Un' EC2 istanza in esecuzione Windows aggiunta a quel AWS Managed Microsoft AD. Se hai bisogno di aiuto per eseguire questa operazione, consulta Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory.

  > **Important**
  >
  > L'account amministratore per AWS Managed Microsoft AD deve disporre dell'accesso amministrativo a questa istanza.

- I seguenti strumenti Windows del server sono installati su quell'istanza:
  - Strumenti AD DS e AD LDS
  - DNS

  Se hai bisogno di aiuto per eseguire questa operazione, consulta Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.
- Un Microsoft Active Directory autogestito (on-premise)

  È necessario disporre dell'accesso amministrativo a questa directory. Gli stessi strumenti Windows del server elencati sopra devono essere disponibili anche per questa directory.
- Una connessione attiva tra la rete autogestita e il VPC contenente AWS Managed Microsoft AD. Se hai bisogno di assistenza, consulta il documento sulle opzioni di connettività di Amazon Virtual Private Cloud (VPC).
- Una policy di sicurezza locale impostata correttamente. Verifica `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` e assicurati che contenga almeno le seguenti pipe con tre nomi:

  - netlogon
  - samr
  - lsarpc
- Il NetBIOS e i nomi di dominio devono essere univoci e non possono essere gli stessi per stabilire una relazione di trust

Per ulteriori informazioni sui prerequisiti per la creazione di una relazione di trust, consulta Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito.

Configurazione del tutorial

Per questo tutorial, abbiamo già creato un Microsoft AD AWS gestito e un dominio autogestito. La rete autogestita è connessa al VPC di AWS Managed Microsoft AD. Di seguito sono riportate le proprietà delle due directory:

AWS Microsoft AD gestito in esecuzione su AWS

- Nome di dominio (FQDN): ad.example.com MyManaged
- Nome NetBIOS: AD MyManaged
- Indirizzi DNS: 10.0.10.246, 10.0.20.121
- CIDR VPC: 10.0.0.0/16

Il AWS Managed Microsoft AD risiede nell'ID VPC: vpc-12345678.

Dominio Microsoft AD AWS gestito o autogestito

- Nome del dominio (FQDN): corp.example.com
- Nome NetBIOS: CORP
- Indirizzi DNS: 172.16.10.153
- CIDR autogestito: 172.16.0.0/16

Fase successiva

Fase 1: Preparazione del dominio di AD autogestito

Fase 1: Preparazione del dominio di AD autogestito

In primo luogo, è necessario completare varie fasi preliminari sul tuo dominio autogestito (on-premise).

Configurazione del firewall gestito autogestito

È necessario configurare il firewall autogestito in modo che le seguenti porte siano aperte a tutte CIDRs le sottoreti utilizzate dal VPC che contiene Managed Microsoft AD. AWS In questo tutorial, consentiamo il traffico in entrata e in uscita da 10.0.0.0/16 (il blocco CIDR del VPC del nostro Managed AWS Microsoft AD) sulle seguenti porte:

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticazione Kerberos
- TCP/UDP 389 - Lightweight Directory Access Protocol (LDAP)
- TCP 445 - Server Message Block (SMB)
- TCP 9389 - Active Directory Web Services (ADWS) (opzionale: questa porta deve essere aperta se si desidera utilizzare il nome NetBIOS anziché il nome di dominio completo per l'autenticazione con applicazioni come AWS Amazon o WorkDocs Amazon Quick Suite.)

> **Note**
>
> SMBv1 non è più supportato.
> Queste sono le porte minime necessarie per connettere il VPC alla directory autogestita. La propria configurazione specifica potrebbe richiedere l'apertura di porte aggiuntive.

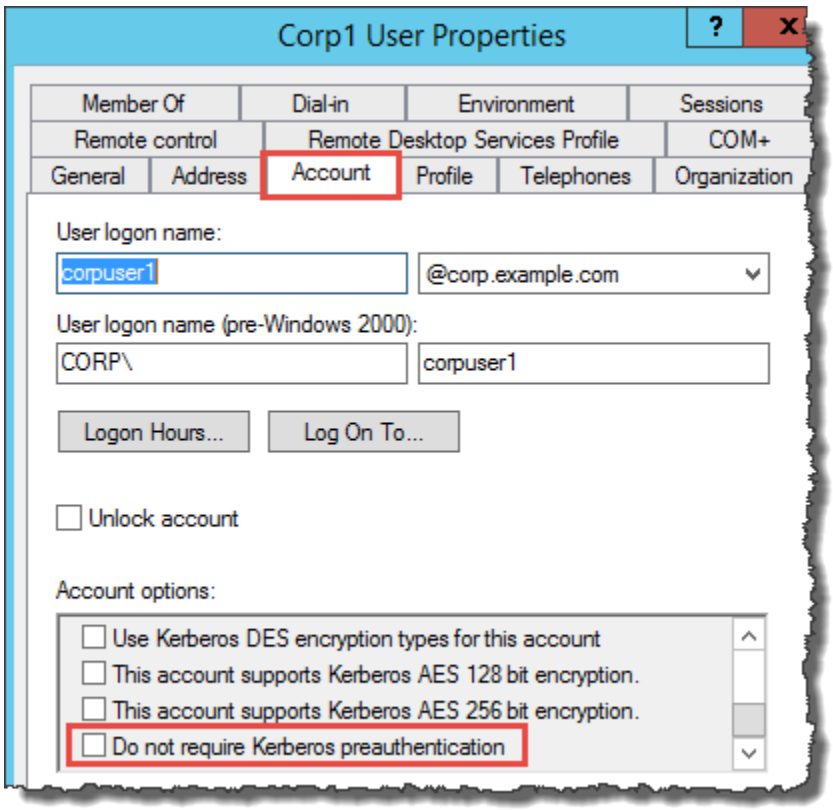
Assicurarsi che la preautenticazione di Kerberos sia abilitata

La preautenticazione di Kerberos deve essere abilitata per gli account utente in entrambe le directory. Questa è l'impostazione predefinita, ma controlliamo le proprietà di qualsiasi utente causale per assicurarci che non siano state apportate modifiche.

Per visualizzare le impostazioni Kerberos dell'utente

1. Sul controller di dominio gestito dal cliente, apri Server Manager.

2. Nel menu Tools (Strumenti), scegli Active Directory Users and Computers (Strumento Users and Computers (Utenti e computer) di Active Directory).
3. Scegli la cartella Users (Utenti) e apri il menu contestuale (clic sul tasto destro). Seleziona un account utente casuale elencato nel riquadro di destra. Scegli Properties (Proprietà).
4. Seleziona la scheda Account. Nell'elenco Account options (Opzioni account), scorri verso il basso e assicurati che Do not require Kerberos preauthentication (Non richiedere la preautenticazione Kerberos) non sia selezionato.



Configurazione dei server d'inoltro condizionale DNS per il dominio autogestito

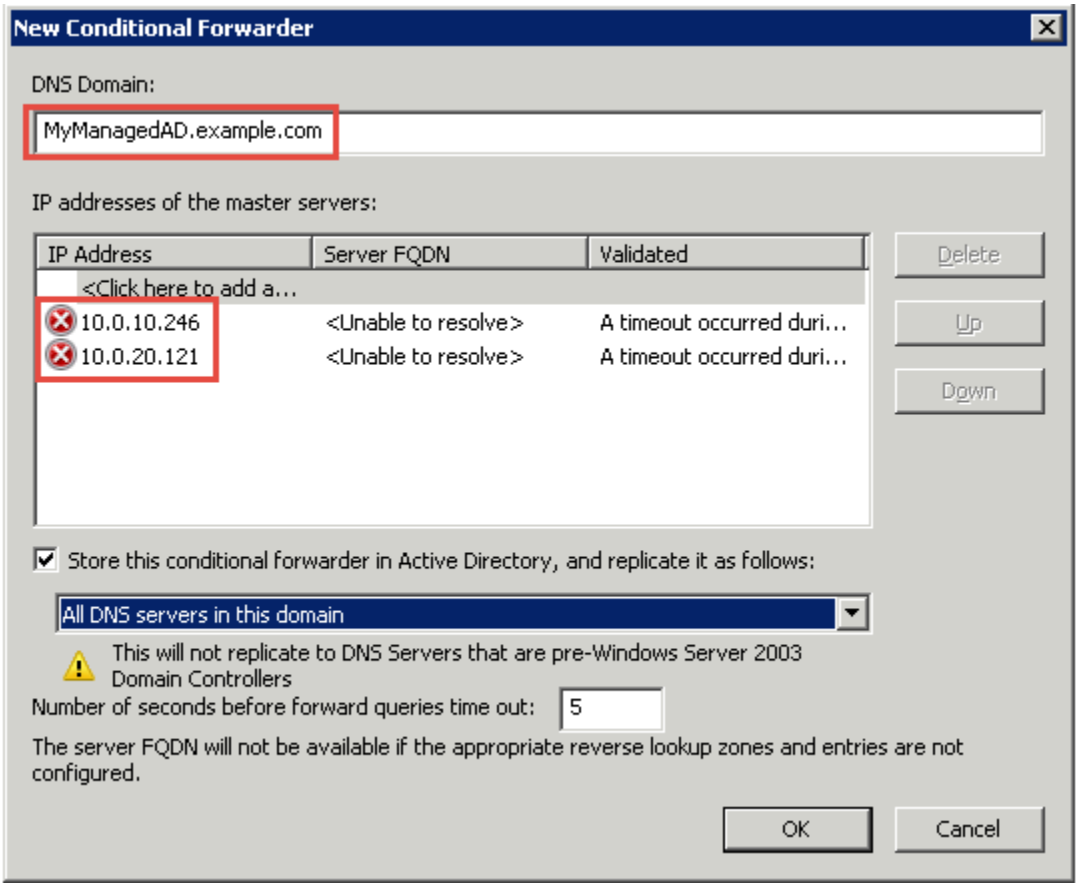
È necessario configurare i server d'inoltro condizionale DNS su ciascun dominio. Prima di eseguire questa operazione sul tuo dominio autogestito, otterrai alcune informazioni sul tuo AWS Managed Microsoft AD.

Configurazione dei server d'inoltro condizionale sul dominio autogestito

1. Accedi a Console di gestione AWS e apri la AWS Directory Service console.
2. Nel riquadro di navigazione seleziona Directories (Directory).
3. Scegli l'ID della directory del tuo AWS Managed Microsoft AD.

4. Nella pagina Details (Dettagli), prendi nota dei valori in Directory name (Nome directory) e in DNS address (Indirizzo DNS) della tua directory.
5. Ora torna al controller di dominio autogestito. Aprire Server Manager.
6. Nel menu Tools (Strumenti), seleziona DNS.
7. Nella struttura della console, espandi il server DNS del dominio per il quale configuri il trust. Il nostro server è WIN-5V70 CN7 VJ0.corp.example.com.
8. Nella struttura della console, scegli Conditional Forwarders (Serve d'inoltro condizionale).
9. Nel menu Action (Operazione), scegli New conditional forwarder (Nuovo server d'inoltro condizionale).
10. Nel dominio DNS, digita il nome di dominio completo (FQDN) del tuo Managed AWS Microsoft AD, come indicato in precedenza. In questo esempio, il nome di dominio completo è AD.example.com. MyManaged
11. Scegli gli indirizzi IP dei server primari e digita gli indirizzi DNS della directory AWS Managed Microsoft AD, che hai annotato in precedenza. In questo esempio, sono: 10.0.10.246, 10.0.20.121

    Dopo aver inserito l'indirizzo DNS, potresti ricevere un errore "timeout" o "unable to resolve" ("impossibile risolvere"). In genere, puoi ignorare questi errori.



12. Seleziona Store this conditional forwarder in Active Directory, and replicate it as follows (Memorizza questo server d'inoltro condizionale in Active Directory e replicalo come segue).
13. Seleziona All DNS servers in this domain (Tutti i server DNS in questo dominio), quindi seleziona OK.

Fase successiva

Fase 2: preparazione di Microsoft AD gestito da AWS

Fase 2: preparazione di Microsoft AD gestito da AWS

Ora prepariamo AWS Managed Microsoft AD per la relazione di fiducia. Molte delle fasi seguenti sono quasi identiche a quelle appena completate per il dominio autogestito. Questa volta, tuttavia, stai lavorando con il tuo AWS Managed Microsoft AD.

Configurazione delle sottoreti VPC e dei gruppi di sicurezza

È necessario consentire il traffico dalla rete autogestita al VPC contenente AWS Managed Microsoft AD. A tale scopo, è necessario assicurarsi che le regole ACLs associate alle sottoreti utilizzate per

distribuire Managed AWS Microsoft AD e le regole dei gruppi di sicurezza configurate sui controller di dominio consentano entrambe il traffico necessario per supportare i trust.

I requisiti di porta variano in base alla versione di Windows Server utilizzata dal controller di dominio e dai servizi o applicazioni che sfruttano il trust. Per gli scopi di questo tutorial, sarà necessario aprire le seguenti porte:

In entrata

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticazione Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB
- TCP/UDP 464 - Autenticazione Kerberos
- TCP 636 - LDAPS (LDAP su TLS/SSL)
- TCP 3268-3269 - Catalogo globale
- TCP/UDP 49152-65535 - Porte temporanee per RPC

> **Note**
>
> SMBv1 non è più supportato.

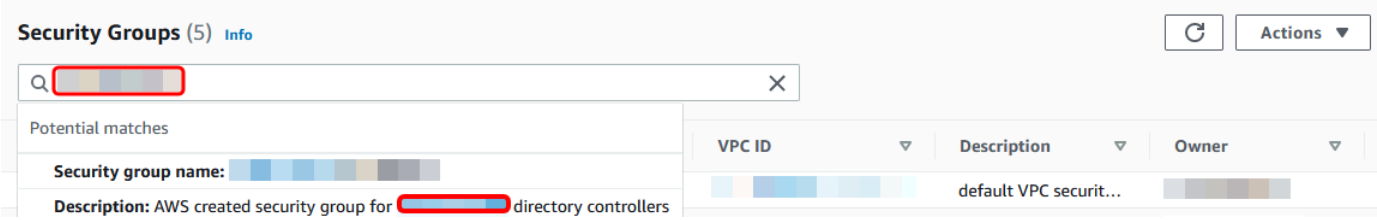
In uscita

- ALL

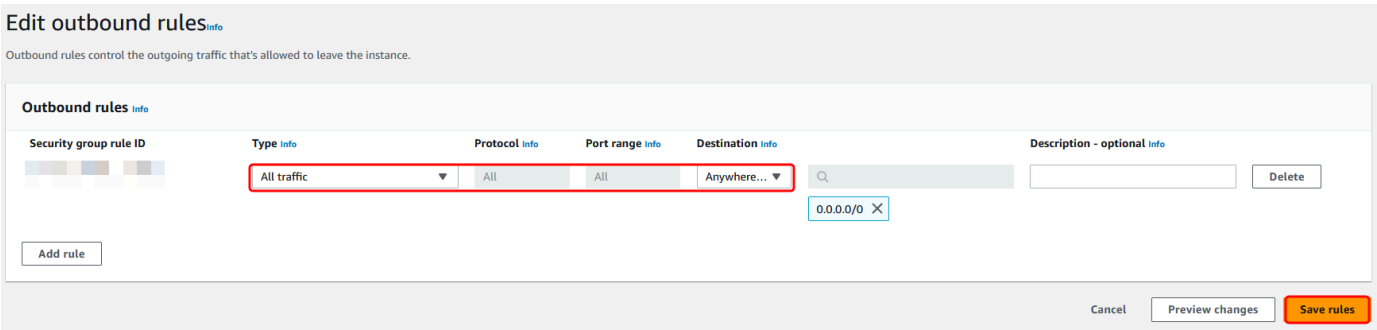
> **Note**
>
> Queste sono le porte minime necessarie per riuscire a connettere il VPC e la directory autogestita. La propria configurazione specifica potrebbe richiedere l'apertura di porte aggiuntive.

Per configurare le regole in entrata e in uscita del controller di dominio Microsoft AD AWS gestito

1. Tornare alla console AWS Directory Service. Nell'elenco delle directory, prendi nota dell'ID della directory AWS Managed Microsoft AD.
2. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
4. Utilizza la casella di ricerca per cercare il tuo ID di directory Microsoft AD AWS gestito. Nei risultati della ricerca, seleziona il gruppo di sicurezza con la descrizione**`AWS created security group for yourdirectoryID directory controllers`**.



5. Vai alla scheda Outbound Rules (Regole in uscita) per tale gruppo di sicurezza. Scegli Modifica regole, quindi Aggiungi regola. Inserisci i valori seguenti per la nuova regola:
   - Type (Tipo): traffico ALL
   - Protocol (Protocollo): ALL
   - Destination (Destinazione) determina il traffico che può lasciare i controller di dominio e dove può andare. Specifica un singolo indirizzo IP o un intervallo di indirizzi IP nella notazione CIDR (ad esempio, 203.0.113.5/32). Puoi specificare anche il nome o l'ID di un altro gruppo di sicurezza nella stessa regione. Per ulteriori informazioni, consulta Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory.
6. Seleziona Salva regola.

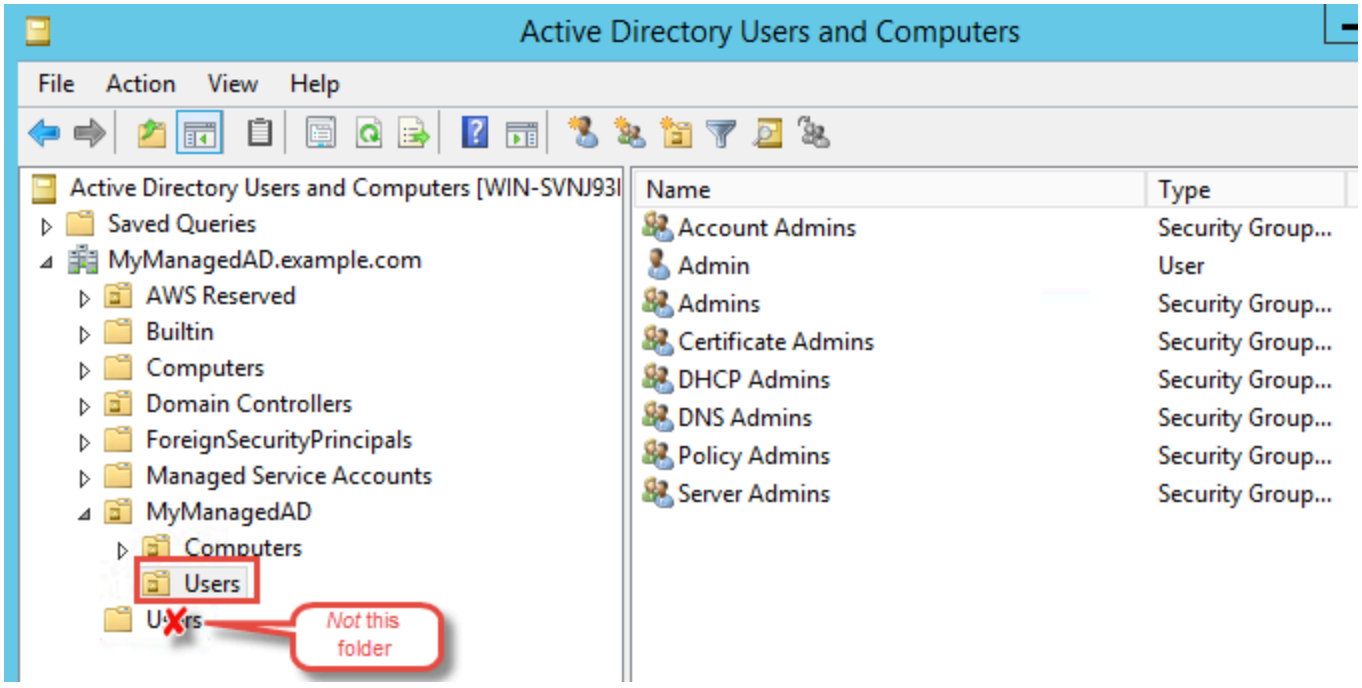


Assicurarsi che la preautenticazione di Kerberos sia abilitata

Ora vuoi confermare che anche gli utenti del tuo AWS Managed Microsoft AD abbiano abilitato la preautenticazione Kerberos. Si tratta della stesso processo completato per la directory autogestita. Questa è l'impostazione predefinita, ma controlliamo per assicurarci che non siano state apportate modifiche.

Visualizzazione delle impostazioni Kerberos dell'utente

1. Accedi a un'istanza che fa parte della tua directory di Microsoft AD AWS gestita utilizzando il comando AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo per il dominio o un account a cui sono state delegate le autorizzazioni per la gestione degli utenti nel dominio.
2. Se non sono installati, installa gli strumenti DNS e Utenti e computer di Active Directory. Scopri come installare questi strumenti in Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.
3. Aprire Server Manager. Nel menu Tools (Strumenti), scegli Active Directory Users and Computers (Strumento Users and Computers (Utenti e computer) di Active Directory).
4. Scegli la cartella Users (Utenti) nel dominio. Da notare che questa è la cartella Users (Utenti) sotto il nome NetBIOS e non la cartella Users (Utenti) sotto il nome del dominio completo (FQDN).



5. Nell'elenco di utenti, fai clic con il pulsante destro del mouse su un utente, quindi scegli Proprietà (Properties).
6. Seleziona la scheda Account. Nell'elenco Account options (Opzioni account), assicurati che Do not require Kerberos preauthentication (Non richiedere la preautenticazione Kerberos) non sia selezionato.

Fase successiva

Fase 3: creazione della relazione di trust

Fase 3: creazione della relazione di trust

Ora che il lavoro di preparazione è completato, le fasi finali servono a creare i trust. Prima crei la fiducia sul tuo dominio autogestito e infine sul tuo AWS Managed Microsoft AD. In caso di problemi durante il processo di creazione del trust, consultare Motivo stato di creazione trust per ricevere assistenza.

Configurazione dell'attendibilità nell'Active Directory autogestito

In questo tutorial, è possibile configurare un trust tra foreste bidirezionale. Tuttavia, se si crea un trust tra foreste unidirezionale occorre tenere presente che le direzioni del trust su ciascuno dei domini devono essere complementari. Ad esempio, se crei un trust unidirezionale in uscita sul tuo dominio autogestito, devi creare un trust unidirezionale in entrata sul tuo Managed Microsoft AD. AWS

> **Note**
>
> AWS Managed Microsoft AD supporta anche i trust esterni. Tuttavia, ai fini di questo tutorial, verrà creato un trust tra foreste bidirezionale.

Per configurare l'attendibilità nell'Active Directory autogestito

1. Aprire Server Manager e nel menu Tools (Strumenti) scegliere Active Directory Domains and Trusts (Trust e domini di Active Directory).
2. Aprire il menu contestuale (pulsante destro del mouse) del dominio e scegliere Properties (Proprietà).
3. Scegliere la scheda Trusts (Trust) e scegliere New trust (Nuovo trust). Digita il nome del tuo AWS Managed Microsoft AD e scegli Avanti.

4. Scegliere Forest Trust (Trust tra foreste). Scegli Next (Successivo).
5. Scegliere Two-way (Bidirezionale). Scegli Next (Successivo).
6. Scegliere This domain only (Solo questo dominio). Scegli Next (Successivo).
7. Scegliere Forest-wide authentication (Autenticazione a livello di foresta). Scegli Next (Successivo).
8. Digitare una Trust password (Password di trust). Assicurati di ricordare questa password perché ti servirà quando configuri l'attendibilità per AWS Managed Microsoft AD.
9. Nella finestra di dialogo successiva, confermare le impostazioni e scegliere Next (Avanti). Confermare la corretta creazione del trust e scegliere nuovamente Next (Avanti).
10. Scegliere No, do not confirm the outgoing trust (No, non confermare il trust in uscita). Scegli Next (Successivo).
11. Scegliere No, do not confirm the incoming trust (No, non confermare il trust in ingresso). Scegli Next (Successivo).

Configura l'attendibilità nella tua directory AWS Managed Microsoft AD

Infine, si configura la relazione di trust della foresta con la directory AWS Managed Microsoft AD. Poiché hai creato un trust di foresta bidirezionale nel dominio autogestito, crei anche un trust bidirezionale utilizzando la directory Managed AWS Microsoft AD.

> **Note**
>
> Le relazioni di fiducia sono una funzionalità globale di AWS Managed Microsoft AD. Se utilizzi Configurazione della replica multiarea per Managed AWS Microsoft AD, è necessario eseguire le seguenti procedure in Regione principale. Le modifiche verranno applicate automaticamente in tutte le Regioni replicate. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per configurare l'attendibilità nella directory AWS Managed Microsoft AD

1. Tornare alla console AWS Directory Service.
2. Nella pagina Directory, scegli il tuo ID Microsoft AD AWS gestito.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:

- Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.

4. Nella sezione Trust relationships (Relazioni di trust), scegli Actions (Azioni), quindi seleziona Add trust relationship (Aggiungi relazione di trust).
5. Nella pagina Aggiungi una relazione di trust, specifica il Tipo di trust. In questo caso, scegliamo Trust tra foreste. Digita il nome completo del dominio autogestito (in questo tutorial **`corp.example.com`**). Digita la stessa password di trust utilizzata durante la creazione del trust sul dominio autogestito. Specificare la direzione. In questo caso scegliamo Bidirezionale.
6. Nel campo Server d'inoltro condizionale, inserisci l'indirizzo IP del server DNS autogestito. In questo esempio, inserire 172.16.10.153.
7. (Facoltativo) Scegli Aggiungi un altro indirizzo IP e inserisci un secondo indirizzo IP del proprio server DNS locale. È possibile specificare fino a un totale di quattro server DNS.
8. Scegli Aggiungi.

Congratulazioni. Ora hai una relazione di trust tra il tuo dominio autogestito (corp.example.com) e il tuo Managed AWS Microsoft AD (AD.example.com). MyManaged È possibile configurare solo una relazione tra questi due domini. Se, ad esempio, si desidera modificare la direzione del trust in unidirezionale, sarebbe prima di tutto necessario eliminare questa relazione di trust esistente e crearne una nuova.

Per ulteriori informazioni, incluse le istruzioni sulla verifica o sull'eliminazione di trust, consultare Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito.

Tutorial: creazione di una relazione di trust tra due domini Microsoft AD gestito da AWS

Questo tutorial illustra tutti i passaggi necessari per impostare una relazione di trust tra due domini AWS Directory Service per Microsoft Active Directory.

Argomenti

- Fase 1: preparazione di Microsoft AD gestito da AWS
- Fase 2: Creare la relazione di trust con un altro dominio Microsoft AD AWS gestito

Vedi anche

[Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito]

Fase 1: preparazione di Microsoft AD gestito da AWS

In questa sezione, preparerai il tuo AWS Managed Microsoft AD per la relazione di trust con un altro AWS Managed Microsoft AD. Molte delle fasi seguenti sono quasi identiche a quelle completate in [Tutorial: creazione di una relazione di trust tra il tuo Microsoft AD gestito da AWS e il dominio di Active Directory autogestito]. Questa volta, tuttavia, stai configurando gli ambienti Microsoft AD AWS gestiti per funzionare tra loro.

Configurazione delle sottoreti VPC e dei gruppi di sicurezza

È necessario consentire il traffico da una rete AWS Managed Microsoft AD al VPC contenente l'altro Managed AWS Microsoft AD. A tale scopo, è necessario assicurarsi che le regole ACLs associate alle sottoreti utilizzate per distribuire Managed AWS Microsoft AD e le regole dei gruppi di sicurezza configurate sui controller di dominio consentano entrambe il traffico necessario per supportare i trust.

I requisiti di porta variano in base alla versione di Windows Server utilizzata dal controller di dominio e dai servizi o applicazioni che sfruttano il trust. Per gli scopi di questo tutorial, sarà necessario aprire le seguenti porte:

In entrata

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticazione Kerberos
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

> **Note**
>
> SMBv1 non è più supportato.

- TCP/UDP 464 - Autenticazione Kerberos
- TCP 636 - LDAPS (LDAP su TLS/SSL)
- TCP 3268-3269 - Catalogo globale

- TCP/UDP 1024-65535 - Porte temporanee per RPC

In uscita

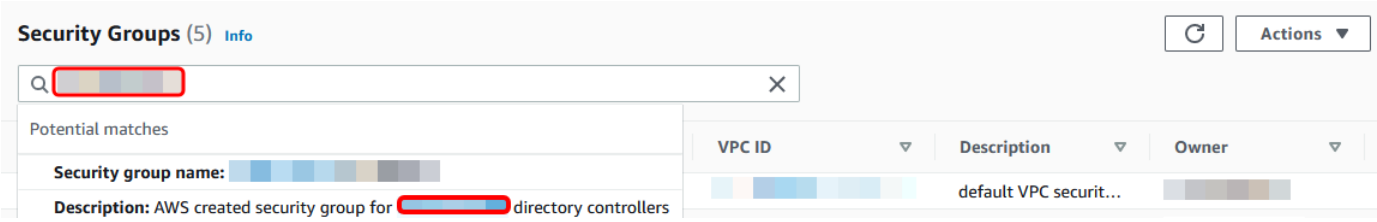
- ALL

> **Note**
>
> Queste sono le porte minime necessarie per poterle connettere VPCs da entrambi i AWS Managed Microsoft AD. La propria configurazione specifica potrebbe richiedere l'apertura di porte aggiuntive. Per ulteriori informazioni, consulta Come configurare un firewall per domini e trust di Active Directory sul sito Web di Microsoft.

Per configurare le regole in uscita del controller di dominio Microsoft AD AWS gestito

> **Note**
>
> Ripeti i passaggi da 1 a 6 riportati di seguito per ogni directory.

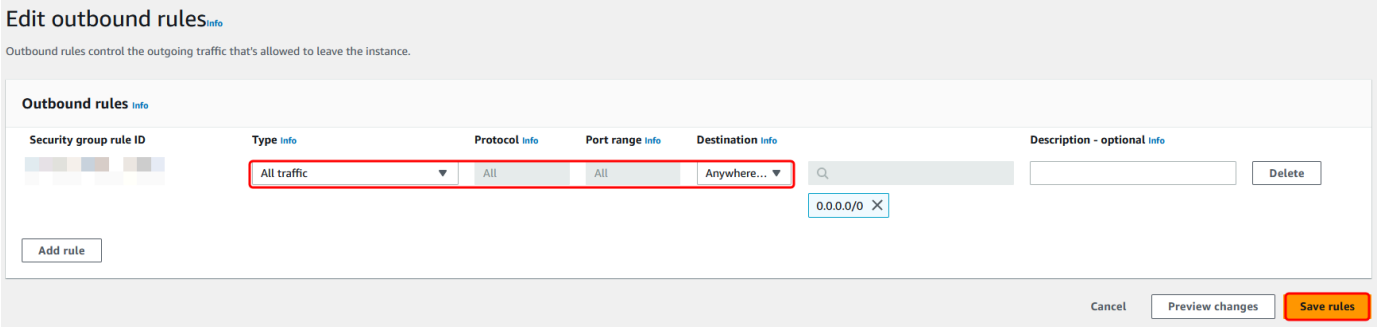
1. Accedere alla console AWS Directory Service. Nell'elenco delle directory, prendi nota dell'ID della directory AWS Managed Microsoft AD.
2. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
4. Utilizza la casella di ricerca per cercare il tuo ID di directory Microsoft AD AWS gestito. Nei risultati della ricerca, seleziona l'elemento con la descrizione**`AWS created security group for yourdirectoryID directory controllers`**.



5. Vai alla scheda Outbound Rules (Regole in uscita) per tale gruppo di sicurezza. Scegli Edit (Modifica), quindi seleziona Add another rule (Aggiungi un'altra regola). Inserisci i valori seguenti per la nuova regola:

- Type (Tipo): traffico ALL
- Protocol (Protocollo): ALL
- Destination (Destinazione) determina il traffico che può lasciare i controller di dominio e dove può andare. Specifica un singolo indirizzo IP o un intervallo di indirizzi IP nella notazione CIDR (ad esempio, 203.0.113.5/32). Puoi specificare anche il nome o l'ID di un altro gruppo di sicurezza nella stessa regione. Per ulteriori informazioni, consulta Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory.

6. Seleziona Salva.



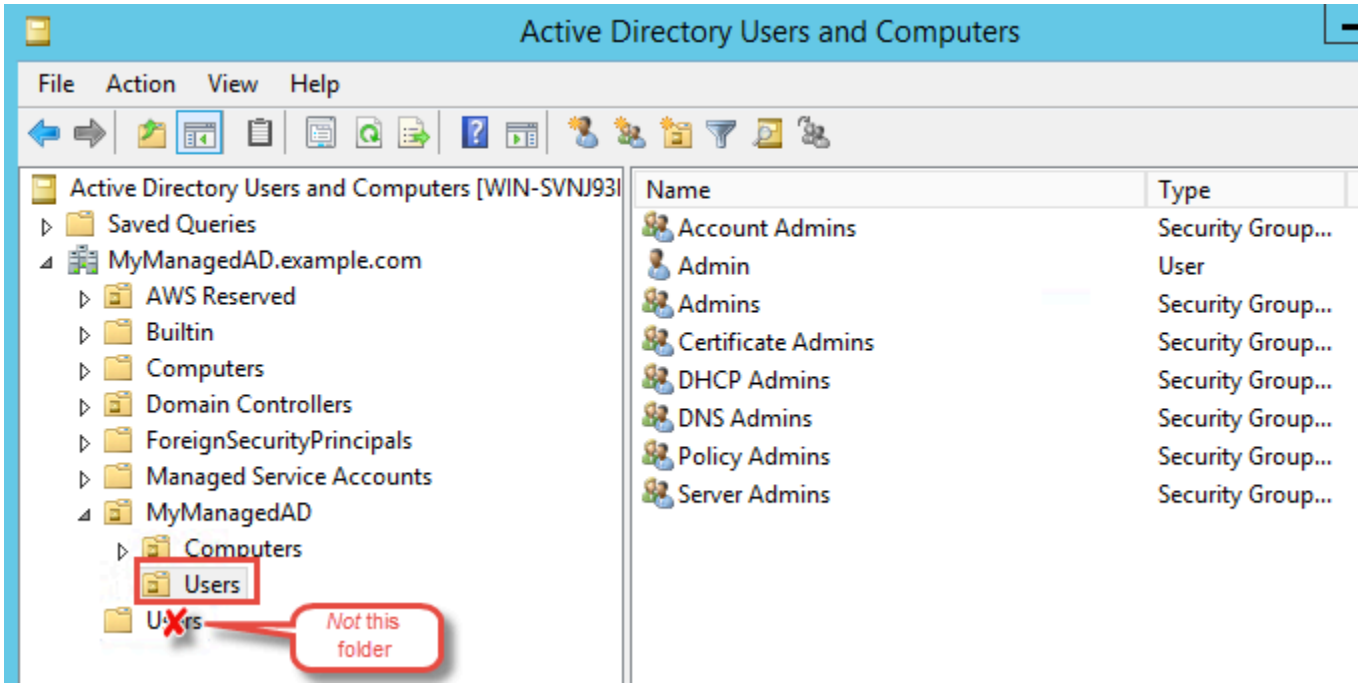
Assicurarsi che la preautenticazione di Kerberos sia abilitata

Ora vuoi confermare che anche gli utenti del tuo AWS Managed Microsoft AD abbiano abilitato la preautenticazione Kerberos. Si tratta della stesso processo completato per la directory locale. Questa è l'impostazione predefinita, ma controlliamo per assicurarci che non siano state apportate modifiche.

Visualizzazione delle impostazioni Kerberos dell'utente

1. Accedi a un'istanza che fa parte della tua directory di Microsoft AD AWS gestita utilizzando il comando AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo per il dominio o un account a cui sono state delegate le autorizzazioni per la gestione degli utenti nel dominio.
2. Se non sono installati, installa gli strumenti DNS e Utenti e computer di Active Directory. Scopri come installare questi strumenti in Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.
3. Aprire Server Manager. Nel menu Tools (Strumenti), scegli Active Directory Users and Computers (Strumento Users and Computers (Utenti e computer) di Active Directory).

4. Scegli la cartella Users (Utenti) nel dominio. Da notare che questa è la cartella Users (Utenti) sotto il nome NetBIOS e non la cartella Users (Utenti) sotto il nome del dominio completo (FQDN).



5. Nell'elenco di utenti, fai clic con il pulsante destro del mouse su un utente, quindi scegli Proprietà (Properties).
6. Seleziona la scheda Account. Nell'elenco Account options (Opzioni account), assicurati che Do not require Kerberos preauthentication (Non richiedere la preautenticazione Kerberos) non sia selezionato.

Fase successiva

Fase 2: Creare la relazione di trust con un altro dominio Microsoft AD AWS gestito

Fase 2: Creare la relazione di trust con un altro dominio Microsoft AD AWS gestito

Ora che il lavoro di preparazione è completo, i passaggi finali consistono nel creare i trust tra i due domini Microsoft AD AWS gestiti. In caso di problemi durante il processo di creazione del trust, consultare Motivo stato di creazione trust per ricevere assistenza.

Configura l'affidabilità nel tuo primo dominio Microsoft AD AWS gestito

In questo tutorial, è possibile configurare un trust tra foreste bidirezionale. Tuttavia, se si crea un trust tra foreste unidirezionale occorre tenere presente che le direzioni del trust su ciascuno dei domini

devono essere complementari. Ad esempio, se si crea un trust unidirezionale in uscita su questo primo dominio, è necessario creare un trust unidirezionale in entrata sul secondo dominio AWS Microsoft AD gestito.

> **Note**
>
> AWS Managed Microsoft AD supporta anche i trust esterni. Tuttavia, ai fini di questo tutorial, verrà creato un trust tra foreste bidirezionale.

Per configurare l'attendibilità nel tuo primo dominio Microsoft AD AWS gestito

1. Apri la AWS Directory Service console.
2. Nella pagina Directory, scegli il tuo primo ID Microsoft AD AWS gestito.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), scegli Actions (Azioni), quindi seleziona Add trust relationship (Aggiungi relazione di trust).
5. Nella pagina Aggiungi una relazione di trust, digita il nome di dominio completo del secondo dominio AWS Microsoft AD gestito. Assicurati di ricordare questa password poiché ti servirà quando configuri l'attendibilità per il tuo secondo AWS Managed Microsoft AD. Specificare la direzione. In questo caso scegli Bidirezionale.
6. Nel campo Conditional forwarder, inserisci l'indirizzo IP del tuo secondo server DNS AWS Microsoft AD gestito.
7. (Facoltativo) Scegli Aggiungi un altro indirizzo IP e inserisci un secondo indirizzo IP per il secondo server DNS Microsoft AD AWS gestito. È possibile specificare fino a un totale di quattro server DNS.
8. Scegli Aggiungi. A questo punto, il trust ha esito negativo, come previsto, finché non viene creato l'altro lato del trust.

Configura l'attendibilità nel tuo secondo dominio Microsoft AD AWS gestito

Ora, configuri la relazione di trust della foresta con la tua seconda directory Microsoft AD AWS gestita. Poiché hai creato un trust di foresta bidirezionale nel primo dominio Microsoft AD AWS gestito, crei anche un trust bidirezionale utilizzando questo dominio AWS Microsoft AD gestito.

Per configurare l'attendibilità nel secondo dominio Microsoft AD AWS gestito

1. Tornare alla console AWS Directory Service.
2. Nella pagina Directory, scegli il tuo secondo ID Microsoft AD AWS gestito.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), scegli Actions (Azioni), quindi seleziona Add trust relationship (Aggiungi relazione di trust).
5. Nella pagina Aggiungi una relazione di trust, digita il nome di dominio completo del tuo primo dominio AWS Microsoft AD gestito. Digitare la stessa password di trust utilizzata durante la creazione del trust sul dominio in loco. Specificare la direzione. In questo caso scegli Bidirezionale.
6. Nel campo Server d'inoltro condizionale, inserisci l'indirizzo IP del primo server DNS di Microsoft AD gestito da AWS .
7. (Facoltativo) Scegli Aggiungi un altro indirizzo IP e inserisci un secondo indirizzo IP per il tuo primo server DNS Microsoft AD AWS gestito. È possibile specificare fino a un totale di quattro server DNS.
8. Scegli Aggiungi. La verifica del trust avviene poco dopo.
9. Ora torna al trust creato nel primo dominio e verifica nuovamente la relazione di trust.

Congratulazioni. Ora hai una relazione di trust tra i tuoi due domini Microsoft AD AWS gestiti. È possibile configurare solo una relazione tra questi due domini. Se, ad esempio, si desidera modificare la direzione del trust in unidirezionale, sarebbe prima di tutto necessario eliminare questa relazione di trust esistente e crearne una nuova.

Estendi lo schema AWS Managed Microsoft AD

AWS Microsoft AD gestito utilizza schemi per organizzare e applicare il modo in cui vengono archiviati i dati delle directory. Il processo di aggiunta delle definizioni allo schema viene definito «estensione dello schema». Le estensioni dello schema consentono di modificare lo schema della directory AWS Managed Microsoft AD utilizzando un file LDAP Data Interchange Format (LDIF) valido. Per ulteriori informazioni sugli schemi AD e su come estendere gli schemi, consulta gli argomenti elencati di seguito.

Quando estendere lo schema AWS Managed Microsoft AD

È possibile estendere lo schema AWS Managed Microsoft AD aggiungendo nuove classi di oggetti e attributi. Ad esempio, puoi eseguire questa operazione se disponi di un'applicazione che richiede modifiche dello schema, al fine di supportare funzionalità Single Sign-On.

Puoi utilizzare le estensioni di schema anche per abilitare il supporto per applicazioni che si affidano a specifici attributi e classi di oggetto di Active Directory. Ciò può essere particolarmente utile nel caso in cui sia necessario migrare le applicazioni aziendali che dipendono da AWS Managed Microsoft AD nel AWS cloud.

Ogni attributo o classe che viene aggiunto a uno schema di Active Directory esistente deve essere definito con un ID univoco. In questo modo, quando le aziende aggiungono estensioni allo schema, possono avere la certezza che queste siano univoche e che non siano in conflitto tra loro. Questi IDs sono denominati AD Object Identifiers (OIDs) e sono archiviati in AWS Managed Microsoft AD.

Per iniziare, consulta Tutorial: estensione dello schema AWS Managed Microsoft AD.

Argomenti correlati

- Estendi lo schema AWS Managed Microsoft AD
- Elementi dello schema

Argomenti

- Tutorial: estensione dello schema AWS Managed Microsoft AD

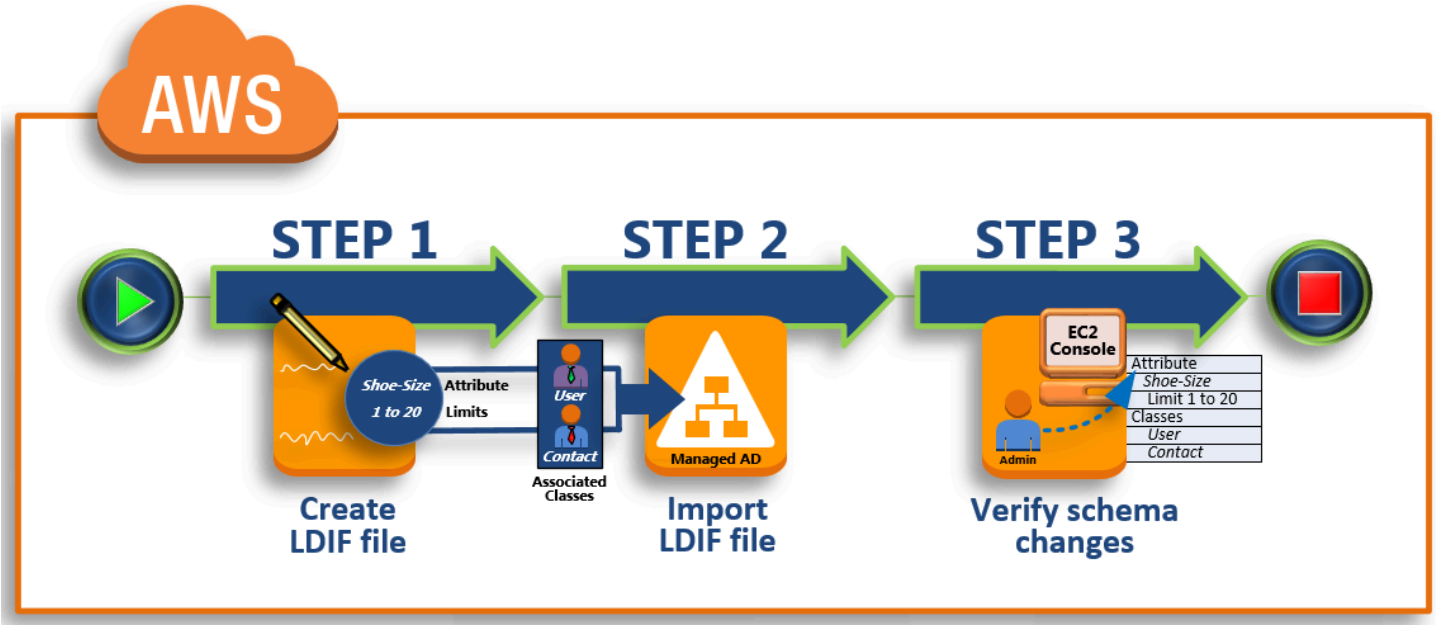
Tutorial: estensione dello schema AWS Managed Microsoft AD

In questo tutorial, imparerai come estendere lo schema della tua AWS directory Directory Service for Microsoft Active Directory, nota anche come AWS Managed Microsoft AD, aggiungendo attributi e classi univoci che soddisfano i tuoi requisiti specifici. AWSLe estensioni dello schema Microsoft AD gestite possono essere caricate e applicate solo utilizzando un file di script LDIF (Lightweight Directory Interchange Format) valido.

Gli attributi (attributeSchema) definiscono i campi nel database mentre le classi (classSchema) definiscono le tabelle nel database. Ad esempio, tutti gli oggetti utente in Active Directory sono definiti dalla classe di schema user, mentre le singole proprietà di un utente, come l'indirizzo e-mail o il numero di telefono, sono definite da un attributo.

Se desideri aggiungere una nuova proprietà, ad esempio Dimensione-piede, dovrai definire un nuovo attributo, che sarebbe di tipo integer. Puoi anche definire limiti superiore e inferiore, ad esempio da 1 a 20. Una volta creato l'oggetto attributeSchema Dimensione-piede, devi modificare l'oggetto classSchema utente per contenere tale attributo. Gli attributi possono essere collegati a più classi. Ad esempio, Dimensione-piede può anche essere aggiunto alla classe contatto. Per ulteriori informazioni sugli schemi Active Directory, consulta Quando estendere lo schema AWS Managed Microsoft AD.

Questo flusso di lavoro ha tre fasi di base.



Fase 1: creazione del file LDIF

In primo luogo, devi creare un file LDIF e definire i nuovi attributi e le classi a cui gli attributi devono essere aggiunti. Puoi usare questo file per la prossima fase del flusso di lavoro.

Fase 2: importazione del file LDIF

In questo passaggio, si utilizza la AWS Directory Service console per importare il file LDIF nell'ambiente Microsoft Active Directory.

Fase 3: verifica della corretta esecuzione dell'estensione dello schema

Infine, in qualità di amministratore, si utilizza un' EC2 istanza per verificare che le nuove estensioni vengano visualizzate nello snap-in dello schema di Active Directory.

Fase 1: creazione del file LDIF

Un file LDIF è un formato standard per lo scambio di dati in testo semplice per rappresentare il contenuto della directory LDAP (Lightweight Directory Access Protocol) e le richieste di aggiornamento. LDIF trasmette il contenuto della directory come un insieme di record, un record per ogni oggetto (o voce). Rappresenta anche le richieste di aggiornamento, come Add (Aggiungi), Modify (Modifica), Delete (Elimina) e Rename (Rinomina), come insieme di record, un record per ogni richiesta di aggiornamento.

AWS Directory ServiceImporta il file LDIF con le modifiche dello schema eseguendo l'`ldifde.exe`applicazione nella directory Managed AWS Microsoft AD. Pertanto, sarà utile comprendere la sintassi dello script LDIF. Per ulteriori informazioni, consulta la sezione relativa alle LDIF Scripts.

Diversi strumenti LDIF di terze parti possono estrarre, ripulire e aggiornare gli aggiornamenti dello schema. Indipendentemente dallo strumento che utilizzi, è importante capire che tutti gli identificatori utilizzati nel file LDIF devono essere unici.

Consigliamo vivamente di rivedere i seguenti concetti e suggerimenti prima di creare il file LDIF.

- Elementi dello schema: scopri gli elementi dello schema come attributi, classi IDs, oggetti e attributi collegati. Per ulteriori informazioni, consulta Elementi dello schema.

- Sequenza di elementi: assicurati che l'ordine in cui sono disposti gli elementi nel file LDIF segua il Directory Information Tree (DIT) dall'alto verso il basso. Le regole generali per il sequenziamento in un file LDIF includono quanto segue:

  - Separare gli elementi con una riga vuota.
  - Elencare gli elementi figlio dopo i loro elementi padre.
  - Verificare che gli elementi, come attributi o classi di oggetti, esistano nello schema. Se non sono presenti, devi aggiungerli allo schema prima che possa essere utilizzato. Ad esempio, prima di poter assegnare un attributo a una classe, l'attributo deve essere creato.
- Formato del DN: per ogni nuova istruzione nel file LDIF, definisci il nome distinto (DN) come prima riga dell'istruzione. Il DN identifica un oggetto Active Directory all'interno dell'albero dell'oggetto Active Directory e deve contenere i componenti del dominio per la directory. Ad esempio, i componenti del dominio per la directory in questo tutorial sono `DC=example,DC=com`.

  Il DN deve includere il nome comune (CN) dell'oggetto Active Directory. La prima voce CN rappresenta l'attributo o il nome della classe. Per estendere lo schema di Active Directory, utilizzare`CN=Schema,CN=Configuration`. Ricorda che non puoi modificare il contenuto degli oggetti Active Directory. Segue il formato DN generale.

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  Per questo tutorial, il DN per il nuovo attributo Dimensione-piede sarà simile a:

  ```
  dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
  ```
- Avvisi: esamina gli avvisi di seguito prima di estendere lo schema.
  - Prima di estendere lo schema Active Directory, è importante esaminare gli avvisi di Microsoft sull'impatto di questa operazione. Per ulteriori informazioni, consulta What You Must Know Before Extending the Schema (Che cosa sapere prima di estendere lo schema).
  - Non puoi eliminare un attributo o una classe dello schema. Pertanto, se si commette un errore e non si desidera eseguire il ripristino dal backup, è possibile solo disabilitare l'oggetto. Per ulteriori informazioni, consulta Disabling Existing Classes and Attributes (Disabilitazione degli attributi e delle classi esistenti).
  - Le modifiche a non defaultSecurityDescriptor sono supportate.

Per ulteriori informazioni su come vengono costruiti i file LDIF e vedere un file LDIF di esempio che può essere utilizzato per testare le estensioni dello schema di AWS Microsoft AD gestito, consulta l'articolo How to Extension your Managed AWS Microsoft AD Directory Schema sul Security Blog. AWS

Fase successiva

Fase 2: importazione del file LDIF

Fase 2: importazione del file LDIF

È possibile estendere lo schema importando un file LDIF dalla AWS Directory Service console o utilizzando l'API. Per ulteriori informazioni su come eseguire questa operazione con l'estensione dello schema APIs, consulta l'AWS Directory ServiceAPI Reference. Al momento, AWS non supporta applicazioni esterne, come Microsoft Exchange, per eseguire direttamente gli aggiornamenti dello schema.

> **Important**
>
> Quando si effettua un aggiornamento allo schema della directory AWS Managed Microsoft AD, l'operazione non è reversibile. In altre parole, una volta creata una nuova classe o attributo, Active Directory non consente di rimuoverla. Tuttavia, è possibile effettuarne la disabilitazione.
> Se devi eliminare le modifiche allo schema, un'opzione è il ripristino della directory da una snapshot precedente. Il ripristino di una snapshot riporta lo schema e i dati della directory a un punto precedente, non riguarda solo lo schema. Nota, l'età massima supportata di uno snapshot è di 180 giorni. Per ulteriori informazioni, consulta Useful shelf life of a system-state backup of Active Directory nel sito Web Microsoft.

Prima dell'inizio del processo di aggiornamento, AWS Managed Microsoft AD scatta un'istantanea per preservare lo stato corrente della directory.

> **Note**
>
> Le estensioni dello schema sono una funzionalità globale di AWS Managed Microsoft AD. Se utilizzi Configurazione della replica multiarea per Managed AWS Microsoft AD, è necessario eseguire le seguenti procedure in Regione principale. Le modifiche verranno applicate automaticamente in tutte le Regioni replicate. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per importare il file LDIF

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Manutenzione. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Manutenzione.
4. Nella sezione Schema extensions (Estensioni dello schema), seleziona Actions (Azioni), quindi scegli Upload and update schema (Carica e aggiorna schema).
5. Nella finestra di dialogo, fai clic su Browse (Cerca), seleziona un file LDIF valido, digita una descrizione e quindi scegli Update Schema (Aggiorna schema).

> **Important**
>
> Estendere lo schema è un'operazione critica. Non applicate alcun aggiornamento dello schema nell'ambiente di produzione senza prima averlo testato con l'applicazione in un ambiente di sviluppo o di test.

Come si applica il file LDIF

Dopo il caricamento del file LDIF, Managed AWS Microsoft AD adotta misure per proteggere la directory dagli errori in quanto applica le modifiche nell'ordine seguente.

1. Convalida il file LDIF. Poiché gli script LDIF possono manipolare qualsiasi oggetto nel dominio, Managed AWS Microsoft AD esegue controlli subito dopo il caricamento per garantire che l'operazione di importazione non abbia esito negativo. Questi includono anche controlli per garantire quanto segue:
   - Gli oggetti da aggiornare sono conservati solo nel container dello schema
   - La parte DC (controller dei domini) corrisponde al nome del dominio in cui è in esecuzione lo script LDIF
2. Acquisisce una snapshot della directory. Puoi usare la snapshot per ripristinare la directory in caso di problemi con l'applicazione dopo aver aggiornato lo schema.

3. Applica le modifiche a un singolo DC. AWSMicrosoft AD gestito isola uno dei tuoi DCs e applica gli aggiornamenti nel file LDIF al controller di dominio isolato. Quindi seleziona uno dei tuoi DCs schemi come schema principale, rimuove il controller di dominio dalla replica delle directory e applica il file LDIF utilizzando. `Ldifde.exe`
4. La replica avviene per tutti. DCs AWSMicrosoft AD gestito aggiunge nuovamente il DC isolato alla replica per completare l'aggiornamento. Mentre ciò accade, la directory continua a fornire senza interruzioni il servizio Active Directory alle applicazioni.

Approfondimenti

Fase 3: verifica della corretta esecuzione dell'estensione dello schema

Fase 3: verifica della corretta esecuzione dell'estensione dello schema

Dopo aver completato il processo di importazione, è importante verificare che gli aggiornamenti dello schema siano stati applicati alla directory. Questo è particolarmente importante prima di migrare o aggiornare qualsiasi applicazione che si basa sull'aggiornamento dello schema. Puoi farlo utilizzando una serie di strumenti LDAP o scrivendo uno strumento di test che emette i comandi LDAP appropriati.

Questa procedura utilizza lo snap-in dello schema di Active Directory and/or PowerShell per verificare che gli aggiornamenti dello schema siano stati applicati. È necessario eseguire questi strumenti da un computer che fa parte del dominio appartenente al proprio AWS Managed Microsoft AD. Può trattarsi di un server Windows in esecuzione nella rete locale con accesso al cloud privato virtuale (VPC) o tramite una connessione VPN (Virtual Private Network). Puoi anche eseguire questi strumenti su un'istanza Amazon EC2 Windows (vedi Come avviare una nuova EC2 istanza con un'unione di dominio senza interruzioni).

Per verificare tramite lo snap-in Active Directory Schema (Schema Active Directory)

1. Installa lo schema Snap-In di Active Directory seguendo le istruzioni sul TechNetsito Web.
2. Apri Microsoft Management Console (MMC) ed espandi l'albero AD Schema (Schema AD) per la directory.
3. Esplora le cartelle Classes (Classi) e Attributes (Attributi) fino a trovare le modifiche dello schema apportate in precedenza.

Per verificare utilizzando PowerShell

1. Aprire una PowerShell finestra.
2. Utilizza il cmdlet `Get-ADObject` come mostrato di seguito per verificare la modifica dello schema. Esempio:

   ```
   get-adobject -Identity 'CN=Shoe-
   Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
   ```

Fase facoltativa

Aggiungere un valore al nuovo attributo - Facoltativo

Aggiungere un valore al nuovo attributo - Facoltativo

Utilizza questo passaggio facoltativo quando hai creato un nuovo attributo e desideri aggiungere un nuovo valore all'attributo nella directory AWS Managed Microsoft AD.

Per aggiungere un valore a un attributo

1. Apri l'utilità della riga di PowerShell comando e imposta il nuovo attributo con il comando seguente. In questo esempio, aggiungeremo un nuovo valore EC2 InstanceID all'attributo per un computer specifico.

   ```
   PS C:\> set-adcomputer -Identity computer name -add @{example-
   EC2InstanceID = 'EC2 instance ID'}
   ```
2. È possibile verificare se il valore EC2 InstanceID è stato aggiunto all'oggetto computer eseguendo il comando seguente:

   ```
   PS C:\> get-adcomputer -Identity computer name –Property example-
   EC2InstanceID
   ```

Risorse correlate

I seguenti collegamenti alle risorse si trovano sul sito Web di Microsoft e forniscono informazioni correlate.

- Extending the Schema (Windows) (Estensione dello schema (Windows))

- Active Directory Schema (Windows) (Schema Active Directory (Windows))
- Active Directory Schema (Schema Active Directory)
- Amministrazione di Windows: Estensione dello schema di Active Directory
- Restrictions on Schema Extension (Windows) (Restrizioni sull'estensione dello schema (Windows))
- Ldifde

Modi per aggiungere un' EC2 istanza Amazon al tuo AWS Managed Microsoft AD

Puoi aggiungere facilmente un' EC2 istanza Amazon al tuo dominio Active Directory all'avvio dell'istanza. Per ulteriori informazioni, consulta Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory. Puoi anche avviare un' EC2 istanza e aggiungerla a un dominio Active Directory direttamente dalla Directory Service console con AWS Systems ManagerAutomation.

Se devi aggiungere manualmente un' EC2 istanza al tuo dominio Active Directory, devi avviare l'istanza nella regione e nel gruppo di sicurezza o nella sottorete appropriati, quindi aggiungere l'istanza al dominio.

Per essere in grado di connettersi in remoto a queste istanze, è necessario disporre di connettività IP per le istanze dalla rete da cui ti connetti. Nella maggior parte dei casi, questo richiede che un gateway Internet sia associato al VPC e che l'istanza disponga di un indirizzo IP pubblico.

Argomenti

- Avvio di un'istanza di amministrazione delle directory in AWS Managed Microsoft AD Active Directory
- Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory
- Unire un'istanza Amazon EC2 Linux alla tua directory AWS gestita di Microsoft AD Active Directory
- Unire un'istanza Amazon EC2 Mac alla tua directory AWS gestita di Microsoft AD Active Directory
- Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD
- Creazione o modifica di un set di opzioni DHCP per AWS Managed Microsoft AD

Avvio di un'istanza di amministrazione delle directory in AWS Managed Microsoft AD Active Directory

Questa procedura avvia un'Windowsistanza di amministrazione EC2 delle directory Amazon nell'Console di gestione AWSutilizzo di AWS Systems Manager Automation per gestire le directory. Puoi farlo anche eseguendo l'automazione AWS-Create DSManagement Instance direttamente nella console di automazione. AWS Systems Manager

Per ulteriori informazioni, consulta i collegamenti seguenti:

- Semplificazione dell'unione di domini Active Directory con AWS Systems Manager
- In che modo posso AWS Systems Manager aggiungere un' EC2 Windowsistanza in esecuzione al mio dominio? Directory Service

Prerequisiti

Per completare questo tutorial sono necessari i seguenti prerequisiti:

- Dovrai configurare. AWS Systems Manager Per ulteriori informazioni, consulta ConfigurazioneAWS Systems Manager.
- Avrai bisogno di un ruolo di profilo dell'istanza IAM che consenta Systems Manager e AWS Managed Microsoft AD.
  - Per ulteriori informazioni su Systems Manager, vedere Configurazione delle autorizzazioni di istanza richieste per Systems Manager.
  - Il ruolo dell'istanza IAM richiede le seguenti policy AWS gestite in modo che l'Windowsistanza di amministrazione delle EC2 directory possa aggiungere il dominio al tuo AWS Managed Microsoft AD:
    - **`AmazonSSMManagedInstanceCore`**
    - **`AmazonSSMDirectoryServiceAccess`**
- Il VPC connesso a Managed AWS Microsoft AD deve consentire l'accesso agli endpoint pubbliciDirectory Service. Per ulteriori informazioni, consulta Prerequisiti per la creazione di un AWS Managed Microsoft AD.
- Devi avere le seguenti autorizzazioni abilitate nel tuo account per avviare un' EC2 istanza di amministrazione delle directory dalla console:
  - `ds:DescribeDirectories`

- ec2:AuthorizeSecurityGroupIngress
- ec2:CreateSecurityGroup
- ec2:CreateTags
- ec2:DeleteSecurityGroup
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeKeyPairs
- ec2:DescribeSecurityGroups
- ec2:DescribeVpcs
- ec2:RunInstances
- ec2:TerminateInstances
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeInstanceInformation

- `ssm:GetAutomationExecution`
- `ssm:GetParameters`
- `ssm:ListCommandInvocations`
- `ssm:ListCommands`
- `ssm:ListDocuments`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`
- `ssm:GetDocument`

Avvio di un' EC2 istanza di amministrazione delle directory in Console di gestione AWS

1. Accedi alla console Directory Service.
2. In Active Directory, scegli Directory.
3. Scegliete l'ID della directory in cui desiderate avviare un' EC2 istanza di amministrazione delle directory.
4. Nella pagina della directory, nell'angolo in alto a destra, scegli Operazioni.
5. Nell'elenco a discesa Azioni, scegli Launch directory administration EC2 instance.
6. Nella pagina Launch Directory Administration EC2 Instance, in Parametri di input, completa i campi.

    a. (Facoltativo) È possibile fornire una key pair per l'istanza. Dall'elenco a discesa Key Pair Name, opzionale, seleziona una coppia di chiavi.

    b. (Facoltativo) Scegli AWS CLIil comando Visualizza per vedere un esempio che utilizzi AWS CLI per eseguire questa automazione.
7. Seleziona Invia.
8. Viene eseguito il reindirizzamento alla pagina della directory. Nella parte superiore dello schermo viene visualizzata una flashbar verde per indicare che l'avvio è stato iniziato con successo.

Visualizzazione dell' EC2istanza di amministrazione delle directory

Se non è stata avviata alcuna EC2 istanza per una directory, viene visualizzato un trattino (-) in Istanza di amministrazione EC2 della directory.

1. In Active Directory, scegli Directory e seleziona la directory che desideri visualizzare.

2. In Dettagli della directory, in EC2 Istanza di amministrazione della directory, scegli una o tutte le istanze da visualizzare.
3. Quando scegli un'istanza, vieni indirizzato alla pagina EC2 Connetti all'istanza per connettere un desktop remoto all'istanza.

Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory

Puoi avviare e aggiungere un' EC2 Windowsistanza Amazon a un AWS Managed Microsoft AD. In alternativa, puoi aggiungere manualmente un' EC2 Windowsistanza esistente a un AWS Managed Microsoft AD.

Seamlessly join EC2 Windows instance

Questa procedura unisce senza problemi un' EC2 Windowsistanza Amazon al tuo Managed AWS Microsoft AD. Se devi eseguire un'unione di dominio senza interruzioni su più Account AWS domini, consulta. Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2 Per ulteriori informazioni su Amazon EC2, consulta What is Amazon EC2? .

Prerequisiti

Per aggiungere facilmente un dominio a un' EC2 istanza, dovrai completare quanto segue:

- Avere un Microsoft AD AWS gestito. Per ulteriori informazioni, consulta Creazione del tuo AWS Managed Microsoft AD.
- Avrai bisogno delle seguenti autorizzazioni IAM per unirti senza problemi a un' EC2Windowsistanza:
  - Profilo di istanza IAM con le seguenti autorizzazioni IAM:
    - `AmazonSSMManagedInstanceCore`
    - `AmazonSSMDirectoryServiceAccess`
  - Il dominio utente che si unisce perfettamente EC2 a AWS Managed Microsoft AD necessita delle seguenti autorizzazioni IAM:
    - Directory ServiceAutorizzazioni:
      - `"ds:DescribeDirectories"`
      - `"ds:CreateComputer"`

- Autorizzazioni Amazon VPC:
  - `"ec2:DescribeVpcs"`
  - `"ec2:DescribeSubnets"`
  - `"ec2:DescribeNetworkInterfaces"`
  - `"ec2:CreateNetworkInterface"`
  - `"ec2:AttachNetworkInterface"`
- EC2 Autorizzazioni:
  - `"ec2:DescribeInstances"`
  - `"ec2:DescribeImages"`
  - `"ec2:DescribeInstanceTypes"`
  - `"ec2:RunInstances"`
  - `"ec2:CreateTags"`
- AWS Systems ManagerAutorizzazioni:
  - `"ssm:DescribeInstanceInformation"`
  - `"ssm:SendCommand"`
  - `"ssm:GetCommandInvocation"`
  - `"ssm:CreateBatchAssociation"`

Quando viene creato AWS Managed Microsoft AD, viene creato un gruppo di sicurezza con regole in entrata e in uscita. Per ulteriori informazioni su queste regole e porte, consulta. Cosa viene creato con AWS Managed Microsoft AD Per aggiungere facilmente un dominio a un' EC2 Windowsistanza, il VPC su cui stai lanciando l'istanza deve consentire le stesse porte consentite nelle regole in entrata e in uscita del gruppo di sicurezza Microsoft AD AWS gestito.

- A seconda della sicurezza di rete e delle impostazioni del firewall, potrebbe esserti richiesto di consentire traffico in uscita aggiuntivo. Questo traffico sarebbe destinato a HTTPS (porta 443) verso i seguenti endpoint:

Endpoint	Ruolo
`ec2messages. region .amazonaws.com`	Crea ed elimina i canali di sessione con il servizio Session Manager. Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ssm. region .amazonaws.com`	Endpoint per. AWS Systems Manager Session Manager Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ssmmessages. region .amazonaws.com`	Crea ed elimina i canali di sessione con il servizio Session Manager. Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ds. region .amazonaws.com`	Endpoint per. Directory Service Per ulteriori informazioni, consulta Disponibilità regionale per Directory Service.

- Si consiglia di utilizzare un server DNS che risolva il nome di dominio Microsoft AD AWS gestito. A tale scopo, è possibile creare un set di opzioni DHCP. Per ulteriori informazioni, consulta Creazione o modifica di un set di opzioni DHCP per AWS Managed Microsoft AD.
  - Se scegli di non creare un set di opzioni DHCP, i tuoi server DNS saranno statici e configurati dal tuo Managed AWS Microsoft AD.

Per unirti senza problemi a un'istanza Amazon EC2 Windows

1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nella EC2 Dashboard, nella sezione Launch instance, scegli Launch instance.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per l' EC2 istanza di Windows.

5. (Facoltativo) Scegli Aggiungi tag aggiuntivi per aggiungere una o più coppie chiave-valore di tag per organizzare, tracciare o controllare l'accesso per questa EC2 istanza.
6. Nella sezione Applicazione e immagine del sistema operativo (Amazon Machine Image), scegli Windows nel riquadro Guida rapida. Puoi modificare l'Amazon Machine Image (AMI) di Windows dall'elenco a discesa Amazon Machine Image (AMI).
7. Nella sezione Tipo di istanza, scegli il tipo di istanza che desideri utilizzare dall'elenco a discesa Tipo di istanza.
8. Nella sezione Coppia di chiavi (accesso), puoi scegliere se creare una nuova coppia di chiavi o selezionare una coppia di chiavi esistente.

   a. Per creare una nuova coppia di chiavi, scegli Crea nuova coppia di chiavi.

   b. Inserisci un nome per la coppia di chiavi e seleziona un'opzione per il Tipo di coppia di chiavi e il Formato del file della chiave privata.

   c. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegli .pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegli .ppk.

   d. Scegli crea coppia di chiavi.

   e. Il file della chiave privata viene automaticamente scaricato dal browser. Salvare il file della chiave privata in un luogo sicuro.

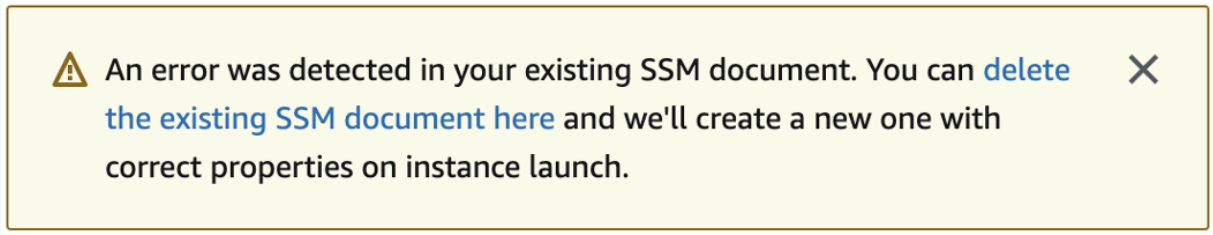
   > **Important**
   >
   > Questo è l'unico momento in cui salvare il file della chiave privata.

9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto il traffico esterno instradato a un gateway Internet. In caso contrario, non potrai connetterti in remoto all'istanza.

    Per ulteriori informazioni su come connettersi a un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.
11. In Assegna automaticamente IP pubblico, scegli Abilita.

Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta l'indirizzo IP delle EC2 istanze Amazon nella Amazon EC2 User Guide.

12. Nelle impostazioni Firewall (gruppi di sicurezza), puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
13. Nelle impostazioni Configurazione dell'archiviazione, puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
14. Seleziona la sezione Dettagli avanzati, scegli il tuo dominio dall'elenco a discesa Directory di aggiunta al dominio.

> **Note**
>
> Dopo aver scelto la directory di accesso al dominio, potresti vedere:
>
> 
>
>
> Questo errore si verifica se la procedura guidata di EC2 avvio identifica un documento SSM esistente con proprietà impreviste. Puoi effettuare una delle seguenti operazioni:
>
> - Se hai già modificato il documento SSM e le proprietà sono previste, scegli chiudi e procedi all'avvio dell' EC2 istanza senza modifiche.
> - Seleziona qui il link Elimina il documento SSM esistente per eliminare il documento SSM. Ciò consentirà la creazione di un documento SSM con le proprietà corrette. Il documento SSM verrà creato automaticamente all'avvio dell' EC2 istanza.

15. In Profilo dell'istanza IAM, puoi selezionare un profilo dell'istanza IAM esistente o crearne uno nuovo. Seleziona un profilo di istanza IAM a cui sono SSMDirectory ServiceAccess associate le policy AWS gestite Amazon SSMManaged InstanceCore e Amazon dall'elenco a discesa del profilo dell'istanza IAM. Per crearne uno nuovo, scegli il link Crea nuovo profilo IAM, quindi procedi come segue:

    1. Scegli Crea ruolo.
    2. In Seleziona entità attendibile, scegli Servizio AWS.

3. In Use case (Caso d'uso), scegli EC2.
4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le SSMDirectory ServiceAccess politiche di Amazon SSMManaged InstanceCore e Amazon. Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Scegli Next (Successivo).

   > **Note**
   >
   > Amazon SSMDirectory ServiceAccess fornisce le autorizzazioni per unire le istanze a un Active Directory gestito da. Directory Service Amazon SSMManaged InstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il AWS Systems Manager servizio. Per ulteriori informazioni sulla creazione di un ruolo con queste autorizzazioni e per informazioni su altre autorizzazioni e policy che puoi assegnare al tuo ruolo IAM, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager.

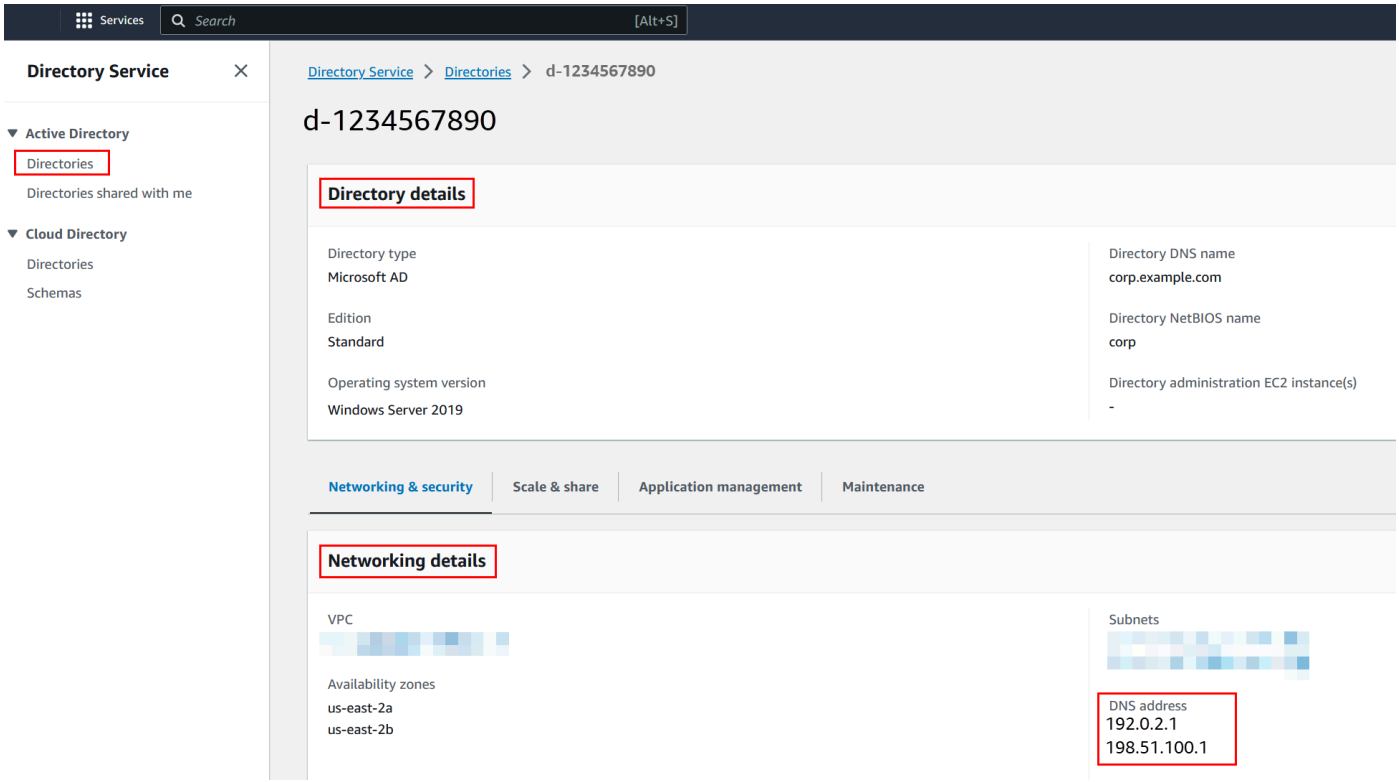
5. Nella pagina Denomina, rivedi e crea inserisci un Nome ruolo. Avrai bisogno di questo nome di ruolo da associare all' EC2istanza.
6. (Facoltativo) Puoi fornire una descrizione del profilo dell'istanza IAM nel campo Descrizione.
7. Scegli Crea ruolo.
8. Torna alla pagina Avvia un'istanza e scegli l'icona di aggiornamento accanto al profilo dell'istanza IAM. Il tuo nuovo profilo dell'istanza IAM dovrebbe essere visibile nell'elenco a discesa Profilo dell'istanza IAM. Scegli il nuovo profilo e lascia il resto delle impostazioni con i valori predefiniti.

16. Scegliere Launch Instance (Avvia istanza).

Manually join EC2 Windows instance

Per aggiungere manualmente un' EC2 Windowsistanza Amazon esistente a una AWS Managed Microsoft AD Active Directory, l'istanza deve essere avviata utilizzando i parametri specificati inUnire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory.

Avrai bisogno degli indirizzi IP dei server AWS Managed Microsoft AD DNS. Queste informazioni sono disponibili nelle sezioni Servizi di directory > Directory > ID directory relativo alla directory > Dettagli della directory e Rete e sicurezza.



Per aggiungere un'istanza di Windows a un Active Directory Microsoft AD AWS gestito

1. Connettiti all'istanza utilizzando qualsiasi client Remote Desktop Protocol.
2. Aprire la finestra di dialogo TCP/ IPv4 properties sull'istanza.

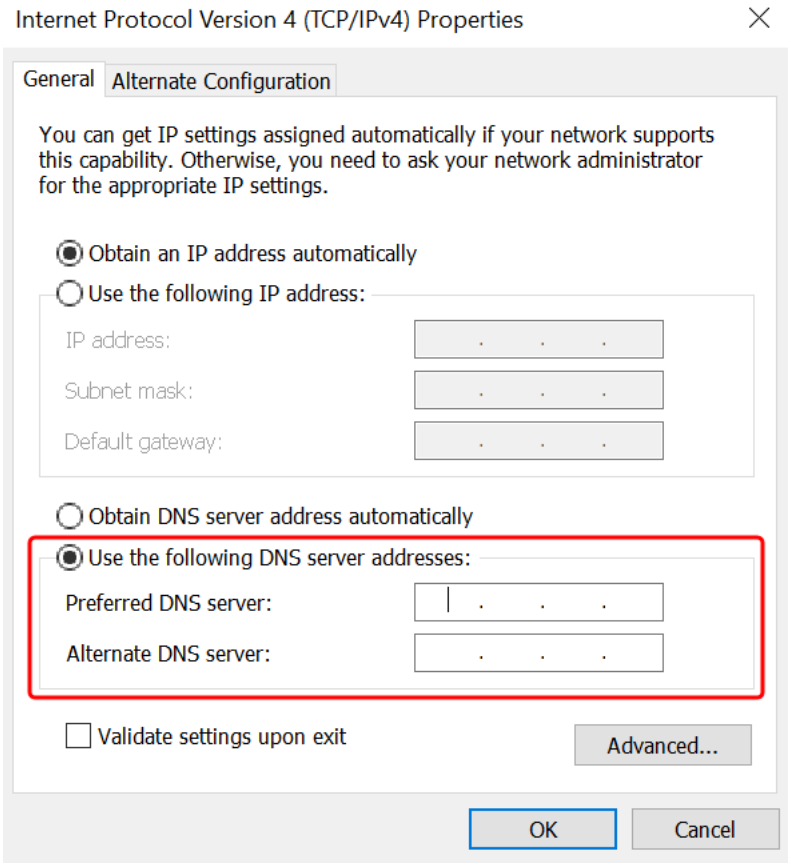
    a. Apri Network Connections (Connessioni di rete).

    > **Tip**
    >
    > Puoi aprire le Network Connections (Connessioni di rete) direttamente eseguendo quanto segue da un prompt del comando sull'istanza.
    >
    > ```
    > %SystemRoot%\system32\control.exe ncpa.cpl
    > ```

    b. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per qualsiasi connessione di rete abilitata e scegli Properties (Proprietà).

    c. Nella finestra di dialogo delle proprietà di connessione, apri (doppio clic) Internet Protocol Version 4 (Protocollo Internet versione 4).

3. Seleziona Usa i seguenti indirizzi di server DNS, modifica gli indirizzi del server DNS preferito e del server DNS alternativo con gli indirizzi IP dei server DNS gestiti forniti da AWS Microsoft AD e scegli OK.



4. Apri la finestra di dialogo System Properties (Proprietà del sistema) per l'istanza, seleziona la scheda Computer Name (Nome computer) e scegli Change (Modifica).

> **Tip**
>
> Puoi aprire la finestra di dialogo System Properties (Proprietà di sistema) direttamente eseguendo quanto segue da un prompt del comando sull'istanza.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Nel campo Membro di, seleziona Dominio, inserisci il nome completo del tuo AWS Managed Microsoft AD Active Directory e scegli OK.
6. Quando viene richiesto di specificare il nome e la password per l'amministratore del dominio, immetti il nome utente e la password di un account che dispone di privilegi di aggiunta di

dominio. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

> **Note**
>
> È possibile immettere il nome completo del dominio o il nome NetBIOS, seguito da una barra rovesciata (\) e quindi dal nome utente. Il nome utente sarebbe Admin. Ad esempio **`corp.example.com\admin`** o **`corp\admin`**.

7. Dopo aver ricevuto il messaggio che ti invita al dominio, riavvia l'istanza perché le modifiche diventino effettive.

Ora che l'istanza è stata aggiunta al dominio AWS gestito di Microsoft AD Active Directory, puoi accedere a quell'istanza in remoto e installare le utilità per gestire la directory, ad esempio aggiungere utenti e gruppi. Gli strumenti di amministrazione di Active Directory possono essere utilizzati per creare utenti e gruppi. Per ulteriori informazioni, consulta Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.

> **Note**
>
> Puoi anche utilizzare Amazon Route 53 per elaborare le query DNS anziché modificare manualmente gli indirizzi DNS sulle tue istanze Amazon. EC2 Per ulteriori informazioni, consulta Integrazione della risoluzione DNS del servizio di directory Amazon Route 53 Resolver e inoltro delle query DNS in uscita alla rete.

Unire un'istanza Amazon EC2 Linux alla tua directory AWS gestita di Microsoft AD Active Directory

Puoi avviare e aggiungere un'istanza EC2 Linux al tuo AWS Managed Microsoft AD inConsole di gestione AWS. Puoi anche aggiungere manualmente un'istanza EC2 Linux al tuo AWS Managed Microsoft AD. È inoltre possibile utilizzare strumenti come Winbind per aggiungere un dominio a un'istanza EC2 Linux al proprio Managed AWS Microsoft AD.

Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0

- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le distribuzioni precedenti a Ubuntu 14 e Red Hat Enterprise Linux 7 e 8 non supportano la funzionalità seamless domain join.

Modi per aggiungere un dominio a un'istanza EC2 Linux:

- Unire senza problemi un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory
- Unire senza problemi un'istanza Amazon EC2 Linux a un AWS Managed Microsoft AD condiviso
- Aggiungere manualmente un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory
- Aggiungere manualmente un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory utilizzando Winbind

Unire senza problemi un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory

Questa procedura unisce senza problemi un'istanza Amazon EC2 Linux alla tua directory gestita di AWS Microsoft AD Active Directory. Per completare questa procedura, dovrai creare un Gestione dei segreti AWS segreto che può comportare costi aggiuntivi. Per ulteriori informazioni, consultare Gestione dei segreti AWSPrezzi.

Se è necessario eseguire un'unione di dominio senza interruzioni su più AWS account, è possibile scegliere facoltativamente di abilitare la condivisione della Directory.

Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64-bit x86)

- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le distribuzioni precedenti a Ubuntu 14 e Red Hat Enterprise Linux 7 e 8 non supportano la funzionalità seamless domain join.

Per una dimostrazione sul processo di collegamento senza problemi di un'istanza Linux al tuo Managed AWS Microsoft AD Active Directory, guarda il video seguente YouTube .

Partecipa EC2 alla demo del dominio AD senza interruzioni di Amazon per Linux

Prerequisiti

Prima di poter configurare l'aggiunta senza soluzione di continuità al dominio EC2 su un'istanza Linux, devi completare le procedure descritte in queste sezioni.

Prerequisiti di rete per un'unione fluida del dominio

Per aggiungere facilmente un dominio a un'istanza EC2 Linux, è necessario completare quanto segue:

- Avrai bisogno delle seguenti autorizzazioni IAM per unirti senza problemi a un' EC2istanza Linux:
  - Avere un Microsoft AD AWS gestito. Per ulteriori informazioni, consulta Creazione del tuo AWS Managed Microsoft AD.
  - Avrai bisogno delle seguenti autorizzazioni IAM per unirti senza problemi a un' EC2Windowsistanza:
    - Profilo di istanza IAM con le seguenti autorizzazioni IAM:
      - `AmazonSSMManagedInstanceCore`
      - `AmazonSSMDirectoryServiceAccess`
    - Il dominio utente che si unisce perfettamente EC2 a AWS Managed Microsoft AD necessita delle seguenti autorizzazioni IAM:
      - Directory ServiceAutorizzazioni:

        - `"ds:DescribeDirectories"`
        - `"ds:CreateComputer"`
    - Autorizzazioni Amazon VPC:
        - `"ec2:DescribeVpcs"`
        - `"ec2:DescribeSubnets"`
        - `"ec2:DescribeNetworkInterfaces"`
        - `"ec2:CreateNetworkInterface"`
        - `"ec2:AttachNetworkInterface"`
    - EC2 Autorizzazioni:
        - `"ec2:DescribeInstances"`
        - `"ec2:DescribeImages"`
        - `"ec2:DescribeInstanceTypes"`
        - `"ec2:RunInstances"`
        - `"ec2:CreateTags"`
    - AWS Systems ManagerAutorizzazioni:
        - `"ssm:DescribeInstanceInformation"`
        - `"ssm:SendCommand"`
        - `"ssm:GetCommandInvocation"`
        - `"ssm:CreateBatchAssociation"`
- Quando viene creato AWS Managed Microsoft AD, viene creato un gruppo di sicurezza con regole in entrata e in uscita. Per ulteriori informazioni su queste regole e porte, consulta. Cosa viene creato con AWS Managed Microsoft AD Per aggiungere facilmente un dominio a un'istanza EC2 Linux, il VPC su cui stai lanciando l'istanza deve consentire le stesse porte consentite nelle regole in entrata e in uscita del gruppo di sicurezza Microsoft AD AWS gestito.
    - A seconda della sicurezza di rete e delle impostazioni del firewall, potrebbe esserti richiesto di consentire traffico in uscita aggiuntivo. Questo traffico sarebbe destinato a HTTPS (porta 443) verso i seguenti endpoint:

Endpoint	Ruolo
`ec2messages.` *`region`*`.amazonaws.com`	Crea ed elimina i canali di sessione con il servizio Session Manager. Per ulteriori

Endpoint	Ruolo
	informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ssm.region.amazonaws.com`	Endpoint per. AWS Systems Manager Session Manager Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ssmmessages. region.amazonaws.com`	Crea ed elimina i canali di sessione con il servizio Session Manager. Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ds.region.amazonaws.com`	Endpoint per. Directory Service Per ulteriori informazioni, consulta Disponibilità regionale per Directory Service.
`secretsmanager. region.amazonaws.com`	Endpoint per. Gestione dei segreti AWS Per ulteriori informazioni, consulta Endpoint e quote per Gestione dei segreti AWS.

- Si consiglia di utilizzare un server DNS che risolva il nome di dominio Microsoft AD AWS gestito. A tale scopo, è possibile creare un set di opzioni DHCP. Per ulteriori informazioni, consulta Creazione o modifica di un set di opzioni DHCP per AWS Managed Microsoft AD.
  - Se scegli di non creare un set di opzioni DHCP, i tuoi server DNS saranno statici e configurati dal tuo Managed AWS Microsoft AD.

Selezione dell'account del servizio di aggiunta ottimizzata del dominio

Puoi aggiungere facilmente computer Linux al tuo dominio AWS gestito di Microsoft AD Active Directory. A tale scopo, è necessario utilizzare un account utente con le autorizzazioni per la creazione di account computer per aggiungere i computer al dominio. Sebbene gli amministratori delegati AWS o i membri di altri gruppi possano disporre di privilegi sufficienti per aggiungere computer al dominio, non è consigliabile utilizzarli. Come best practice, si consiglia di utilizzare un account del servizio con i privilegi minimi necessari per aggiungere i computer al dominio.

Per delegare un account con i privilegi minimi necessari per aggiungere i computer al dominio, puoi eseguire i seguenti comandi. PowerShell È necessario eseguire questi comandi da un computer Windows aggiunto al dominio su cui è installato Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD. Inoltre, è necessario utilizzare un account che disponga dell'autorizzazione a modificare le autorizzazioni sull'unità organizzativa o sul container del computer. Il PowerShell comando imposta le autorizzazioni che consentono all'account del servizio di creare oggetti informatici nel contenitore di computer predefinito del dominio.

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty
 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext
 -Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects
 in the Computers container.
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'CreateChild',
 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

Se preferisci utilizzare un'interfaccia utente grafica (GUI), puoi utilizzare il processo manuale descritto in Delegare privilegi all'account del servizio.

Creazione dei segreti per archiviare l'account del servizio di dominio

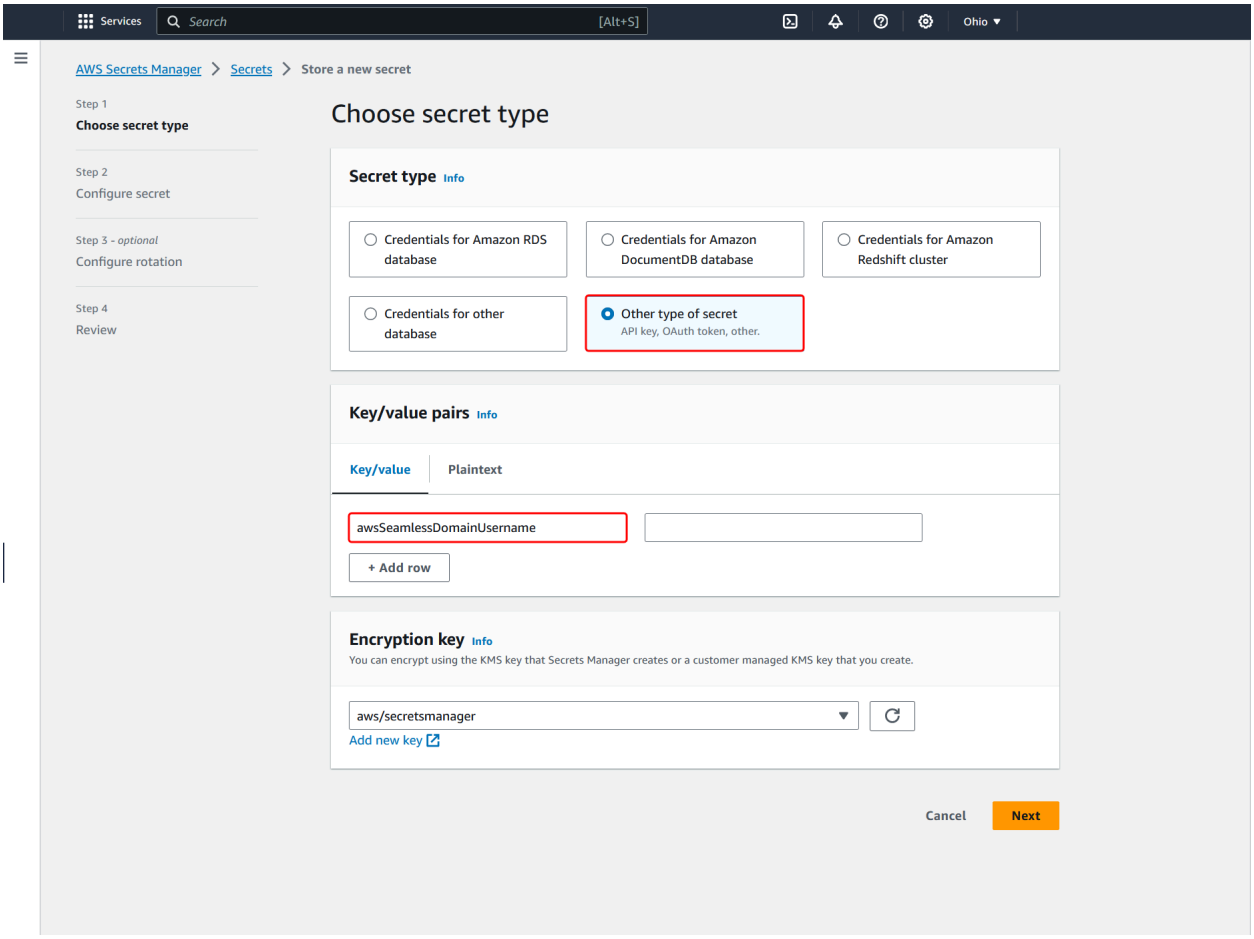
È possibile utilizzare Gestione dei segreti AWS per archiviare l'account del servizio di dominio. Per ulteriori informazioni, consulta Creare un Gestione dei segreti AWS segreto.

> **Note**
>
> Secrets Manager è a pagamento. Per ulteriori informazioni, consulta la sezione Prezzi nella Guida Gestione dei segreti AWS per l'utente.

Per creare segreti e archiviare le informazioni sull'account del servizio di dominio

1. Accedi a Console di gestione AWS e apri la Gestione dei segreti AWS console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Archivia un nuovo segreto, procedere nel seguente modo:
   a. In Tipo segreto, scegli Altro tipo di segreti.
   b. In Coppie chiave/valore, procedi come segue:
      i. Nella prima casella, inserisci **`awsSeamlessDomainUsername`**. Nella stessa riga, nella casella successiva, inserisci il nome utente per il tuo account di servizio. Ad esempio, se hai utilizzato il PowerShell comando in precedenza, il nome dell'account del servizio sarebbe**`awsSeamlessDomain`**.

      > **Note**
      >
      > Devi inserire **`awsSeamlessDomainUsername`** esattamente come è. Assicurati che non vi siano spazi iniziali o finali. In caso contrario, l'aggiunta del dominio avrà esito negativo.



ii. Scegli Aggiungi riga.

iii. Nella nuova riga, nella prima casella, inserisci **`awsSeamlessDomainPassword`**. Nella stessa riga, nella casella successiva, inserisci la password per il tuo account del servizio.

> **Note**
>
> Devi inserire **`awsSeamlessDomainPassword`** esattamente come è. Assicurati che non vi siano spazi iniziali o finali. In caso contrario, l'aggiunta del dominio avrà esito negativo.

iv. In Chiave di crittografia, lascia il valore predefinito`aws/secretsmanager`. Gestione dei segreti AWScrittografa sempre il segreto quando scegli questa opzione. Puoi anche scegliere una chiave creata da te.

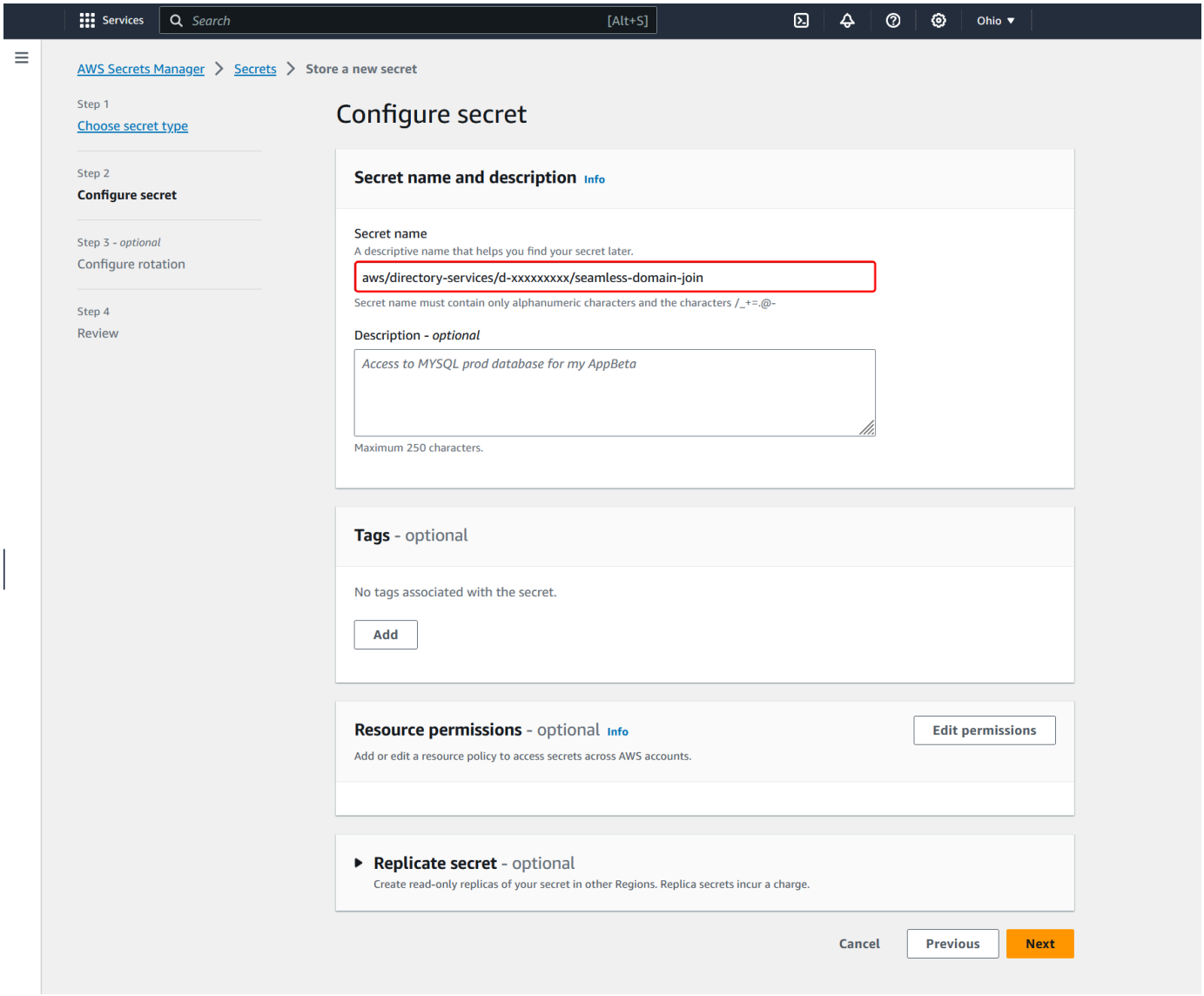
v. Scegli Next (Successivo).

4. In Nome segreto, inserisci un nome segreto che includa l'ID della tua directory utilizzando il seguente formato, sostituendolo *d-xxxxxxxxx* con il tuo ID di directory:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Questo nome viene utilizzato per recuperare i segreti nell'applicazione.

> **Note**
>
> Devi inserirlo **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** esattamente così com'è, ma sostituirlo *d-xxxxxxxxxx* con l'ID della tua directory. Assicurati che non vi siano spazi iniziali o finali. In caso contrario, l'aggiunta del dominio avrà esito negativo.



5. Lascia tutto il resto impostato sui valori predefiniti, quindi scegli Avanti.
6. In Configura rotazione automatica, lascia selezionata Disabilita rotazione automatica e scegli Successivo.

   Puoi attivare la rotazione di questo segreto dopo averlo archiviato.
7. Controlla le impostazioni, quindi scegli Archivia per salvare le modifiche. La console Secrets Manager restituisce l'elenco dei segreti nel tuo account con il nuovo segreto ora incluso nell'elenco.
8. Scegli il nome segreto appena creato dall'elenco e prendi nota del valore ARN segreto. Lo utilizzerai nella sezione successiva.

Attiva la rotazione per il segreto dell'account del servizio di dominio

Ti consigliamo di modificare regolarmente i segreti per migliorare il tuo livello di sicurezza.

Per attivare la rotazione per il segreto dell'account del servizio di dominio

- Segui le istruzioni riportate in Configurare la rotazione automatica per Gestione dei segreti AWS i segreti nella Guida per l'Gestione dei segreti AWSutente.

  Per il passaggio 5, utilizzare il modello di rotazione Microsoft Active Directory credenziali nella Guida per l'Gestione dei segreti AWSutente.

  Per assistenza, consulta Risoluzione dei problemi di Gestione dei segreti AWS rotazione nella Guida per l'Gestione dei segreti AWSutente.

Creazione della policy e del ruolo IAM richiesti

Utilizza i seguenti passaggi preliminari per creare una policy personalizzata che consenta l'accesso in sola lettura al tuo Secrets Manager seamless domain join secret (che hai creato in precedenza) e per creare un nuovo ruolo Linux IAM. EC2 DomainJoin

Creazione della policy di lettura IAM di Secrets Manager

Utilizzi la console IAM per creare una policy che conceda l'accesso in sola lettura al segreto di Secrets Manager.

Per creare la policy di lettura IAM di Secrets Manager

1. Accedi Console di gestione AWS come utente autorizzato a creare policy IAM. Quindi apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, Gestione degli accessi, scegli Politiche.
3. Scegli Crea policy.
4. Seleziona la scheda JSON e copia il testo dal documento della seguente policy JSON. Quindi incollalo nella casella di testo JSON.

> **Note**
>
> Assicurati di sostituire l'ARN della regione e della risorsa con la regione e l'ARN effettivi del segreto che hai creato in precedenza.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Quando hai terminato, seleziona Successivo. In Validatore di policy vengono segnalati eventuali errori di sintassi. Per ulteriori informazioni, consulta Convalida delle policy IAM.
6. Nella pagina Verifica policy, inserisci un nome per la policy, ad esempio **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Consulta la sezione Riepilogo per visualizzare le autorizzazioni concesse dalla policy. Seleziona Crea policy per salvare le modifiche. La nuova policy appare nell'elenco delle policy gestite ed è pronta a collegarsi a un'identità.

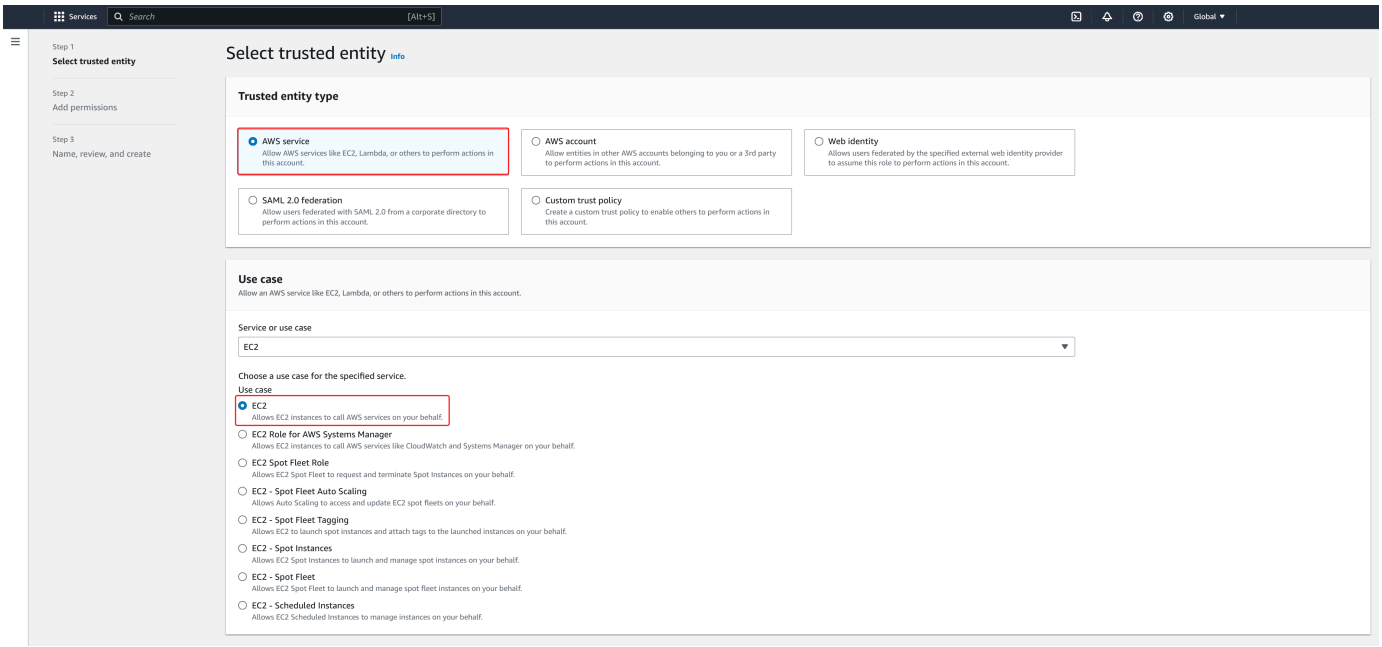
> **Note**
>
> Consigliamo di creare una policy per ogni segreto. In questo modo, ti assicuri che le istanze abbiano accesso solo al segreto in questione e riduci al minimo l'impatto se un'istanza viene compromessa.

Crea il ruolo Linux EC2 DomainJoin

Utilizzi la console IAM per creare il ruolo che utilizzerai per aggiungere il dominio alla tua EC2 istanza Linux.

Per creare il EC2 DomainJoin ruolo Linux

1. Accedi Console di gestione AWS come utente autorizzato a creare policy IAM. Quindi apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, in Gestione degli accessi, scegli Ruoli.
3. Nel riquadro del contenuto seleziona Crea ruolo.
4. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio).
5. In Caso d'uso, scegli EC2, quindi scegli Avanti.



6. In Filtra policy, procedi come segue:

   a. Specificare **`AmazonSSMManagedInstanceCore`**. Dopodiché, seleziona la casella di controllo per tale elemento nell'elenco.

   b. Specificare **`AmazonSSMDirectoryServiceAccess`**. Dopodiché, seleziona la casella di controllo per tale elemento nell'elenco.

   c. Inserisci **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (o il nome della policy creata nella procedura precedente). Dopodiché, seleziona la casella di controllo per tale elemento nell'elenco.

   d. Dopo aver aggiunto le tre politiche sopra elencate, seleziona Crea ruolo.

> **Note**
>
> Amazon SSMDirectory ServiceAccess fornisce le autorizzazioni per unire le istanze a un Active Directory gestito da. Directory Service Amazon SSMManaged InstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il AWS Systems Manager servizio. Per ulteriori informazioni sulla creazione di un ruolo con queste autorizzazioni e per informazioni su altre autorizzazioni e policy che puoi assegnare al tuo ruolo IAM, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager.

7. Inserisci un nome per il tuo nuovo ruolo, ad esempio **`LinuxEC2DomainJoin`** o un altro nome che preferisci nel campo Nome del ruolo.
8. (Facoltativo) Per Role Description (Descrizione ruolo), immetti una descrizione.
9. (Facoltativo) Scegli Aggiungi nuovo tag nel Passaggio 3: Aggiungi tag per aggiungere tag. Le coppie chiave-valore dei tag vengono utilizzate per organizzare, tracciare o controllare l'accesso per questo ruolo.
10. Scegli Crea ruolo.

Unisciti senza problemi alla tua istanza Linux

Per unirti senza problemi alla tua istanza Linux

1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal selettore della regione nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nella EC2 Dashboard, nella sezione Launch instance, scegli Launch instance.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua EC2 istanza Linux.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivi per aggiungere una o più coppie chiave-valore di tag per organizzare, tracciare o controllare l'accesso per questa EC2 istanza.
6. Nella sezione Applicazione e immagine del sistema operativo (Amazon Machine Image), scegli un'AMI Linux che desideri avviare.

> **Note**
>
> L'AMI utilizzato deve avere AWS Systems Manager (SSM Agent) la versione 2.3.1644.0 o successiva. Per verificare la versione dell'Agente SSM installata nell'AMI avviando un'istanza da quest'ultima, consulta Ottenere la versione dell'Agente SSM attualmente installata. Se è necessario aggiornare l'agente SSM, vedere Installazione e configurazione dell'agente SSM su istanze per Linux. EC2
> SSM utilizza il `aws:domainJoin` plug-in quando aggiunge un'istanza Linux a un dominio Active Directory. Il plugin cambia il nome host per le istanze Linux nel formato EC2 AMAZ-. *XXXXXXX* Per ulteriori informazioni in merito*`aws:domainJoin`*, consultate AWS Systems ManagerCommand Document Plugin reference nella Guida per l'AWS Systems Managerutente.

7. Nella sezione Tipo di istanza, scegli il tipo di istanza che desideri utilizzare dall'elenco a discesa Tipo di istanza.
8. Nella sezione Coppia di chiavi (accesso), puoi scegliere se creare una nuova coppia di chiavi o selezionare una coppia di chiavi esistente. Per creare una nuova coppia di chiavi, scegli Crea nuova coppia di chiavi. Inserisci un nome per la coppia di chiavi e seleziona un'opzione per il Tipo di coppia di chiavi e il Formato del file della chiave privata. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegli .pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegli .ppk. Scegli crea coppia di chiavi. Il file della chiave privata viene automaticamente scaricato dal browser. Salvare il file della chiave privata in un luogo sicuro.

> **Important**
>
> Questo è l'unico momento in cui salvare il file della chiave privata.

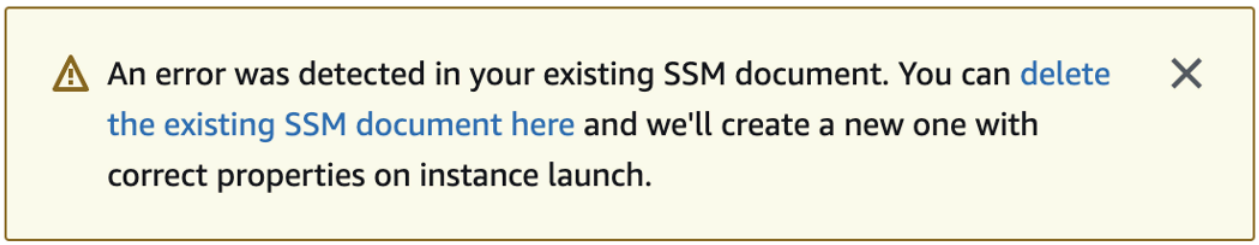
9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto il traffico esterno instradato a un gateway Internet. In caso contrario, non potrai connetterti in remoto all'istanza.

    Per ulteriori informazioni su come connettersi a un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.

11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta l'indirizzo IP delle EC2 istanze Amazon nella Amazon EC2 User Guide.

12. Nelle impostazioni Firewall (gruppi di sicurezza), puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
13. Nelle impostazioni Configurazione dell'archiviazione, puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
14. Seleziona la sezione Dettagli avanzati, scegli il tuo dominio dall'elenco a discesa Directory di aggiunta al dominio.

> **Note**
>
> Dopo aver scelto la directory di accesso al dominio, potresti vedere:
>
> 
>
>
> Questo errore si verifica se la procedura guidata di EC2 avvio identifica un documento SSM esistente con proprietà impreviste. Puoi effettuare una delle seguenti operazioni:
>
> - Se hai già modificato il documento SSM e le proprietà sono previste, scegli chiudi e procedi all'avvio dell' EC2 istanza senza modifiche.
> - Seleziona qui il link Elimina il documento SSM esistente per eliminare il documento SSM. Ciò consentirà la creazione di un documento SSM con le proprietà corrette. Il documento SSM verrà creato automaticamente all'avvio dell' EC2 istanza.

15. Per il profilo dell'istanza IAM, scegli il ruolo IAM creato in precedenza nella sezione dei prerequisiti Step 2: Creazione del ruolo Linux EC2 DomainJoin .
16. Scegliere Launch Instance (Avvia istanza).

> **Note**
>
> Se stai eseguendo l'aggiunta ottimizzata di un dominio con SUSE Linux, è necessario un riavvio prima che le autenticazioni funzionino. Per riavviare SUSE dal terminale Linux, digita sudo reboot.

Unire senza problemi un'istanza Amazon EC2 Linux a un AWS Managed Microsoft AD condiviso

In questa procedura, unirai senza problemi un'istanza Amazon EC2 Linux a un AWS Managed Microsoft AD condiviso. A tale scopo, creerai una policy di lettura Gestione dei segreti AWS IAM nel ruolo dell' EC2istanza nell'account in cui desideri avviare l'istanza EC2 Linux. A questo si farà riferimento `Account 2` in questa procedura. Questa istanza utilizzerà l'AD AWS gestito di Microsoft che viene condiviso dall'altro account denominato`Account 1`.

Prerequisiti

Prima di poter unire senza problemi un'istanza Amazon EC2 Linux a un AWS Managed Microsoft AD condiviso, dovrai completare quanto segue:

- I passaggi da 1 a 3 del tutorial,Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2 . Questo tutorial illustra la configurazione della rete e la condivisione di AWS Managed Microsoft AD.
- La procedura descritta inUnire senza problemi un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory.

Passaggio 1. Crea il EC2 DomainJoin ruolo Linux nell'Account 2

In questo passaggio, utilizzerai la console IAM per creare il ruolo IAM che utilizzerai per aggiungere il dominio all'istanza EC2 Linux mentre sei connesso`Account 2`.

Crea il EC2 DomainJoin ruolo Linux

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, scegli Ruoli.
3. Nella pagina Ruoli, seleziona Crea ruolo.

4. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio).
5. In Caso d'uso, scegli EC2, quindi scegli Avanti
6. In Filtra policy, procedi come segue:

   a. Specificare `AmazonSSMManagedInstanceCore`. Quindi seleziona la casella di controllo relativa all'elemento nell'elenco.

   b. Specificare `AmazonSSMDirectoryServiceAccess`. Quindi seleziona la casella di controllo relativa a quell'elemento nell'elenco.

   c. Dopo aver aggiunto queste politiche, seleziona Crea ruolo.

   > **Note**
   >
   > `AmazonSSMDirectoryServiceAccess`fornisce le autorizzazioni per unire le istanze a un Active Directory gestito da. Directory Service `AmazonSSMManagedInstanceCore`fornisce le autorizzazioni minime necessarie per l'uso. AWS Systems Manager Per ulteriori informazioni sulla creazione di un ruolo con queste autorizzazioni e per informazioni su altre autorizzazioni e policy che puoi assegnare al tuo ruolo IAM, consulta Configurare le autorizzazioni di istanza richieste per Systems Manager nella Guida per l'utente. AWS Systems Manager

7. Inserisci un nome per il tuo nuovo ruolo, ad esempio **`LinuxEC2DomainJoin`** o un altro nome che preferisci nel campo Nome del ruolo.
8. (Facoltativo) Per la descrizione del ruolo, inserisci una descrizione.
9. (Facoltativo) Scegli Aggiungi nuovo tag nel Passaggio 3: Aggiungi tag per aggiungere tag. Le coppie chiave-valore dei tag vengono utilizzate per organizzare, tracciare o controllare l'accesso per questo ruolo.
10. Scegli Crea ruolo.

Passaggio 2. Crea l'accesso alle risorse su più account per condividere segreti Gestione dei segreti AWS

La sezione successiva illustra i requisiti aggiuntivi che devono essere soddisfatti per unire senza problemi le istanze EC2 Linux con un Managed AWS Microsoft AD condiviso. Questi requisiti includono la creazione di politiche relative alle risorse e il loro collegamento ai servizi e alle risorse appropriati.

Per consentire agli utenti di un account di accedere ai Gestione dei segreti AWS segreti di un altro account, è necessario consentire l'accesso sia in una politica delle risorse che in una politica di identità. Questo tipo di accesso è denominato accesso alle risorse tra account.

Questo tipo di accesso è diverso dalla concessione dell'accesso alle identità nello stesso account del segreto di Secrets Manager. È inoltre necessario consentire l'utilizzo della chiave Identity to Use AWS Key Management Service(KMS) con cui il segreto è crittografato. Questa autorizzazione è necessaria in quanto non è possibile utilizzare la chiave AWS gestita (`aws/secretsmanager`) per l'accesso tra account diversi. Invece, crittograferai il tuo segreto con una chiave KMS creata da te e quindi allegherai una politica di chiave. Per modificare la chiave di crittografia per un segreto, vedi Modificare un Gestione dei segreti AWS segreto.

> **Note**
>
> Sono previste delle tariffe associateGestione dei segreti AWS, a seconda del segreto utilizzato. Per l'elenco completo dei prezzi aggiornati, consulta la pagina dei prezziGestione dei segreti AWS. Puoi utilizzare il Chiave gestita da AWS `aws/secretsmanager` programma creato da Secrets Manager per crittografare i tuoi segreti gratuitamente. Se crei le tue chiavi KMS per crittografare i tuoi segreti, ti AWS addebiterà la tariffa KMS correnteAWS. Per ulteriori informazioni, consultare AWS Key Management ServicePrezzi.

I passaggi seguenti consentono di creare le politiche delle risorse per consentire agli utenti di unire senza problemi un'istanza EC2 Linux a un AWS Managed Microsoft AD condiviso.

Allega una politica delle risorse al segreto nell'Account 1

1. Apri la console Secrets Manager all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Dall'elenco dei segreti, scegli il tuo segreto che hai creato durante ilPrerequisiti.
3. Nella pagina dei dettagli del segreto, nella scheda Panoramica, scorri verso il basso fino a Autorizzazioni per le risorse.
4. Seleziona Modifica autorizzazioni.
    - Nel campo della politica, inserisci la seguente politica. La seguente politica consente a Linux EC2 DomainJoin in `Account 2` di accedere al secret in`Account 1`. Sostituisci il valore ARN con il valore ARN per il tuo `Account 2LinuxEC2DomainJoin` ruolo creato nella Fase 1. Per utilizzare questa politica, consulta Allegare una politica di autorizzazioni a un segreto. Gestione dei segreti AWS

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/LinuxEC2DomainJoin"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

Aggiungi una dichiarazione alla politica chiave per la chiave KMS nell'Account 1

1. Apri la console Secrets Manager all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Nel riquadro di navigazione a sinistra, seleziona Customer managed keys.
3. Nella pagina Chiavi gestite dal cliente, seleziona la chiave che hai creato.
4. Nella pagina Dettagli chiave, vai a Politica chiave e seleziona Modifica.
5. La seguente dichiarazione sulla politica chiave consente `ApplicationRole` di `Account 2` utilizzare la chiave KMS `Account 1` per decrittografare il segreto in. `Account 1` Per utilizzare questa istruzione, aggiungerla al criterio chiave per la chiave KMS. Per ulteriori informazioni, vedere Modifica di una policy delle chiavi.

```
{
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
```

```
  "Resource": "*"
}
```

Crea una politica di identità per l'identità nell'Account 2

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione a sinistra, in Gestione degli accessi, seleziona Politiche.
3. Seleziona Create Policy (Crea policy). Scegli JSON nell'editor delle politiche.
4. La seguente politica consente di `ApplicationRole` accedere `Account 2` al secret in `Account 1` e decrittografare il valore segreto utilizzando la chiave di crittografia anch'essa presente. `Account 1` Puoi trovare l'ARN del tuo segreto nella console Secrets Manager nella pagina Dettagli segreti sotto Secret ARN. In alternativa, puoi chiamare describe-secret per identificare l'ARN del segreto. Sostituisci l'ARN della risorsa con l'ARN della risorsa per l'ARN segreto e. `Account 1` Per utilizzare questo criterio, consulta Allegare una politica di autorizzazioni a un segreto. Gestione dei segreti AWS

   JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:us-
east-1:111122223333:secret:secretName-AbCdEf"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Describekey"
      ],
      "Resource": "arn:aws:kms:us-
east-1:111122223333:key/Your_Encryption_Key"
    }
  ]
}
```

5. Seleziona Avanti, quindi seleziona Salva modifiche.
6. Trova e seleziona il ruolo `Account 2` in cui hai creatoAttach a resource policy to the secret in Account 1.
7. In Aggiungi autorizzazioni, seleziona Allega politiche.
8. Nella barra di ricerca, trova la politica in cui hai creato Add a statement to the key policy for the KMS key in Account 1 e seleziona la casella per aggiungere la politica al ruolo. Quindi seleziona Aggiungi autorizzazioni.

Fase 3. Unisciti senza problemi alla tua istanza Linux

Ora puoi utilizzare la procedura seguente per unire senza problemi la tua istanza EC2 Linux al tuo AWS Managed Microsoft AD condiviso.

Per unirti senza problemi alla tua istanza Linux

1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal selettore della regione nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nella EC2 Dashboard, nella sezione Launch instance, scegli Launch instance.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua EC2 istanza Linux.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivi per aggiungere una o più coppie chiave-valore di tag per organizzare, tracciare o controllare l'accesso per questa EC2 istanza.
6. Nella sezione Applicazione e immagine del sistema operativo (Amazon Machine Image), scegli un'AMI Linux che desideri avviare.

> **Note**
>
> L'AMI utilizzato deve avere AWS Systems Manager (SSM Agent) la versione 2.3.1644.0 o successiva. Per verificare la versione dell'Agente SSM installata nell'AMI avviando un'istanza da quest'ultima, consulta Ottenere la versione dell'Agente SSM attualmente installata. Se è necessario aggiornare l'agente SSM, vedere Installazione e configurazione dell'agente SSM su istanze per Linux. EC2
> SSM utilizza il `aws:domainJoin` plug-in quando aggiunge un'istanza Linux a un dominio Active Directory. Il plugin cambia il nome host per le istanze Linux nel formato

EC2 AMAZ-. *XXXXXXX* Per ulteriori informazioni in merito*aws:domainJoin*, consultate AWS Systems ManagerCommand Document Plugin reference nella Guida per l'AWS Systems Managerutente.

7. Nella sezione Tipo di istanza, scegli il tipo di istanza che desideri utilizzare dall'elenco a discesa Tipo di istanza.
8. Nella sezione Coppia di chiavi (accesso), puoi scegliere se creare una nuova coppia di chiavi o selezionare una coppia di chiavi esistente. Per creare una nuova coppia di chiavi, scegli Crea nuova coppia di chiavi. Inserisci un nome per la coppia di chiavi e seleziona un'opzione per il Tipo di coppia di chiavi e il Formato del file della chiave privata. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegli .pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegli .ppk. Scegli crea coppia di chiavi. Il file della chiave privata viene automaticamente scaricato dal browser. Salvare il file della chiave privata in un luogo sicuro.

   Important

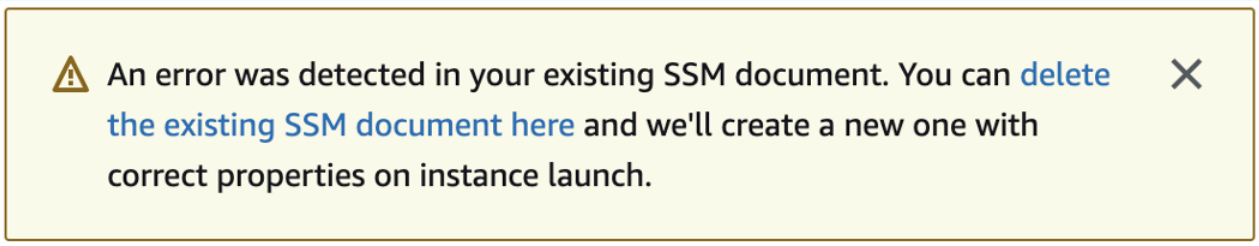
   Questo è l'unico momento in cui salvare il file della chiave privata.

9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto il traffico esterno instradato a un gateway Internet. In caso contrario, non potrai connetterti in remoto all'istanza.

    Per ulteriori informazioni su come connettersi a un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta l'indirizzo IP delle EC2 istanze Amazon nella Amazon EC2 User Guide.
12. Nelle impostazioni Firewall (gruppi di sicurezza), puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
13. Nelle impostazioni Configurazione dell'archiviazione, puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.

14. Seleziona la sezione Dettagli avanzati, scegli il tuo dominio dall'elenco a discesa Directory di aggiunta al dominio.

> **Note**
>
> Dopo aver scelto la directory di accesso al dominio, potresti vedere:
>
> 
>
>
> Questo errore si verifica se la procedura guidata di EC2 avvio identifica un documento SSM esistente con proprietà impreviste. Puoi effettuare una delle seguenti operazioni:
>
> - Se hai già modificato il documento SSM e le proprietà sono previste, scegli chiudi e procedi all'avvio dell' EC2 istanza senza modifiche.
> - Seleziona qui il link Elimina il documento SSM esistente per eliminare il documento SSM. Ciò consentirà la creazione di un documento SSM con le proprietà corrette. Il documento SSM verrà creato automaticamente all'avvio dell' EC2 istanza.

15. Per il profilo dell'istanza IAM, scegli il ruolo IAM creato in precedenza nella sezione dei prerequisiti Step 2: Creazione del ruolo Linux EC2 DomainJoin .
16. Scegliere Launch Instance (Avvia istanza).

> **Note**
>
> Se stai eseguendo l'aggiunta ottimizzata di un dominio con SUSE Linux, è necessario un riavvio prima che le autenticazioni funzionino. Per riavviare SUSE dal terminale Linux, digita sudo reboot.

Aggiungere manualmente un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory

Oltre alle EC2 Windows istanze Amazon, puoi anche aggiungere determinate istanze Amazon EC2 Linux alla tua Managed AWS Microsoft AD Active Directory. Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64-bit x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le altre distribuzioni e versioni di Linux potrebbero non funzionare, sebbene non siano state testate.

Unisci un'istanza Linux al tuo AWS Managed Microsoft AD

Prima di poter collegare un'istanza Amazon Linux, CentOS, Red Hat o Ubuntu alla tua directory, l'istanza deve essere avviata come specificato in Unisciti senza problemi alla tua istanza Linux.

> **Important**
>
> Alcune delle procedure seguenti, se non eseguite correttamente, possono rendere l'istanza non raggiungibile o inutilizzabile. Pertanto, ti consigliamo vivamente di effettuare un backup o effettuare uno snapshot dell'istanza prima di eseguire queste procedure.

Per collegare un'istanza Linux alla tua directory

Segui i passaggi descritti per l'istanza Linux specifica utilizzando una delle seguenti schede:

Amazon Linux

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP dei server DNS dei server DNS Directory Service forniti. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza di Amazon Linux a 64 bit sia aggiornata.

```
sudo yum -y update
```

4. Installa i pacchetti Amazon Linux necessari sull'istanza Linux.

> **Note**
>
> Alcuni di questi pacchetti potrebbero essere già installati.
> Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Per assistenza nella determinazione della versione di Amazon Linux che stai utilizzando, consulta Identificazione delle immagini Amazon Linux nella Amazon EC2 User Guide for Linux Instances.

5. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

6. Imposta il servizio SSH per permettere l'autenticazione della password.
   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

      ```
      sudo vi /etc/ssh/sshd_config
      ```

   b. Imposta `PasswordAuthentication` su `yes`.

      ```
      PasswordAuthentication yes
      ```

   c. Riavvia il servizio SSH.

      ```
      sudo systemctl restart sshd.service
      ```

      In alternativa:

      ```
      sudo service sshd restart
      ```

7. Dopo il riavvio dell'istanza, connettiti ad essa con qualsiasi client SSH e aggiungi il gruppo AWS Delegated Administrators all'elenco sudoers eseguendo i seguenti passaggi:
   a. Apri il file `sudoers` tramite il comando seguente:

      ```
      sudo visudo
      ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

      ```
      ## Add the "AWSDelegated Administrators" group from the example.com domain.
      ```

```
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

CentOS

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configurate l'istanza Linux per utilizzare gli indirizzi IP dei server DNS dei server DNS forniti. Directory Service A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza di CentOS 7 sia aggiornata.

```
sudo yum -y update
```

4. Installa i pacchetti CentOS 7 necessari sull'istanza Linux.

> **Note**
>
> Alcuni di questi pacchetti potrebbero essere già installati.
> Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega

di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

6. Imposta il servizio SSH per permettere l'autenticazione della password.
   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Imposta `PasswordAuthentication` su `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Riavvia il servizio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   In alternativa:

   ```
   sudo service sshd restart
   ```

7. Dopo il riavvio dell'istanza, connettiti ad essa con qualsiasi client SSH e aggiungi il gruppo AWS Delegated Administrators all'elenco sudoers eseguendo i seguenti passaggi:
   a. Apri il file `sudoers` tramite il comando seguente:

   ```
   sudo visudo
   ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

   ```
   ## Add the "AWSDelegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

Red Hat

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configurate l'istanza Linux per utilizzare gli indirizzi IP dei server DNS dei server DNS forniti. Directory Service A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Red Hat - 64bit sia aggiornata.

```
sudo yum -y update
```

4. Installa i pacchetti Red Hat necessari nell'istanza Linux.

> **Note**
>
> Alcuni di questi pacchetti potrebbero essere già installati.
> Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

Il AMAccountnome s di un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

6. Imposta il servizio SSH per permettere l'autenticazione della password.

   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Imposta `PasswordAuthentication` su `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Riavvia il servizio SSH.

   ```
   sudo systemctl restart sshd.service
   ```

   In alternativa:

   ```
   sudo service sshd restart
   ```

7. Dopo il riavvio dell'istanza, connettiti ad essa con qualsiasi client SSH e aggiungi il gruppo AWS Delegated Administrators all'elenco sudoers eseguendo i seguenti passaggi:

   a. Apri il file `sudoers` tramite il comando seguente:

   ```
   sudo visudo
   ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

   ```
   ## Add the "AWSDelegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

SUSE

1. Connettiti all'istanza tramite qualsiasi client SSH.

2. Configura l'istanza Linux per utilizzare gli indirizzi IP del server DNS forniti dal Directory Service. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza di SUSE Linux 15 sia aggiornata.

   a. Collega il repository dei pacchetti.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Aggiorna SUSE.

   ```
   sudo zypper update -y
   ```

4. Installa i pacchetti SUSE Linux 15 richiesti sulla propria istanza Linux.

   > **Note**
   >
   > Alcuni di questi pacchetti potrebbero essere già installati.
   > Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

   ```
   sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
   ```

5. Collega l'istanza alla directory tramite il comando seguente.

   ```
   sudo realm join -U join_account example.com --verbose
   ```

   join_account

   Il AMAccount nome s nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Si noti che sono attesi entrambi i seguenti rendimenti.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Abilitare manualmente SSSD in PAM.

```
sudo pam-config --add --sss
```

7. Modifica nsswitch.conf per abilitare SSSD in nsswitch.conf

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Aggiungi la riga seguente a/etc/pam.d/common-session per creare automaticamente una home directory al login iniziale

```
sudo vi /etc/pam.d/common-session
```

```
session optional pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Riavviare l'istanza per completare il processo di aggiunta al dominio.

```
sudo reboot
```

10. Riconnettiti all'istanza utilizzando qualsiasi client SSH per verificare che l'aggiunta al dominio sia stata completata correttamente e finalizzare ulteriori passaggi.

    a. Per confermare che l'istanza è stata registrata nel dominio

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

b. Per verificare lo stato del daemon SSSD

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
           ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
           ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. Per consentire a un utente l'accesso tramite SSH e console

```
sudo realm permit join_account@example.com
```

Per consentire l'accesso a un gruppo di dominio tramite SSH e console

```
sudo realm permit -g 'AWSDelegated Administrators'
```

O per consentire a tutti gli utenti di accedere

```
sudo realm permit --all
```

12. Imposta il servizio SSH per permettere l'autenticazione della password.

    a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Imposta `PasswordAuthentication` su `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Riavvia il servizio SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    In alternativa:

    ```
    sudo service sshd restart
    ```

13. 13. Dopo il riavvio dell'istanza, connettiti ad essa con qualsiasi client SSH e aggiungi il gruppo AWS Delegated Administrators all'elenco sudoers eseguendo i seguenti passaggi:

    a. Aprire il file sudoers con il seguente comando:

    ```
    sudo visudo
    ```

    b. Aggiungi il codice seguente alla fine del file sudoers e salva il file.

    ```
    ## Add the "Domain Admins" group from the awsad.com domain.
    %AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
    ```

Ubuntu

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configurate l'istanza Linux per utilizzare gli indirizzi IP dei server DNS dei server DNS forniti. Directory Service A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Ubuntu - 64bit sia aggiornata.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Installa i pacchetti Ubuntu necessari nell'istanza Linux.

> **Note**
>
> Alcuni di questi pacchetti potrebbero essere già installati.
> Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Disattivare la risoluzione DNS inversa e impostare l'area di autenticazione predefinita sul nome di dominio completo del dominio. Perché un realm possa funzionare, le istanze Ubuntu devono essere risolvibili in modo inverso nel DNS. In caso contrario, dovrai disabilitare il DNS inverso in /etc/krb5.conf come segue:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

Il AMAccountnome s di un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

7. Imposta il servizio SSH per permettere l'autenticazione della password.
   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

      ```
      sudo vi /etc/ssh/sshd_config
      ```

   b. Imposta `PasswordAuthentication` su `yes`.

      ```
      PasswordAuthentication yes
      ```

   c. Riavvia il servizio SSH.

      ```
      sudo systemctl restart sshd.service
      ```

      In alternativa:

      ```
      sudo service sshd restart
      ```

8. Dopo il riavvio dell'istanza, connettiti ad essa con qualsiasi client SSH e aggiungi il gruppo AWS Delegated Administrators all'elenco sudoers eseguendo i seguenti passaggi:
   a. Apri il file `sudoers` tramite il comando seguente:

      ```
      sudo visudo
      ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

      ```
      ## Add the "AWSDelegated Administrators" group from the example.com domain.
      ```

```
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

Limitazioni di accesso all'account

Poiché tutti gli account vengono definiti in Active Directory, per impostazione predefinita tutti gli utenti nella directory possono accedere all'istanza. Puoi permettere solo a utenti specifici di accedere all'istanza con ad_access_filter in sssd.conf. Esempio:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica che agli utenti è consentito solo l'accesso all'istanza se membri di un determinato gruppo.

cn

Il nome canonico del gruppo a cui è consentito l'accesso. In questo esempio, il nome del gruppo è. *admins*

ou

È l'unità organizzativa in cui si trova il gruppo di cui sopra. In questo esempio, l'unità organizzativa è*Testou*.

dc

È il componente di dominio del tuo dominio. In questo esempio, *example*.

dc

È un componente di dominio aggiuntivo. In questo esempio, *com*.

È necessario aggiungere manualmente ad_access_filter a /etc/sssd/sssd.conf.

Apri il file /etc/sssd/sssd.conf in un editor di testo.

```
sudo vi /etc/sssd/sssd.conf
```

A questo punto, il tuo sssd.conf potrebbe avere questo aspetto:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Perché la configurazione diventi effettiva, devi riavviare il servizio sssd:

```
sudo systemctl restart sssd.service
```

In alternativa, puoi usare:

```
sudo service sssd restart
```

Poiché tutti gli account vengono definiti in Active Directory, per impostazione predefinita tutti gli utenti nella directory possono accedere all'istanza. Puoi permettere solo a utenti specifici di accedere all'istanza con ad_access_filter in sssd.conf.

Esempio:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica che agli utenti è consentito solo l'accesso all'istanza se membri di un determinato gruppo.

cn

Il nome canonico del gruppo a cui è consentito l'accesso. In questo esempio, il nome del gruppo è*admins*.

ou

È l'unità organizzativa in cui si trova il gruppo di cui sopra. In questo esempio, l'unità organizzativa è*Testou*.

dc

È il componente di dominio del tuo dominio. In questo esempio, *example*.

dc

È un componente di dominio aggiuntivo. In questo esempio, *com*.

È necessario aggiungere manualmente ad_access_filter a /etc/sssd/sssd.conf.

1. Apri il file /etc/sssd/sssd.conf in un editor di testo.

```
sudo vi /etc/sssd/sssd.conf
```

2. A questo punto, il tuo sssd.conf potrebbe avere questo aspetto:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

3. Perché la configurazione diventi effettiva, devi riavviare il servizio sssd:

```
sudo systemctl restart sssd.service
```

In alternativa, puoi usare:

```
sudo service sssd restart
```

Mappatura degli ID

La mappatura degli ID può essere eseguita con due metodi per mantenere un'esperienza unificata tra le identità UNIX/Linux User Identifier (UID) e Group Identifier (GID) e le identità SID (Windows e Active Directory Security Identifier). Questi metodi sono:

1. Centralizzato
2. Distribuito

> **Note**
>
> La mappatura centralizzata dell'identità degli utenti in Active Directory richiede l'interfaccia del sistema operativo portatile o POSIX.

Mappatura centralizzata delle identità degli utenti

Active Directory o un altro servizio LDAP (Lightweight Directory Access Protocol) fornisce UID e GID agli utenti Linux. In Active Directory, questi identificatori vengono memorizzati negli attributi degli utenti se l'estensione POSIX è configurata:

- UID: il nome utente Linux (String)
- Numero UID: il numero ID utente Linux (numero intero)
- Numero GID: il numero ID del gruppo Linux (numero intero)

Per configurare un'istanza Linux per utilizzare l'UID e il GID di Active Directory, impostali `ldap_id_mapping = False` nel file sssd.conf. Prima di impostare questo valore, verifica di aver aggiunto un UID, un numero UID e un numero GID agli utenti e ai gruppi in Active Directory.

Mappatura distribuita delle identità degli utenti

Se Active Directory non ha l'estensione POSIX o se scegli di non gestire centralmente la mappatura delle identità, Linux può calcolare i valori UID e GID. Linux utilizza l'identificatore di sicurezza (SID) univoco dell'utente per mantenere la coerenza.

Per configurare la mappatura distribuita degli ID utente, impostala `ldap_id_mapping = True` nel file sssd.conf.

Problemi comuni

Se lo impostil`dap_id_mapping = False`, a volte l'avvio del servizio SSSD fallirà. Il motivo di questo errore è dovuto al fatto che le modifiche UIDs non sono supportate. Ti consigliamo di eliminare la cache SSSD ogni volta che passi dalla mappatura degli ID agli attributi POSIX o dagli attributi POSIX alla mappatura degli ID. Per ulteriori dettagli sulla mappatura degli ID e sui parametri ldap_id_mapping, consultate la pagina man sssd-ldap (8) nella riga di comando di Linux.

Connect all'istanza Linux

Quando un utente effettua la connessione all'istanza tramite un client SSH, gli verrà richiesto di inserire il proprio nome utente. L'utente può immettere il nome utente nei formati `username@example.com` o `EXAMPLE\username` . La risposta apparirà simile alla seguente, a seconda della distribuzione Linux utilizzata:

Amazon Linux, Red Hat Enterprise Linux e CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
```

```
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Aggiungere manualmente un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory utilizzando Winbind

Puoi utilizzare il servizio Winbind per aggiungere manualmente le tue istanze Amazon EC2 Linux a un dominio AWS Microsoft AD Active Directory gestito. Ciò consente agli utenti locali di Active Directory esistenti di utilizzare le proprie credenziali di Active Directory quando accedono alle istanze Linux unite al sistema gestito di AWS Microsoft AD Active Directory. Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64-bit x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le altre distribuzioni e versioni di Linux potrebbero non funzionare, sebbene non siano state testate.

Unisci un'istanza Linux alla tua directory AWS gestita di Microsoft AD Active Directory

> **Important**
>
> Alcune delle procedure seguenti, se non eseguite correttamente, possono rendere l'istanza non raggiungibile o inutilizzabile. Pertanto, ti consigliamo vivamente di effettuare un backup o effettuare uno snapshot dell'istanza prima di eseguire queste procedure.

Per collegare un'istanza Linux alla tua directory

Segui i passaggi descritti per l'istanza Linux specifica utilizzando una delle seguenti schede:

Amazon Linux/CENTOS/REDHAT

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP del server DNS forniti dal Directory Service. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Linux sia aggiornata.

   ```
   sudo yum -y update
   ```

4. Installa i pacchetti Samba/Winbind richiesti sull'istanza Linux.

   ```
   sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
   ```

5. Effettua un backup del file `smb.conf` principale in modo da poterlo ripristinare in caso di errore:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Apri il file di configurazione originale [`/etc/samba/smb.conf`] in un editor di testo.

```
sudo vim /etc/samba/smb.conf
```

Inserisci le informazioni sull'ambiente del tuo dominio Active Directory come mostrato nell'esempio seguente:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Apri il file host [`/etc/hosts`] in un editor di testo.

```
sudo vim /etc/hosts
```

Aggiungi l'indirizzo IP privato dell'istanza Linux come segue:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Se non hai specificato il tuo indirizzo IP nel file `/etc/hosts`, potresti ricevere il seguente errore DNS durante il collegamento dell'istanza al dominio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`

Questo errore indica che il collegamento è avvenuto con successo ma il comando [net ads] non è riuscito a registrare il record DNS nel DNS.

8. Collega l'istanza Linux ad Active Directory utilizzando l'utility net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifica il file di configurazione PAM, usa il comando seguente per aggiungere le voci necessarie per l'autenticazione winbind:

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. Imposta il servizio SSH per permettere l'autenticazione della password modificando il file `/etc/ssh/sshd_config`.

a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

```
sudo vi /etc/ssh/sshd_config
```

b. Imposta `PasswordAuthentication` su `yes`.

```
PasswordAuthentication yes
```

c. Riavvia il servizio SSH.

```
sudo systemctl restart sshd.service
```

In alternativa:

```
sudo service sshd restart
```

11. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi i privilegi root per l'utente o il gruppo del dominio all'elenco dei sudoers seguendo la procedura seguente:
    a. Apri il file `sudoers` tramite il comando seguente:

    ```
    sudo visudo
    ```

    b. Aggiungi i gruppi o gli utenti richiesti dal tuo dominio Trusting o Trusted come segue, quindi salvalo.

    ```
    ## Adding Domain Users/Groups.
    %domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
    %domainname\\groupname ALL=(ALL:ALL) ALL
    domainname\\username ALL=(ALL:ALL) ALL
    %Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
    Trusted_DomainName\\username ALL=(ALL:ALL) ALL
    ```

    (L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

SUSE

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP del server DNS forniti dal Directory Service. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza di SUSE Linux 15 sia aggiornata.
    a. Collega il repository dei pacchetti.

    ```
    sudo SUSEConnect -p PackageHub/15.1/x86_64
    ```

b. Aggiorna SUSE.

```
sudo zypper update -y
```

4. Installa i pacchetti Samba/Winbind richiesti sull'istanza Linux.

```
sudo zypper in -y samba samba-winbind
```

5. Effettua un backup del file `smb.conf` principale in modo da poterlo ripristinare in caso di errore:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Apri il file di configurazione originale [`/etc/samba/smb.conf`] in un editor di testo.

```
sudo vim /etc/samba/smb.conf
```

Inserisci le informazioni sull'ambiente del dominio Active Directory come mostrato nell'esempio seguente:

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. Apri il file host [`/etc/hosts`] in un editor di testo.

```
sudo vim /etc/hosts
```

Aggiungi l'indirizzo IP privato dell'istanza Linux come segue:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Se non hai specificato il tuo indirizzo IP nel file `/etc/hosts`, potresti ricevere il seguente errore DNS durante il collegamento dell'istanza al dominio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Questo errore indica che il collegamento è avvenuto con successo ma il comando [net ads] non è riuscito a registrare il record DNS nel DNS.

8. Collega l'istanza Linux alla directory tramite il comando seguente.

```
sudo net ads join -U join_account@example.com
```

join_account

Il AMAccount nome s nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifica il file di configurazione PAM, usa il comando seguente per aggiungere le voci necessarie per l'autenticazione Winbind:

```
sudo pam-config --add --winbind --mkhomedir
```

10. Apri il file di configurazione Name Service Switch [`/etc/nsswitch.conf`] in un editor di testo.

```
vim /etc/nsswitch.conf
```

Aggiungi la direttiva Winbind come illustrato di seguito.

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. Imposta il servizio SSH per permettere l'autenticazione della password modificando il file `/etc/ssh/sshd_config`.

    a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

    ```
    sudo vim /etc/ssh/sshd_config
    ```

    b. Imposta `PasswordAuthentication` su `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Riavvia il servizio SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    In alternativa:

    ```
    sudo service sshd restart
    ```

12. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi i privilegi root per l'utente o il gruppo del dominio all'elenco dei sudoers seguendo la procedura seguente:

    a. Apri il file `sudoers` tramite il comando seguente:

    ```
    sudo visudo
    ```

    b. Aggiungi i gruppi o gli utenti richiesti dal tuo dominio Trusting o Trusted come segue, quindi salvalo.

    ```
    ## Adding Domain Users/Groups.
    %domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
    %domainname\\groupname ALL=(ALL:ALL) ALL
    domainname\\username ALL=(ALL:ALL) ALL
    %Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
    Trusted_DomainName\\username ALL=(ALL:ALL) ALL
    ```

(L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

Ubuntu

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP del server DNS forniti dal Directory Service. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Linux sia aggiornata.

   ```
   sudo apt-get -y upgrade
   ```

4. Installa i pacchetti Samba/Winbind richiesti sull'istanza Linux.

   ```
   sudo apt -y install samba winbind libnss-winbind libpam-winbind
   ```

5. Effettua un backup del file `smb.conf` principale in modo da poterlo ripristinare in caso di errore.

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. Apri il file di configurazione originale [`/etc/samba/smb.conf`] in un editor di testo.

   ```
   sudo vim /etc/samba/smb.conf
   ```

   Inserisci le informazioni sull'ambiente del dominio Active Directory come mostrato nell'esempio seguente:

   ```
   [global]
    workgroup = example
    security = ads
    realm = example.com
    idmap config * : rangesize = 1000000
    idmap config * : range = 1000000-19999999
   ```

```
idmap config * : backend = autorid
winbind enum users = no
winbind enum groups = no
template homedir = /home/%U@%D
template shell = /bin/bash
winbind use default domain = false
```

7. Apri il file host [`/etc/hosts`] in un editor di testo.

```
sudo vim /etc/hosts
```

Aggiungi l'indirizzo IP privato dell'istanza Linux come segue:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Se non hai specificato il tuo indirizzo IP nel file `/etc/hosts`, potresti ricevere il seguente errore DNS durante il collegamento dell'istanza al dominio:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Questo errore indica che il collegamento è avvenuto con successo ma il comando [net ads] non è riuscito a registrare il record DNS nel DNS.

8. Collega l'istanza Linux ad Active Directory utilizzando l'utility net.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
Enter join_account@example.com's password:
```

```
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Modifica il file di configurazione PAM, usa il comando seguente per aggiungere le voci necessarie per l'autenticazione Winbind:

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Apri il file di configurazione Name Service Switch [`/etc/nsswitch.conf`] in un editor di testo.

```
vim /etc/nsswitch.conf
```

Aggiungi la direttiva Winbind come illustrato di seguito.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Imposta il servizio SSH per permettere l'autenticazione della password modificando il file `/etc/ssh/sshd_config`.
    a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

    ```
    sudo vim /etc/ssh/sshd_config
    ```

    b. Imposta `PasswordAuthentication` su `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Riavvia il servizio SSH.

    ```
    sudo systemctl restart sshd.service
    ```

    In alternativa:

    ```
    sudo service sshd restart
    ```

12. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi i privilegi root per l'utente o il gruppo del dominio all'elenco dei sudoers seguendo la procedura seguente:
    a. Apri il file `sudoers` tramite il comando seguente:

```
sudo visudo
```

b. Aggiungi i gruppi o gli utenti richiesti dal tuo dominio Trusting o Trusted come segue, quindi salvalo.

```
## Adding Domain Users/Groups.
%domainname\\AWS\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

Connect all'istanza Linux

Quando un utente effettua la connessione all'istanza tramite un client SSH, gli verrà richiesto di inserire il proprio nome utente. L'utente può immettere il nome utente nei formati `username@example.com` o `EXAMPLE\username` . La risposta apparirà simile alla seguente, a seconda della distribuzione Linux utilizzata:

Amazon Linux, Red Hat Enterprise Linux e CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Unire un'istanza Amazon EC2 Mac alla tua directory AWS gestita di Microsoft AD Active Directory

Questa procedura unisce manualmente un'istanza Amazon EC2 Mac al tuo AWS Managed Microsoft AD Active Directory.

Prerequisiti

- Le istanze Amazon EC2 Mac richiedono Amazon EC2 Dedicated Hosts. È necessario allocare un host dedicato e avviare un'istanza sull'host. Per ulteriori informazioni, consulta Launch a Mac nella Amazon EC2 User Guide.
- Si consiglia di creare un set di opzioni DHCP per AWS Managed Microsoft AD Active Directory. Ciò consentirà a tutte le istanze del tuo Amazon VPC di puntare al dominio specificato e ai server DNS di risolvere i relativi nomi di dominio. Per ulteriori informazioni, consulta Creazione o modifica di un set di opzioni DHCP per AWS Managed Microsoft AD.

> **Note**
>
> I prezzi degli host dedicati variano in base all'opzione di pagamento selezionata. Per ulteriori informazioni, consulta la Guida per l' EC2 utente di Amazon Pricing and Billing in Amazon.

Unire manualmente un'istanza Mac

1. Usa il seguente comando SSH per connetterti alla tua istanza Mac. Per ulteriori informazioni sulla connessione all'istanza Mac, vedi Connessione all'istanza Mac.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
   ```

2. Dopo esserti connesso all'istanza Mac, crea una password per l'*ec2-user*account utilizzando il seguente comando:

   ```
   sudo passwd ec2-user
   ```

3. Quando richiesto nella riga di comando, fornisci una password per l'*ec2-user*account. Puoi aggiornare il sistema operativo e il software seguendo la procedura in Aggiornamento del sistema operativo e del software nella Amazon EC2 User Guide.

4. Usa il *dsconfigad* comando seguente per aggiungere l'istanza Mac al dominio AWS gestito di Microsoft AD Active Directory. Assicurati di sostituire il nome di dominio, il nome del computer e l'unità organizzativa con le informazioni sul dominio Microsoft AD Active Directory AWS gestito. Per ulteriori informazioni, consulta Configurazione dell'accesso al dominio in Directory Utility on Mac sul sito web di Apple.

   > **Warning**
   >
   > Il nome del computer non deve contenere un trattino. I trattini potrebbero impedire l'associazione a Managed AWS Microsoft AD Active Directory.

   ```
   sudo dsconfigad -add domainName -computer computerName -username Username -
   ou "Your-AWS-Delegated-Organizational-Unit"
   ```

   L'esempio seguente mostra come dovrebbe apparire il comando quando si aggiunge un utente amministrativo su un'istanza Mac denominata **myec2mac01** nel dominio: **example.com**

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Usa il comando seguente per aggiungere gli amministratori AWS delegati all'utente amministrativo sulla tua istanza Mac:

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. Utilizzare il comando seguente per confermare che l'aggiunta al dominio AWS Managed Microsoft AD Active Directory è avvenuta correttamente:

```
dsconfigad -show
```

Hai unito correttamente l'istanza Mac alla tua directory AWS gestita di Microsoft AD Active Directory. Ora puoi accedere alla tua istanza Mac utilizzando le credenziali di AWS Managed Microsoft AD Active Directory.

Quando accedi per la prima volta alla tua istanza Mac, dovresti avere la possibilità di accedere come utente «Altro». A questo punto, puoi utilizzare le credenziali del dominio Active Directory per accedere all'istanza Mac. Se non ti viene fornito «Altro» nella schermata di accesso dopo aver completato questi passaggi, accedi come ec2-user e poi disconnettiti.

Per accedere utilizzando l'interfaccia utente grafica con un utente di dominio, segui i passaggi in Connect all'interfaccia grafica utente (GUI) dell'istanza nella Amazon EC2 User Guide.

Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD

Per aggiungere un computer a AWS Managed Microsoft AD, è necessario un account con privilegi per aggiungere computer alla directory.

Con AWS Directory Service for Microsoft Active Directory, i membri dei gruppi Admins e AWSDelegated Server Administrators dispongono di questi privilegi.

Tuttavia, come best practice, dovresti utilizzare un account che disponga solo dei privilegi minimi necessari. La seguente procedura mostra come creare un nuovo gruppo denominato `Joiners` e delegare i privilegi necessari a questo gruppo per aggiungere i computer alla directory.

Devi eseguire questa procedura su un computer che è stato aggiunto alla directory e che abbia installato lo snap-in di MMC Utenti e computer di Active Directory. Inoltre, è necessario aver eseguito l'accesso come amministratore del dominio.

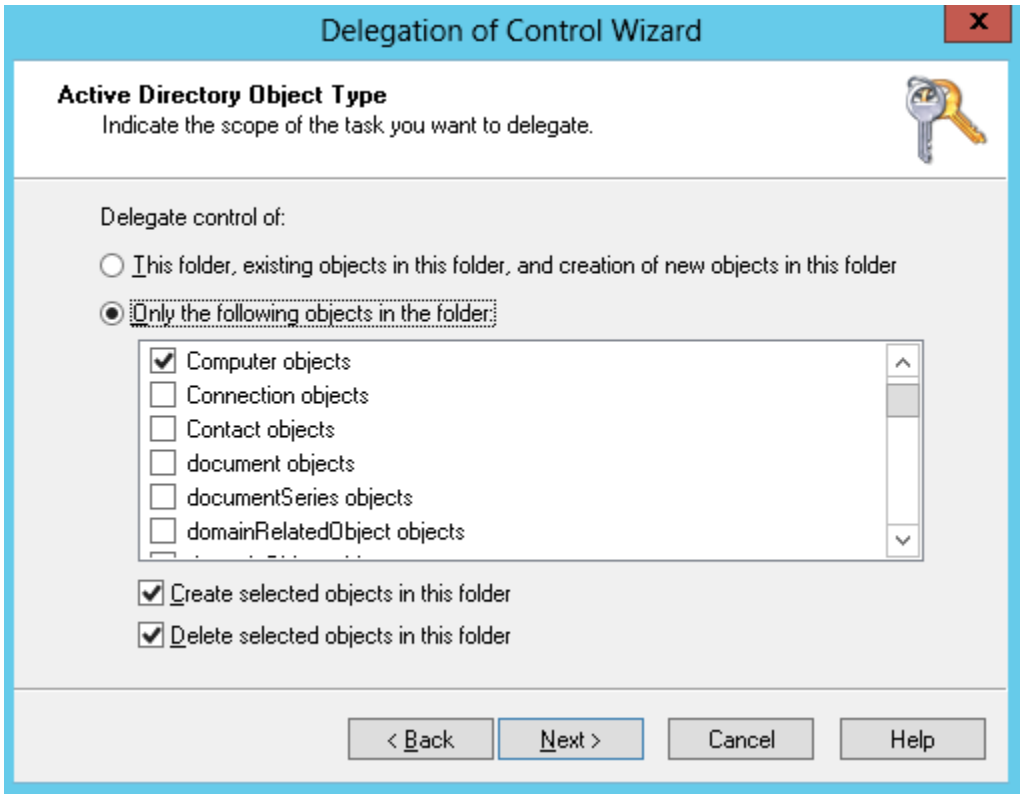
Per delegare i privilegi di iscrizione per Managed AWS Microsoft AD

1. Apri Active Directory User and Computers (Utenti e computer di Active Directory) e seleziona l'unità organizzativa che ha il tuo nome NetBIOS nell'albero di spostamento, quindi selezionare l'unità organizzativa Users (Utenti).

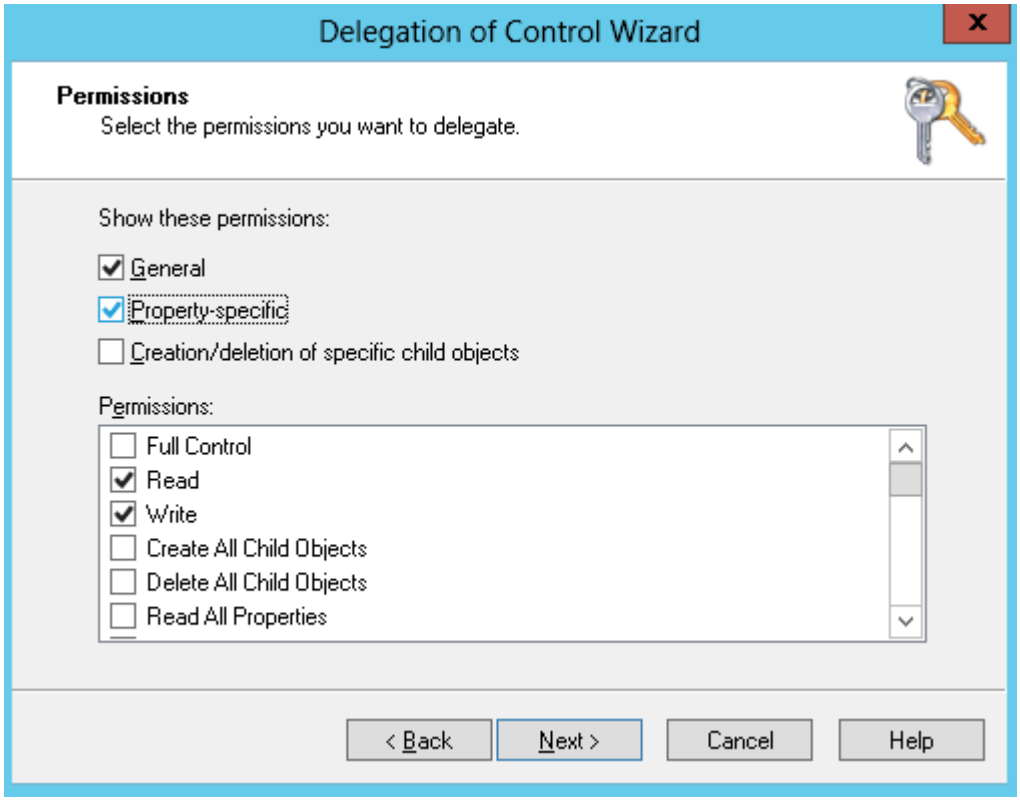
   > **Important**
   >
   > Quando si avvia un AWS Directory Service per Microsoft Active Directory, AWS crea un'unità organizzativa (OU) che contiene tutti gli oggetti della directory. Questa unità organizzativa, che ha lo stesso nome NetBIOS che hai digitato al momento della creazione della directory, si trova nella radice del dominio. La radice del dominio è di proprietà e gestita daAWS. Non puoi apportare modifiche alla radice del dominio stessa, pertanto devi creare il gruppo **`Joiners`** all'interno dell'unità organizzativa che ha il tuo nome NetBIOS.

2. Apri il menu contestuale (tasto destro del mouse) per Users (Utenti), scegli New (Nuovo), quindi Group (Gruppo).
3. Nella finestra New Object - Group (Nuovo oggetto - Gruppo), digita quanto segue e scegli OK.
   - Per Group name (Nome gruppo), digita **`Joiners`**.
   - In Group scope (Ambito del gruppo), scegli Global (Globale).
   - Per Group type (Tipo gruppo), scegli Security (Sicurezza).
4. Nell'albero di spostamento, seleziona il container Computers (Computer) sotto il tuo nome NetBIOS. Nel menu Action (Operazione), scegli Delegate Control (Delega controllo).
5. Nella pagina Delegation of Control Wizard (Delega guidata del controllo), scegli Next (Avanti), quindi scegli Add (Aggiungi).
6. Nella finestra Select Users, Computers, or Groups (Seleziona utenti, computer o gruppi), digita `Joiners` e scegli OK. Se viene trovato più di un oggetto, selezionare il gruppo `Joiners` creato sopra. Scegli Next (Successivo).
7. Nella pagina Operazioni da delegare, selezionare Crea un'operazione personalizzata per eseguire la delega, quindi scegliere Avanti.

8. Seleziona Only the following objects in the folder (Solo i seguenti oggetti contenuti nella cartella), quindi Computer objects (Oggetti computer).
9. Selezionare Crea gli oggetti selezionati in questa cartella e Elimina gli oggetti selezionati in questa cartella. Quindi scegli Successivo.



10. Seleziona Read (Lettura) e Write (Scrittura), quindi scegli Next (Avanti).



11. Verificare le informazioni nella pagina Completing the Delegation of Control Wizard (Completamento della delega guidata del controllo) e scegli Finish (Termina).
12. Crea un utente con una password complessa e aggiungilo al gruppo `Joiners`. Questo utente deve trovarsi nel container Users (Utenti) presente sotto il tuo nome NetBIOS. L'utente disporrà quindi privilegi sufficienti per connettere le istanze alla directory.

Creazione o modifica di un set di opzioni DHCP per AWS Managed Microsoft AD

AWSconsiglia di creare un set di opzioni DHCP per la Directory Service directory e di assegnare le opzioni DHCP impostate al VPC in cui si trova la directory. Questo permette alle istanze in tale VPC di puntare al dominio e ai server DNS specificati per risolvere i propri nomi di dominio.

Per ulteriori informazioni sui set di opzioni DHCP, consulta Set di opzioni DHCP nella Guida per l'utente di Amazon VPC.

Creazione di un set opzioni DHCP per la tua directory

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, scegliere DHCP Options Sets (Set di opzioni DHCP), quindi selezionare Create DHCP options set (Crea set di opzioni DHCP).
3. Nella pagina Crea set di opzioni DHCP, fornisci i seguenti valori per la directory:

   Nome

   Un tag opzionale per il set di opzioni.

   Nome dominio

   Il nome completo della tua directory, ad esempio `corp.example.com`.

   Server dei nomi di dominio (DNS)

   Gli indirizzi IP dei server DNS della directory AWS fornita dall'utente.

   > **Note**
   >
   > Puoi trovare questi indirizzi accedendo al riquadro di navigazione della console AWS Directory Service, selezionando Directory e quindi l'ID directory corretto.

   Server NTP

   Lasciare questo campo vuoto.

   Server dei nomi NetBIOS

   Lasciare questo campo vuoto.

   Tipo di nodo NetBIOS

   Lasciare questo campo vuoto.
4. Selezionare Create DHCP options set (Crea set di opzioni DHCP). Il nuovo set di opzioni DHCP viene visualizzato nell'elenco delle opzioni DHCP.
5. Prendi nota dell'ID del nuovo set di opzioni DHCP (dopt-). *xxxxxxxx* Devi utilizzarlo per associare il nuovo set di opzioni al tuo VPC.

Modifica del set opzioni DHCP associato a un VPC

Dopo aver creato un set di opzioni DHCP, non puoi modificarle. Se desideri che il tuo VPC utilizzi un altro set di opzioni DHCP, devi creare un nuovo set e associarlo al tuo VPC. Puoi anche impostare il tuo VPC senza utilizzare alcuna opzione DHCP.

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegli Your. VPCs
3. Seleziona il VPC, quindi scegli Azioni, Modifica impostazioni VPC.
4. Per il set di opzioni DHCP, seleziona un set di opzioni o scegli Nessun set di opzioni DHCP, quindi scegli Salva.

Per modificare il set di opzioni DHCP associato a un VPC utilizzando la riga di comando, vedere quanto segue:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Gestione di utenti e gruppi in AWS Managed Microsoft AD

Puoi gestire utenti e gruppi in AWS Managed Microsoft AD. Crei un utente per rappresentare una persona o un'entità che può accedere alla tua directory. Puoi anche creare un gruppo per concedere e negare le autorizzazioni a più di un utente alla volta. È possibile aggiungere non solo utenti a un gruppo, ma anche gruppi a un gruppo. Quando aggiungi un utente a un gruppo, l'utente eredita i ruoli e le autorizzazioni assegnati al gruppo. Quando si aggiunge un gruppo a un gruppo, i gruppi condividono una relazione padre-figlio, in base alla quale il gruppo figlio eredita i ruoli e le autorizzazioni assegnati al gruppo principale. Puoi anche copiare le appartenenze ai gruppi di un utente in un altro utente.

È possibile gestire utenti e gruppi the section called “Dati del Directory Service” utilizzando i seguenti metodi:

- Console di gestione AWS
- AWS CLI
- AWSAPI dei dati del servizio Directory Service
- AWS Tools for Windows PowerShell

Per una dimostrazione della AWS Directory Service Data CLI, guarda il YouTube seguente video.

Gestisci utenti e gruppi in AWS Managed Microsoft AD utilizzando CRUD APIs

In alternativa, puoi utilizzare un'istanza aggiunta a un dominio.

Gestisci utenti e gruppi con Console di gestione AWS

Puoi gestire utenti e gruppi Console di gestione AWS con AWS Directory Service Data. Directory Service Data è un'estensione Directory Service che offre la possibilità di eseguire attività di gestione degli oggetti integrate. Alcune di queste attività includono la creazione di utenti e gruppi e l'aggiunta di utenti ai gruppi e di gruppi a un gruppo.

Per ulteriori informazioni, vedere AWSGestire utenti e gruppi di Microsoft AD gestiti con Console di gestione AWS.

> **Note**
>
> Per utilizzare questa funzionalità, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi.
> Puoi gestire utenti e gruppi solo utilizzando la Console di gestione AWS cartella principale Regione AWS della tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
> Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.

Gestisci utenti e gruppi con AWS CLI

Puoi gestire utenti e gruppi con AWS CLI la AWSDirectory Service Data API. Directory Service Data è un'estensione Directory Service che offre la possibilità di eseguire attività integrate di gestione degli oggetti utilizzando il `ds-data` namespace. Alcune di queste attività includono la creazione di utenti e gruppi e l'aggiunta di utenti ai gruppi e di gruppi a un gruppo.

Crea un utente con AWS Directory Service Data CLI

Di seguito è riportato un AWS CLI comando di esempio che utilizza lo spazio dei `ds-data` nomi per creare un utente.

```
aws ds-data create-user --directory-id d-1234567890 --sam-account-name "jane.doe" --
region your-Primary-Region-name
```

> **Note**
>
> Per utilizzarloAWS CLI, deve essere abilitato. Per ulteriori informazioni, consulta Abilitazione o disabilitazione della gestione di utenti e gruppi o dei dati del AWS Directory Service.
> Puoi gestire utenti e gruppi solo con la CLI dei dati del AWS Directory Service dalla principale Regione AWS della tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
> Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare AWS policy gestite come. AWSpolitica gestita: AWSDirectoryServiceDataFullAccessoppure. Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta la sezione Best practice per la sicurezza in IAM

Per ulteriori informazioni, vedere AWSGestire utenti e gruppi di Microsoft AD gestiti con AWS CLI.

Gestisci utenti e gruppi con AWS Strumenti per PowerShell

AWS Strumenti per PowerShellFornisce due moduli separati per la gestioneAWS Directory Service: `AWS.Tools.DirectoryService` (DS) e `AWS.Tools.DirectoryServiceData` (DSD). Quando lavori conAWS Directory Service, assicurati di utilizzare il modulo appropriato per l'operazione prevista.

- Il `DirectoryService` modulo contiene cmdlet per la gestione della configurazione e dell'amministrazione dei servizi di directory, inclusi cmdlet come`Enable-DSDirectoryDataAccess`, e. `Disable-DSDirectoryDataAccess` `Reset-DSUserPassword`
- Il `DirectoryServiceData` modulo contiene cmdlet per l'esecuzione di operazioni all'interno di una directory, incentrati in particolare sulla gestione di utenti e gruppi. Questi cmdlet DSD

includono operazioni di gestione degli utenti (`New-DSDUser`,`Get-DSDUser`, e`Remove-DSDUser`)`Update-DSDUser`, operazioni di gestione dei gruppi (`New-DSDGroup`, and,`Remove-DSDGroup`) `Get-DSDGroup`Update-DSDGroup, gestione delle appartenenze ai gruppi (e`Remove-DSDGroupMember`) e `Add-DSDGroupMember` funzionalità di ricerca (and). `Search-DSDUser` `Search-DSDGroup`

Gestisci utenti e gruppi con un'istanza locale o un'istanza Amazon EC2

Se i AWS Directory Service Data non supportano il tuo caso d'uso, ti consigliamo di gestire utenti e gruppi con un'istanza o EC2 un'istanza locale.

Per creare utenti e gruppi in un AWS Managed Microsoft AD, puoi utilizzare qualsiasi istanza (locale o EC2) aggiunta al tuo AWS Managed Microsoft AD. È necessario accedere come utente con privilegi per creare utenti e gruppi. Dovrai anche installare gli strumenti di Active Directory sull'istanza in modo da poter aggiungere utenti e gruppi con lo strumento Utenti e computer di Active Directory.

- È possibile distribuire un' EC2 istanza preconfigurata con strumenti di amministrazione di Active Directory preinstallati dalla Directory Service console di gestione. Per ulteriori informazioni, consulta Avvio di un'istanza di amministrazione delle directory in AWS Managed Microsoft AD Active Directory.
- Se è necessario distribuire un' EC2 istanza autogestita con strumenti amministrativi e installare gli strumenti necessari, consulta. Fase 3: Implementa un' EC2 istanza Amazon per gestire il tuo AWS Managed Microsoft AD Active Directory

Argomenti

- AWSGestisci utenti e gruppi di Microsoft AD gestiti con Console di gestione AWSAWS CLI, o AWS Strumenti per PowerShell
- Gestisci utenti e gruppi con un' EC2 istanza Amazon

AWSGestisci utenti e gruppi di Microsoft AD gestiti con Console di gestione AWSAWS CLI, o AWS Strumenti per PowerShell

Puoi usare Console di gestione AWSAWS CLI, o AWS Strumenti per PowerShell per gestire gli utenti e i gruppi di Microsoft AD AWS gestito conAWS Dati del Directory Service. La AWS Directory Service Data CLI utilizza lo spazio dei `ds-data` nomi. Per ulteriori informazioni suAWS CLI, vedere Guida

introduttiva a. AWS CLI Per ulteriori informazioni suAWS Strumenti per PowerShell, consulta la Guida AWS Strumenti per PowerShell per l'utente.

Per ulteriori informazioni sulla creazione, la visualizzazione, l'aggiornamento e l'eliminazione di utenti e gruppi di Microsoft AD AWS gestiti, vedere le procedure seguenti.

Procedure di gestione di utenti e gruppi

- Abilitazione o disabilitazione della gestione di utenti e gruppi o dei dati del AWS Directory Service
- Creazione di un utente Microsoft AD AWS gestito
- Visualizzazione e aggiornamento di un utente di Microsoft AD AWS gestito
- Eliminazione di un AWS utente Microsoft AD gestito
- Disabilitazione di un utente di Microsoft AD AWS gestito
- Reimpostazione e attivazione della password di un utente AWS Microsoft AD gestito
- Creazione di un gruppo Microsoft AD AWS gestito
- Visualizzazione e aggiornamento dei dettagli di un gruppo AWS Managed Microsoft AD
- Eliminazione di un AWS gruppo Microsoft AD gestito
- Aggiungere e rimuovere membri di AWS Managed Microsoft AD ai gruppi e ai gruppi
- Copiare le appartenenze AWS a un gruppo Microsoft AD gestito nel Console di gestione AWS

Abilitazione o disabilitazione della gestione di utenti e gruppi o dei dati del AWS Directory Service

Per utilizzare la gestione di utenti e gruppi o i dati del AWS Directory Service, è necessario abilitarla. Una volta abilitata, è possibile gestire utenti e gruppi da Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

> **Important**
>
> - Puoi abilitare questa funzionalità solo dalla cartella principale Regione AWS della tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
> - Per un elenco delle aree che supportano i dati del AWS Directory Service, vedereSupportato Regioni AWS per i dati del Directory Service.
> - I controlli di accesso per i dati dei Servizi di AWS Directory sono diversi dai controlli di accesso per Servizi AWS Amazon WorkSpaces, Amazon Quick Suite e Amazon WorkMail.

Per ulteriori informazioni, consulta AWSautorizzazione dell'applicazione con Directory Service Data.

Abilitazione dei dati del AWS Directory Service

Utilizzare la procedura seguente per abilitare la gestione di utenti e gruppi o i dati di AWS Directory Service per un AWS Managed Microsoft AD esistente con Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Console di gestione AWS

È possibile abilitare la gestione di utenti e gruppi conConsole di gestione AWS.

Per abilitare la gestione di utenti e gruppi

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina dei dettagli della Directory, per abilitare la gestione di utenti e gruppi, seleziona Abilita.
3. Nella finestra di dialogo Abilita la gestione di utenti e gruppi, seleziona Abilita.

AWS CLI

Di seguito viene descritto come formattare una richiesta che abilita la AWS Directory Service Data CLI. È necessario includere il numero di Directory ID nella richiesta.

> **Note**
>
> I comandi Enable AWS Directory Service Data CLI utilizzano. `aws ds`

Per abilitare la AWS Directory Service Data CLI

- Apri ed esegui AWS CLI il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
aws ds enable-directory-data-access --directory-id d-1234567890
```

AWS Strumenti per PowerShell

Per abilitare i dati del servizio di Directory Service with Tools for PowerShell

- Apri PowerShell ed esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
Enable-DSDirectoryDataAccess -DirectoryId d-1234567890
```

Disabilitazione dei dati del AWS Directory Service

Utilizzare la procedura seguente per disabilitare la gestione di utenti e gruppi o i dati di AWS Directory Service per un AWS Managed Microsoft AD esistente con Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Console di gestione AWS

È possibile disabilitare la gestione di utenti e gruppi conConsole di gestione AWS.

Per disabilitare la gestione di utenti e gruppi

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina dei dettagli della directory, per disabilitare la gestione di utenti e gruppi, seleziona Disabilita.
3. Nella finestra di dialogo Disabilita la gestione di utenti e gruppi, seleziona Disabilita.

AWS CLI

Di seguito viene descritto come formattare una richiesta che disabilita la AWS Directory Service Data CLI. È necessario includere il numero di Directory ID nella richiesta.

> **Note**
>
> I comandi di disabilitazione utilizzati dalla CLI del AWS Directory Service Data. `aws ds`

Per disabilitare la CLI dei dati del AWS Directory Service

- Apri ed esegui AWS CLI il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
aws ds disable-directory-data-access --directory-id d-1234567890
```

AWS Strumenti per PowerShell

Per disabilitare i dati del Directory Service with Tools for PowerShell

- Apri PowerShell ed esegui il comando seguente, sostituendo l'ID di directory con il tuo ID di directory Microsoft AD AWS gestito:

```
Disable-DSDirectoryDataAccess -DirectoryId d-123456789
```

Creazione di un utente Microsoft AD AWS gestito

Utilizzare la procedura seguente per creare un nuovo utente Microsoft AD AWS gestito con gestione di utenti e gruppi o AWS Directory Service Data in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.

Console di gestione AWS

È possibile creare un nuovo account utente Microsoft AD AWS gestito inConsole di gestione AWS. Quando si crea un nuovo account utente, si specificano i dettagli del nuovo utente e si determina se aggiungere il nuovo utente a un gruppo o copiare le appartenenze al gruppo di un altro utente nel nuovo utente.

Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

Per creare un utente AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Nella pagina dei dettagli della Directory, nella sezione Utenti, scegli Crea account utente.
5. Viene visualizzata la pagina Specificare i dettagli dell'utente. Nella sezione Informazioni richieste, immettere un nome utente e una password di accesso. I nomi di accesso utente devono soddisfare le seguenti condizioni:
   - Deve essere un nome di accesso univoco
   - Può contenere fino a 20 caratteri
   - Può contenere solo caratteri alfanumerici
   - ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
   - La password deve rispettare i requisiti della politica in materia di password. Rivolgiti al tuo AWS amministratore per ulteriori informazioni.

> **Warning**
>
> Il nome di accesso utente non può essere modificato dopo la creazione dell'utente.

a. (Facoltativo) Nella sezione Informazioni principali, puoi inserire un nome e un cognome per l'utente. Puoi anche inserire un nome visualizzato e una descrizione per l'utente.

b. (Facoltativo) Nella sezione Metodi di contatto, puoi inserire un indirizzo e-mail e i numeri di telefono dell'utente.

c. (Facoltativo) Nella sezione Informazioni relative alla mansione, puoi inserire un reparto, un responsabile, un ufficio e una società per l'utente.

d. (Facoltativo) Nella sezione Indirizzo, puoi inserire un indirizzo per l'utente.

e. (Facoltativo) Nella sezione Impostazioni dell'account, puoi inserire note, una lingua preferita e il nome principale del servizio per l'utente.

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la Microsoftdocumentazione.

6. Scegli Avanti dopo aver fornito i dettagli dell'account utente.
7. Nella pagina Aggiungi utenti ai gruppi - opzionale, puoi aggiungere l'utente a un nuovo gruppo o a un gruppo esistente. Puoi anche copiare l'appartenenza al gruppo di un utente esistente nel nuovo utente. Se non desideri aggiungere un utente a un gruppo, scegli Avanti. Vai al passaggio 12 per continuare questa procedura.
8. (Facoltativo) Per creare un nuovo gruppo, vedi Creare un gruppo Microsoft AD AWS gestito.
9. (Facoltativo) Per aggiungere un nuovo utente a un gruppo esistente:

   - Seleziona il gruppo a cui desideri aggiungere il nuovo utente nella sezione Gruppi. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca.

10. (Facoltativo) Per copiare l'appartenenza al gruppo di un utente esistente in un nuovo utente:

    a. Scegli la scheda Copia l'appartenenza al gruppo dall'utente. Per trovare un utente con un'appartenenza al gruppo che desideri copiare, inserisci il nome di accesso utente nella casella di ricerca nella sezione Utenti.

    b. Nella sezione Gruppi selezionati, seleziona i gruppi di cui il nuovo utente deve diventare membro.

11. Scegli Avanti quando sei pronto per creare il nuovo account utente.
12. Nella pagina Rivedi e crea utente, rivedi tutte le scelte che hai fatto. Selezionare Create user (Crea utente).
13. Dopo aver configurato l'utente, sei passato alla pagina dei dettagli del nuovo utente. Viene visualizzato un banner che indica che l'utente è stato creato correttamente.

> **Important**
>
> Se ricevi un messaggio di errore che ti informa che non sei autorizzato a creare un utente, segui le istruzioni contenute nel messaggio di errore per richiedere che l'amministratore ti conceda l'accesso.

AWS CLI

Di seguito viene descritto come formattare una richiesta che crea un nuovo account utente di Microsoft AD AWS gestito con la AWS Directory Service Data CLI. È necessario includere il numero ID della directory e un nome di accesso utente nella richiesta. È inoltre possibile includere altri attributi, ad esempio un nome visualizzato dall'utente con l'`DisplayName`attributo. Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

Per creare un utente AWS Managed Microsoft AD con AWS CLI

- Aprire ed eseguire il comando seguente, sostituendo l'ID directory, il nome utente e il nome visualizzato con l'ID AWS Managed Microsoft AD Directory e le credenziali desiderate: AWS CLI

```
aws ds-data create-user \
  --directory-id d-1234567890 \
  --sam-account-name "jane.doe" \
  --other-attributes '{
    "DisplayName" : { "S": "jane.doe"},
    "Department":{ "S": "Legal"}
    }‘
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che crea un nuovo account utente Microsoft AD AWS gestito conAWS Strumenti per PowerShell. È necessario includere il numero ID della directory e un nome di accesso utente nella richiesta. È inoltre possibile includere altri attributi, ad esempio un nome visualizzato dall'utente con l'`DisplayName`attributo. Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

Per creare un utente AWS Managed Microsoft AD con Tools for PowerShell

- Apri PowerShell ed esegui il comando seguente, sostituendo l'ID directory, il nome utente e il nome visualizzato con l'ID AWS Managed Microsoft AD Directory e le credenziali desiderate:

```
New-DSDUser `
    -DirectoryId d-1234567890 `
    -SAMAccountName "jane.doe" `
    -OtherAttribute @{
        DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'jane.doe' }
        Department = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'Legal' }
    }
```

Visualizzazione e aggiornamento di un utente di Microsoft AD AWS gestito

Utilizzare la procedura seguente per visualizzare o aggiornare i dettagli di un utente di Microsoft AD AWS gestito con la gestione di utenti e gruppi o i dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Visualizzazione dei dettagli di un utente di AWS Managed Microsoft AD

È possibile visualizzare i dettagli di un utente in Console di gestione AWS oAWS CLI. I dettagli dell'utente includono informazioni sul profilo e sull'account e l'appartenenza al gruppo.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come

o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.

- Creazione di un utente Microsoft AD AWS gestito.

Console di gestione AWS

È possibile visualizzare i dettagli di un utente di Microsoft AD AWS gestito inConsole di gestione AWS.

Per visualizzare i dettagli di un utente di Microsoft AD AWS gestito e i dettagli dell'account con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Users (Utenti). La scheda mostra un elenco di utenti presenti nella tua directory.
5. Seleziona un utente. Verrai indirizzato alla schermata dei dettagli utente. La schermata dei dettagli utente mostra le seguenti informazioni:

   - Gruppi di cui l'utente è membro (appartenenze ai gruppi)
   - Dettagli del profilo (come informazioni primarie come nome di accesso dell'utente, nome, cognome, ecc.)
   - Impostazioni dell'account (ad esempio informazioni sull'account come nome principale dell'utente, nome principale del servizio, nome distinto, ecc.)
   - Stato dell'account

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la Microsoftdocumentazione.

AWS CLI

ConAWS CLI, puoi visualizzare i dettagli di un utente, tra cui informazioni sul profilo e sull'account e l'appartenenza ai gruppi.

Per visualizzare il profilo e i dettagli dell'account di un utente di Microsoft AD AWS gestito con AWS CLI

Di seguito viene descritto come visualizzare i dettagli di un utente di AWS Managed Microsoft AD con la AWS Directory Service Data CLI.

- Per visualizzare i dettagli di un utente, apri ed esegui il AWS CLI comando seguente, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
aws ds-data describe-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Per visualizzare le appartenenze ai gruppi di un utente

Di seguito viene descritto come visualizzare l'appartenenza al gruppo di un utente Microsoft AD AWS gestito con la AWS Directory Service Data CLI.

- Per visualizzare le appartenenze ai gruppi di un utente, apri ed esegui il comando seguenteAWS CLI, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
aws ds-data list-groups-for-member --directory-id d-1234567890 --sam-account-name
 "jane.doe"
```

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la Microsoftdocumentazione.

AWS Strumenti per PowerShell

Con Tools for PowerShell, puoi visualizzare i dettagli di un utente, tra cui informazioni sul profilo e sull'account e l'appartenenza ai gruppi.

Per visualizzare il profilo e i dettagli dell'account di un utente di Microsoft AD AWS gestito con Tools for PowerShell

Di seguito viene descritto come visualizzare i dettagli di un utente di Microsoft AD AWS gestito con gli strumenti per PowerShell.

- Per visualizzare i dettagli di un utente, apri ed esegui il PowerShell comando seguente, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
Get-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Per visualizzare le appartenenze ai gruppi di un utente

Di seguito viene descritto come visualizzare l'appartenenza al gruppo di un utente Microsoft AD AWS gestito con gli Strumenti per PowerShell.

- Per visualizzare le appartenenze ai gruppi di un utente, apri ed esegui il comando seguentePowerShell, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
(Get-DSDGroupsForMemberList -DirectoryId d-1234567890 -SAMAccountName
 "jane.doe").Groups
```

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la Microsoftdocumentazione.

Aggiornamento dei dettagli di un utente di AWS Managed Microsoft AD

Utilizzare la procedura seguente per aggiornare un utente di Microsoft AD AWS gestito con la gestione di utenti e gruppi o i dati di AWS Directory Service inConsole di gestione AWS,AWS CLI,AWS Strumenti per PowerShell.

> **Note**
>
> La lunghezza minima dell'attributo è 1.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.

- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Creazione di un utente Microsoft AD AWS gestito.

Console di gestione AWS

È possibile aggiornare i dettagli di un utente di AWS Managed Microsoft AD inConsole di gestione AWS.

Per aggiornare i dettagli di un utente di AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Users (Utenti). La scheda mostra un elenco di utenti presenti nella tua directory.
5. Seleziona un utente. Per trovare un utente, inserisci il nome di accesso dell'utente nella casella di ricerca nella sezione Utenti. Verrai indirizzato alla schermata dei dettagli utente.
6. Per modificare i gruppi di cui l'utente è membro, scegli Gruppi. Da questa scheda, puoi aggiungere e rimuovere l'utente dai gruppi. Per ulteriori informazioni, vedere Aggiungere un membro di AWS Managed Microsoft AD a un gruppo.

7. Per modificare i dettagli del profilo dell'utente, scegli Profilo, quindi scegli Modifica. Oppure scegli Azioni, quindi scegli Modifica utente. Effettua e rivedi gli aggiornamenti, quindi scegli Salva.

   > **Warning**
   >
   > Il nome di accesso utente non può essere modificato dopo la creazione dell'utente.

8. Per modificare le impostazioni dell'account dell'utente, scegli Impostazioni dell'account utente. Oppure scegli Azioni, quindi scegli Modifica utente. Effettua e rivedi gli aggiornamenti, quindi scegli Salva.

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la Microsoftdocumentazione.

AWS CLI

Di seguito viene descritto come formattare una richiesta che aggiorna i dettagli di un utente di Microsoft AD AWS gestito con AWS Directory Service Data CLI.

Quando si aggiorna l'account di un utente, è necessario includere il numero ID della directory e il nome di accesso utente. È inoltre necessario includere il tipo di aggiornamento e l'attributo che si desidera aggiornare nella richiesta, ad esempio il cognome dell'utente con il `Surname` parametro. Per ulteriori informazioni, vedere Attributi dei dati del servizio di AWS Directory Service.

- Per aggiornare i dettagli di un utente, apri ed esegui il comando seguenteAWS CLI, sostituendo l'ID directory, il nome utente, il tipo di utente e il valore dell'attributo con l'ID AWS Managed Microsoft AD Directory, il nome utente e il tipo di utente e il valore dell'attributo desiderati:

```
aws ds-data update-user --directory-id d-1234567890 --sam-account-name "jane.doe" --
update-type "REPLACE" --surname "Doe"
```

> **Note**
>
> Quando si rimuovono gli attributi utente con il comando CLI update-user, è necessario specificare l'attributo e il valore esatto da rimuovere. Per determinare gli attributi dell'utente, usa il comando describe-user.

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la documentazione. Microsoft

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che aggiorna i dettagli di un utente di Microsoft AD AWS gestito conAWS Strumenti per PowerShell.

Quando si aggiorna l'account di un utente, è necessario includere il numero ID della directory e il nome di accesso utente. È inoltre necessario includere il tipo di aggiornamento e l'attributo che si desidera aggiornare nella richiesta, ad esempio il cognome dell'utente con il `Surname` parametro. Per ulteriori informazioni, vedere Attributi dei dati del servizio di AWS Directory Service.

- Per aggiornare i dettagli di un utente, apri ed esegui il comando seguentePowerShell, sostituendo l'ID directory, il nome utente, il tipo di utente e il valore dell'attributo con l'ID AWS Managed Microsoft AD Directory, il nome utente e il tipo di utente e il valore dell'attributo desiderati:

```
Update-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe" -UpdateType
 "REPLACE" -Surname "Doe"
```

Per ulteriori informazioni sugli attributi utente, consulta AWSAttributi dei dati del Directory Service la Microsoftdocumentazione.

Eliminazione di un AWS utente Microsoft AD gestito

Utilizzare la procedura seguente per eliminare un utente di Microsoft AD AWS gestito con gestione di utenti e gruppi o AWS Directory Service Data in Console di gestione AWSAWS CLI,AWS Strumenti per PowerShell.

> **Important**
>
> Quando si elimina l'account di un utente da una directory, vengono rimosse tutte le informazioni sull'utente, incluse le autorizzazioni di cui dispone l'utente per accedere al proprio account e alle proprie applicazioni.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Creazione di un utente Microsoft AD AWS gestito.

Console di gestione AWS

È possibile eliminare un account utente Microsoft AD AWS gestito inConsole di gestione AWS.

Per eliminare un account utente Microsoft AD AWS gestito con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Users (Utenti). La scheda mostra un elenco di utenti presenti nella tua directory.
5. Scegli l'utente di cui desideri eliminare l'account. Per trovare un utente, inserisci il nome di accesso utente nella casella di ricerca nella sezione Utenti. Verrai indirizzato alla schermata dei dettagli utente.
6. Scegli Azioni. Quindi scegli Elimina account utente e Elimina nuovamente l'account utente.

AWS CLI

Di seguito viene descritto come formattare una richiesta che elimina un account utente di Microsoft AD AWS gestito con la AWS Directory Service Data CLI.

Per eliminare un account utente Microsoft AD AWS gestito con AWS CLI

- Aprire ed eseguire il AWS CLI comando seguente, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
aws ds-data delete-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che elimina un account utente di Microsoft AD AWS gestito conAWS Strumenti per PowerShell.

Per eliminare un account utente Microsoft AD AWS gestito con AWS Strumenti per PowerShell

- Apri PowerShell ed esegui il comando seguente, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
Remove-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Disabilitazione di un utente di Microsoft AD AWS gestito

Utilizzare la procedura seguente per disabilitare un utente di Microsoft AD AWS gestito con la gestione di utenti e gruppi o i dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

> **Important**
>
> Quando si disattiva l'account di un utente, l'utente perde tutte le autorizzazioni di accesso all'account e alle applicazioni.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Creazione di un utente Microsoft AD AWS gestito.

Console di gestione AWS

È possibile disabilitare un account utente Microsoft AD AWS gestito inConsole di gestione AWS.

Per disabilitare un account utente Microsoft AD AWS gestito con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Users (Utenti). La scheda mostra un elenco di utenti presenti nella tua directory.
5. Scegli l'utente di cui desideri disabilitare l'account. Verrai indirizzato alla schermata dei dettagli utente.
6. Scegli Azioni. Quindi scegli Disabilita l'account utente e Disabilita nuovamente l'account utente.

> **Note**
>
> Per riattivare l'account dell'utente, è necessario reimpostare la password dell'utente. Per ulteriori informazioni, consulta Reimpostazione e attivazione della password di un utente AWS Microsoft AD gestito.

AWS CLI

Di seguito viene descritto come formattare una richiesta che disabilita un account utente di Microsoft AD AWS gestito con la AWS Directory Service Data CLI.

Per disabilitare un account utente Microsoft AD AWS gestito con AWS CLI

- Aprire ed eseguire il AWS CLI comando seguente, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
aws ds-data disable-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

> **Note**
>
> Per riattivare l'account utente, è necessario reimpostare la password dell'utente. Per ulteriori informazioni, consulta Reimpostazione e attivazione della password di un utente AWS Microsoft AD gestito.

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che disabilita un account utente di Microsoft AD AWS gestito conAWS Strumenti per PowerShell.

Per disabilitare un account utente Microsoft AD AWS gestito con AWS Strumenti per PowerShell

- ApriPowerShell; ed esegui il comando seguente, sostituendo l'ID directory e il nome utente con l'ID e il nome utente di AWS Managed Microsoft AD Directory:

```
Disable-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

> **Note**
>
> Per riattivare l'account utente, è necessario reimpostare la password dell'utente. Per ulteriori informazioni, consulta Reimpostazione e attivazione della password di un utente AWS Microsoft AD gestito.

Reimpostazione e attivazione della password di un utente AWS Microsoft AD gestito

Utilizzare la procedura seguente per reimpostare la password di un utente Microsoft AD AWS gestito e abilitare il relativo account con la gestione di utenti e gruppi o i dati di AWS Directory Service inConsole di gestione AWS,AWS CLI,AWS Strumenti per PowerShell.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Creazione di un utente Microsoft AD AWS gestito.

Console di gestione AWS

È possibile reimpostare la password di un utente Microsoft AD AWS gestito per abilitare il relativo account inConsole di gestione AWS. È possibile eseguire questa operazione dalla schermata Directory o dalla schermata dei dettagli della directory.

Directory

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli Azioni, quindi scegli Reimposta la password utente e abilita l'account.
    a. In Nome di accesso utente, inserisci il nome di accesso utente dell'utente di cui desideri reimpostare la password.
    b. In Nuova password, inserisci la nuova password dell'utente.
    c. In Conferma password, inserisci nuovamente la nuova password dell'utente.
4. Dopo aver confermato la nuova password dell'utente, scegli Reimposta la password e abilita l'account.

Dettagli della rubrica

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Users (Utenti). La scheda mostra un elenco di utenti presenti nella tua directory.
5. Seleziona l'utente di cui desideri reimpostare la password.
6. Scegli Azioni, quindi scegli Reimposta la password utente e abilita l'account.
    a. In Nuova password, inserisci la nuova password dell'utente.
    b. In Conferma password, inserisci nuovamente la nuova password dell'utente.
7. Dopo aver confermato la nuova password dell'utente, scegli Reimposta la password e abilita l'account.

AWS CLI

Puoi reimpostare la password di un utente di AWS Managed Microsoft AD per abilitarne l'account con la AWS Directory Service Data CLI.

> **Note**
>
> Il comando di reimpostazione della password dell'utente utilizza`aws ds`.

Per reimpostare la password di un utente di Microsoft AD AWS gestito con AWS CLI

- Per reimpostare la password di un utente, apri ed esegui il comando seguente, sostituendo l'ID directory, il nome utente e la password con l'ID AWS Managed Microsoft AD Directory, il nome utente e le credenziali desiderate: AWS CLI

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "your-password"
```

AWS Strumenti per PowerShell

Puoi reimpostare la password di un utente di Microsoft AD AWS gestito con cui abilitare il suo accountAWS Strumenti per PowerShell.

Per reimpostare la password di un utente di Microsoft AD AWS gestito con AWS Strumenti per PowerShell

- Per reimpostare la password di un utente, apri ed esegui il comando seguente, sostituendo l'ID directory, il nome utente e la password con l'ID AWS Managed Microsoft AD Directory, il nome utente e le credenziali desiderate: PowerShell

```
Reset-DSUserPassword -DirectoryId d-1234567890 -UserName "jane.doe" -NewPassword
 "your-password"
```

Creazione di un gruppo Microsoft AD AWS gestito

Utilizzare la procedura seguente per creare un gruppo Microsoft AD AWS gestito con gestione di utenti e gruppi o AWS Directory Service Data in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.

Console di gestione AWS

È possibile creare un nuovo gruppo AWS Managed Microsoft AD inConsole di gestione AWS. Quando si crea un nuovo gruppo, si specificano i dettagli del gruppo e si determina il tipo e l'ambito del gruppo. Hai anche la possibilità di aggiungere utenti e gruppi di bambini al nuovo gruppo o aggiungere il nuovo gruppo a un gruppo di genitori.

Per creare un gruppo AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.

4. Scegli Gruppo. La scheda mostra un elenco di gruppi del tuoRegione AWS.
5. Seleziona Crea gruppo. Verrai indirizzato a una procedura in cui finirai di creare il tuo nuovo gruppo.
6. Viene visualizzata la pagina Specificare i dettagli del gruppo. Immettere un nome per il gruppo. I nomi dei gruppi devono soddisfare le seguenti condizioni:

   - Deve essere un nome di gruppo univoco
   - Può contenere fino a 64 caratteri
   - Può contenere solo caratteri alfanumerici
   - ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

   > ⚠ Warning
   >
   > Il nome del gruppo non può essere modificato dopo la creazione del gruppo.

7. Scegli il tipo di gruppo tra uno dei seguenti:

   - Sicurezza
   - Distribution (Distribuzione)
     - Per ulteriori informazioni, consulta the section called “Tipo gruppo”.
8. Scegli l'ambito del gruppo tra uno dei seguenti:

   - Dominio locale
   - Universale
   - Globale
     - È possibile attivare Confronta ambiti per visualizzare un grafico delle somiglianze e delle differenze tra gli ambiti di gruppo. Per ulteriori informazioni, consulta the section called “Ambito del gruppo”.
9. Dopo aver fornito le informazioni principali e i metodi di contatto, scegli Avanti.
10. Viene visualizzata la pagina Aggiungi utenti al gruppo - Facoltativo e puoi aggiungere utenti al nuovo gruppo. Per trovare un utente da aggiungere al gruppo, inserisci il nome di accesso dell'utente nella casella di ricerca nella sezione Utenti. Seleziona gli utenti che desideri aggiungere al gruppo e scegli Avanti.

11. Viene visualizzata la pagina Aggiungi gruppi di bambini - Facoltativo e puoi aggiungere gruppi esistenti al nuovo gruppo. I gruppi esistenti diventano gruppi figli del gruppo appena creato. Quando aggiungi un gruppo di bambini al tuo gruppo, il gruppo diventa il gruppo di genitori e il gruppo di bambini eredita tutti i ruoli e le autorizzazioni del gruppo. Per trovare i gruppi da aggiungere, inserisci il nome del gruppo nella casella di ricerca nella sezione Aggiungi gruppi di bambini. Seleziona i gruppi di bambini che desideri aggiungere al nuovo gruppo e scegli Avanti.
12. Viene visualizzata la pagina Aggiungi gruppi di genitori - Opzionale e puoi aggiungere il nuovo gruppo ai gruppi esistenti. Il nuovo gruppo diventa il gruppo principale dei gruppi esistenti. Quando aggiungi il tuo gruppo a un gruppo di genitori, il gruppo diventa il gruppo figlio e eredita tutti i ruoli e le autorizzazioni del gruppo di genitori. Per trovare i gruppi da aggiungere, inserisci il nome del gruppo nella casella di ricerca nella sezione Aggiungi gruppi principali. Seleziona i gruppi principali che desideri aggiungere al nuovo gruppo e scegli Avanti.
13. Nella pagina Rivedi e crea gruppo, rivedi le tue scelte, quindi scegli Crea gruppo.

AWS CLI

Di seguito viene descritto come formattare una richiesta che crea un gruppo AWS Managed Microsoft AD con la AWS Directory Service Data CLI. Quando crei un nuovo gruppo, devi includere il tuo numero di Directory ID e il nome del gruppo. È inoltre possibile aggiungere altri attributi, ad esempio un nome di visualizzazione del gruppo con l'`DisplayName`attributo. Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

Per creare un gruppo AWS Managed Microsoft AD con AWS CLI

- Aprire ed eseguire il AWS CLI comando seguente, sostituendo l'ID directory, il nome utente e il nome visualizzato del gruppo con l'ID AWS Managed Microsoft AD Directory, il nome utente e il nome visualizzato del gruppo desiderato:

```
aws ds-data create-group \
    --directory-id d-1234567890 \
    --sam-account-name "your-group-name" \
    --other-attributes '{
        "DisplayName": { "S": "myGroupDisplayName"}
        "Description":{ "S": "myGroupDescription"}
```

```
    }'
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che crea un gruppo Microsoft AD AWS gestito conAWS Strumenti per PowerShell. Quando crei un nuovo gruppo, devi includere il tuo numero di Directory ID e il nome del gruppo. È inoltre possibile aggiungere altri attributi, ad esempio un nome di visualizzazione del gruppo con l'`DisplayName`attributo. Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

Per creare un gruppo AWS Managed Microsoft AD con AWS Strumenti per PowerShell

- Apri PowerShell ed esegui il comando seguente, sostituendo l'ID directory, il nome utente e il nome visualizzato del gruppo con l'ID AWS Managed Microsoft AD Directory, il nome utente e il nome visualizzato del gruppo desiderato:

```
New-DSDGroup `
    -DirectoryId d-1234567890 `
    -SAMAccountName "your-group-name" `
    -OtherAttribute @{
        DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'myGroupDisplayName' }
        Description = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
 'myGroupDescription' }
    }
```

Visualizzazione e aggiornamento dei dettagli di un gruppo AWS Managed Microsoft AD

Utilizzare la procedura seguente per visualizzare o aggiornare i dettagli di un gruppo Microsoft AD AWS gestito con la gestione di utenti e gruppi o i dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Visualizzazione dei dettagli di un gruppo Microsoft AD AWS gestito

Puoi visualizzare o aggiornare i dettagli di un gruppo in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Creazione di un gruppo Microsoft AD AWS gestito.

Console di gestione AWS

È possibile visualizzare i dettagli di un gruppo Microsoft AD AWS gestito inConsole di gestione AWS.

Per visualizzare i dettagli del gruppo AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegli Gruppo. La scheda mostra un elenco di gruppi del tuoRegione AWS.
5. Scegli un gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. Verrai indirizzato alla schermata dei dettagli del gruppo. La schermata dei dettagli del gruppo mostra le seguenti informazioni:
   - La scheda Membri elenca gli utenti e i gruppi di bambini che sono membri del gruppo.

- La scheda Gruppi di genitori elenca i gruppi principali di cui il gruppo è membro.
- La scheda Proprietà elenca le proprietà del gruppo (come le informazioni principali come il nome del gruppo, il nome visualizzato del gruppo, ecc.).

AWS CLI

Puoi visualizzare i dettagli di un gruppo AWS Managed Microsoft AD con la AWS Directory Service Data CLI.

Per visualizzare i dettagli di un gruppo AWS Managed Microsoft AD con AWS CLI

Di seguito viene descritto come visualizzare i dettagli di un gruppo Microsoft AD AWS gestito conAWS CLI.

- Per visualizzare i dettagli di un gruppo, apri ed esegui il comando seguente, sostituendo l'ID della directory e il nome del gruppo con l'ID e il nome del gruppo di Microsoft AD Directory AWS gestito: AWS CLI

```
aws ds-data describe-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

Per visualizzare i membri del gruppo AWS Managed Microsoft AD con AWS CLI

Di seguito viene descritto come visualizzare i membri di un gruppo Microsoft AD AWS gestito conAWS CLI.

- Per visualizzare i dettagli di un gruppo, apri ed esegui il comando seguente, sostituendo l'ID della directory e il nome del gruppo con l'ID e il nome del gruppo di Microsoft AD Directory AWS gestito: AWS CLI

```
aws ds-data list-group-members --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Strumenti per PowerShell

È possibile visualizzare i dettagli di un gruppo Microsoft AD AWS gestito conAWS Strumenti per PowerShell.

Per visualizzare i dettagli di un gruppo AWS Managed Microsoft AD con AWS Strumenti per PowerShell

Di seguito viene descritto come visualizzare i dettagli di un gruppo Microsoft AD AWS gestito con gli Strumenti per PowerShell.

- Per visualizzare i dettagli di un gruppo, apri ed esegui il comando seguente, sostituendo l'ID della directory e il nome del gruppo con l'ID e il nome del gruppo di Microsoft AD Directory AWS gestito: PowerShell

```
Get-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Per visualizzare i membri del gruppo AWS Managed Microsoft AD con AWS Strumenti per PowerShell

Di seguito viene descritto come visualizzare i membri di un gruppo Microsoft AD AWS gestito con gli Strumenti per PowerShell.

- Per visualizzare i dettagli di un gruppo, apri ed esegui il comando seguente, sostituendo l'ID della directory e il nome del gruppo con l'ID e il nome del gruppo di Microsoft AD Directory AWS gestito: PowerShell

```
(Get-DSDGroupMemberList -DirectoryId d-1234567890 -SAMAccountName "your-group-
name").Members
```

Aggiornamento dei dettagli di un gruppo AWS Managed Microsoft AD

Utilizzare la procedura seguente per aggiornare i dettagli di un gruppo Microsoft AD AWS gestito con la gestione di utenti e gruppi o i dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.

- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Creazione di un gruppo Microsoft AD AWS gestito.

Console di gestione AWS

Puoi aggiornare i dettagli di un gruppo conConsole di gestione AWS. Per ulteriori informazioni, consulta AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

Per aggiornare i dettagli di un gruppo AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegli Gruppo. La scheda mostra un elenco di gruppi del tuoRegione AWS.
5. Scegli un gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. Verrai indirizzato alla schermata dei dettagli del gruppo.
6. Per modificare gli utenti e i gruppi di bambini che sono membri del tuo gruppo, scegli Membri. Da questa scheda, puoi aggiungere e rimuovere utenti e gruppi di bambini dal tuo gruppo. Per ulteriori informazioni, consulta Aggiungere e rimuovere membri dai gruppi e dai gruppi ai gruppi.
7. Per modificare i gruppi di genitori di cui il tuo gruppo è membro, scegli Gruppi di genitori. Da questa scheda, puoi aggiungere e rimuovere il tuo gruppo dai gruppi di genitori. Per ulteriori informazioni, consulta Aggiungere e rimuovere membri dai gruppi e dai gruppi ai gruppi.

8. Per modificare le proprietà del gruppo, scegli Proprietà, quindi scegli Modifica. Oppure scegli Azioni, quindi scegli Modifica gruppo. Effettua e rivedi gli aggiornamenti, quindi scegli Salva.

AWS CLI

Di seguito viene descritto come formattare una richiesta che aggiorna i dettagli di un gruppo AWS Managed Microsoft AD con la AWS Directory Service Data CLI.

Quando si aggiorna un gruppo, è necessario includere il numero ID della directory e il nome del gruppo. È inoltre necessario includere il tipo di aggiornamento e l'attributo che si desidera aggiornare nella richiesta, ad esempio un indirizzo e-mail di gruppo con il `EmailAddress` parametro. Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

- Per aggiornare i dettagli di un gruppo AWS Managed Microsoft AD con AWS CLI

  Per aggiornare i dettagli di un gruppo, apri ed esegui il AWS CLI comando seguente, sostituendo l'ID directory, il nome del gruppo, il tipo di aggiornamento e l'attributo con l'ID AWS Managed Microsoft AD Directory, il nome del gruppo e il tipo e l'attributo di aggiornamento desiderati:

```
aws ds-data update-group --directory-id d-1234567890 --sam-account-name "your-group-name" --update-type "REPLACE" --group-scope "global"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che aggiorna i dettagli di un gruppo Microsoft AD AWS gestito conAWS Strumenti per PowerShell.

Quando aggiorni un gruppo, devi includere il numero ID della directory e il nome del gruppo. È inoltre necessario includere il tipo di aggiornamento e l'attributo che si desidera aggiornare nella richiesta, ad esempio un indirizzo e-mail di gruppo con il `EmailAddress` parametro. Per ulteriori informazioni, consultare AWSAttributi dei dati del Directory Service e Tipo di gruppo e ambito del gruppo.

- Per aggiornare i dettagli di un gruppo AWS Managed Microsoft AD con AWS Strumenti per PowerShell

  Per aggiornare i dettagli di un gruppo, apri ed esegui il PowerShell comando seguente, sostituendo l'ID directory, il nome del gruppo, il tipo di aggiornamento e l'attributo con l'ID AWS Managed Microsoft AD Directory, il nome del gruppo e il tipo e l'attributo di aggiornamento desiderati:

```
Update-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name" -
UpdateType "REPLACE" -GroupScope "global"
```

Eliminazione di un AWS gruppo Microsoft AD gestito

Utilizzare la procedura seguente per eliminare un gruppo Microsoft AD AWS gestito con gestione di utenti e gruppi o AWS Directory Service Data in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

> **Important**
>
> Quando si elimina un gruppo, vengono rimosse tutte le informazioni sul gruppo, incluse le autorizzazioni ereditate dai membri del gruppo.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS:

AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.

- Crea un gruppo AWS Managed Microsoft AD.

Console di gestione AWS

È possibile eliminare un gruppo AWS Managed Microsoft AD inConsole di gestione AWS.

Per eliminare un gruppo AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegli Gruppo. La scheda mostra un elenco di gruppi del tuoRegione AWS.
5. Scegli il gruppo che desideri eliminare. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. Verrai indirizzato alla schermata dei dettagli del gruppo.
6. Scegliere Delete group (Elimina gruppo). Viene visualizzata una finestra di dialogo in cui puoi scegliere Conferma per eliminare il gruppo.

AWS CLI

Di seguito viene descritto come formattare una richiesta che elimina un gruppo AWS Managed Microsoft AD con la AWS Directory Service Data CLI.

Per eliminare un gruppo AWS Managed Microsoft AD con AWS CLI

- Aprire ed eseguire il comando seguente, sostituendo l'ID della directory e il nome del gruppo con l'ID di directory Microsoft AD AWS gestito e il nome del gruppo: AWS CLI

```
aws ds-data delete-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che elimina un gruppo Microsoft AD AWS gestito con. AWS Strumenti per PowerShell

Per eliminare un gruppo AWS Managed Microsoft AD con AWS Strumenti per PowerShell

- Apri PowerShell ed esegui il comando seguente, sostituendo l'ID della directory e il nome del gruppo con l'ID di directory Microsoft AD AWS gestito e il nome del gruppo:

```
Remove-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Aggiungere e rimuovere membri di AWS Managed Microsoft AD ai gruppi e ai gruppi

Con l'API AWS Directory Service Data, un membro può essere un utente, un gruppo o un computer. Un utente rappresenta una persona o un'entità che può accedere alla tua directory. I gruppi consentono di concedere e negare le autorizzazioni a più di un utente alla volta.

Utilizzare le seguenti procedure per aggiungere o rimuovere un utente di Microsoft AD AWS gestito da un gruppo o un gruppo da un altro gruppo con la gestione di utenti e gruppi o i dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

Aggiungere un utente a un gruppo

Utilizzare la procedura seguente per aggiungere un utente Microsoft AD AWS gestito a un gruppo con gestione di utenti e gruppi o dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

> **Important**
>
> Quando aggiungi un utente AWS Managed Microsoft AD a un gruppo, l'utente eredita i ruoli e le autorizzazioni assegnati al gruppo. Questi ruoli e autorizzazioni fanno parte delle appartenenze ai gruppi dell'utente.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.

- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Crea un utente AWS Managed Microsoft AD.
- Crea un gruppo AWS Managed Microsoft AD.

Console di gestione AWS

È possibile aggiungere un membro di AWS Managed Microsoft AD a un gruppo conConsole di gestione AWS.

Per aggiungere un utente AWS Managed Microsoft AD a un gruppo con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Groups (Gruppi). Per trovare i gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.
5. Scegli un gruppo. Verrai indirizzato alla schermata dei dettagli del gruppo.
6. Scegli Membri. La scheda mostra un elenco di utenti e gruppi di bambini per tipo di membro del gruppo.
7. Nella scheda Membri, scegli Aggiungi membro.

8. In Membri, seleziona l'utente che desideri aggiungere al gruppo, quindi scegli Aggiungi membro al gruppo. Per trovare membri, inserisci il nome di accesso utente per gli utenti e il nome del gruppo per i gruppi nella casella di ricerca nella sezione Membri.

AWS CLI

Di seguito viene descritto come formattare una richiesta che aggiunge un membro AWS Managed Microsoft AD a un gruppo con la AWS Directory Service Data CLI.

Per aggiungere un utente AWS Managed Microsoft AD a un gruppo con AWS CLI

- Per aggiungere un utente a un gruppo, apri ed esegui il comando seguenteAWS CLI, sostituendo l'ID directory, il gruppo e i nomi dei membri con il tuo ID AWS Managed Microsoft AD Directory e i nomi dei gruppi e dei membri:

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "your-group-
name" --member-name "jane.doe"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che aggiunge un membro di AWS Managed Microsoft AD a un gruppo conAWS Strumenti per PowerShell.

Per aggiungere un utente AWS Managed Microsoft AD a un gruppo con AWS Strumenti per PowerShell

- Per aggiungere un utente a un gruppo, apri ed esegui il comando seguentePowerShell, sostituendo l'ID directory, il gruppo e i nomi dei membri con il tuo ID AWS Managed Microsoft AD Directory e i nomi dei gruppi e dei membri:

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -
MemberName "jane.doe"
```

Rimuovere un utente da un gruppo

Con l'API AWS Directory Service Data, un membro può essere un utente, un gruppo o un computer. Un utente rappresenta una persona o un'entità che può accedere alla tua directory. I gruppi consentono di concedere e negare le autorizzazioni a più di un utente alla volta.

Utilizzare la procedura seguente per rimuovere un utente di Microsoft AD AWS gestito da un gruppo con gestione di utenti e gruppi o dati di AWS Directory Service in Console di gestione AWSAWS CLI, oAWS Strumenti per PowerShell.

> **Important**
>
> Quando rimuovi un utente di Microsoft AD AWS gestito da un gruppo, l'utente perde l'accesso ai ruoli e alle autorizzazioni assegnati al gruppo. Questi ruoli e autorizzazioni fanno parte dell'appartenenza al gruppo.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Crea un utente AWS Managed Microsoft AD.
- Crea un gruppo AWS Managed Microsoft AD.

Console di gestione AWS

Puoi rimuovere un membro di AWS Managed Microsoft AD da un gruppo conConsole di gestione AWS.

Per rimuovere un utente AWS Managed Microsoft AD da un gruppo con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Groups (Gruppi). La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.
5. Scegli un gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. Verrai indirizzato alla schermata dei dettagli del gruppo.
6. Scegli Membri. La scheda mostra un elenco di utenti e gruppi di bambini per tipo di membro del gruppo.
7. Seleziona l'utente che desideri rimuovere dal gruppo, quindi scegli Rimuovi. Per trovare utenti, inserisci il nome di accesso dell'utente nella casella di ricerca nella sezione Membri.
8. Conferma di voler rimuovere l'utente dal gruppo, quindi scegli nuovamente Rimuovi.

AWS CLI

Di seguito viene descritto come formattare una richiesta che rimuove un membro di AWS Managed Microsoft AD da un gruppo con la AWS Directory Service Data CLI.

Per rimuovere un utente AWS Managed Microsoft AD da un gruppo con AWS CLI

- Per rimuovere un utente da un gruppo, apri ed esegui il comando seguenteAWS CLI, sostituendo l'ID directory, il gruppo e i nomi dei membri con l'ID, il gruppo e i nomi dei membri AWS gestiti di Microsoft AD Directory:

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che rimuove un membro di AWS Managed Microsoft AD da un gruppo conAWS Strumenti per PowerShell.

Per rimuovere un utente AWS Managed Microsoft AD da un gruppo con AWS Strumenti per PowerShell

- Per rimuovere un utente da un gruppo, apri ed esegui il comando seguentePowerShell, sostituendo l'ID directory, il gruppo e i nomi dei membri con l'ID, il gruppo e i nomi dei membri AWS gestiti di Microsoft AD Directory:

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -
MemberName "jane.doe"
```

Aggiungere un gruppo a un gruppo

Quando si aggiunge un gruppo Microsoft AD AWS gestito a un altro gruppo, i gruppi condividono una relazione padre-figlio. Il gruppo di figli ottiene l'accesso ai ruoli e alle autorizzazioni assegnati al gruppo principale. Puoi aggiungere un gruppo di bambini al tuo gruppo e il tuo gruppo a un gruppo di genitori.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.

- Crea un gruppo AWS Managed Microsoft AD.

Console di gestione AWS

È possibile aggiungere un gruppo Microsoft AD AWS gestito a un gruppo conConsole di gestione AWS.

Per aggiungere un gruppo di bambini al tuo gruppo con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Groups (Gruppi). La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.
5. Scegli un gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. Verrai indirizzato alla schermata dei dettagli del gruppo.
6. Scegli Membri. La scheda mostra un elenco di utenti e gruppi di bambini per tipo di membro del gruppo.
7. Scegli Aggiungi membro.
8. In Membri, seleziona i gruppi di bambini che desideri aggiungere al gruppo, quindi scegli Aggiungi membro al gruppo.

Per aggiungere un gruppo di genitori a un gruppo con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Groups (Gruppi). La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.

5. Scegli un gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi. Verrai indirizzato alla schermata dei dettagli del gruppo.
6. Scegli Gruppi di genitori. La scheda mostra un elenco di gruppi di cui il gruppo è membro.
7. Scegli Aggiungi gruppi di genitori.
8. In Gruppi, seleziona i gruppi a cui desideri aggiungere il gruppo, quindi scegli nuovamente Aggiungi gruppi principali.

AWS CLI

Di seguito viene descritto come formattare una richiesta che aggiunge un gruppo AWS Managed Microsoft AD a un gruppo con la AWS Directory Service Data CLI.

Per aggiungere un gruppo di bambini al gruppo con AWS CLI

- Per aggiungere un gruppo figlio a un gruppo principale, apri ed esegui il comando seguenteAWS CLI, sostituendo l'ID directory, il gruppo e i nomi dei membri con l'ID, il gruppo e i nomi dei membri AWS gestiti di Microsoft AD Directory:

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che aggiunge un gruppo Microsoft AD AWS gestito a un gruppo conAWS Strumenti per PowerShell.

Per aggiungere un gruppo di bambini al gruppo con AWS Strumenti per PowerShell

- Per aggiungere un gruppo figlio a un gruppo principale, apri ed esegui il comando seguentePowerShell, sostituendo l'ID directory, il gruppo e i nomi dei membri con l'ID, il gruppo e i nomi dei membri AWS gestiti di Microsoft AD Directory:

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

Rimuovere un gruppo da un gruppo

Quando rimuovi un gruppo Microsoft AD AWS gestito da un altro gruppo, i gruppi non condividono più una relazione padre-figlio. Il gruppo figlio perde l'accesso ai ruoli e alle autorizzazioni assegnati al gruppo principale. Puoi rimuovere un gruppo di bambini dal tuo gruppo e il tuo gruppo da un gruppo di genitori.

Prima di iniziare una delle due procedure, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.
- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Crea un gruppo AWS Managed Microsoft AD.

Console di gestione AWS

È possibile rimuovere un gruppo Microsoft AD AWS gestito in un gruppo conConsole di gestione AWS.

Per rimuovere un gruppo di bambini dal tuo gruppo con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.

4. Scegliere Groups (Gruppi). La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.
5. Scegli un gruppo. Verrai indirizzato alla schermata dei dettagli del gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi.
6. Scegli Membri. La scheda mostra un elenco di utenti e gruppi di bambini per tipo di membro del gruppo.
7. Seleziona i gruppi di bambini che desideri rimuovere dal gruppo, quindi scegli Rimuovi.
8. Conferma il gruppo o i gruppi di bambini che desideri rimuovere dal gruppo, quindi scegli nuovamente Rimuovi.

Per rimuovere il tuo gruppo da un gruppo di genitori con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Groups (Gruppi). La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.
5. Scegli un gruppo. Verrai indirizzato alla schermata dei dettagli del gruppo. Per trovare gruppi, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi.
6. Scegli Gruppi principali. La scheda mostra un elenco di gruppi di cui il gruppo è membro.
7. Seleziona il gruppo principale da cui desideri rimuovere il gruppo, quindi scegli Rimuovi gruppi di genitori.
8. Conferma il gruppo principale da cui desideri rimuovere il gruppo, quindi scegli nuovamente Rimuovi gruppi di genitori.

AWS CLI

Di seguito viene descritto come formattare una richiesta che rimuove un gruppo AWS Managed Microsoft AD in un gruppo con la AWS Directory Service Data CLI.

- Per rimuovere un gruppo figlio da un gruppo principale con il AWS CLI

  Per aggiungere e rimuovere un gruppo figlio da un gruppo principale, apri ed esegui il comando seguenteAWS CLI, sostituendo l'ID directory, il gruppo e i nomi dei membri con l'ID, il gruppo e i nomi dei membri AWS gestiti di Microsoft AD Directory:

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Strumenti per PowerShell

Di seguito viene descritto come formattare una richiesta che rimuove un gruppo Microsoft AD AWS gestito in un gruppo conAWS Strumenti per PowerShell.

- Per rimuovere un gruppo di bambini da un gruppo di genitori con AWS Strumenti per PowerShell

  Per aggiungere e rimuovere un gruppo figlio da un gruppo principale, apri ed esegui il comando seguentePowerShell, sostituendo l'ID directory, il gruppo e i nomi dei membri con l'ID, il gruppo e i nomi dei membri AWS gestiti di Microsoft AD Directory:

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

Copiare le appartenenze AWS a un gruppo Microsoft AD gestito nel Console di gestione AWS

È possibile copiare le appartenenze ai gruppi da un utente di Microsoft AD AWS gestito a un altro utente in. Console di gestione AWS Le appartenenze ai gruppi sono i ruoli e le autorizzazioni che un utente eredita quando lo aggiungi a un gruppo.

Prima di iniziare questa procedura, è necessario completare quanto segue:

- Creazione del tuo AWS Managed Microsoft AD.
- Per utilizzare la gestione di utenti e gruppi o la AWS Directory Service Data CLI, è necessario abilitarla. Per ulteriori informazioni, consulta Abilitare la gestione di utenti e gruppi o Directory Service Data.

- Puoi abilitare questa funzionalità solo dal primario Regione AWS per la tua directory. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
- Avrai bisogno delle autorizzazioni IAM necessarie per utilizzare i dati del AWS Directory Service. Per ulteriori informazioni, consulta Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni. Per iniziare a concedere le autorizzazioni ai tuoi utenti e carichi di lavoro, puoi utilizzare policy AWS gestite come o. AWSpolitica gestita: AWSDirectoryServiceDataFullAccess Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess Per ulteriori informazioni, consulta Best practice per la sicurezza in IAM.
- Crea un gruppo AWS Managed Microsoft AD.

Per copiare le appartenenze ai gruppi AWS Managed Microsoft AD con Console di gestione AWS

1. Apri la Directory Service console all'indirizzo https://console.aws.amazon.com/directoryservicev2/.
2. Dal riquadro di navigazione, scegli Active Directory, quindi scegli Directory. Verrai indirizzato alla schermata Directory in cui puoi visualizzare un elenco di directory presenti nel tuo. Regione AWS
3. Scegli una cartella. Verrai indirizzato alla schermata dei dettagli della directory.
4. Scegliere Groups (Gruppi). La scheda mostra un elenco di gruppi presenti nel tuoRegione AWS.
5. Scegli l'utente di cui desideri copiare l'account di appartenenza al gruppo. Per trovare un utente, inserisci il nome di accesso utente nella casella di ricerca nella sezione Utenti. Verrai indirizzato alla schermata dei dettagli utente.
6. Scegli Copia tutte le appartenenze al gruppo. Verrai indirizzato a una procedura in cui puoi specificare quali gruppi vuoi copiare.

    a. Per Verifica i gruppi da copiare, in Gruppi da copiare, seleziona i gruppi con ruoli e autorizzazioni che desideri copiare, quindi scegli Avanti.

    b. Per Seleziona account di destinazione, in Tipo di account, scegli Account utente esistente per copiare le appartenenze ai gruppi in un account utente esistente. In alternativa, scegli Nuovo account utente per creare un nuovo utente e copiare le appartenenze ai gruppi nel nuovo account utente. Per trovare un gruppo, inserisci il nome del gruppo nella casella di ricerca nella sezione Gruppi selezionati.

        i. (Facoltativo) Se scegli Account utente esistente, seleziona gli account di destinazione in cui vuoi copiare i ruoli e le autorizzazioni, quindi scegli Avanti.

ii. (Facoltativo) Se scegli Nuovo account utente, completa la procedura, quindi scegli Avanti. Per informazioni sulla creazione di un utente, consultaCreazione di un utente.

c. Per Rivedi e copia le appartenenze ai gruppi, rivedi le tue scelte, quindi scegli Copia l'appartenenza al gruppo.

Gestisci utenti e gruppi con un' EC2 istanza Amazon

Questa sezione include le procedure per la gestione di utenti e gruppi con un' EC2 istanza Amazon aggiunta al tuo AWS Managed Microsoft AD.

Ti consigliamo di gestire utenti e gruppi con un' EC2 istanza Amazon se l'API Directory Service Data non supporta il tuo caso d'uso. Per ulteriori informazioni, consulta il AWS Directory Service Data API Reference.

> **Note**
>
> Prima di completare le procedure descritte nei seguenti argomenti, è necessario installare gli strumenti di amministrazione di Active Directory. Per ulteriori informazioni, vedere Installare gli strumenti di amministrazione di Active Directory.

Argomenti

- Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD
- Creazione di un utente Microsoft AD AWS gestito
- Eliminare l'account di un utente con un' EC2 istanza Amazon
- Reimpostazione di una password utente AWS Microsoft AD gestita
- Creazione di un gruppo Microsoft AD AWS gestito
- Aggiungere un utente AWS Managed Microsoft AD a un gruppo

Installazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD

Puoi gestire il tuo AWS Managed Microsoft AD Active Directory utilizzandoActive Directory Domain Services and Active Directory Lightweight Directory Services Tools. Per utilizzarliActive Directory Domain Services and Active Directory Lightweight Directory Services Tools, è necessario installarli. Le seguenti procedure illustrano come installare questi strumenti su un'istanza di Amazon EC2

Windows Server o con un PowerShell comando. In alternativa, puoi avviare un' EC2istanza di amministrazione delle directory su cui sono già installati questi strumenti.

EC2 Windows Server instance

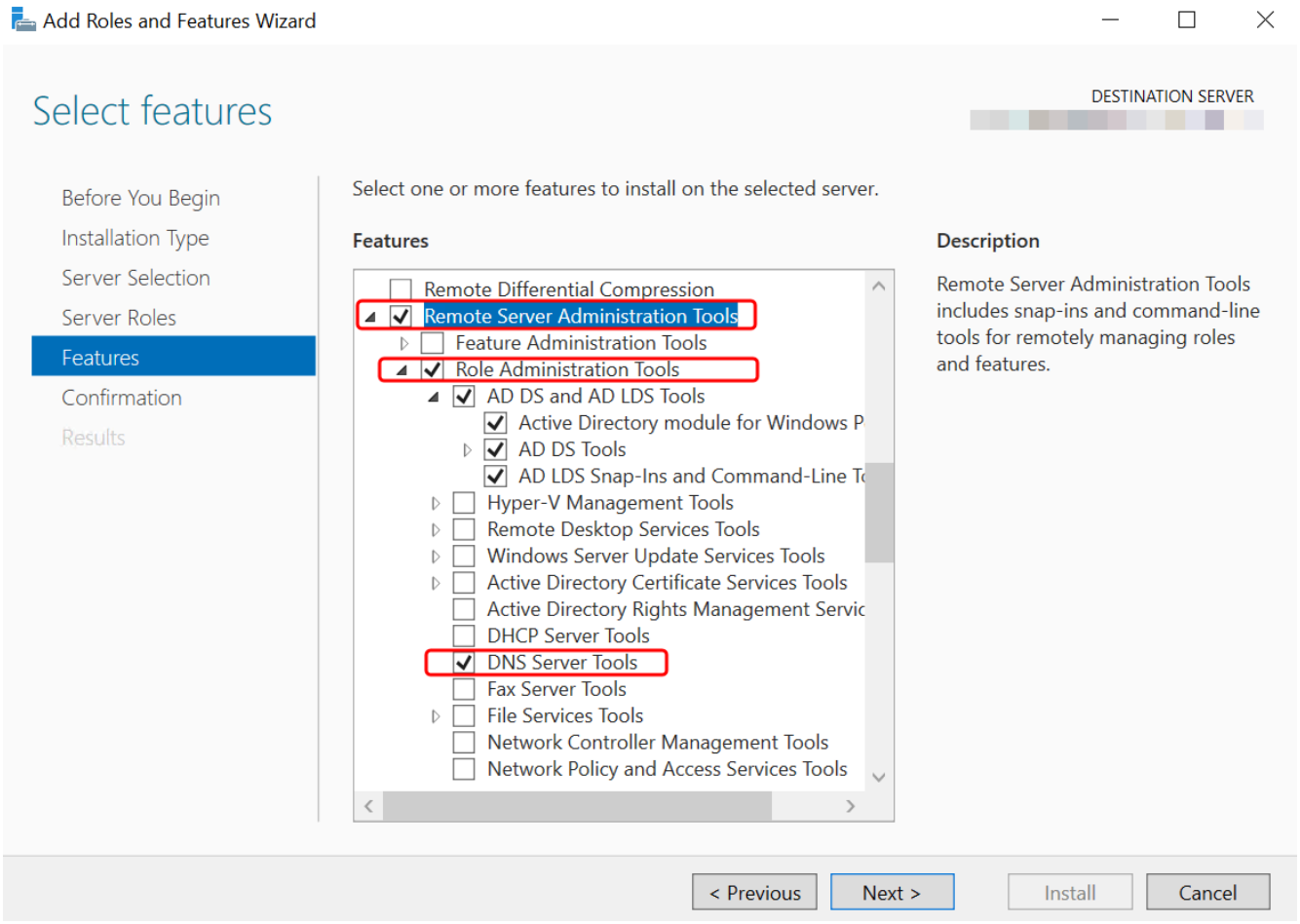
Prima di iniziare questa procedura, completa quanto segue:

1. Crea un Microsoft AD Active Directory AWS gestito. Per ulteriori informazioni, consulta Creazione del tuo AWS Managed Microsoft AD.
2. Avvia e unisci un'istanza di EC2 Windows Server al tuo AWS Managed Microsoft AD Active Directory. L' EC2 istanza necessita delle seguenti politiche per creare utenti e gruppi: **`AmazonSSMManagedInstanceCore`** e**`AmazonSSMDirectoryServiceAccess`**. Per ulteriori informazioni, consultare Avvio di un'istanza di amministrazione delle directory in AWS Managed Microsoft AD Active Directory e Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory.
3. Avrai bisogno delle credenziali per l'amministratore del dominio Active Directory. Queste credenziali sono state create al momento della creazione di AWS Managed Microsoft AD. Se hai seguito la procedura riportata inCreazione del tuo AWS Managed Microsoft AD, il nome utente dell'amministratore include il nome NetBIOS,. **`corp\admin`**

Installazione degli strumenti di amministrazione di Active Directory su un'istanza EC2 Windows del server

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella EC2 console Amazon, scegli Istanze, seleziona l'istanza di Windows Server, quindi scegli Connect.
3. Nella pagina Collega all'istanza, scegli Client RDP.
4. Nella scheda Client RDP, scegli Scarica il file del desktop remoto, quindi scegli Ottieni password per recuperare la password.
5. Nella sezione Ottieni la password di Windows, scegli Carica il file della chiave privata. Scegli il file della chiave privata .pem associato all'istanza di Windows Server. Dopo aver caricato il file della chiave privata, seleziona Decrittografa la password.
6. Nella finestra di dialogo Sicurezza di Windows, copia le credenziali di amministratore locale per il computer Windows Server a cui accedere. Il nome utente può avere i seguenti formati: ***`NetBIOS-Name`*`\admin`** o***`DNS-Name`*`\admin`**. Ad esempio, **`corp\admin`** sarebbe il nome utente se hai seguito la procedura inCreazione del tuo AWS Managed Microsoft AD.

7. Una volta effettuato l'accesso all'istanza di Windows Server, apri Server Manager dal menu Start scegliendo Server Manager.
8. Nel pannello di controllo Server Manager scegli Aggiungi ruoli e funzionalità.
9. In Aggiunta guidata ruoli e funzionalità scegliere Tipo di installazione, selezionare Installazione basata su ruoli o basata su funzionalità e scegliere Avanti.
10. In Selezione server verificare che sia selezionato il server locale, quindi scegliere Funzionalità nel riquadro di navigazione a sinistra.
11. Nell'albero Funzionalità, apri Strumenti di amministrazione remota del server, Strumenti di amministrazione del ruolo e Strumenti AD DS e AD LDS. Con AD DS e AD LDS Tools selezionati, vengono selezionati il modulo Active Directory per PowerShell, AD DS Tools, gli snap-in e gli strumenti da riga di comando di AD LDS. Scorri verso il basso e seleziona Strumenti server DNS, quindi scegli Successivo.



12. Verificare che le informazioni siano corrette e scegliere Installa. Quando l'installazione della funzionalità è terminata, Active Directory Domain Services e gli strumenti Active Directory

Lightweight Directory Services sono disponibili nel menu Start nella cartella Strumenti di amministrazione.

PowerShell

È possibile installare gli strumenti di amministrazione di Active Directory utilizzandoPowerShell. Ad esempio, è possibile installare gli strumenti di amministrazione remota di Active Directory da un PowerShell prompt utilizzando`Install-WindowsFeature RSAT-ADDS`. Per ulteriori informazioni, vedere Install- WindowsFeature sul sito Web Microsoft.

Directory administration instance

È possibile avviare un' EC2 istanza di amministrazione delle directory in Console di gestione AWS cui sono già installati Active Directory Domain Services e Active Directory Lightweight Directory Services Tools seguendo le procedure riportate inAvvio di un'istanza di amministrazione delle directory in AWS Managed Microsoft AD Active Directory.

Creazione di un utente Microsoft AD AWS gestito

È possibile creare utenti Microsoft AD AWS gestiti con gli strumenti di amministrazione di Active Directory ePowerShell. Prima di poter creare utenti con gli strumenti di amministrazione di Active Directory, è necessario completare la procedura inInstallazione degli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD.

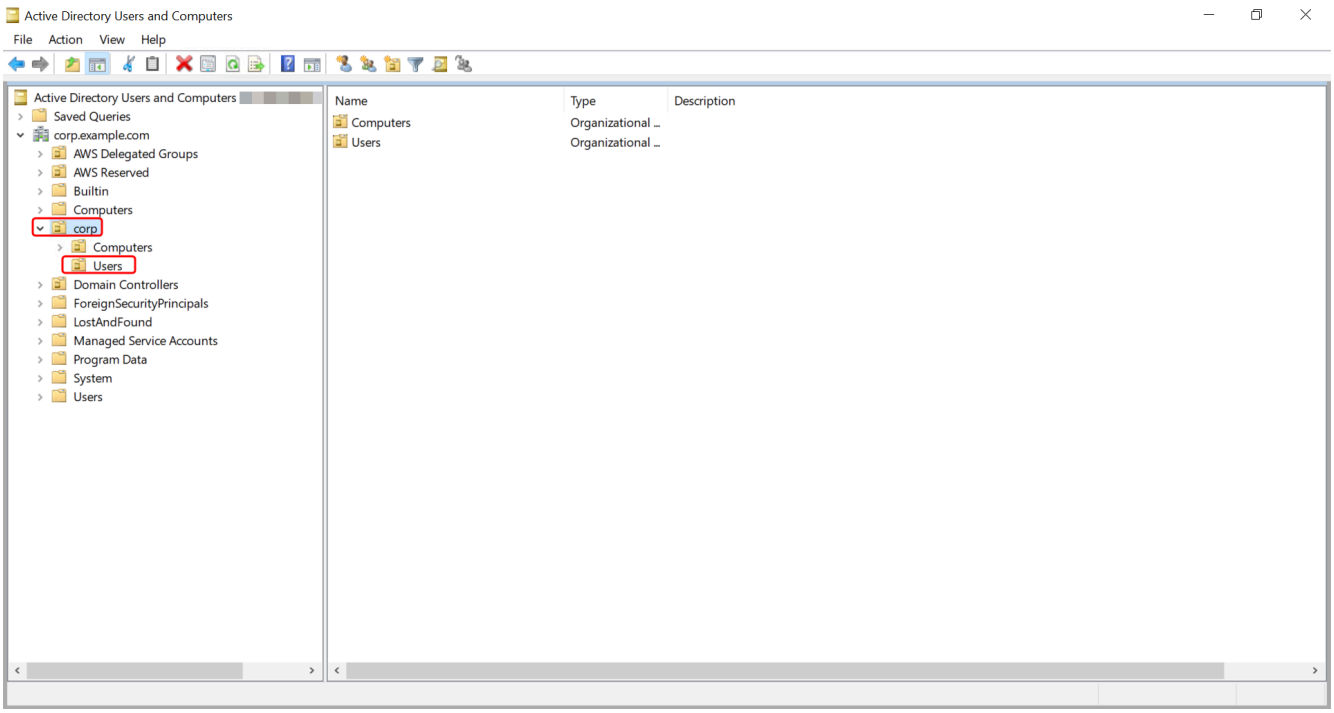
Active Directory Administration Tools

Utilizzare la procedura seguente per creare un utente Microsoft AD AWS gestito con gli strumenti di amministrazione di Active Directory.

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Aprire lo strumento Utenti e computer di Active Directory dal menu Start di Windows. È disponibile un collegamento a questo strumento nella cartella Strumenti di amministrazione di Windows.

> **Tip**
>
> Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Nell'albero delle directory, selezionare un'unità organizzativa sotto l'unità organizzativa con nome NetBIOS della directory in cui si desidera archiviare l'utente (ad esempio,**`corp\Users`**). Per ulteriori informazioni sulla struttura dell'unità organizzativa utilizzata dalle directory in AWS, vedere. Cosa viene creato con AWS Managed Microsoft AD



4. Nel menu Operazioni, scegli Nuovo, quindi Utente per aprire la nuova procedura guidata per un nuovo utente.
5. Nella prima pagina della procedura guidata, inserisci i valori per i campi seguenti, quindi scegli Successivo.
   - Nome
   - Cognome
   - User logon name (Nome di accesso dell'utente)

6. Nella seconda pagina della procedura guidata, inserisci una password temporanea in Password e Conferma password. Verifica che l'opzione L'utente deve modificare la password al prossimo accesso sia selezionata. Nessuna delle altre opzioni deve essere selezionata. Scegli Next (Successivo).
7. Nella terza pagina della procedura guidata, verifica che le informazioni del nuovo utente siano corrette e scegli Termina. Il nuovo utente verrà visualizzato nella cartella Users (Utenti).

PowerShell

Utilizzare la procedura seguente per creare un utente Microsoft AD AWS gestito conPowerShell.

1. Connect all'istanza aggiunta al dominio Active Directory come amministratore di Active Directory.
2. Aprire PowerShell.
3. Digita il seguente comando sostituendo il nome utente **`jane.doe`** con il nome utente dell'utente che desideri creare. Ti verrà richiesto di PowerShell fornire una password per il nuovo utente. Per ulteriori informazioni sui requisiti di complessità delle password di Active Directory, consulta Microsoftla documentazione. Per ulteriori informazioni sul ADUser comando New-, vedere Microsoftla documentazione.

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -
AsSecureString 'Password')
```

Eliminare l'account di un utente con un' EC2 istanza Amazon

Puoi utilizzare la seguente procedura per eliminare un utente con un' EC2 istanza Amazon aggiunta al tuo AWS Managed Microsoft AD.

> **Note**
>
> Prima di completare questa procedura, è necessario installare gli strumenti di amministrazione di Active Directory. Per ulteriori informazioni, vedere Installare gli strumenti di amministrazione di Active Directory.

Per eliminare un utente

1. Apri lo strumento Utenti e computer di Active Directory. Trovi una scorciatoia a questo strumento nella cartella Strumenti amministrativi Windows.

   > **Tip**
   >
   > Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

2. Nell'albero delle directory, seleziona l'unità organizzativa contenente l'utente da eliminare (ad esempio, Corp\Users).
3. Seleziona l'utente che desideri eliminare. Dal menu Operazioni, scegli Elimina.
4. Viene visualizzata una finestra di dialogo che richiede di confermare se desideri eliminare l'utente. Scegli Sì per eliminare l'utente.

Gli utenti eliminati vengono archiviati temporaneamente nel Cestino di AD. Per ulteriori informazioni sul Cestino di AD, consulta The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting nel blog Ask the Directory Services Team di Microsoft.

Reimpostazione di una password utente AWS Microsoft AD gestita

Gli utenti devono rispettare le politiche relative alle password definite in Active Directory. A volte ciò può convincere gli utenti, incluso l'amministratore di Active Directory, a dimenticare la password. Quando ciò accade, puoi reimpostare rapidamente la password dell'utente utilizzando Directory Service se l'utente risiede in AWS Managed Microsoft AD.

Devi accedere come utente con le autorizzazioni necessarie per reimpostare le password. Per ulteriori informazioni sulle autorizzazioni, consultare Panoramica della gestione delle autorizzazioni di accesso alle risorse Directory Service.

Puoi reimpostare la password per qualsiasi utente in Active Directory con le seguenti eccezioni:

- È possibile reimpostare la password per qualsiasi utente all'interno dell'unità organizzativa (OU) basata sul nome NetBIOS utilizzato durante la creazione di Active Directory. Ad esempio, se

seguissi la procedura indicata nel Creazione del tuo AWS Managed Microsoft AD tuo NetBIOS, il nome sarebbe CORP e le password degli utenti che potresti reimpostare sarebbero membri dell'unità organizzativa. Corp/Users

- Non è possibile reimpostare la password di alcun utente al di fuori dell'unità organizzativa basata sul nome NetBIOS utilizzato durante la creazione di Active Directory. Ad esempio, non è possibile reimpostare la password di un utente in AWSReserved OU. Per ulteriori informazioni sulla struttura dell'unità organizzativa per AWS Managed Microsoft AD, vedereCosa viene creato con AWS Managed Microsoft AD.

Per ulteriori informazioni su come vengono applicate le politiche relative alle password quando viene reimpostata una password in AWS Managed Microsoft AD, vedereCome vengono applicate le politiche relative alle password.

È possibile utilizzare uno dei seguenti strumenti per reimpostare una password utente di Microsoft AD AWS gestito:

- Console di gestione AWS
- AWS CLI
- PowerShell

Console di gestione AWS

Utilizzare la procedura seguente per reimpostare una password utente di Microsoft AD AWS gestito conConsole di gestione AWS.

1. Nel riquadro di navigazione della Directory Serviceconsole, in Active Directory, scegli Directory, quindi seleziona Active Directory nell'elenco in cui desideri reimpostare la password utente.
2. Nella pagina dei Dettagli della directory, scegli Operazioni, Reimposta password utente.
3. Nella finestra di dialogo Reimposta la password utente, in Nome utente digita il nome utente dell'utente la cui password deve essere modificata.
4. Digita una password in Nuova password e Conferma password, quindi scegli Reimposta password.

AWS CLI

Utilizzare la procedura seguente per reimpostare una password utente di Microsoft AD AWS gestito conAWS CLI.

1. Per installareAWS CLI, vedi Installare o aggiornare la versione più recente di AWS CLI.
2. Aprire ilAWS CLI.
3. Digita il comando seguente e sostituisci l'ID di directory, il nome utente **`jane.doe`** e la password **`P@ssw0rd`** con l'ID di Active Directory e le credenziali desiderate. Per ulteriori informazioni reset-user-password, consulta la sezione AWS CLICommand Reference.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

PowerShell

Utilizzare la procedura seguente per reimpostare una password utente di Microsoft AD AWS gestito conPowerShell.

1. Connect all'istanza aggiunta al dominio Active Directory come amministratore di Active Directory.
2. Aprire PowerShell.
3. Digita il comando seguente sostituendo il nome utente**`jane.doe`**, l'ID di directory e la password **`P@ssw0rd`** con l'ID di Active Directory e le credenziali desiderate. Per ulteriori informazioni, vedere Reset- DSUser Password Cmdlet.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Creazione di un gruppo Microsoft AD AWS gestito

Puoi creare gruppi nel tuo AWS Managed Microsoft AD. Utilizza la seguente procedura per creare un gruppo di sicurezza con un' EC2 istanza Amazon aggiunta alla tua directory AWS Managed Microsoft AD. Prima di poter creare gruppi di sicurezza, è necessario completare le procedure descritte in Installazione degli strumenti di amministrazione di Active Directory.

Active Directory Administration Tools

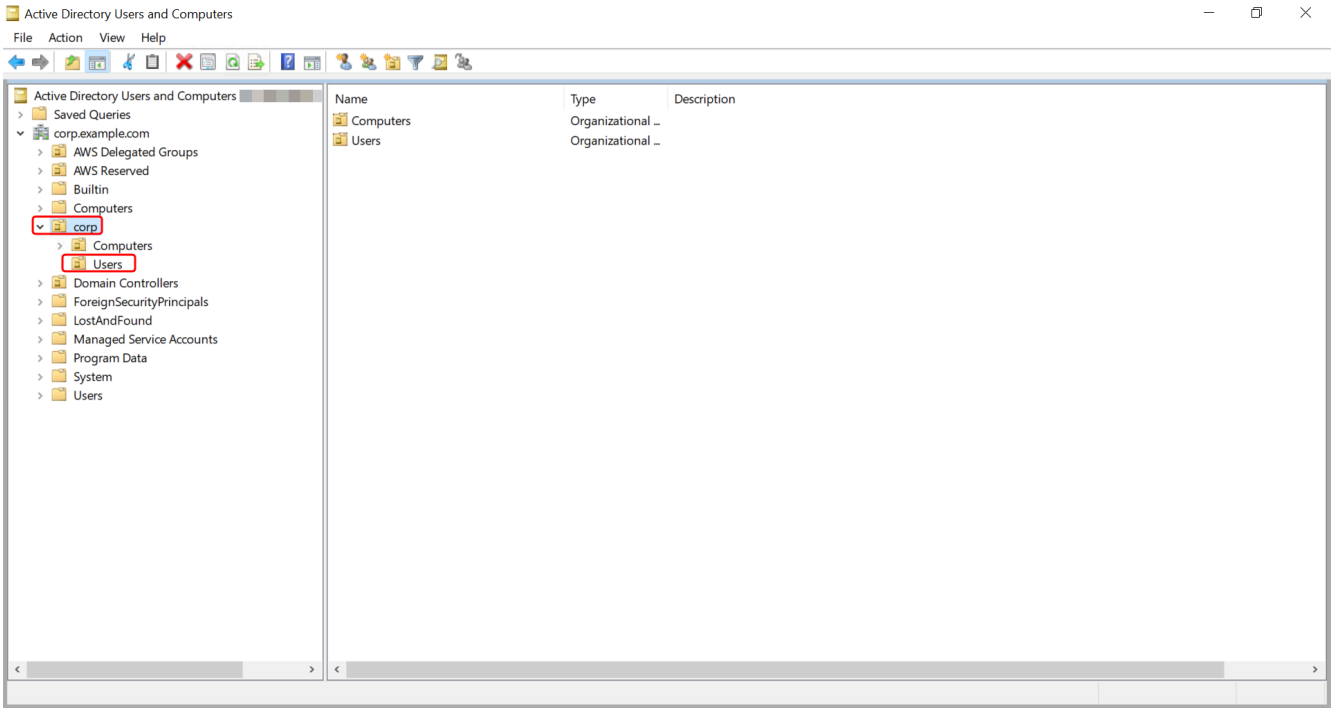
Utilizzare le seguenti procedure per creare un gruppo Microsoft AD AWS gestito con gli strumenti di amministrazione di Active Directory.

Creazione di un gruppo

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Apri lo strumento Utenti e computer di Active Directory. Trovi una scorciatoia a questo strumento nella cartella Administrative Tools (Strumenti amministrativi).

   > **Tip**
   >
   > Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Nell'albero delle directory, seleziona un'unità organizzativa sotto quella con nome NetBIOS della directory in cui desideri archiviare il gruppo (ad esempio, Corp\Users). Per ulteriori informazioni sulla struttura dell'unità organizzativa utilizzata dalle directory in AWS, vedereCosa viene creato con AWS Managed Microsoft AD.



4. Nel menu Action (Operazioni), fai clic su New (Nuovo), quindi fai clic su Group (Gruppo) per aprire la procedura guidata per un nuovo gruppo.
5. Digita un nome per il gruppo in Nome gruppo, seleziona un Ambito del gruppo che soddisfi le tue esigenze e seleziona Sicurezza per il Tipo di gruppo. Per ulteriori informazioni sull'ambito dei gruppi di Active Directory e sui gruppi di sicurezza, consulta Gruppi di sicurezza di Active Directory nella documentazione di Microsoft Windows Server.
6. Fai clic su OK. Il nuovo gruppo di sicurezza verrà visualizzato nella cartella Utenti.

PowerShell

È possibile utilizzare PowerShell i comandi per creare gruppi. Per ulteriori informazioni, consulta la PowerShell documentazione Novità ADGroup in Windows Server 2022.

Aggiungere un utente AWS Managed Microsoft AD a un gruppo

È possibile aggiungere utenti Microsoft AD AWS gestiti a un gruppo. Utilizza la seguente procedura per aggiungere un utente a un gruppo di sicurezza con un' EC2 istanza Amazon aggiunta alla tua directory AWS Managed Microsoft AD.

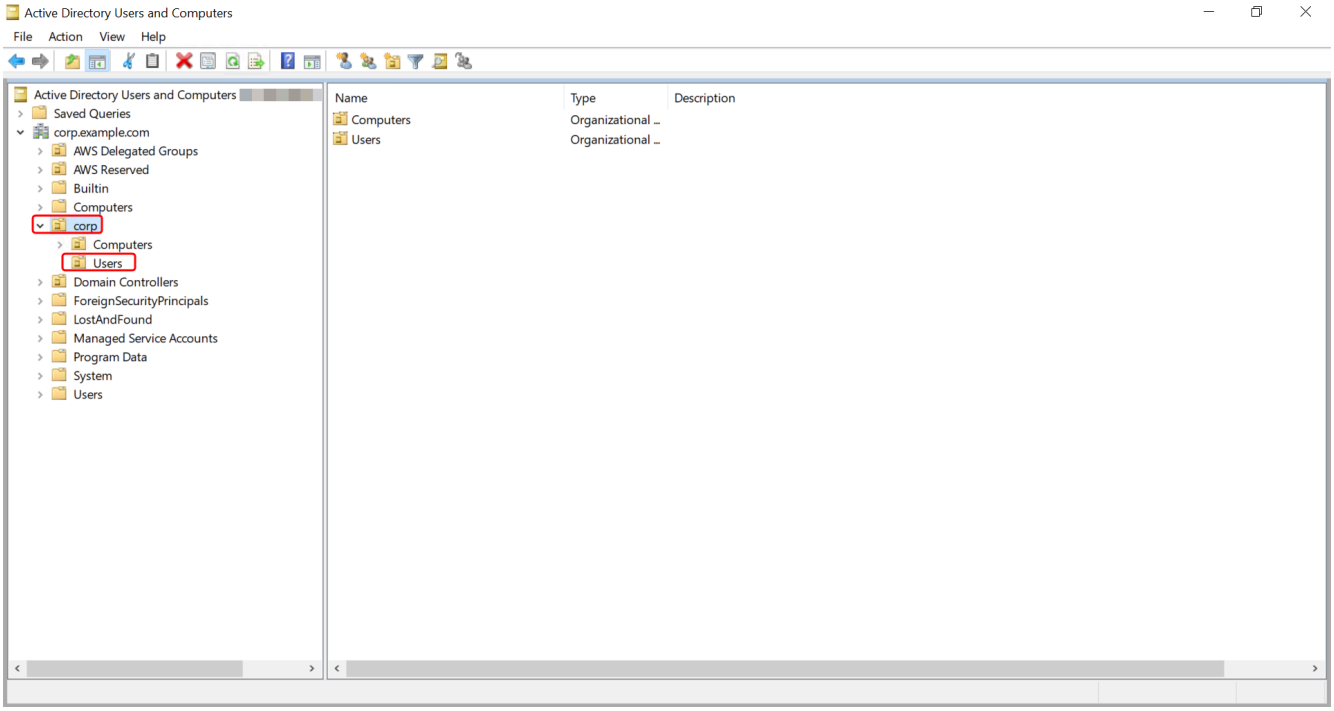
Active Directory Administration Tools

Aggiunta di un utente a un gruppo

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Apri lo strumento Utenti e computer di Active Directory. Trovi una scorciatoia a questo strumento nella cartella Administrative Tools (Strumenti amministrativi).

> **Tip**
>
> Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Nell'albero delle directory, seleziona l'unità organizzativa sotto quella con il nome NetBIOS della directory in cui è archiviato il gruppo e seleziona il gruppo a cui desideri aggiungere un utente come membro.



4. Nel menu Operazioni, fai clic su Proprietà per aprire la finestra di dialogo delle proprietà del gruppo.

5. Seleziona la scheda Membri e fai clic su Aggiungi….
6. Per Immettere i nomi degli oggetti da selezionare, digitare il nome utente che si desidera aggiungere e fare clic su OK. Il nome verrà visualizzato nell'elenco Membri. Fai nuovamente clic su OK per aggiornare l'appartenenza al gruppo.
7. Verifica che l'utente sia ora membro del gruppo selezionandolo nella cartella Utenti e facendo clic su Proprietà nel menu Operazioni per aprire la finestra di dialogo delle proprietà. Seleziona la scheda Membro di. Il nome del gruppo dovrebbe essere visualizzato nell'elenco dei gruppi a cui appartiene l'utente.

AWS Dati del Directory Service

AWS Directory Service Data è un'estensione di AWS Directory Service. Puoi creare, leggere, aggiornare e utilizzare Active Directory (AD) utenti, gruppi e appartenenze a Active Directory (AD) da un AWS Directory Service per Microsoft Active Directory senza distribuire istanze di gestione AD dedicate su un'istanza Amazon. EC2 Puoi anche eseguire attività di gestione degli oggetti integrate tra le directory senza alcuna connettività di rete diretta. Ciò semplifica il provisioning e la gestione degli accessi per ottenere implementazioni completamente automatizzate. Per ulteriori informazioni, consulta il AWS Directory Service Data API Reference.

Directory Service Data supporta operazioni di scrittura di utenti `CreateUser` e `CreateGroup` gruppi, ad esempio all'interno di AWS Managed Microsoft AD presente nell'unità organizzativa (OU). Directory Service Data supporta operazioni di lettura, ad esempio `ListUsers` e `ListGroups` su tutti gli utenti, i gruppi e le appartenenze ai gruppi all'interno di AWS Managed Microsoft AD e tra ambienti affidabili. Directory Service Data supporta l'aggiunta e la rimozione di membri del gruppo dai gruppi dell'unità organizzativa e dell'unità organizzativa Gruppi AWS delegati, in modo da poter delegare le autorizzazioni aggiungendo utenti a oggetti di gruppo delegati specifici. Per ulteriori informazioni, consulta Gestione di utenti e gruppi in AWS Managed Microsoft AD.

> **Note**
>
> I dati del Directory Service sono disponibili solo nella tua regione principale. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.

Argomenti

- Replica e coerenza

- AWSAttributi dei dati del Directory Service
- Tipo di gruppo e ambito del gruppo

Replica e coerenza

L'API Directory Service Data si connette ai controller di dominio Microsoft AD AWS gestiti per eseguire operazioni sugli oggetti directory sottostanti. Active Directory è una piattaforma sostanzialmente coerente e la replica avviene continuamente tra i controller di dominio delle Directory Service directory. Per impostazione predefinita, ogni Directory Service directory viene creata con due controller di dominio.

Directory Service Data tenta di mantenere un'esperienza coerente utilizzando lo stesso controller di dominio per tutte le richieste. Nel caso in cui un controller di dominio non sia disponibile, Directory Service Data passa a un controller di dominio alternativo. Durante questi eventi, è possibile notare l'eventuale coerenza tra i controller di dominio mentre gli oggetti vengono replicati tra i controller di dominio.

I limiti delle directory variano AWS a seconda dell'edizione Managed Microsoft AD:

- Edizione standard: supporta 8 transazioni al secondo per le operazioni di lettura e 4 TPS per le operazioni di scrittura per directory.
- Edizione Enterprise: supporta 16 transazioni al secondo per le operazioni di lettura e 8 TPS per le operazioni di scrittura per directory.

> **Note**
>
> È previsto un limite di 10 richieste simultanee per le edizioni Standard ed Enterprise.

- Account AWS— Supporta un totale di 100 transazioni al secondo per le operazioni di Directory Service Data in tutte le directory.

AWSAttributi dei dati del Directory Service

Questo argomento descrive come utilizzare gli attributi nel AWSDirectory Service Data API Reference.

Attributi di richiesta

I seguenti attributi devono essere definiti nei parametri del corpo della richiesta. Per un esempio di come definire questi attributi, vedere CreateGroupnel AWSDirectory Service Data API Reference.

Nome dell'attributo Directory Service Data	nome visualizzato LDAP	Console di gestione AWS	PowerShell alias	Tipo di accesso	Tipo di oggetto	Valore dell'attributo	Ricercabile
DistinguishedName	distinguishedName	Nome distinto	Nessuno	ReadOnly	Utente, gruppo	Stringa	No
EmailAddress	posta	Indirizzo e-mail	EmailAddress	Creabile	Utente	Stringa	Sì
Abilitato	Nessuno	Abilitato	Abilitato	Mutable	Utente	Boolean	No
GivenName	givenName	Nome	GivenName	Creabile	Utente	Stringa	Sì
GroupScope	GroupScope	Ambito del gruppo	Nessuno	Creabile	Gruppo	Enum	No
GroupType	Tipo di gruppo	Tipo gruppo	Nessuno	Creabile	Gruppo	Enum	No
SamAccountName	s Nome AMAccount	User logon name (Nome di accesso dell'utente)	s AMAccount Nome	Creabile	Utente, gruppo	Stringa	Sì
SID	ID degli oggetti	Identificatore di	SID	ReadOnly	Utente, gruppo	Stringa	No

Nome dell'attributo Directory Service Data	nome visualizzato LDAP	Console di gestione AWS	PowerShell alias	Tipo di accesso	Tipo di oggetto	Valore dell'attributo	Ricercabile
		sicurezza utente/ gruppo (SID)					
Cognome	sn	Cognome	Surname	Creabile	Utente	Stringa	Sì
UserPrincipalName	userPrincipalName	Nome principale dell'utente	UserPrincipalName	ReadOnly	Utente	Stringa	No

Altri attributi

I seguenti attributi devono essere definiti `OtherAttributes` e non devono essere mappati a nessun parametro del corpo della richiesta. Quando definisci altri attributi nelle tue richieste, devi specificare il nome dell'attributo, il tipo di dati e il valore per ogni attributo. Per un esempio di come definire questi attributi, vedere CreateUsernel AWSDirectory Service Data API Reference.

> **Note**
>
> I nomi di questi attributi non fanno distinzione tra maiuscole e minuscole quando vengono forniti come input e sono l'equivalente del nome visualizzato LDAP.

Nome dell'attributo Directory Service Data	nome visualizzato LDAP	Console di gestione AWS	PowerShell alias	Tipo di accesso	Tipo di oggetto	Valore dell'attributo	Ricercabile
Assistente	assistente	Assistente	Nessuno	ReadOnly	Utente	Stringa	No
Cn	cn	Common Name (Nome comune)	Nessuno	ReadOnly	Utente, gruppo	Stringa	No
Co	co	Paese/regione	Paese	Mutable	Utente	Stringa	No
Azienda	company	Azienda	Azienda	Creabile	Utente	Stringa	No
Dipartimento	department	Department	Department	Creabile	Utente	Stringa	No
Descrizione	description	Description	Description	Creabile	Utente, gruppo	Stringa	No
DirectReports	Rapporti diretti	Rapporti diretti	Nessuno	ReadOnly	Utente	Set di stringhe	No
DisplayName	displayName	Display name (Nome visualizzato)	DisplayName	Creabile	Utente, gruppo	Stringa	Sì
Facsimile Telephone Number	facsimileTelephoneNumber	Fax	Fax	Creabile	Utente, gruppo	Stringa	No

Nome dell'attributo Directory Service Data	nome visualizzato LDAP	Console di gestione AWS	PowerShell alias	Tipo di accesso	Tipo di oggetto	Valore dell'attributo	Ricercabile
HomePhon	homePhone	Numero di telefono di casa	HomePhon	Creabile	Utente	Stringa	No
Informazioni	Info	Note	Nessuno	Mutable	Utente, gruppo	Stringa	No
Iniziali	iniziali	Initials	Initials	Mutable	Utente	Stringa	No
IpPhone	telefono IP	Telefono IP	Nessuno	Mutable	Utente	Stringa	No
L	l	City	City	Creabile	Utente	Stringa	Sì
Manager	manager	Manager	Manager	Mutable	Utente	Stringa	No
Mail (Posta)	posta	Indirizzo e-mail	EmailAddress	Mutable	Gruppo	Stringa	Sì
Mobile	mobile	numero di cellulare	MobilePhone	Mutable	Utente	Stringa	No
ObjectClass	Classe oggetto	Utente/Gruppo	Nessuno	ReadOnly	Gruppo	Stringa	No
ObjectGUID	Guid dell'oggetto	Identificatore univoco globale (GUID)	Nessuno	ReadOnly	Utente, gruppo	Stringa	No

Nome dell'attributo Directory Service Data	nome visualizzato LDAP	Console di gestione AWS	PowerShell alias	Tipo di accesso	Tipo di oggetto	Valore dell'attributo	Ricercabile
Cercapersone	cercapersone	cercapersone	Nessuno	Mutable	Utente	Stringa	No
PhysicalDeliveryOfficeName	physicalDeliveryOfficeNome	Ufficio	Nessuno	Creabile	Utente	Stringa	Sì
PostalCode	postalCode	Zip/codice postale	PostalCode	Creabile	Utente	Stringa	No
PreferredLanguage	Lingua preferita	Lingua preferita	Nessuno	Mutable	Utente	Stringa	No
ProxyAddresses	Indirizzi proxy	Indirizzo proxy	Nessuno	ReadOnly	Utente, gruppo	Stringa multivalore	Sì
ServicePrincipalName	servicePrincipalName	Nome principale del servizio	ServicePrincipalName	Mutable	Utente	Stringa multivalore	No
St	st	Stato/Provincia	Stato	Creabile	Utente	Stringa	No
StreetAddress	Indirizzo	Indirizzo	StreetAddress	Creabile	Utente	Stringa	No
TelephoneNumber	Numero di telefono	Numero di telefono	OfficePhone	Creabile	Utente	Stringa	No

Nome dell'attributo Directory Service Data	nome visualizzato LDAP	Console di gestione AWS	PowerShell alias	Tipo di accesso	Tipo di oggetto	Valore dell'attributo	Ricercabile
Titolo	titolo	Mansione	Titolo	Mutable	Utente	Stringa	No
WhenChanged	Quando è cambiato	Ultimo aggiornamento	Nessuno	ReadOnly	Utente, gruppo	Stringa	No
WWWHomepage	una WWHome pagina	URL della home page	w WWHome Pagina	Mutable	Utente, gruppo	Stringa	No

Tipo di gruppo e ambito del gruppo

I gruppi in AWS Managed Microsoft AD hanno sia un tipo di gruppo che un ambito di gruppo. Per ulteriori informazioni su ciascuno di essi, consulta le sezioni seguenti.

Argomenti

- Tipo gruppo
- Ambito del gruppo

Tipo gruppo

Il tipo di gruppo determina a quali risorse condivise all'interno di Active Directory possono accedere i membri del gruppo. Esistono due tipi di gruppo:

- Sicurezza: puoi assegnare autorizzazioni a questi gruppi in modo che i membri del gruppo possano accedere alle risorse condivise di Active Directory.
- Distribuzione: è possibile utilizzare questo tipo per creare liste di distribuzione e-mail. Questi membri del gruppo non possono accedere alle risorse condivise di Active Directory.

Non ci sono limitazioni quando si passa da un tipo di gruppo all'altro.

Per ulteriori informazioni sui tipi di gruppo, consulta la documentazione Microsoft.

Ambito del gruppo

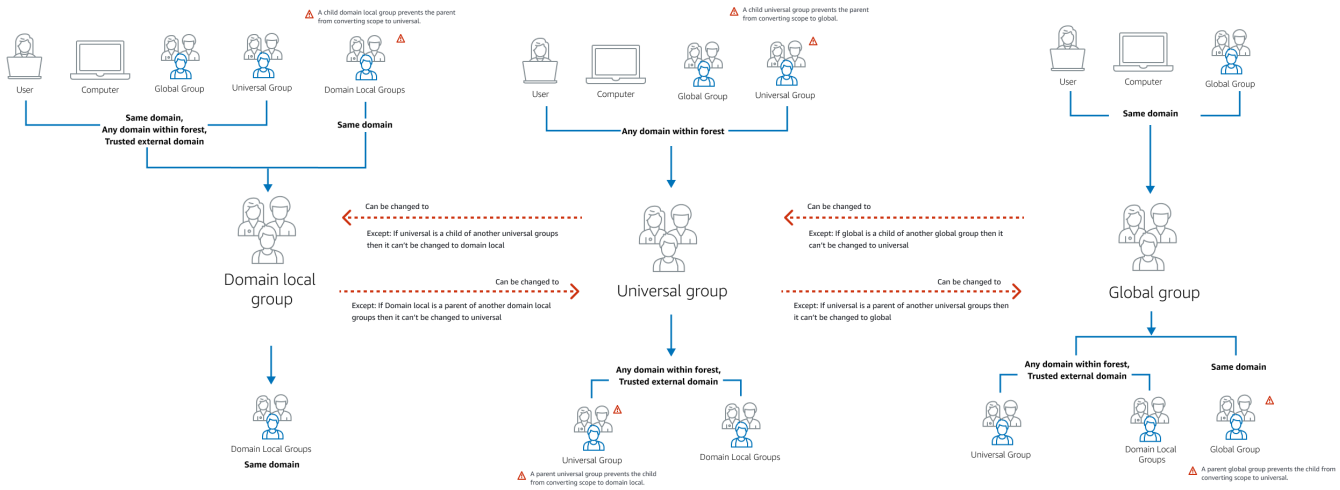
L'ambito del gruppo determina il modo in cui i membri del gruppo vengono definiti con l'albero o la foresta del dominio. Esistono tre ambiti di gruppo:

- Dominio locale: per assegnare le autorizzazioni ai membri del gruppo che si trovano nello stesso dominio.
- Universale: per assegnare le autorizzazioni ai membri del gruppo che si trovano all'interno di qualsiasi dominio.
- Globale: per assegnare le autorizzazioni ai membri del gruppo che si trovano all'interno di qualsiasi dominio o foresta.

Esistono delle limitazioni quando si modifica l'ambito di un gruppo. L'elenco e il diagramma seguenti descrivono queste limitazioni.

- Modifica dell'ambito del gruppo da Domain Local a Universal: Sì
  - A meno che il gruppo locale del dominio non sia padre di un altro gruppo locale di dominio.
- Modifica dell'ambito del gruppo da Universal a Domain Local - Sì
  - A meno che il gruppo universale non sia un gruppo figlio di un altro gruppo universale.
- Modifica dell'ambito del gruppo da Universale a Globale - Sì
  - A meno che il gruppo universale non sia il genitore di un altro gruppo universale.
- Modifica dell'ambito del gruppo da Globale a Universale - Sì
  - A meno che il gruppo globale non sia figlio di un altro gruppo globale.

Per ulteriori informazioni sugli ambiti di gruppo, consulta Microsoftla documentazione.



Connessione di AWS Managed Microsoft AD a Microsoft Entra Connect Sync

Questo tutorial illustra i passaggi necessari per l'installazione e Microsoft Entra Connect Syncla sincronizzazione Microsoft Entra IDcon AWS Managed Microsoft AD.

In questo tutorial, esegui quanto indicato di seguito:

1. Crea un utente di dominio Microsoft AD AWS gestito.
2. Scarica Entra Connect Sync.
3. Viene utilizzato PowerShell per eseguire uno script per fornire le autorizzazioni appropriate per l'utente appena creato.
4. Installare Entra Connect Sync.

Prerequisiti

Per completare questo tutorial, occorre quanto indicato di seguito:

- Un Microsoft AD AWS gestito. Per ulteriori informazioni, consulta the section called “Creazione del tuo AWS Managed Microsoft AD”.
- Un'istanza di Amazon EC2 Windows Server aggiunta al tuo AWS Managed Microsoft AD. Per ulteriori informazioni, consulta Unirsi a un'istanza Windows.

- Un EC2 Windows server con Active Directory Administration Tools installato per gestire AWS Managed Microsoft AD. Per ulteriori informazioni, consulta the section called “Installazione degli strumenti di amministrazione di AD”.

Crea un utente di dominio Active Directory

Questo tutorial presuppone che tu abbia già un AWS Managed Microsoft AD e un'istanza EC2 Windows Server con Active Directory Administration Tools installato. Per ulteriori informazioni, consulta the section called “Installazione degli strumenti di amministrazione di AD”.

1. Connect all'istanza in cui è Administration Tools stato installato Active Directory.
2. Crea un utente di dominio Microsoft AD AWS gestito. Questo utente diventerà il Active Directory Directory Service (AD DS) Connector account destinatarioEntra Connect Sync. Per i passaggi dettagliati di questo processo, vederethe section called “Creazione di un utente”.

Scarica Entra Connect Sync

- Scarica Entra Connect Sync dal Microsoftsito Web sull' EC2 istanza che è l'amministratore di AWS Managed Microsoft AD.

> **Warning**
>
> Non aprire o eseguire Entra Connect Sync a questo punto. I passaggi successivi forniranno le autorizzazioni necessarie per l'utente di dominio creato nel passaggio 1.

Esegui script PowerShell

- Apri PowerShell come amministratore ed esegui lo script seguente.

  Durante l'esecuzione dello script, ti verrà chiesto di inserire il AMAccountnome s per l'utente di dominio appena creato nel passaggio 1.

  > **Note**
  >
  > Per ulteriori informazioni sull'esecuzione dello script, consulta quanto segue:

- È possibile salvare lo script con l'`ps1`estensione in una cartella come**`temp`**. Quindi, puoi usare il seguente PowerShell comando per caricare lo script:

  ```
  import-module "c:\temp\entra.ps1"
  ```

- Dopo aver caricato lo script, è possibile utilizzare il seguente comando per impostare le autorizzazioni necessarie per eseguire lo script, sostituendolo *`Entra_Service_Account_Name`* con il nome dell'account del Entra servizio:

  ```
  Set-EntraConnectSvcPerms -ServiceAccountName Entra_Service_Account_Name
  ```

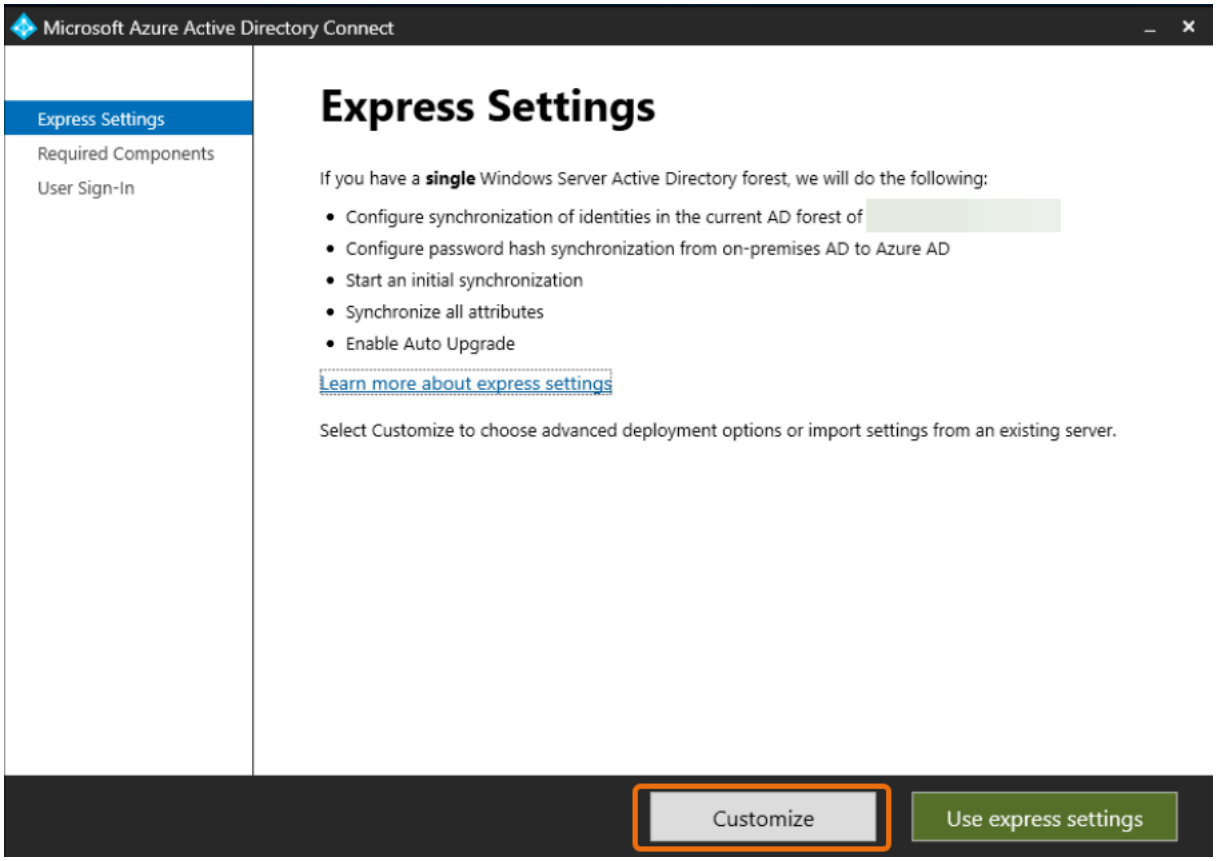
```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

try {
    # Attempt to import the module
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
    Import-Module $modulePath -ErrorAction Stop
    Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }
```

```
    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    Try {
        $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
 Stop | Select-Object -ExpandProperty 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get service account DN $_"
    }

    Foreach ($OU in $OUs) {
        try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
 $ADConnectorAccountDN -ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
 on OU $OU"
    }
    catch {
        Write-Host "An error occurred while setting permissions for
 $ADConnectorAccountDN on OU $OU : $_"
    }
    }
}
```

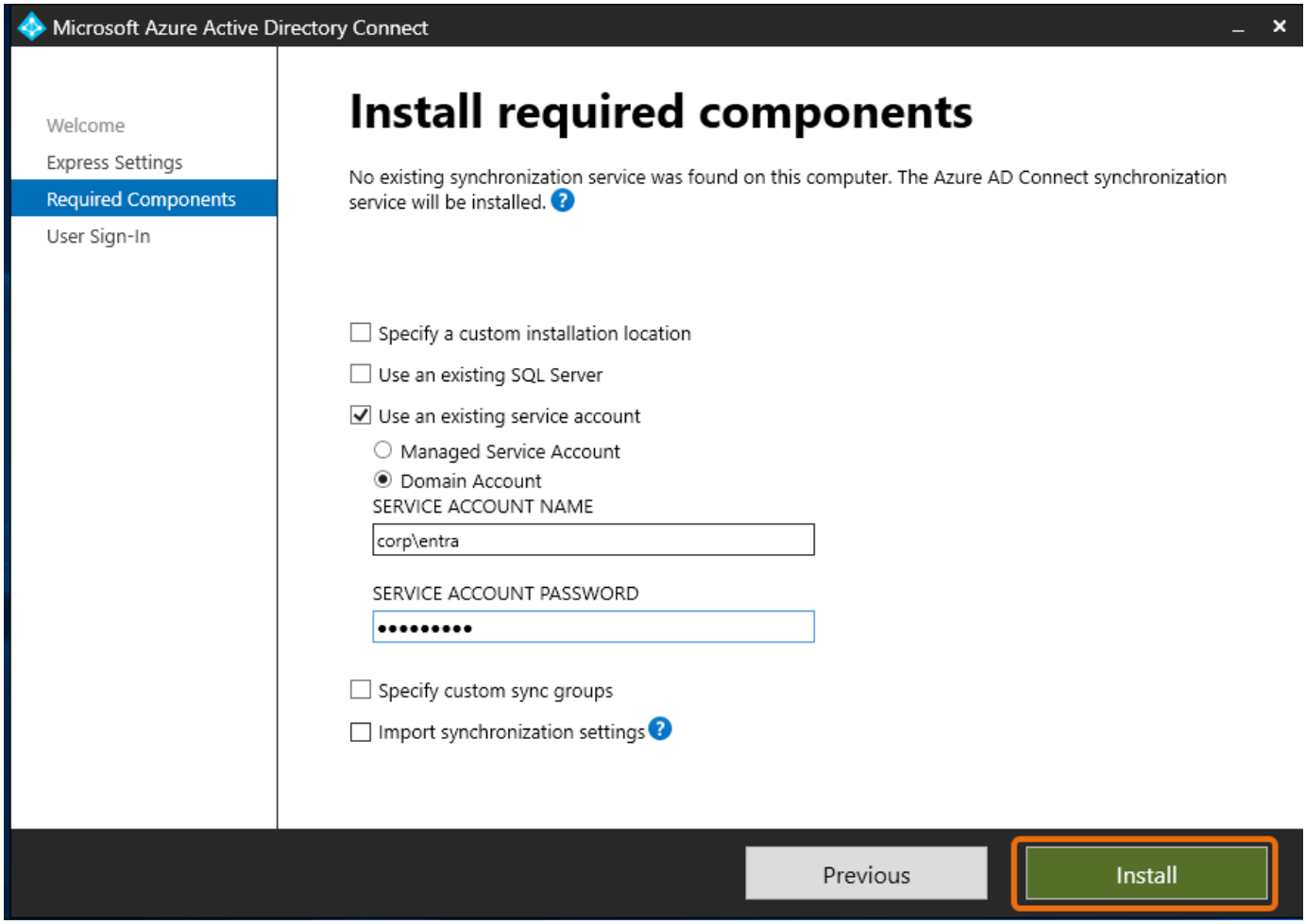
Installazione di Entra Connect Sync

1. Una volta completato lo script, è possibile eseguire il file di Microsoft Entra Connect configurazione scaricato (precedentemente noto comeAzure Active Directory Connect).

2. Una Microsoft Azure Active Directory Connect finestra si apre dopo aver eseguito il file di configurazione del passaggio precedente. Nella finestra Express Settings, seleziona Personalizza.



3. Nella finestra Installa i componenti richiesti, seleziona la casella di controllo Usa un account di servizio esistente. In NOME DELL'ACCOUNT DI SERVIZIO e PASSWORD DELL'ACCOUNT DI SERVIZIO, inserisci il AD DS Connector account nome e la password dell'utente creato nel passaggio 1. Ad esempio, se il tuo AD DS Connector account nome è`entra`, il nome dell'account sarà`corp\entra`. Quindi seleziona Installa.



4. Nella finestra Accesso utente, seleziona una delle seguenti opzioni:

   a. Autenticazione pass-through: questa opzione consente di accedere ad Active Directory con nome utente e password.

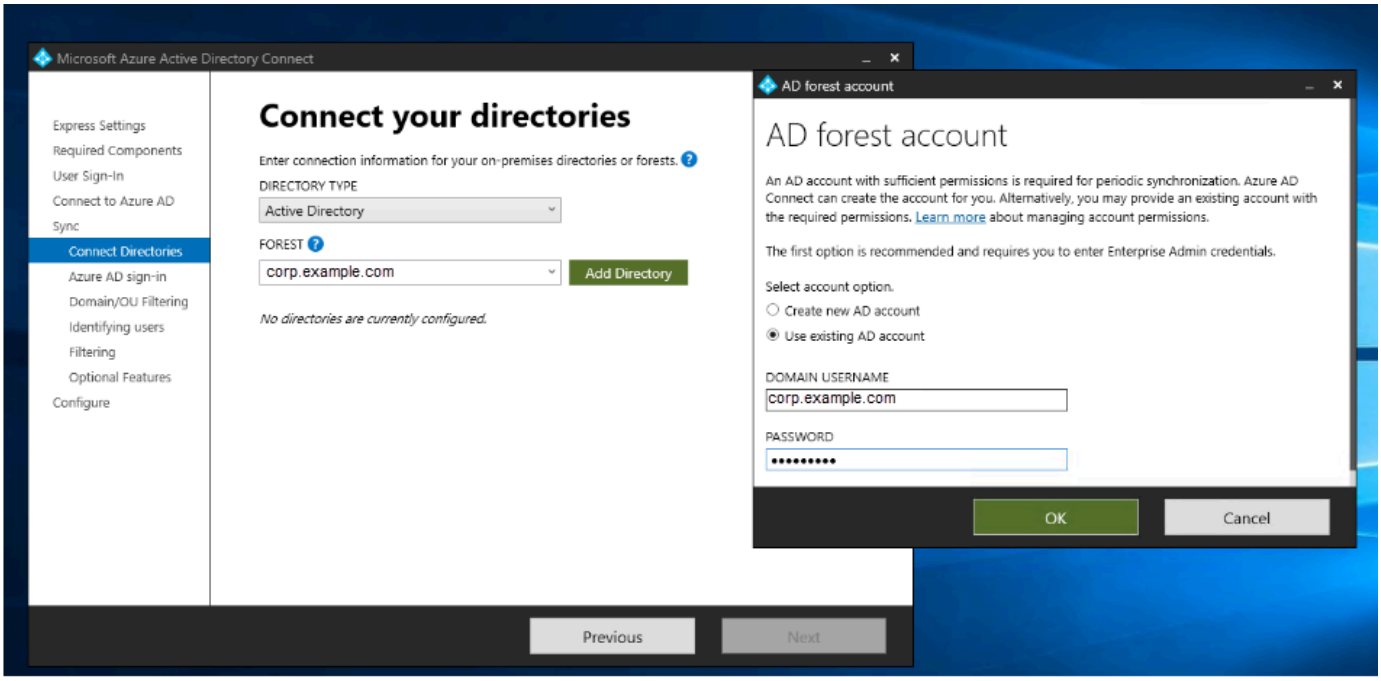
   b. Non configurare: consente di utilizzare l'accesso federato con Microsoft Entra (precedentemente noto come Azure Active Directory (AzureAD)) o. Office 365

   Quindi seleziona Avanti.

5. AzureNella finestra Connect to, inserisci il nome utente e la password di Global Administrator per Entra ID e seleziona Avanti.

6. Nella finestra Connect your directories, scegli Active Directory per DIRECTORY TYPE. Scegli la foresta per il tuo AWS Managed Microsoft AD for FOREST. Quindi seleziona Aggiungi directory.

7. Viene visualizzata una finestra pop-up che richiede le opzioni del tuo account. Seleziona Usa un account AD esistente. Inserisci il AD DS Connector account nome utente e la password creati nel passaggio 1, quindi seleziona OK. Quindi seleziona Avanti.



8. Nella finestra di Azure ADaccesso, seleziona Continua senza abbinare tutti i suffissi UPN ai domini verificati, solo se non hai aggiunto un vanity domain verificato. Entra ID Quindi seleziona Avanti.
9. Nella finestra di filtraggio Dominio/OU, seleziona le opzioni più adatte alle tue esigenze. Per ulteriori informazioni, vedere Entra Connect Sync: Configurazione del filtro nella documentazione. Microsoft Quindi seleziona Avanti.
10. Nella finestra Identificazione degli utenti, filtri e funzionalità opzionali, mantieni i valori predefiniti e seleziona Avanti.
11. Nella finestra Configura, rivedi le impostazioni di configurazione e seleziona Configura. L'installazione di Entra Connect Sync verrà completata e gli utenti inizieranno la sincronizzazione con. Microsoft Entra ID

AWS Tutorial gestiti per laboratori di test Microsoft AD

Questa sezione fornisce una serie di tutorial guidati per aiutarti a creare un ambiente di test lab in AWS cui sperimentare con Managed AWS Microsoft AD.

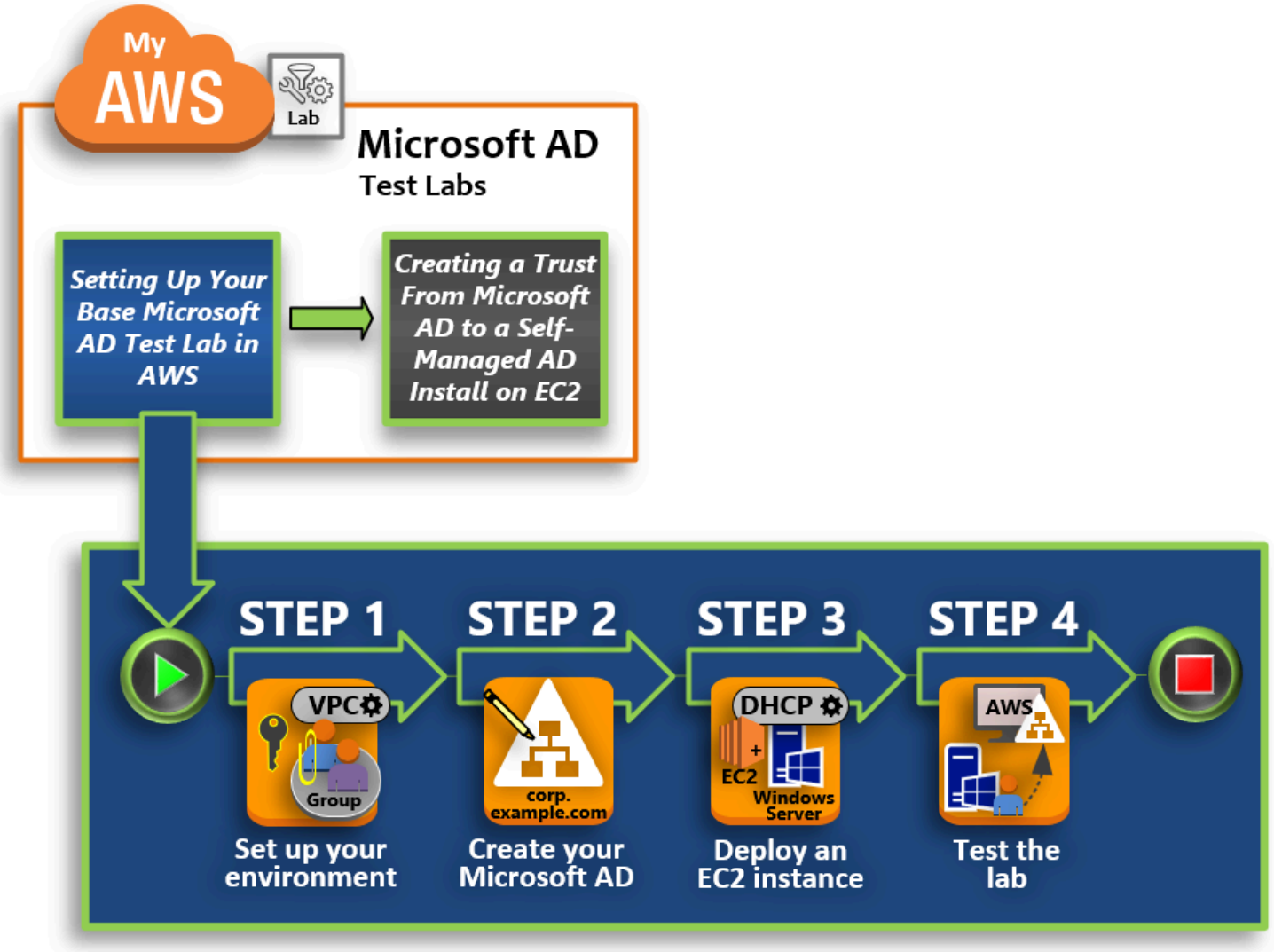
Argomenti

- Tutorial: configurazione del laboratorio di test Microsoft AD AWS gestito di base in AWS
- Tutorial: creazione di un trust da AWS Managed Microsoft AD a un'installazione di Active Directory autogestita su Amazon EC2

Tutorial: configurazione del laboratorio di test Microsoft AD AWS gestito di base in AWS

Questo tutorial ti insegna come configurare il tuo AWS ambiente per prepararti a una nuova installazione di AWS Managed Microsoft AD che utilizza una nuova EC2 istanza Amazon che esegue Windows Server 2019. Quindi ti insegna a utilizzare gli strumenti di amministrazione tipici di Active Directory per gestire l'ambiente Microsoft AD AWS gestito dall'istanza di EC2 Windows. Una volta completato il tutorial, avrai impostato i prerequisiti di rete e avrai configurato una nuova foresta Microsoft AD AWS gestita.

Come illustrato nella figura seguente, il lab creato con questo tutorial è il componente fondamentale per l'apprendimento pratico di Managed AWS Microsoft AD. Successivamente, puoi aggiungere tutorial opzionali per ulteriore esperienza pratica. Questa serie di tutorial è ideale per tutti coloro che hanno iniziato da poco a utilizzare Microsoft AD gestito da AWS e che desiderano un laboratorio di sviluppo per scopi di valutazione. questo tutorial dura circa un'ora.



[Fase 1: Configurare AWS l'ambiente per AWS Managed Microsoft AD Active Directory]

Dopo aver completato le attività preliminari, crei e configuri un Amazon VPC nella EC2 tua istanza.

[Passaggio 2: crea la tua directory Microsoft AD Active Directory AWS gestita]

In questo passaggio, configuri AWS Managed Microsoft AD AWS per la prima volta.

[Fase 3: Implementa un' EC2 istanza Amazon per gestire il tuo AWS Managed Microsoft AD Active Directory]

Qui vengono illustrate le varie attività successive alla distribuzione necessarie per consentire ai computer client di connettersi al nuovo dominio e configurare un nuovo sistema Windows Server. EC2

Fase 4: verifica che il laboratorio di sviluppo di base sia operativo

Infine, in qualità di amministratore, verifichi di poter accedere e connetterti a AWS Managed Microsoft AD dal tuo sistema Windows Server EC2. Una volta che hai testato la funzionalità del tuo lab, puoi continuare ad aggiungere altri moduli di guide lab di sviluppo.

Prerequisiti

Se prevedi di usare solo i passaggi dell'interfaccia utente descritti in questo tutorial per creare il tuo lab di sviluppo, è possibile ignorare questa sezione relativa ai prerequisiti e passare alla Fase 1. Tuttavia, se prevedi di utilizzare AWS CLI comandi o AWS Tools for Windows PowerShell moduli per creare il tuo ambiente di test lab, devi prima configurare quanto segue:

- Utente IAM con chiave di accesso e chiave di accesso segreta: per utilizzare i AWS Tools for Windows PowerShell moduli AWS CLI or è necessario un utente IAM con una chiave di accesso. Se non si disponi di una chiave di accesso, consulta Creazione, modifica e visualizzazione delle chiavi di accesso (Console di gestione AWS).
- AWS Command Line Interface(opzionale): scaricalo e installalo AWS CLI su Windows. Una volta installato, apri il prompt dei comandi o la PowerShell finestra, quindi digita`aws configure`. Nota che è necessaria la chiave di accesso e la chiave segreta per completare la configurazione. Guarda i prerequisiti iniziali per le fasi relative alle modalità di esecuzione di questa operazione. Ti verrà richiesto:
  - AWSID della chiave di accesso [Nessuno]: `AKIAIOSFODNN7EXAMPLE`
  - AWSchiave di accesso segreta [Nessuna]: `wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY`
  - Il nome di default della regione [Nessuno]: `us-west-2`
  - Il formato di output di default: [Nessuno]: `json`
- AWS Tools for Windows PowerShell(opzionale): scarica e installa la versione più recente AWS Tools for Windows PowerShell del modulo https://aws.amazon.com/powershell/, quindi esegui il comando seguente. Nota che è necessaria la tua chiave di accesso e la chiave segreta per completare la configurazione. Guarda i prerequisiti iniziali per le fasi relative alle modalità di esecuzione di questa operazione.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Fase 1: Configurare AWS l'ambiente per AWS Managed Microsoft AD Active Directory

Prima di poter creare AWS Managed Microsoft AD nel tuo laboratorio di AWS test, devi prima configurare la tua coppia di EC2 chiavi Amazon in modo che tutti i dati di accesso siano crittografati.

Creazione di una coppia di chiavi

Se già disponi una coppia di chiavi, questa fase può essere ignorata. Per ulteriori informazioni sulle coppie di EC2 chiavi Amazon, consulta Create key pairs.

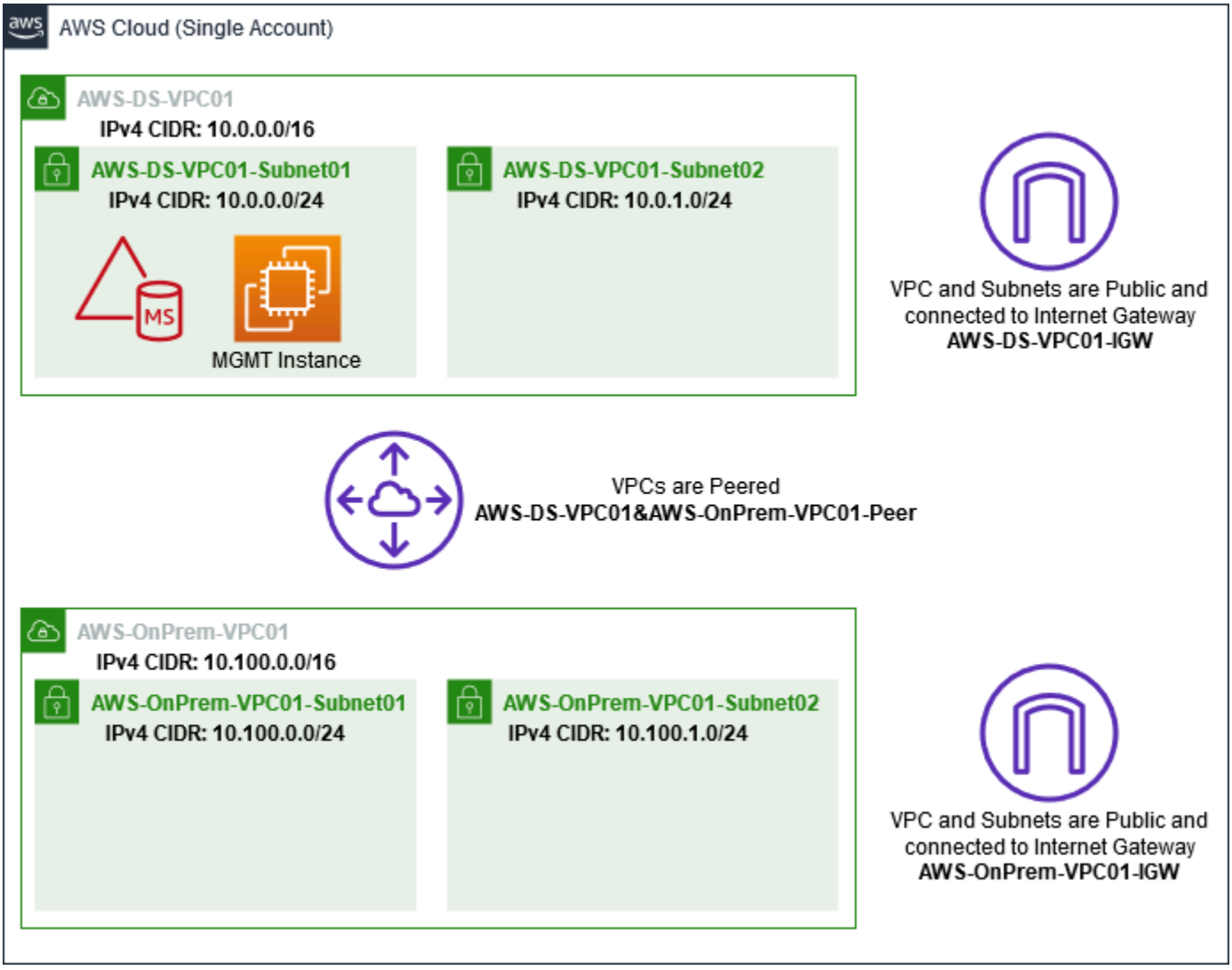
Come creare una coppia di chiavi

1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel pannello di navigazione, in Network & Security (Sicurezza e rete), scegli Key Pairs (Coppie di chiavi) e quindi scegliere Crea Key Pair (Crea coppia di chiavi).
3. Per Nome coppia di chiavi, digitare **`AWS-DS-KP`**. Per Formato file coppia di chiavi, selezionare pem, quindi scegliere Crea.
4. Il file della chiave privata viene automaticamente scaricato dal browser. Il nome di file è il nome che hai specificato quando hai creato la coppia di chiavi con estensione `.pem`. Salvare il file della chiave privata in un luogo sicuro.

> **Important**
>
> Questo è l'unico momento in cui salvare il file della chiave privata. È necessario fornire il nome della coppia di chiavi quando avvii un'istanza e la chiave privata corrispondente ogni volta che decripti la password per l'istanza.

Crea, configura ed esegui il peering di due Amazon VPCs

Come illustrato nella figura seguente, al termine di questo processo in più fasi, avrai creato e configurato due sottoreti pubbliche VPCs, due sottoreti pubbliche per VPC, un Internet Gateway per VPC e una connessione peering VPC tra. VPCs Abbiamo scelto di utilizzare reti pubbliche VPCs e sottoreti per motivi di semplicità e costi. Per i carichi di lavoro di produzione, ti consigliamo di utilizzare il formato privato. VPCs Per maggiori informazioni sul miglioramento della sicurezza VPC, consulta Sicurezza in Amazon Virtual Private Cloud.



Tutti gli PowerShell esempi utilizzano le informazioni VPC riportate di seguito e sono integrati in us-west-2. AWS CLI Puoi scegliere qualsiasi regione supportata in cui creare l'ambiente. Per ulteriori informazioni, consulta Cos'è Amazon VPC?

Passaggio 1: creane due VPCs

In questo passaggio, è necessario crearne due VPCs nello stesso account utilizzando i parametri specificati nella tabella seguente. AWSMicrosoft AD gestito supporta l'uso di account separati con Condividi il tuo AWS Managed Microsoft AD questa funzionalità. Il primo VPC verrà utilizzato per Managed AWS Microsoft AD. Il secondo VPC verrà utilizzato per le risorse che possono essere utilizzate successivamente in Tutorial: creazione di un trust da AWS Managed Microsoft AD a un'installazione di Active Directory autogestita su Amazon EC2.

Informazioni gestite su Active Directory VPC	Informazioni sul VPC on-premise
Targhetta con nome: AWS -DS-VPC01	Targhetta con nome: AWS - -VPC01 OnPrem
IPv4 Blocco CIDR: 10.0.0.0/16	IPv4 Blocco CIDR: 10.100.0.0/16
IPv6 Blocco CIDR: nessun blocco CIDR IPv6	IPv6 Blocco CIDR: nessun blocco CIDR IPv6
Tenancy: predefinito	Tenancy: predefinito

Per istruzioni dettagliate, consulta Creazione di un VPC.

Passaggio 2: Creare due sottoreti per VPC

Dopo aver creato il, sarà VPCs necessario creare due sottoreti per VPC utilizzando i parametri specificati nella tabella seguente. Per questo laboratorio di test ogni sottorete sarà /24. Ciò consente di emettere fino a 256 indirizzi per sottorete. Ogni sottorete deve essere un in una AZ separata. Mettere ogni sottorete in una AZ separata è uno dei Prerequisiti per la creazione di un AWS Managed Microsoft AD.

Informazioni sulla sottorete AWS-DS-VPC01:	AWS- Informazioni sulla sottorete OnPrem - VPC01
Targhetta con nome: -DS-VPC01-subnet01 AWS VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS Zona di disponibilità predefinita: us-west-2a IPv4 Blocco CIDR: 10.0.0.0/24	Tag con nome: - -VPC01-subnet01 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - AWS -VPC01 OnPrem Zona di disponibilità predefinita: us-west-2a IPv4 Blocco CIDR: 10.100.0.0/24
Tag con nome: AWS -DS-VPC01-subnet02 VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS Zona di disponibilità: us-west-2b IPv4 Blocco CIDR: 10.0.1.0/24	Tag con nome: - -VPC01-subnet02 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - AWS -VPC01 OnPrem

Informazioni sulla sottorete AWS-DS-VPC01:	AWS- Informazioni sulla sottorete OnPrem - VPC01
	Zona di disponibilità: us-west-2b IPv4 Blocco CIDR: 10.10.1.0/24

Per istruzioni dettagliate, consulta Creazione di una sottorete nel VPC.

Fase 3: Creare e collegare un Internet Gateway al VPCs

Poiché utilizziamo public, VPCs dovrete creare e collegare un gateway Internet al vostro dispositivo VPCs utilizzando i parametri specificati nella tabella seguente. Questo vi permetterà di connettervi e gestire le vostre EC2 istanze.

Informazioni sul gateway Internet AWS-DS-VPC01	AWS- Informazioni sull'OnPremInternet Gateway -VPC01
Targhetta con nome: -DS-VPC01-IGW AWS VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS	Targhetta con nome: - -VPC01-IGW AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - AWS -VPC01 OnPrem

Per istruzioni dettagliate, consulta Gateway Internet.

Fase 4: Configurare una connessione peering VPC tra AWS -DS-VPC01 e - -VPC01 AWS OnPrem

Poiché ne hai già creati due VPCs in precedenza, dovrai collegarli in rete utilizzando il peering VPC utilizzando i parametri specificati nella tabella seguente. Sebbene ci siano molti modi per connettere il tuo VPCs, questo tutorial utilizzerà il peering VPC. AWSManaged Microsoft AD supporta molte soluzioni per connettere il tuo VPCs, alcune di queste includono il peering VPC, il Transit Gateway e la VPN.

Denominazione della connessione peering: AWS -DS-VPC01& - -VPC01-Peer AWS OnPrem VPC (richiedente): vpc-xxxxxxxxxxxxxxxxxxx -DS-VPC01 AWS Account: il mio account

Regione: questa regione

VPC (accetta): vpc-xxxxxxxxxxxxxxxxx - -VPC01 AWS OnPrem

Per istruzioni su come creare una connessione di peering VPC con un altro VPC dal tuo account, consulta Creazione di una connessione di peering VPC con un altro VPC nell'account.

Passaggio 5: aggiungi due percorsi alla tabella di routing principale di ogni VPC

Affinché i gateway Internet e la connessione peering VPC creati nei passaggi precedenti funzionino, è necessario aggiornare la tabella di routing principale di VPCs entrambi utilizzando i parametri specificati nella tabella seguente. Verranno aggiunti due route: 0.0.0.0/0 che sarà indirizzato a tutte le destinazioni non esplicitamente note alla tabella del percorso e 10.0.0.0/16 o 10.100.0.0/16 che verranno instradati a ciascun VPC tramite la connessione peering VPC stabilita sopra.

Puoi trovare facilmente la tabella di routing corretta per ogni VPC filtrando il tag del nome VPC (AWS-DS-VPC01 o - -VPC01). AWS OnPrem

Informazioni sull'instradamento 1 AWS-DS-VPC01	Informazioni sull'instradamento 2 AWS-DS-VPC01	AWS- Informazioni sulla route 1 -VPC01 OnPrem	AWS- Informazioni sulla route 2 OnPrem -VPC01
Destinazione: 0.0.0.0/0 Destinazione: igw-xxxxxxxxxxxxxxxxx - DS-VPC01-IGW AWS	Destinazione: 10.100.0.0/16 Obiettivo: pcx-xxxxx xxxxxxxxxxxxx AWS -DS-VPC01& - - VPC01-Peer AWS OnPrem	Destinazione: 0.0.0.0/0 Obiettivo: igw-xxxxx xxxxxxxxxxxxx AWS -onPrem-VPC01	Destinazione: 10.0.0.0/16 Obiettivo: pcx-xxxxx xxxxxxxxxxxxx AWS -DS-VPC01& - - VPC01-Peer AWS OnPrem

Per istruzioni su come aggiungere route a una tabella di route VPC, consulta Aggiunta e rimozione di route da una tabella di route.

Crea gruppi di sicurezza per le EC2 istanze Amazon

Per impostazione predefinita, AWS Managed Microsoft AD crea un gruppo di sicurezza per gestire il traffico tra i relativi controller di dominio. In questa sezione, dovrai creare 2 gruppi di sicurezza

(uno per ogni VPC) che verranno utilizzati per gestire il traffico all'interno del tuo VPC per le tue EC2 istanze utilizzando i parametri specificati nelle tabelle seguenti. È inoltre possibile aggiungere una regola che consente l'ingresso di RDP (3389) da qualunque luogo e l'ingresso di tutti i tipi di traffico dal VPC locale. Per ulteriori informazioni, consulta Gruppi EC2 di sicurezza Amazon per istanze Windows.

Informazioni sul gruppo di sicurezza AWS-DS-VPC01:
Nome del gruppo di sicurezza: AWS DS Test Lab Security Group
Descrizione: AWS DS Test Lab Security Group
VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS

Regole di sicurezza in entrata per -DS-VPC01 AWS

Tipo	Protocollo	Intervallo porte	Origine	Tipo di traffico
Regola TCP personalizzata	TCP	3389	Il mio IP	Remote Desktop (Desktop remoto)
All Traffic	Tutti	Tutti	10.0.0.0/16	Tutto il traffico VPC locale

Regole dei gruppi di sicurezza in uscita per -DS-VPC01 AWS

Tipo	Protocollo	Intervallo porte	Destinazione	Tipo di traffico
All Traffic	Tutti	Tutti	0.0.0.0/0	Tutto il traffico

AWS- Informazioni sul gruppo di sicurezza -VPC01: OnPrem
Nome del gruppo di sicurezza: AWS OnPrem Test Lab Security Group.
Descrizione: AWS OnPrem Test Lab Security Group.

AWS- Informazioni sul gruppo di sicurezza -VPC01: OnPrem
VPC: vpc-xxxxxxxxxxxxxxxxx - AWS -VPC01 OnPrem

Regole di sicurezza in entrata per - -VPC01 AWS OnPrem

Tipo	Protocollo	Intervallo porte	Origine	Tipo di traffico
Regola TCP personalizzata	TCP	3389	Il mio IP	Remote Desktop (Desktop remoto)
Regola TCP personalizzata	TCP	53	10.0.0.0/16	DNS
Regola TCP personalizzata	TCP	88	10.0.0.0/16	Kerberos
Regola TCP personalizzata	TCP	389	10.0.0.0/16	LDAP
Regola TCP personalizzata	TCP	464	10.0.0.0/16	Kerberos cambia/imposta la password
Regola TCP personalizzata	TCP	445	10.0.0.0/16	SMB/CIFS
Regola TCP personalizzata	TCP	135	10.0.0.0/16	Replica
Regola TCP personalizzata	TCP	636	10.0.0.0/16	LDAP SSL
Regola TCP personalizzata	TCP	49152 - 65535	10.0.0.0/16	RPC
Regola TCP personalizzata	TCP	3268 - 3269	10.0.0.0/16	LDAP GC & LDAP GC SSL

Tipo	Protocollo	Intervallo porte	Origine	Tipo di traffico
Regola UDP personalizzata	UDP	53	10.0.0.0/16	DNS
Regola UDP personalizzata	UDP	88	10.0.0.0/16	Kerberos
Regola UDP personalizzata	UDP	123	10.0.0.0/16	Ora di Windows
Regola UDP personalizzata	UDP	389	10.0.0.0/16	LDAP
Regola UDP personalizzata	UDP	464	10.0.0.0/16	Kerberos cambia/imposta la password
All Traffic	Tutti	Tutti	10.100.0.0/16	Tutto il traffico VPC locale

Regole del gruppo di sicurezza in uscita per - -VPC01 AWS OnPrem

Tipo	Protocollo	Intervallo porte	Destinazione	Tipo di traffico
All Traffic	Tutti	Tutti	0.0.0.0/0	Tutto il traffico

Per istruzioni dettagliate su come creare e aggiungere regole ai gruppi di sicurezza, consulta Utilizzo dei gruppi di sicurezza.

Passaggio 2: crea la tua directory Microsoft AD Active Directory AWS gestita

È possibile utilizzare tre metodi differenti per creare la tua directory. È possibile utilizzare la Console di gestione AWS procedura (consigliata per questo tutorial) oppure utilizzare AWS Tools for Windows PowerShell le procedure AWS CLI o per creare la directory.

Metodo 1: per creare la directory AWS Managed Microsoft AD (Console di gestione AWS)

1. Nel riquadro di navigazione della Console AWS Directory Service, scegli Directory, quindi seleziona Configura directory.
2. Nella pagina Seleziona il tipo di directory, scegli Microsoft AD gestito da AWS, quindi seleziona Successivo.
3. Nella pagina Enter directory information (Inserisci le informazioni sulla directory), fornisci le seguenti informazioni, quindi seleziona Next (Successivo).

   - Per Edition (Edizione), scegli Standard Edition o Enterprise Edition. Per ulteriori informazioni sulle edizioni, consulta Servizio di directory AWS per Microsoft Active Directory.
   - In Directory DNS name (Nome DNS directory), digita **`corp.example.com`**.
   - In Directory NetBIOS name (Nome NetBIOS della directory), digita **`corp`**.
   - In Directory description (Descrizione directory), digita **`AWSDS Managed`**.
   - Per Admin password (Amministratore password) digita la password da utilizzare per questo account e digitala nuovamente in Confirm password (Conferma password). Questo Admin (Amministratore) dell'account è creato automaticamente durante il processo di creazione della directory. La password non può includere la parola admin. La password dell'amministratore della directory applica la distinzione tra maiuscole e minuscole e deve contenere tra 8 e 64 caratteri, inclusi. Deve anche contenere un carattere di almeno tre delle seguenti quattro categorie:
     - Lettere minuscole (a-z)
     - Lettere maiuscole (A-Z)
     - Numeri (0-9)
     - Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
4. Nella pagina Choose VPC and subnets (Scegli VPC e sottoreti) fornire le seguenti informazioni, quindi selezionare Next (Successivo).

   - Per VPC, scegli l'opzione che inizia con AWS-DS-VPC01 e termina con (10.0.0.0/16).
   - Per Sottoreti, scegli le sottoreti pubbliche 10.0.0.0/24 e 10.0.1.0/24.
5. Nella pagina Review & create (Rivedi e crea), esaminare le informazioni relative alla directory ed eseguire eventuali modifiche. Quando le informazioni sono corrette, scegli Create Directory (Crea directory). La creazione di una directory richiede dai 20 ai 40 minuti. Una volta creato, il valore Status cambia in Active (Attivo).

Metodo 2: creare il tuo AWS Managed Microsoft AD (PowerShell) (opzionale)

1. Aprire PowerShell.
2. Digita il seguente comando. Assicuratevi di utilizzare i valori forniti nel passaggio 4 della Console di gestione AWS procedura precedente.

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
 -Description "AWSDS Managed" - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

Metodo 3: per creare il tuo AWS Managed Microsoft AD (AWS CLI) (opzionale)

1. Aprire ilAWS CLI.
2. Digita il seguente comando. Accertarsi di utilizzare i valori forniti nel passaggio 4 della Console di gestione AWS procedura precedente.

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWSDS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

Fase 3: Implementa un' EC2 istanza Amazon per gestire il tuo AWS Managed Microsoft AD Active Directory

Per questo laboratorio, utilizziamo EC2 istanze Amazon con indirizzi IP pubblici per semplificare l'accesso all'istanza di gestione da qualsiasi luogo. In un ambiente di produzione, puoi utilizzare istanze che si trovano in un VPC privato accessibili solo tramite una VPN Direct Connect o un collegamento. Non è necessario che l'istanza abbia un indirizzo IP pubblico.

In questa sezione vengono illustrate le varie attività successive alla distribuzione necessarie per consentire ai computer client di connettersi al dominio utilizzando Windows Server sulla nuova istanza. EC2 Usa la Windows Server nella fase successiva per verificare che il lab sia operativo.

Facoltativo: crea un set di opzioni DHCP in AWS -DS-VPC01 per la tua directory

In questa procedura facoltativa, configuri un ambito di opzioni DHCP in modo che EC2 le istanze nel tuo VPC utilizzino automaticamente il tuo Managed AWS Microsoft AD per la risoluzione DNS. Per ulteriori informazioni, consulta la pagina relativa ai Set di opzioni DHCP.

Creazione di un set opzioni DHCP per la tua directory

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere DHCP Options Sets (Set di opzioni DHCP), quindi selezionare Create DHCP options set (Crea set di opzioni DHCP).
3. Nella pagina Create DHCP options set (Crea set opzioni DHCP), fornire i seguenti valori per la directory:
   - In Name (Nome) digitare **`AWSDS DHCP`**.
   - Per Domain name (Nome dominio), digitare **`corp.example.com`**.
   - Per Domain name servers (Server dei nomi di dominio), digita gli indirizzi IP dei server DNS della tua directory fornita da AWS.

     > **Note**
     >
     > Per trovare questi indirizzi, vai alla pagina Directory Service Directory, quindi scegli l'ID di directory applicabile. Nella pagina Dettagli, identifica e utilizza IPs quelli visualizzati nell'indirizzo DNS.
     > In alternativa, per trovare questi indirizzi, vai alla pagina Directory del Directory Service e scegli l'ID directory applicabile. Quindi, scegli Dimensiona e condividi. In Controller di dominio, identifica e utilizza IPs quelli visualizzati nell'indirizzo IP.

   - Lascia vuoto per le impostazioni NTP servers (Server NTP), NetBIOS name servers (Server dei nomi NetBIOS) e NetBIOS node type (Tipo di nodo NetBIOS).
4. Scegliere Create DHCP options set (Crea set di opzioni DHCP) e Close (Chiudi). Il nuovo set di opzioni DHCP viene visualizzato nel tuo elenco delle opzioni DHCP.
5. Prendi nota dell'ID del nuovo set di opzioni DHCP (dopt -). *`xxxxxxxx`* Si utilizza al termine di questa procedura, quando si associa il nuovo set di opzioni al VPC.

   > **Note**
   >
   > L'aggiunta ai domini uniforme funziona senza dover configurare un set di opzioni DHCP.

6. Nel riquadro di navigazione, scegli Your. VPCs
7. Nell'elenco VPCs, seleziona AWSDS VPC, scegli Azioni, quindi scegli Modifica set di opzioni DHCP.

8. Nella pagina Edit DHCP options set (Modifica set di opzioni DHCP), selezionare le opzioni registrate nella fase e sceglie reSave.

Crea un ruolo per aggiungere istanze Windows al tuo dominio Microsoft AD AWS gestito

Utilizza questa procedura per configurare un ruolo che unisce un'istanza Amazon EC2 Windows a un dominio. Per ulteriori informazioni, consulta Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory.

Per configurare EC2 l'aggiunta di istanze Windows al tuo dominio

1. Aprire la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio).
4. Immediatamente in Scegli il servizio che utilizzerà questo ruolo, scegli EC2, quindi scegli Avanti: Autorizzazioni.
5. Nella pagina Attached permissions policy (Policy autorizzazioni collegate), eseguire quanto segue:

   - Seleziona la casella accanto alla politica SSMManaged InstanceCore gestita da Amazon. Questa policy fornisce le autorizzazioni minime necessarie per utilizzare il servizio Systems Manager.
   - Seleziona la casella accanto a Amazon SSMDirectory ServiceAccess managed policy. La policy fornisce le autorizzazioni per collegare le istanze a una Active Directory gestita da Directory Service.

   Per informazioni su queste regole gestite e altre policy che puoi collegare a un profilo dell'istanza IAM per Systems Manager, consulta Creazione di un profilo di istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager. Per ulteriori informazioni sulle policy, consulta Policy gestite da AWS nella Guida per l'utente IAM.
6. Scegliere Next: Tags (Successivo: Tag).
7. (Facoltativo) Aggiungere una o più coppie chiave-valore di tag per organizzare, monitorare o controllare l'accesso per questo ruolo, quindi scegliere Next: Review (Successivo: Rivedi).
8. Per Nome ruolo, inserisci un nome per il ruolo che descrive che viene utilizzato per unire le istanze a un dominio, ad EC2DomainJoinesempio.

9. (Facoltativo) Per Role Description (Descrizione ruolo), immetti una descrizione.
10. Scegliere Create role (Crea ruolo). Il sistema visualizza di nuovo la pagina Ruoli.

Crea un' EC2 istanza Amazon e unisciti automaticamente alla directory

In questa procedura configuri un sistema Windows Server in un' EC2 istanza che può essere utilizzata in seguito per amministrare utenti, gruppi e politiche in Active Directory.

Per creare un' EC2 istanza e aggiungerla automaticamente alla directory

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. Nella pagina Passaggio 1, accanto a Microsoft Windows Server 2019 Base, ami-***xxxxxxxxxxxxxxxxx*** scegli Seleziona.
4. Nella pagina Fase 2, seleziona t3.micro (nota, è possibile scegliere un tipo di istanza più grande) e quindi selezionare Successivo: configura Dettagli istanza.
5. Nella pagina Step 3 (Fase 3), esegui le operazioni seguenti:
   - Per Rete, scegli il VPC che termina con AWS-DS-VPC01 (ad esempio, vpc- | -DS-VPC01). ***xxxxxxxxxxxxxxxxx*** AWS
   - Per Subnet scegli Public subnet 1, che deve essere preconfigurata per la tua zona di disponibilità preferita (ad esempio, subnet- | -DS-VPC01-subnet01 |). ***xxxxxxxxxxxxxxxxx*** AWS ***us-west-2a***
   - Per Auto-assign Public IP (Assegna automaticamente IP pubblico), scegli Enable (Abilita) (se l'impostazione della sottorete non è configurata per l'abilitazione come impostazione predefinita).
   - Per la directory di aggiunta al dominio, scegliete corp.example.com (d-). ***xxxxxxxxxx***
   - Per il ruolo IAM scegli il nome a cui hai assegnato il ruolo dell'istanza, ad esempio. Crea un ruolo per aggiungere istanze Windows al tuo dominio Microsoft AD AWS gestito EC2DomainJoin
   - Lascia le altre impostazioni ai valori predefiniti.
   - Scegli Passaggio successivo: aggiunta dello storage.
6. Nella pagina Step 4 (Fase 4), mantieni le impostazioni predefinite, quindi scegli Next: Add Tags (Successivo: aggiungi tag).

7. Nella pagina Step 5 (Fase 5), scegli Add tag (Aggiungi tag). In Key (Chiave) digita **`corp.example.com-mgmt`** quindi scegli Next: Configure Security Group (Successivo: configura gruppo di sicurezza).
8. Nella pagina Fase 6, scegli Seleziona un gruppo di sicurezza esistente, seleziona Gruppo di sicurezza AWS DS Test Lab (che hai già configurato nel tutorial di base), quindi scegli Analizza e avvia per analizzare l'istanza.
9. Nella pagina Step 7 (Fase 7), analizza la pagina, quindi scegli Launch (Avvia).
10. Nella finestra di dialogo Select an existing key pair or create a new key pair (Seleziona una coppia di chiavi esistente o crea una nuova coppia di chiavi) esegui le operazioni seguenti:
    - Scegli Choose an existing key pair (Scegli una coppia di chiavi esistente).
    - In Seleziona una coppia di chiavi, scegli AWS-DS-KP.
    - Seleziona la casella di controllo I acknowledge... (Acconsento...).
    - Scegliere Launch Instances (Avvia istanze).
11. Scegli Visualizza istanze per tornare alla EC2 console Amazon e visualizzare lo stato della distribuzione.

Installa gli strumenti di Active Directory sulla tua istanza EC2

Puoi scegliere tra due metodi per installare gli strumenti di gestione del dominio Active Directory sulla tua EC2 istanza. Puoi utilizzare l'interfaccia utente di Server Manager (consigliata per questo tutorial) oppurePowerShell.

Per installare gli strumenti di Active Directory sulla tua EC2 istanza (Server Manager)

1. Nella EC2 console Amazon, scegli Istanze, seleziona l'istanza appena creata, quindi scegli Connect.
2. Nella finestra di dialogo Connect To Your Instance, scegli Ottieni password per recuperare la password se non l'hai già fatto, quindi scegli Scarica il file del desktop remoto.
3. Nella finestra di dialogo Windows Security (Sicurezza di Windows), digita le credenziali dell'amministratore locale per il computer Windows Server per effettuare l'accesso (ad esempio, **`administrator`**).
4. Nel menu Start (Inizia), scegli Server Manager.

5. In Dashboard (Pannello di controllo), scegli Add Roles and Features (Aggiungi ruoli e funzionalità).
6. In Add Roles and Features Wizard (Procedura guidata aggiunta ruoli e funzionalità), scegli Next (Successivo).
7. Nella pagina Select installation type (Seleziona tipo di installazione), scegli Role-based or feature-based installation (Installazione basata su ruoli o su funzionalità), quindi scegli Next (Successivo).
8. Nella pagina Select destination server (Seleziona server di destinazione), assicurati che sia selezionato il server locale, quindi scegli Next (Successivo).
9. Nella pagina Select server roles (Seleziona ruoli server), scegli Next (Successivo).
10. Nella pagina Select features (Seleziona funzionalità), effettua le operazioni seguenti:
    - Seleziona la casella di Group Policy Management (Gestione di Group Policy).
    - Espandi Remote Server Administration Tools (Strumenti di amministrazione server remoti) e successivamente espandi Role Administration Tools (Strumenti amministrazione ruoli).
    - Seleziona la casella di controllo AD DS and AD LDS Tools (Strumenti AD DS e AD LDS).
    - Seleziona la casella di controllo DNS Server Tools (Strumenti del server DNS).
    - Scegli Next (Successivo).
11. Nella pagina Confirm installation selections (Conferma selezioni di installazione), verifica l'informazione e quindi scegli Install (Installa). Quando la funzione di installazione è terminata, i seguenti nuovi strumenti o snap-in saranno disponibili nella cartella Strumenti di amministrazione di Windows nel menu Start.
    - Centro di amministrazione di Active Directory
    - Dominio Active Directory e Trust
    - Modulo Active Directory per PowerShell
    - Siti di Active Directory e servizi
    - Utenti Active Directory e computer
    - Modifica ADSI
    - DNS
    - Gestione di Group Policy

Per installare gli strumenti di Active Directory sull' EC2 istanza (PowerShell) (opzionale)

1. Avvia PowerShell.
2. Digita il seguente comando.

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
Tools,RSAT-DNS-Server
```

Fase 4: verifica che il laboratorio di sviluppo di base sia operativo

Utilizza la procedura seguente per verificare che il lab di sicurezza sia stato impostato correttamente prima di aggiungere ulteriori moduli di guida di lab di sicurezza. Questa procedura verifica che Windows Server sia configurato correttamente, possa connettersi al dominio corp.example.com e che possa essere utilizzato per amministrare la foresta gestita di Microsoft AD. AWS

Verifica che il lab di sviluppo sia operativo

1. Esci dall' EC2 istanza in cui hai effettuato l'accesso come amministratore locale.
2. Tornando alla EC2 console Amazon, scegli Istanze nel riquadro di navigazione. Successivamente seleziona l'istanza che hai creato. Scegli Connetti.
3. Nella finestra di dialogo Connect To Your Instance (Connetti all'istanza), scegli Download Remote Desktop File (Scarica file per il desktop remoto).
4. Nella finestra di dialogo Windows Security (Sicurezza di Windows), digita le credenziali del tuo amministratore per il dominio CORP per accedere (per esempio, **`corp\admin`**).
5. Una volta effettuato l'accesso, nel menu Start (Avvia), in Windows Administrative Tools (Strumenti di amministrazione di Windows) scegli Active Directory Users and Computers (Utenti Active Directory e computer).
6. Dovresti vedere corp.example.com visualizzato con tutti gli account predefiniti OUs e associati a un nuovo dominio. In Controllori di dominio, nota i nomi dei controller di dominio che sono stati creati automaticamente quando hai creato il tuo AWS Managed Microsoft AD nel passaggio 2 di questo tutorial.

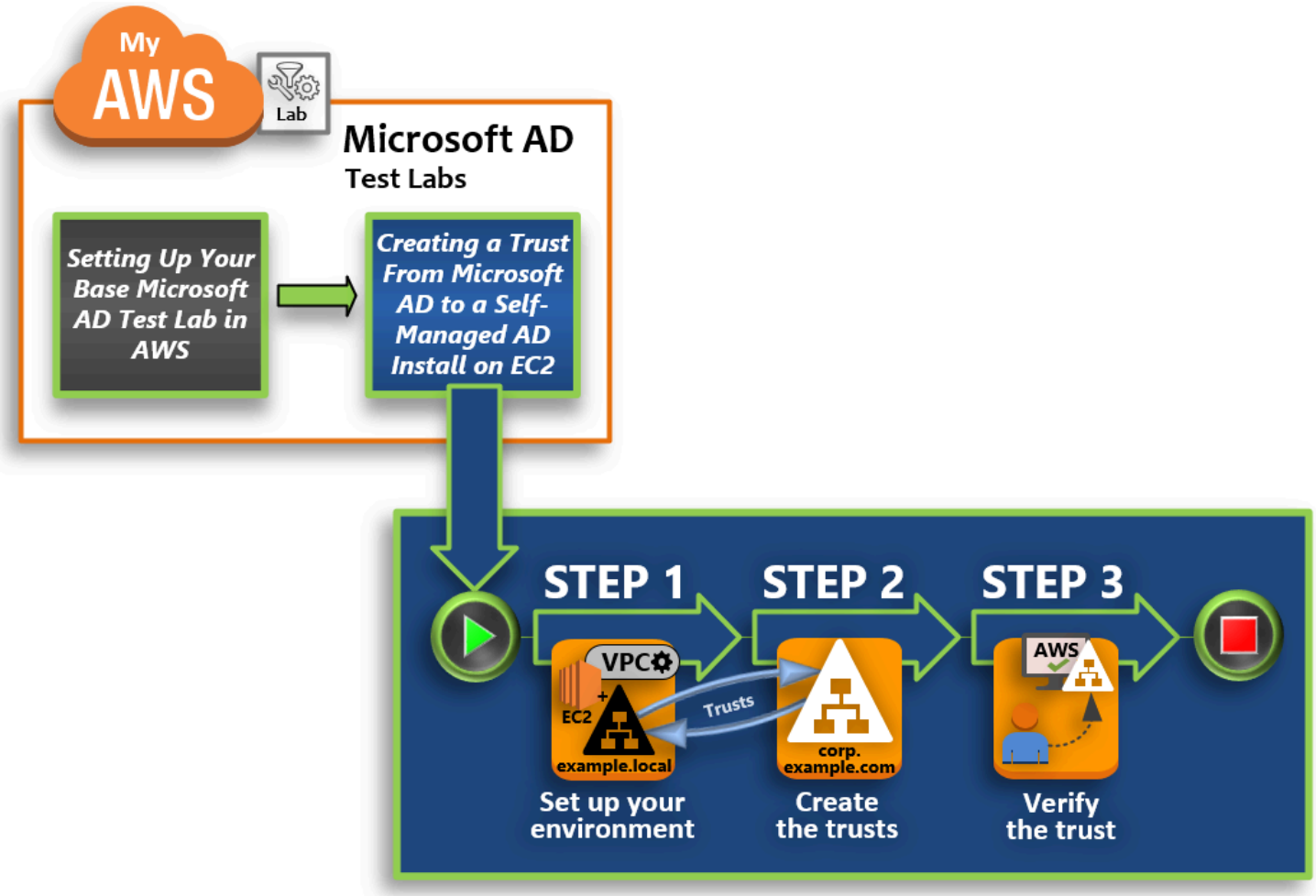
Complimenti! L'ambiente di test di base AWS Managed Microsoft AD è stato ora configurato. Sei pronto per iniziare ad aggiungere il prossimo lab di sicurezza nelle serie.

Tutorial successivo: Tutorial: creazione di un trust da AWS Managed Microsoft AD a un'installazione di Active Directory autogestita su Amazon EC2

Tutorial: creazione di un trust da AWS Managed Microsoft AD a un'installazione di Active Directory autogestita su Amazon EC2

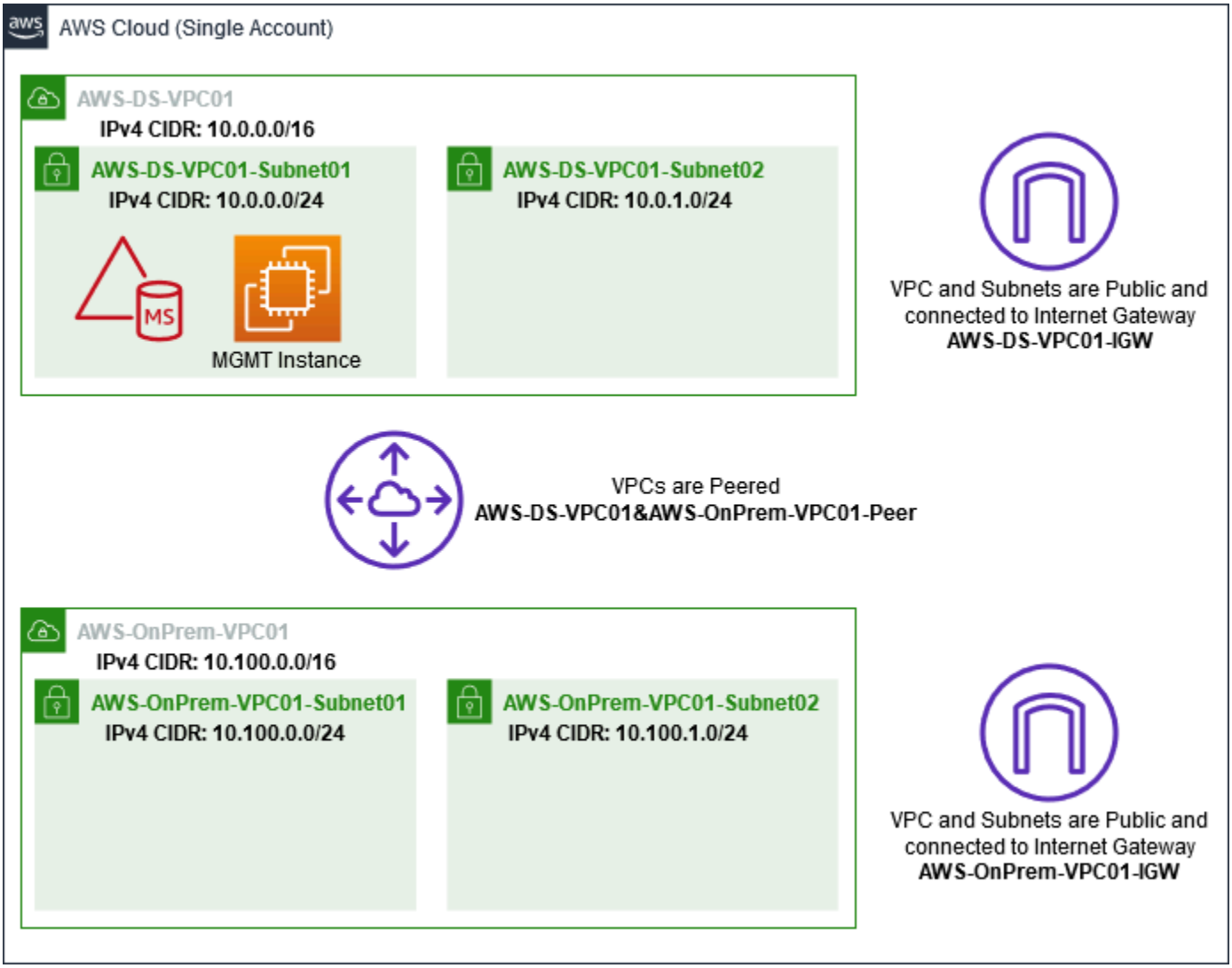
In questo tutorial, imparerai come creare un trust tra la foresta AWS Directory Service for Microsoft Active Directory creata nel tutorial Base. Imparerai anche a creare una nuova foresta nativa di Active Directory su un server Windows in Amazon EC2. Come illustrato nella figura seguente, il lab creato da questo tutorial è il secondo elemento costitutivo necessario per configurare un laboratorio di test AWS Managed Microsoft AD completo. Puoi utilizzare il laboratorio di test per testare le tue soluzioni basate AWS su cloud puro o ibrido.

È necessario creare questo tutorial una sola volta. In seguito potrai aggiungere tutorial facoltativi quando necessario per ampliare l'esperienza.



Fase 1: configurazione dell'ambiente per i trust

In questa sezione, configuri il tuo EC2 ambiente Amazon, distribuisci la tua nuova foresta e prepari il tuo VPC per i trust. AWS



Crea un'istanza di Windows Server 2019 EC2

Utilizza la seguente procedura per creare un server membro di Windows Server 2019 in Amazon EC2.

Per creare un' EC2 istanza di Windows Server 2019

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella EC2 console Amazon, scegli Launch Instance.
3. Nella pagina Passaggio 1, individuare Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxx*** nell'elenco. Quindi scegliere Select (Seleziona).
4. Nella pagina Step 2 (Fase 2), seleziona t2.large, quindi scegli Next: Configure Instance Details (Successivo: configura dettagli istanza).

5. Nella pagina Step 3 (Fase 3), esegui le operazioni seguenti:
   - Per Rete, selezionate vpc- ***xxxxxxxxxxxxxxxxx*** AWS- OnPrem -VPC01 (che avete precedentemente impostato nel tutorial di Base).
   - Per Subnet, seleziona subnet - | - -VPC01-subnet01 ***xxxxxxxxxxxxxxxxx*** | - -VPC01 AWS. OnPrem AWS OnPrem
   - Nell'elenco Auto-assign Public IP (Assegna automaticamente IP pubblico), scegli Enable (Abilita) (se l'impostazione della sottorete non è configurata su Enable (Abilita) per impostazione predefinita).
   - Lascia le altre impostazioni ai valori predefiniti.
   - Scegli Passaggio successivo: aggiunta dello storage.
6. Nella pagina Step 4 (Fase 4), mantieni le impostazioni predefinite, quindi scegli Next: Add Tags (Successivo: aggiungi tag).
7. Nella pagina Step 5 (Fase 5), scegli Add tag (Aggiungi tag). In Key (Chiave) digita **`example.local-DC01`** quindi scegli Next: Configure Security Group (Successivo: configura gruppo di sicurezza).
8. Nella pagina Fase 6, scegli Seleziona un gruppo di sicurezza esistente, seleziona Gruppo di sicurezza AWS On-Prem Test Lab (che hai già configurato nel tutorial di base), quindi scegli Analizza e avvia per analizzare l'istanza.
9. Nella pagina Step 7 (Fase 7), analizza la pagina, quindi scegli Launch (Avvia).
10. Nella finestra di dialogo Select an existing key pair or create a new key pair (Seleziona una coppia di chiavi esistente o crea una nuova coppia di chiavi) esegui le operazioni seguenti:
    - Scegli Choose an existing key pair (Scegli una coppia di chiavi esistente).
    - In Seleziona una coppia di chiavi, scegli AWS-DS-KP (che hai già configurato nel tutorial di base).
    - Seleziona la casella di controllo I acknowledge... (Acconsento...).
    - Scegliere Launch Instances (Avvia istanze).
11. Scegli Visualizza istanze per tornare alla EC2 console Amazon e visualizzare lo stato della distribuzione.

Promozione del server a un controller di dominio

Prima di poter creare trust, è necessario creare e distribuire il primo controller di dominio per una nuova foresta. Durante questo processo puoi configurare una nuova foresta di Active Directory,

installare il DNS e impostare questo server in modo da utilizzare il server DNS locale per la risoluzione dei nomi. È necessario riavviare il server al termine di questa procedura.

> **Note**
>
> Se desideri creare un controller di dominio AWS che si replichi con la tua rete locale, devi prima aggiungere manualmente l' EC2 istanza al tuo dominio locale. Dopo potrai promuovere il server a un controller di dominio.

Promuovere il server a un controller di dominio

1. Nella EC2 console Amazon, scegli Istanze, seleziona l'istanza appena creata, quindi scegli Connect.
2. Nella finestra di dialogo Connect To Your Instance (Connetti all'istanza), scegli Download Remote Desktop File (Scarica file per il desktop remoto).
3. Nella finestra di dialogo Windows Security (Sicurezza di Windows), digita le credenziali dell'amministratore locale per il computer Windows Server per effettuare l'accesso (ad esempio, **`administrator`**). Se non disponi ancora della password dell'amministratore locale, torna alla EC2 console Amazon, fai clic con il pulsante destro del mouse sull'istanza e scegli Ottieni la password di Windows. Vai al file `AWS DS KP.pem` o alla tua chiave `.pem` personale, quindi scegli Decrypt Password (Decrittografa password).
4. Nel menu Start (Inizia), scegli Server Manager.
5. In Dashboard (Pannello di controllo), scegli Add Roles and Features (Aggiungi ruoli e funzionalità).
6. In Add Roles and Features Wizard (Procedura guidata aggiunta ruoli e funzionalità), scegli Next (Successivo).
7. Nella pagina Select installation type (Seleziona tipo di installazione), scegli Role-based or feature-based installation (Installazione basata su ruoli o su funzionalità), quindi scegli Next (Successivo).
8. Nella pagina Select destination server (Seleziona server di destinazione), assicurati che sia selezionato il server locale, quindi scegli Next (Successivo).
9. Nella pagina Select server roles (Seleziona ruoli server), seleziona Active Directory Domain Services (Servizi di dominio di Active Directory). Nella finestra di dialogo Add Roles and Features Wizard (Procedura guidata aggiunta ruoli e funzionalità), verifica che la casella di controllo

Include management tools (if applicable) (Includi strumenti di gestione (se applicabile)) sia selezionata. Scegli Add Features (Aggiungi funzionalità), quindi scegli Next (Successivo).

10. Nella pagina Select features (Seleziona funzionalità), scegli Next (Successivo).
11. Nella pagina Active Directory Domain Services (Servizi di dominio di Active Directory), scegli Next (Successivo).
12. Nella pagina Confirm installation selections (Conferma selezioni di installazione), scegli Install (Installa).
13. Dopo aver installato i binari di Active Directory, scegli Close (Chiudi).
14. Quando Server Manager si apre, scegli un flag nella parte superiore, accanto alla parola Manage (Gestisci). Quando il flag diventa giallo, il server è pronto per essere promosso.
15. Scegli il flag giallo, quindi scegli Promote this server to a domain controller (Promuovi questo server a un controller di dominio).
16. Nella pagina Deployment Configuration (Configurazione di distribuzione), scegli Add a new forest (Aggiungi una nuova foresta). In Root domain name (Nome dominio root), digita **`example.local`**, quindi scegli Next (Successivo).
17. Nella pagina Domain Controller Options (Opzioni controller di dominio), esegui le operazioni seguenti:

    - Sia in Forest functional level (Livello funzionale foresta) che in Domain functional level (Livello funzionale dominio), scegli Windows Server 2016.
    - In Specificare le funzionalità del controller di dominio, verifica che siano selezionati sia il server DNS che Global Catalog (GC).
    - Digita e conferma una password di Directory Services Restore Mode (DSRM). Quindi scegli Successivo.
18. Nella pagina DNS Options (Opzioni DNS), ignora l'avviso sulla delegazione e scegli Next (Successivo).
19. Nella pagina Opzioni aggiuntive, assicurati che EXAMPLE sia elencato come NetBios nome di dominio.
20. Nella pagina Paths (Percorsi), mantieni le impostazioni predefinite, quindi scegli Next (Successivo).
21. Nella pagina Review Options (Analizza opzioni), scegli Next (Successivo). Il server effettuerà ora delle verifiche per accertarsi che tutti i prerequisiti del controller di dominio siano soddisfatti. Potrebbero essere visualizzati dei messaggi di errore, mai puoi ignorarli senza rischi per la sicurezza.

22. Scegli Installa. Una volta completata l'installazione, il server si riavvia e diventa un controller di dominio funzionale.

Configura il VPC

Le tre procedure seguenti ti guidano attraverso le fasi di configurazione del VPC per la connettività di AWS.

Configurazione delle regole in uscita del VPC

1. Nella AWS Directory Service console, prendi nota dell'ID di directory Microsoft AD AWS gestito per corp.example.com che hai creato in precedenza nel tutorial di Base.
2. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Fai clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
4. Cerca il tuo ID di directory AWS Managed Microsoft AD. Nei risultati della ricerca, seleziona l'elemento con la descrizione AWS ha creato il gruppo di sicurezza per i controller d- ***xxxxxx*** directory.

   > **Note**
   >
   > Questo gruppo di sicurezza è stato creato automaticamente quando hai creato la directory all'inizio.

5. Scegli la scheda Outbound Rules (Regole in uscita) per tale gruppo di sicurezza. Scegli Edit (Modifica), scegli Add another rule (Aggiungi un'altra regola), quindi aggiungi i seguenti valori:
   - In Type (Tipo), scegli All Traffic (Tutto il traffico).
   - In Destination (Destinazione), digitare **`0.0.0.0/0`**.
   - Lascia le altre impostazioni ai valori predefiniti.
   - Seleziona Salva.

Per verifica che la preautenticazione Kerberos sia abilitata

1. Nel controller di dominio example.local, apri Server Manager.
2. Nel menu Tools (Strumenti), scegli Active Directory Users and Computers (Strumento Users and Computers (Utenti e computer) di Active Directory).

3. Passa alla directory Utenti, fai clic con il pulsante destro del mouse su un utente, seleziona Proprietà e scegli la scheda Account. Nell'elenco Opzioni account, scorri verso il basso e verifica che Non richiedere l'autenticazione preliminare Kerberos non sia selezionato.
4. Esegui la stessa procedura per il dominio corp.example.com dall'istanza corp.example.com-mgmt .

Configurazione dei server d'inoltro condizionale DNS

> **Note**
>
> Un server di inoltro condizionale è un server DNS in una rete che viene utilizzato per inoltrare query DNS in base al nome di dominio DNS nella query. Ad esempio, un server DNS può essere configurato per inoltrare tutte le query ricevute per i nomi che terminano con widgets.example.com all'indirizzo IP di un server DNS specifico o agli indirizzi IP di più server DNS.

1. Apri la AWS Directory Service console.
2. Nel riquadro di navigazione, seleziona Directory.
3. Seleziona l'ID della directory del tuo AWS Managed Microsoft AD.
4. Annota il nome di dominio completo (FQDN), corp.example.com e gli indirizzi DNS della directory.
5. Ora, torna al controller di dominio example.local, quindi apri Server Manager.
6. Nel menu Tools (Strumenti), seleziona DNS.
7. Nella struttura della console, espandi il server DNS del dominio per il quale configuri il trust e vai a Conditional Forwarders (Server d'inoltro condizionale).
8. Fai clic con il pulsante destro del mouse su Conditional Forwarders(Server d'inoltro condizionale), quindi scegli New Conditional Forwarder (Nuovo server d'inoltro condizionale).
9. Nel dominio DNS digita **`corp.example.com`**.
10. In Indirizzi IP dei server primari, scegli <Fai clic qui per aggiungere... >, digitare il primo indirizzo DNS della directory AWS Managed Microsoft AD (di cui si è preso nota nella procedura precedente), quindi premere Invio. Esegui la stessa procedura per il secondo indirizzo DNS. Dopo aver digitato gli indirizzi DNS, potresti visualizzare un errore del tipo "timeout" o "impossibile risolvere". In genere, puoi ignorare questi errori.

11. Seleziona la casella di controllo Store this conditional forwarder in Active Directory, and replicate it as follows (Memorizza questo server d'inoltro condizionale in Active Directory e replicalo come segue). Nel menu a discesa, scegli All DNS servers in this Forest (Tutti i server DNS di questa foresta), quindi scegli OK.

Fase 2: creazione dei trust

In questa sezione crei due trust tra foreste separati. Un trust viene creato dal dominio Active Directory sull' EC2 istanza e l'altro dal AWS Managed Microsoft AD in AWS.

Per creare l'attendibilità dal tuo EC2 dominio al tuo AWS Managed Microsoft AD

1. Accedi a example.local.
2. Apri Server Manager e nella struttura della console scegli DNS. Prendi nota dell' IPv4 indirizzo indicato per il server. Ne avrai bisogno nella procedura successiva, quando creerai un server d'inoltro condizionale da corp.example.com nella directory example.local.
3. Nel menu Tools (Strumenti), scegli Active Directory Domains and Trust (Domini e trust di Active Directory).
4. Nella struttura della console, fai clic con il pulsante destro del mouse su example.local, quindi scegli Properties (Proprietà).
5. Nella scheda Trusts (Trust), scegli New Trust (Nuovo trust), quindi scegli Next (Successivo).
6. Nella pagina Trust Name (Nome trust), digita **`corp.example.com`**, quindi scegli Next (Successivo).
7. Nella pagina Trust Type (Tipo di trust), scegli Forest trust (Trust tra foreste), quindi scegli Next (Successivo).

> **Note**
>
> AWS Managed Microsoft AD supporta anche i trust esterni. Tuttavia, ai fini di questo tutorial, verrà creato un trust tra foreste bidirezionale.

8. Nella pagina Direction of Trust (Direzione del trust), scegli Two-way (Bidirezionale), quindi scegli Next (Successivo).

> **Note**
>
> Se in seguito si decide di provare questa operazione con un trust unidirezionale, assicurarsi che le istruzioni di attendibilità siano configurate correttamente (in uscita sul dominio trusting, in entrata sul dominio trusted). Per informazioni generali, consulta Informazioni sulla direzione del trust nel sito Web di Microsoft.

9. Nella pagina Sides of Trust (Lato del trust), scegli This domain only (Solo per questo dominio), quindi scegli Next (Successivo).
10. Nella pagina Outgoing Trust Authentication Level (Livello di autenticazione del trust in uscita), scegli Forest-wide authentication (Autenticazione a livello di foresta), quindi scegli Next (Successivo).

> **Note**
>
> Sebbene Selective authentication (Autenticazione selettiva) in un'opzione, per la semplicità di questo tutorial si consiglia di non abilitarlo qui. Quando configurato, limita l'accesso tramite un trust esterno o di foresta solo agli utenti di un dominio o di una foresta attendibili a cui sono state concesse esplicitamente autorizzazioni di autenticazione agli oggetti computer (computer delle risorse) che risiedono nel dominio trusting o nella foresta. Per ulteriori informazioni, consulta Configurazione delle impostazioni di autenticazione selettiva.

11. Nella pagina Trust Password (Password del trust), digita la password del trust due volte, quindi scegli Next (Successivo). Utilizzerai questa stessa password nella prossima procedura.
12. Nella pagina Trust Selections Complete (Selezione dei trust completa), verifica i risultati, quindi scegli Next (Successivo).
13. Nella pagina Trust Creation Complete (Creazione dei trust completa), verifica i risultati, quindi scegli Next (Successivo).
14. Nella pagina Confirm Outgoing Trust (Conferma trust in uscita), scegli No, do not confirm the outgoing trust (Non confermare trust in uscita). quindi scegliere Next.
15. Nella pagina Confirm Incoming Trust (Conferma trust in entrata), scegli No, do not confirm the incoming trust (Non confermare trust in entrata). quindi scegliere Next.

16. Nella pagina Completing the New Trust Wizard (Completamento procedura guidata del nuovo trust), scegli Finish (Fine).

> **Note**
>
> Le relazioni di fiducia sono una funzionalità globale di AWS Managed Microsoft AD. Se utilizzi Configurazione della replica multiarea per Managed AWS Microsoft AD, è necessario eseguire le seguenti procedure in Regione principale. Le modifiche verranno applicate automaticamente in tutte le Regioni replicate. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per creare l'attendibilità dal tuo AWS Managed Microsoft AD al tuo EC2 dominio

1. Apri la AWS Directory Service console.
2. Scegli la directory corp.example.com.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), scegli Actions (Azioni), quindi seleziona Add trust relationship (Aggiungi relazione di trust).
5. Nella finestra di dialogo Add a trust relationship (Aggiungi una relazione di trust), esegui le operazioni seguenti:
   - In Tipo di trust selezionare Trust tra foreste.

     > **Note**
     >
     > Assicurati che il tipo di trust che scegli qui corrisponda allo stesso tipo di fiducia configurato nella procedura precedente (per creare l'attendibilità dal tuo EC2 dominio al tuo AWS Managed Microsoft AD).

   - Per Nome di dominio remoto esistente o nuovo, digitare example.local.

- In Trust password (Password di trust), digita la stessa password fornita nella procedura precedente.
- In Direzione trust, seleziona A due vie.

> **Note**
>
> - Se in seguito si decide di provare questa operazione con un trust unidirezionale, assicurarsi che le istruzioni di attendibilità siano configurate correttamente (in uscita sul dominio trusting, in entrata sul dominio trusted). Per informazioni generali, consulta Informazioni sulla direzione del trust nel sito Web di Microsoft.
> - Sebbene Selective authentication (Autenticazione selettiva) in un'opzione, per la semplicità di questo tutorial si consiglia di non abilitarlo qui. Quando configurato, limita l'accesso tramite un trust esterno o di foresta solo agli utenti di un dominio o di una foresta attendibili a cui sono state concesse esplicitamente autorizzazioni di autenticazione agli oggetti computer (computer delle risorse) che risiedono nel dominio trusting o nella foresta. Per ulteriori informazioni, consulta Configurazione delle impostazioni di autenticazione selettiva.

- In Server d'inoltro condizionale, digita l'indirizzo IP del server DNS della foresta example.local (che hai annotato nella procedura precedente).

> **Note**
>
> Un server di inoltro condizionale è un server DNS in una rete che viene utilizzato per inoltrare query DNS in base al nome di dominio DNS nella query. Ad esempio, un server DNS può essere configurato per inoltrare tutte le query ricevute per i nomi che terminano con widgets.example.com all'indirizzo IP di un server DNS specifico o agli indirizzi IP di più server DNS.

6. Scegli Aggiungi.

Fase 3: verifica del trust

In questa sezione, verifichi se i trust sono stati configurati correttamente tra AWS e Active Directory su Amazon EC2.

Verifica del trust

1. Apri la AWS Directory Service console.
2. Scegli la directory corp.example.com.
3. Nella pagina Dettaglio report, procedi in uno dei seguenti modi:
   - Se nella sezione Replica multiregione sono visualizzate più Regioni, seleziona quella principale, quindi scegli la scheda Rete e sicurezza. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.
   - Se non hai alcuna regione visualizzata in replica multiregione, scegli la scheda Rete e sicurezza.
4. Nella sezione Trust relationships (Relazioni di trust), seleziona la relazione di trust creata.
5. Scegli Actions (Operazioni), quindi scegli Verify trust relationship (Verifica relazione di trust).

Una volta completata la verifica, dovresti visualizzare Verified (Verificato) nella colonna Status (Stato).

Complimenti, hai completato questo tutorial! Ora disponi di un ambiente Active Directory con una multiforesta completamente funzionale dal quale puoi iniziare a provare diversi scenari. Sono stati programmati dei tutorial di lab di sviluppo aggiuntivi per il 2018, ti consigliamo dunque di controllare di tanto in tanto per vedere gli aggiornamenti.

AWS Quote Microsoft AD gestite

Di seguito sono riportate le quote predefinite per AWS Managed Microsoft AD. Salvo ove diversamente specificato, ogni quota si applica a una regione.

AWS Quote Microsoft AD gestite

Risorsa	Quota predefinita
AWS Directory Microsoft AD gestite (edizioni Standard ed Enterprise)	20
AWS Directory Microsoft AD gestite (Hybrid Edition)	5

Risorsa	Quota predefinita
Istantanee manuali (edizioni Standard ed Enterprise) *	5 per Microsoft AD AWS gestito
Età snapshot manuali **	180 giorni
Numero massimo di controller di dominio per directory	20
Domini condivisi per Microsoft AD standard ***	25
Domini condivisi per Microsoft AD Enterprise ***	500
Domini condivisi per Hybrid Microsoft AD ***	125
Numero massimo di certificati emessi da una CA registrati per directory	5
Numero massimo di AWS aree totali in una singola directory AWS gestita di Microsoft AD (Enterprise Edition) ****	5

* La quota di snapshot manuali non può essere modificata.

** L'età massima supportata di uno snapshot manuale è di 180 giorni e non può essere modificata. Ciò è dovuto all'attributo Tombstone-Lifetime degli oggetti eliminati che definisce la durata utile di un backup dello stato del sistema di Active Directory. Non è possibile ripristinare da uno snapshot precedente a 180 giorni. Per ulteriori informazioni, consulta Useful shelf life of a system-state backup of Active Directory nel sito Web Microsoft.

*** La quota predefinita del dominio condiviso si riferisce al numero di account con cui è possibile condividere una singola directory.

**** Ciò include 1 regione primaria e fino a 4 Regioni aggiuntive. Per ulteriori informazioni, consulta Regioni primarie e regioni aggiuntive.

> **Note**
>
> Non è possibile collegare un indirizzo IP pubblico alla propria AWS elastic network interface (ENI).

Per informazioni sulla progettazione delle applicazioni e la distribuzione del carico, consulta Procedure consigliate per la programmazione delle applicazioni per un Microsoft AD AWS gestito.

Per le quote di archiviazione e degli oggetti, consulta la Tabella di confronto nella pagina Prezzi del Servizio di directory AWS.

Risoluzione dei problemi relativi AWS a Managed Microsoft AD

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potresti riscontrare durante la creazione o l'utilizzo di Managed AWS Microsoft AD Active Directory.

Problemi con AWS Managed Microsoft AD

Alcune attività di risoluzione dei problemi possono essere completate solo da Supporto. Ecco alcune delle attività:

- Riavvio dei controller di dominio Directory Service forniti.
- Aggiornamento di Managed AWS Microsoft AD.

Per creare una richiesta di supporto, consulta Creazione di casi di supporto e gestione dei casi.

Problemi con Netlogon e comunicazioni sicure tra i canali

Come mitigazione contro CVE-2020-1472, Microsoft ha rilasciato una patch che modifica il modo in cui le comunicazioni tra i canali sicuri di Netlogon vengono elaborate dai controller di dominio. Dall'introduzione di queste modifiche sicure a Netlogon, alcune connessioni Netlogon (server, workstation e convalide di attendibilità) potrebbero non essere accettate da Managed Microsoft AD. AWS

Per verificare se il problema è correlato a Netlogon o alle comunicazioni su canale sicuro, cerca nei tuoi Amazon CloudWatch Logs l'evento IDs 5827 (per problemi relativi all'autenticazione dei dispositivi) o 5828 (per problemi relativi alla convalida della fiducia di AD). Per informazioni su

CloudWatch AWS Managed Microsoft AD, vedereAbilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS.

Per ulteriori informazioni sulla mitigazione contro CVE-2020-1472, vedi Come gestire le modifiche alle connessioni ai canali sicuri Netlogon associate a CVE-2020-1472 sul sito Web di Netlogon. Microsoft

Quando si tenta di reimpostare la password di un utente, viene visualizzato l'errore «Response Status: 400 Bad Request»

Quando tenti di reimpostare la password di un utente, ricevi un messaggio di errore simile al seguente:

```
Response Status: 400 Bad Request
```

È possibile che si verifichi questo problema quando sono presenti oggetti duplicati nell'unità organizzativa (OU) Microsoft AD AWS gestita con nomi di accesso utente identici. I nomi di accesso utente devono essere univoci. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi ai dati delle directory nella Microsoft documentazione.

Recupero della password

Se un utente dimentica una password o ha problemi di accesso alla directory AWS Managed Microsoft AD, puoi reimpostarne la password utilizzando il Console di gestione AWS, PowerShell o il AWS CLI.

Per ulteriori informazioni, consulta Reimpostazione di una password utente AWS Microsoft AD gestita.

Altre risorse

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

- AWS Knowledge Center: trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- AWS Support Center: ottieni supporto tecnico.
- AWS Premium Support Center: ottieni supporto tecnico premium.

Le seguenti risorse possono aiutarti a risolvere i problemi più comuni di Active Directory.

- Documentazione Active Directory

- AD DSRisoluzione dei problemi

Argomenti

- Errori di aggiunta al dominio dell'istanza Amazon EC2 Linux
- AWS Microsoft AD gestito: spazio di archiviazione a bassa disponibilità
- Errori di estensione dello schema
- Motivo stato di creazione trust

Errori di aggiunta al dominio dell'istanza Amazon EC2 Linux

Quanto segue può aiutarti a risolvere alcuni messaggi di errore che potresti incontrare quando unisci un'istanza Amazon EC2 Linux alla tua directory Managed AWS Microsoft AD.

Istanze Linux non in grado di eseguire l'unione di domini o l'autenticazione

Le istanze di Ubuntu 14.04, 16.04 e 18.04 devono essere risolvibili al contrario nel DNS prima che un realm possa funzionare con Microsoft Active Directory. In caso contrario, si potrebbe verificare uno dei seguenti due scenari:

Scenario 1: istanze Ubuntu non ancora aggiunte a un realm

Nel caso di istanze Ubuntu che stanno tentando di aggiungersi a un realm, il comando `sudo realm join` potrebbe non fornire le autorizzazioni necessarie per l'aggiunta al dominio e potrebbe venire visualizzato il seguente errore:

! Impossibile eseguire l'autenticazione ad active directory: SASL(-1): errore generico: GSSAPI Errore: è stato fornito un nome non valido (eseguito correttamente) adcli: impossibile effettuare il collegamento al dominio di EXAMPLE.COM: impossibile eseguire l'autenticazione ad active directory: SASL(-1): errore generico: GSSAPI Errore: è stato fornito un nome non valido (eseguito correttamente) ! Autorizzazioni insufficienti per aggiungere il realm del dominio: impossibile aggiungere il realm: autorizzazioni insufficienti per aggiungere il dominio

Scenario 2: istanze Ubuntu aggiunte a un realm

Per le istanze di Ubuntu che fanno già parte di un dominio Microsoft Active Directory, i tentativi di accesso tramite SSH all'istanza utilizzando le credenziali del dominio potrebbero fallire con i seguenti errori:

$ ssh admin@EXAMPLE.COM@198.51.100

nessuna identità di questo tipo:/Users/username/.ssh/id_ed25519: nessun file o directory di questo tipo

admin@EXAMPLE.COM@198.51.100's password:

Permission denied, please try again.

admin@EXAMPLE.COM@198.51.100's password:

Se esegui l'accesso all'istanza con una chiave pubblica e verifichi `/var/log/auth.log`, potresti visualizzare i seguenti errori sull'impossibilità di trovare l'utente:

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0 user=admin@EXAMPLE.COM

May 12 01:02:12 ip-192-0-2-0 sshd[2251]: pam_sss(sshd:auth): received for user admin@EXAMPLE.COM: 10 (User not known to the underlying authentication module)

May 12 01:02:14 ip-192-0-2-0 sshd[2251]: Failed password for invalid user admin@EXAMPLE.COM from 203.0.113.0 port 13344 ssh2

May 12 01:02:15 ip-192-0-2-0 sshd[2251]: Connection closed by 203.0.113.0 [preauth]

Tuttavia, il `kinit` dell'utente continuerà a funzionare. Consulta questo esempio:

ubuntu @ip -192-0-2-0: ~$ kinit admin@EXAMPLE.COM Password per admin@EXAMPLE.COM: ubuntu @ip -192-0-2-0: ~$ klist Ticket cache: _1000 Principio predefinito: admin@EXAMPLE.COM FILE:/tmp/krb5cc

Soluzione alternativa

La soluzione consigliata per questi scenari è quella di disabilitare il DNS inverso in `/etc/krb5.conf` nella sezione [libdefaults], come mostrato di seguito:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Problema di autenticazione di trust unidirezionale con aggiunta ottimizzata del dominio

Se è stato stabilito un trust in uscita unidirezionale tra AWS Microsoft AD gestito e Active Directory locale, è possibile che si verifichi un problema di autenticazione quando si tenta di autenticarsi sull'istanza Linux aggiunta al dominio utilizzando le credenziali attendibili di Active Directory con Winbind.

Errori

31 luglio 00:00:00 EC2 AMAZ-T sshd [23832]: password non riuscita per user@corp.example.com dalla porta LSMWq xxx.xxx.xxx.xxx 18309 ssh2

31 luglio 00:05:00 AMAZ-T sshd [23832]: pam_winbind (sshd:auth): ottenimento della password (0x00000390 EC2) LSMWq

31 luglio 00:05:00 AMAZ-T sshd [23832]: pam_winbind (sshd:auth): pam_get_item ha restituito una password EC2 LSMWq

31 luglio 00:05:00 EC2 AMAZ- LSMWq T sshd [23832]: pam_winbind (sshd:auth): richiesta wbcLogonUser fallita: WBC_ERR_AUTH_ERROR, errore PAM: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, Il messaggio di errore era: Il nome dell'oggetto non è stato trovato.

31 luglio 00:05:00 EC2 LSMWq AMAZ-T sshd [23832]: pam_winbind (sshd:auth): errore interno del modulo (retval = PAM_SYSTEM_ERR (4), utente = 'CORP\ user')

Soluzione alternativa

Per risolvere questo problema, è necessario commentare o rimuovere una direttiva dal file di configurazione del modulo PAM (`/etc/security/pam_winbind.conf`) utilizzando la procedura seguente.

1. Apri il file `/etc/security/pam_winbind.conf` in un editor di testo.

   ```
   sudo vim /etc/security/pam_winbind.conf
   ```

2. Commenta o rimuovi la seguente direttiva: krb5_auth = yes.

   ```
   [global]

   cached_login = yes
   krb5_ccache_type = FILE
   ```

```
#krb5_auth = yes
```

3. Arresta il servizio Winbind, quindi riavvialo.

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

AWS Microsoft AD gestito: spazio di archiviazione a bassa disponibilità

Se AWS Managed Microsoft AD non funziona a causa dello scarso spazio di archiviazione disponibile di Active Directory, è necessaria un'azione immediata per riportare la directory allo stato attivo. Le due cause più comuni di questo problema sono trattate nelle sezioni seguenti:

1. La cartella SYSVOL archivia più oggetti rispetto a quelli delle policy di gruppo essenziali
2. Il database di Active Directory ha il volume pieno

Per informazioni sui prezzi dello storage AWS gestito di Microsoft AD, vedi Directory Service Prezzi.

La cartella SYSVOL archivia più oggetti rispetto a quelli delle policy di gruppo essenziali

Una causa comune di questo problema è dovuta alla memorizzazione di file non essenziali per l'elaborazione di policy di gruppo nella cartella SYSVOL. Questi file non essenziali potrebbero essere EXEs o qualsiasi altro file che non sia essenziale per l'elaborazione dei criteri di gruppo. MSIs Gli oggetti essenziali da elaborare per l'elaborazione dei criteri di gruppo sono gli oggetti dei criteri di gruppo, gli Logon/off script e l'archivio centrale per gli oggetti dei criteri di gruppo. Tutti i file non essenziali devono essere archiviati su uno o più file server diversi dai controller di dominio Microsoft AD AWS gestiti.

Se sono necessari file per l'installazione del software Criteri di gruppo. è necessario utilizzare un file server per archiviare i file di installazione. Se preferisci non gestire autonomamente un file server, AWS offre un'opzione di file server gestito, Amazon FSx.

Per rimuovere qualsiasi file non necessario, puoi accedere alla condivisione SYSVOL tramite il percorso UNC (Universal Naming Convention). Ad esempio, se il nome di dominio completo (FQDN) del dominio è example.com, il percorso UNC per SYSVOL sarebbe "\\example.local \SYSVOL\example.local\». Dopo aver individuato e rimosso gli oggetti che non sono essenziali per

l'elaborazione della directory policy di gruppo, è necessario tornare a uno stato attivo entro 30 minuti. Se dopo 30 minuti la rubrica non è attiva, contatta l' AWS assistenza.

Archiviare solo i file delle policy di gruppo essenziali nella condivisione SYSVOL garantirà la non compromissione della directory a causa dell'aumento delle dimensioni di SYSVOL.

Il database di Active Directory ha il volume pieno

Una causa comune di questa compromissione è dovuta al riempimento del volume del database di Active Directory. Per verificare se questo è il caso, è possibile esaminare il numero totale di oggetti nella directory. Abbiamo messo in grassetto la parola Total (Totale) per garantire che gli oggetti Deleted (Eliminati) vengano ancora calcolati nel numero totale di oggetti in una directory.

Per impostazione predefinita, AWS Managed Microsoft AD conserva gli elementi nel Cestino di riciclaggio di AD per 180 giorni prima che diventino un oggetto riciclato. Una volta che un oggetto diventa riciclato (tombstoned), viene mantenuto per altri 180 giorni prima di essere finalmente eliminato dalla directory. Quindi, quando un oggetto viene eliminato, esiste nel database delle directory da 360 giorni. Questo è il motivo per cui è necessario valutare il numero totale di oggetti.

Per ulteriori dettagli sul numero di oggetti supportati da AWS Managed Microsoft AD, vedi Directory Service Prezzi.

Per ottenere il numero totale di oggetti in una directory che include gli oggetti eliminati, è possibile eseguire il PowerShell comando seguente da un'istanza di Windows aggiunta al dominio. Per la procedura di configurazione di un'istanza di gestione, consulta Gestione di utenti e gruppi in AWS Managed Microsoft AD.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

Di seguito è riportato un esempio di output dal comando precedente:

```
Count
10000
```

Se il conteggio totale è superiore al conteggio degli oggetti supportati per le dimensioni della directory elencate nella nota precedente, è stata superata la capacità della directory.

Di seguito sono riportate le possibilità di risoluzione di questo problema:

1. Pulizia AD

a. Eliminare eventuali oggetti AD indesiderati.

b. Rimuovere tutti gli oggetti indesiderati dal Cestino AD. Tenere presente che questo è distruttivo e l'unico modo per recuperare quegli oggetti eliminati sarà eseguire un ripristino della directory.

c. Il comando seguente rimuoverà tutti gli oggetti eliminati dal Cestino di AD.

> **Important**
>
> Utilizzare questo comando con estrema cautela in quanto si tratta di un comando distruttivo e l'unico modo per recuperare gli oggetti eliminati sarà quello di eseguire un ripristino della directory.

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
 'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
 { ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like
 '*\0ADEL:*') }
ForEach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
 $ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

d. Apri una custodia con AWS Support per richiedere che Directory Service recuperi lo spazio libero.

2. Se il tipo di directory è Standard Edition, apri un caso con AWS Support per richiedere l'aggiornamento della directory a Enterprise Edition. Ciò aumenterà anche il costo della directory. Per informazioni sui prezzi, consulta Prezzi di Directory Service.

In AWS Managed Microsoft AD, i membri del gruppo AWS Delegated Deleted Object Lifetime Administrators hanno la possibilità di modificare l'`msDS-DeletedObjectLifetime`attributo che imposta la quantità di tempo, in giorni, in cui gli oggetti eliminati vengono conservati nel Cestino di riciclaggio di AD prima che diventino oggetti riciclati.

> **Note**
>
> Questo è un argomento avanzato. Se configurato in modo inappropriato, può causare la perdita di dati. Si consiglia di leggere prima l'articolo The AD Recycle Bin: Understanding,

Implementing, Best Practices, and Troubleshooting per ottenere una migliore comprensione di questi processi.

La possibilità di modificare il valore dell'attributo `msDS-DeletedObjectLifetime` in un numero inferiore può aiutare a garantire che il numero di oggetti non superi i livelli supportati. Il valore più basso valido su cui è possibile impostare questo attributo è 2 giorni. Una volta superato tale valore, non sarà più possibile recuperare l'oggetto eliminato utilizzando il Cestino AD. Richiederà il ripristino della directory da un'istantanea per recuperare gli oggetti. Per ulteriori informazioni, consulta Ripristino di AWS Managed Microsoft AD con istantanee. Ogni ripristino da uno snapshot può risultare in perdita di dati come sono in un momento specifico.

Per modificare la durata dell'oggetto eliminato della directory eseguire il seguente comando:

> **Note**
>
> Se si esegue il comando così com'è, verrà impostato il valore dell'attributo Durata oggetto eliminato su 30 giorni. Se desideri renderlo più lungo o più corto, sostituisci «30" con il numero che preferisci. Tuttavia, si consiglia di non scegliere un numero maggiore di 180.

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows
 NT,CN=Services,CN=Configuration,$BaseDn" -Partition "CN=Configuration,$BaseDn" -
Replace:@{"msDS-DeletedObjectLifetime" = $DeletedObjectLifetime}
```

Errori di estensione dello schema

Quanto segue può aiutarti a risolvere alcuni messaggi di errore che potresti riscontrare durante l'estensione dello schema per la tua directory Managed AWS Microsoft AD.

Riferimento

Errore

> Aggiungi errore alla voce a partire dalla riga 1: Riferimento Errore lato server: 0x202b Il server ha restituito un riferimento. L'errore esteso del server è: 0000202B: RefErr: DSID-0310082F, dati 0, 1 punti di accesso\ tref 1: 'example.com' Numero di oggetti modificati: 0

Risoluzione dei problemi

> Assicurati che tutti i campi del nome distinti abbiano il nome di dominio corretto. Nell'esempio sopra riportato, `DC=example,dc=com` deve essere sostituito con `DistinguishedName` mostrato dal cmdlet `Get-ADDomain`.

Impossibile leggere il file di importazione

Errore

> Impossibile leggere il file di importazione. Numero di oggetti modificati: 0

Risoluzione dei problemi

> Il file importato LDIF è vuoto (0 byte). Assicurati che sia stato caricato il file corretto.

Errore di sintassi

Errore

> Si è verificato un errore di sintassi nel file di input non andato a buon fine sulla riga 21. L'ultimo token inizia per "q". Numero di oggetti modificati: 0

Risoluzione dei problemi

> Il testo sulla riga 21 non è formattato correttamente. La prima lettera del testo non valido è `A`. Aggiorna la riga 21 con una sintassi LDIF valida. Per ulteriori informazioni su come formattare il file LDIF, consulta Fase 1: creazione del file LDIF.

Esiste un attributo o un valore

Errore

> Aggiungi errore a una voce a partire dalla riga 1: esiste un attributo o un valore Errore lato server: 0x2083 Il valore specificato esiste già. L'errore esteso del server è: 00002083: AtrErr: DSID-03151830, #1:\ t0:00002083: DSID-03151830, problema 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain) :len 4 Numero di oggetti modificati: 0

Risoluzione dei problemi

> La modifica dello schema è già stato applicata.

Nessun attributo di questo tipo

Errore

> Aggiungi errore alla voce a partire dalla riga 1: nessun attributo di questo tipo Errore lato server: 0x2085 Il valore attributo non può essere rimosso perché non è presente nell'oggetto. L'errore esteso del server è: 00002085: AtrErr: DSID-03152367, #1:\ t0:00002085: DSID-03152367, problema 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (mayContain) :len 4 Numero di oggetti modificati: 0

Risoluzione dei problemi

> Il file LDIF sta cercando di rimuovere un attributo da una classe, ma tale attributo non è attualmente collegato alla classe. La modifica dello schema probabilmente è già stata applicata.

Errore

> Aggiungi errore alla voce partire dalla riga 41: nessun attributo di questo tipo 0x57 Il parametro non è corretto. L'errore server esteso è: 0x208d Oggetto directory non trovato. L'errore esteso del server è: «00000057: LdapErr: DSID-0C090D8A, commento: errore nell'operazione di conversione degli attributi, dati 0, v2580" Numero di oggetti modificati: 0

Risoluzione dei problemi

> L'attributo elencato sulla riga 41 non è corretto. Controlla attentamente l'ortografia.

Nessun oggetto di questo tipo

Errore

> Aggiungi errore alla voce a partire dalla riga 1: nessun oggetto di questo tipo Errore lato server: 0x208d Oggetto directory non trovato. L'errore esteso del server è: 0000208D: NameErr: DSID-03100238, problema 2001 (NO_OBJECT), dati 0, migliore corrispondenza tra: 'CN=Schema, CN=Configuration, DC=example, DC=com' Numero di oggetti modificati: 0

Risoluzione dei problemi

> L'oggetto a cui si riferisce il nome distinto (DN) non esiste.

Motivo stato di creazione trust

Quando la creazione dell'attendibilità non riesce per AWS Managed Microsoft AD, il messaggio di stato contiene informazioni aggiuntive. Quanto segue può aiutarti a capire il significato di questi messaggi.

L'accesso viene negato

L'accesso è stato negato nel tentativo di creazione di un trust. La password di attendibilità non è corretta oppure le impostazioni di sicurezza del dominio remoto non consentono la configurazione di un trust. Per ulteriori informazioni sui trust, vedereMigliorare l'efficienza della fiducia con i nomi dei siti e DCLocator. Per risolvere questo problema, prova le seguenti soluzioni:

- Assicurati di utilizzare la stessa password di trust che hai utilizzato durante la creazione del trust corrispondente sul dominio remoto.
- Verifica che le impostazioni di sicurezza del dominio consentano la creazione di trust.
- Verifica che la policy di sicurezza locale sia impostata correttamente. Nello specifico, controlla `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` e assicurati che contenga almeno le seguenti pipe con tre nomi:
  - netlogon
  - samr
  - lsarpc
- Verificate che le pipe sopra menzionate esistano come valori sulla chiave di NullSessionPipesregistro che si trova nel percorso di registro HKLM\ SYSTEM\\ services

\CurrentControlSet\ Parameters. LanmanServer Questi valori devono essere inseriti su righe separate.

> **Note**
>
> Per impostazione predefinita, `Network access: Named Pipes that can be accessed anonymously` non è impostato e verrà visualizzato `Not Defined`. Ciò è normale, in quanto le impostazioni predefinite effettive del controller di dominio di `Network access: Named Pipes that can be accessed anonymously` sono `netlogon`, `samr`, `lsarpc`.

- Verifica la seguente impostazione di firma Server Message Block (SMB) nella politica dei controller di dominio predefiniti. Queste impostazioni sono disponibili in Configurazione computer > Impostazioni di Windows > Impostazioni di sicurezza > Criteri locali/Opzioni di sicurezza. Devono corrispondere alle seguenti impostazioni:
  - Microsoftclient di rete: apposizione di firma digitale alle comunicazioni (sempre): Impostazione predefinita: abilitata
  - Microsoftclient di rete: firma digitale delle comunicazioni (se il server è d'accordo): predefinito: abilitato
  - Microsoftserver di rete: apposizione di firma digitale alle comunicazioni (sempre): abilitato
  - Microsoftserver di rete: firma digitale delle comunicazioni (se il client è d'accordo): Impostazione predefinita: abilitato

Migliorare l'efficienza della fiducia con i nomi dei siti e DCLocator

Il First Site name like non Default-First-Site-Name è un requisito per stabilire relazioni di fiducia tra domini. Tuttavia, l'allineamento dei nomi dei siti tra i domini può migliorare significativamente l'efficienza del processo Domain Controller Locator (). DCLocator Questo allineamento migliora la previsione e il controllo della selezione dei controller di dominio nei trust della foresta.

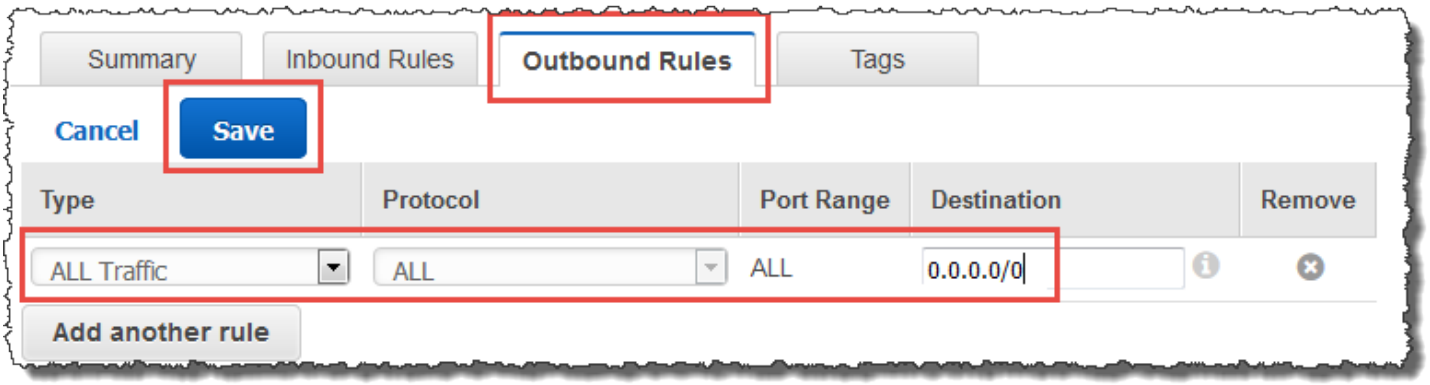
Il DCLocator processo è fondamentale per trovare controller di dominio in diversi domini e foreste. Per ulteriori informazioni sul DCLocator processo, consulta Microsoft la documentazione. La configurazione efficiente del sito consente una localizzazione più rapida e precisa dei controller di dominio, il che porta a migliori prestazioni e affidabilità nelle operazioni tra foreste.

Per ulteriori informazioni su come interagiscono i nomi dei siti e i DCLocator processi, consulta i seguenti articoli: Microsoft

- In che modo i controller di dominio si trovano tra i trust
- Localizzatore di domini nelle foreste

Il nome di dominio specificato non esiste o non può essere contattato

Per risolvere questo problema, assicurati che le impostazioni del gruppo di sicurezza per il tuo dominio e l'elenco di controllo degli accessi (ACL) per il tuo VPC siano corrette e di aver inserito correttamente le informazioni per il tuo server d'inoltro condizionale. AWS configura il gruppo di sicurezza per aprire solo le porte necessarie per le comunicazioni con Active Directory. Nella configurazione predefinita, il gruppo di sicurezza accetta il traffico verso queste porte da qualsiasi indirizzo IP. Il traffico in uscita è limitato al gruppo di sicurezza. Devi aggiornare la regola in uscita sul gruppo di sicurezza per consentire il traffico verso la tua rete on-premise. Per ulteriori informazioni sui requisiti di sicurezza, consulta Fase 2: preparazione di Microsoft AD gestito da AWS.



Se i server DNS per le reti delle altre directory utilizzano indirizzi IP pubblici (non RFC 1918), sarà necessario aggiungere un instradamento IP nella directory dalla console Servizio di directory ai server DNS. Per ulteriori informazioni, consultare Creazione, verifica o eliminazione di una relazione di trust e Prerequisiti.

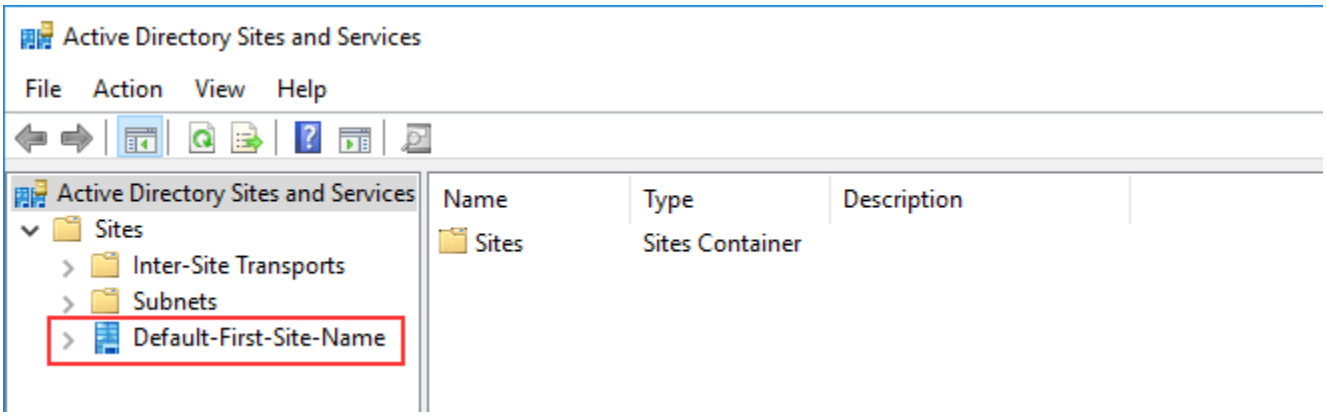
L'Internet Assigned Numbers Authority (IANA) ha riservato i seguenti tre blocchi dello spazio degli indirizzi IP per reti private:

- 10.0.0.0 - 10.255.255.255 (prefisso 10/8)
- 172.16.0.0 - 172.31.255.255 (prefisso 172.16/12)
- 192.168.0.0 - 192.168.255.255 (prefisso 192.168/16)

Per ulteriori informazioni, vedere https://tools.ietf.org/html/rfc1918.

Verifica che il nome del sito AD predefinito per il tuo AWS account Microsoft AD gestito corrisponda al nome del sito AD predefinito nell'infrastruttura locale. Il computer determina il nome del sito utilizzando un dominio di cui il computer è membro, non il dominio dell'utente. Ridenominare il sito in modo che corrisponda a quello on-premise più vicino garantisce che il localizzatore DC utilizzi un controller di dominio del sito più vicino. Se questa operazione non risolve il problema, è possibile che sia stato effettuato il caching delle informazioni da un inoltro condizionale creato in precedenza, che impedisce la creazione di un nuovo trust. Attendi qualche minuto, quindi prova nuovamente a creare il trust e l'inoltro condizionale.

Per ulteriori informazioni su come funziona, consulta Domain Locator Across a Forest Trust sul Microsoft sito Web.



L'operazione non può essere eseguita su questo dominio

Per risolvere il problema, assicurati che sia domini che directory non abbiano nomi NETBIOS sovrapposti. Se i domini/le directory hanno nomi NETBIOS sovrapposti, ricreali con un nome diverso, quindi riprova.

La creazione della relazione di trust non va a buon fine a causa dell'errore "Required and valid domain name"

I nomi DNS possono contenere solo caratteri alfabetici (A-Z), caratteri numerici (0-9), il segno meno (-) e un punto (.). I caratteri di punto sono consentiti solo quando vengono utilizzati per delimitare i componenti dei nomi di stile di dominio. Prendi in considerazione le seguenti soluzioni:

- AWS Microsoft AD gestito non supporta i trust con domini Single label. Per ulteriori informazioni, consulta il Microsoftsupporto per i domini a etichetta singola.

- Secondo RFC 1123 (https://tools.ietf.org/html/rfc1123), gli unici caratteri che possono essere utilizzati nelle etichette DNS sono da «A» a «Z», da «a» a «z», da «0" a «9" e un trattino («-»). Il punto [.] viene utilizzato anche nei nomi DNS, ma solo tra le etichette DNS e alla fine di un FQDN.
- Secondo RFC 952 (https://tools.ietf.org/html/rfc952), un «nome» (Net, Host, Gateway o Domain name) è una stringa di testo composta da un massimo di 24 caratteri tratti dall'alfabeto (A-Z), dalle cifre (0-9), dal segno meno (-) e dal punto (.). Nota che i periodi sono consentiti solo quando servono a delimitare componenti di "nomi in stile di dominio".

Per ulteriori informazioni, consulta Rispetto delle restrizioni relative ai nomi per host e domini sul sito web. Microsoft

Strumento generale per la verifica dei trust

Di seguito sono riportati gli strumenti che possono essere utilizzati per risolvere vari problemi relativi ai trust.

AWS Strumento di risoluzione dei problemi di Systems Manager Automation

Support Automation Workflows (SAW) sfrutta AWS Systems Manager Automation per fornirti un runbook predefinito per. Directory Service Lo strumento AWSSupport-TroubleshootDirectoryTrustrunbook consente di diagnosticare i problemi comuni di creazione di trust tra Managed AWS Microsoft AD e un Active Directory localeMicrosoft.

DirectoryServicePortTest strumento

Lo strumento DirectoryServicePortTestdi test può essere utile per la risoluzione dei problemi di creazione di fiducia tra AWS Managed Microsoft AD e Active Directory locale. Per un esempio su come questo strumento può essere utilizzato, consulta Test di un AD Connector.

Strumento NETDOM e NLTEST

Gli amministratori possono utilizzare gli strumenti della linea di comando Netdom e Nltest per trovare, visualizzare, creare, rimuovere e gestire i trust. Questi strumenti comunicano direttamente con l'autorità LSA su un controller di dominio. Per un esempio su come utilizzare questi strumenti, consulta Netdom e NLTEST sul sito Web. Microsoft

Strumento di acquisizione dei pacchetti

Puoi utilizzare l'utilità integrata di acquisizione dei pacchetti di Windows per esaminare e risolvere un potenziale problema di rete. Per ulteriori informazioni, consulta Acquisizione di una traccia di rete senza installare nulla.

AD Connector

AD Connector è un gateway di directory con cui puoi reindirizzare le richieste di directory all'ambiente locale Microsoft Active Directory senza memorizzare nella cache alcuna informazione nel cloud. AD Connector può essere di due dimensioni, piccolo o grande. Un AD Connector di dimensioni ridotte è progettato per le organizzazioni più piccole ed è destinato a gestire un numero ridotto di operazioni al secondo. Un AD Connector di ampie dimensioni è progettato per le organizzazioni più grandi ed è destinato a gestire un numero da moderato a elevato di operazioni al secondo. È possibile suddividere carichi di applicazioni su più AD Connector per una ricalibrazione in base alle esigenze. Non sono previsti limiti di connessione o dell'utente.

AD Connector non supporta i trust transitivi di Active Directory. AD Connectors e i domini Active Directory locali hanno una relazione 1 a 1. In altre parole, per ogni dominio locale, compresi i domini figlio in una foresta di Active Directory con cui si desidera eseguire l'autenticazione, è necessario creare un AD Connector univoco.

> **Note**
>
> AD Connector non può essere condiviso con altri AWS account. Se questo è un requisito, prendi in considerazione l'utilizzo di AWS Managed Microsoft AD perCondividi il tuo AWS Managed Microsoft AD. AD Connector, inoltre, non supporta il multi-VPC, il che significa che AWS applicazioni come WorkSpacesqueste devono essere fornite nello stesso VPC dell'AD Connector.

Una volta configurato, AD Connector offre i seguenti benefici:

- Gli utenti finali e gli amministratori IT possono utilizzare le credenziali aziendali esistenti per accedere ad AWS applicazioni come WorkSpaces WorkDocs, o Amazon. WorkMail
- Puoi gestire AWS risorse come EC2 istanze Amazon o bucket Amazon S3 tramite l'accesso basato sui ruoli IAM a. Console di gestione AWS
- Puoi applicare in modo coerente le politiche di sicurezza esistenti (come la scadenza delle password, la cronologia delle password e il blocco degli account) indipendentemente dal fatto che gli utenti o gli amministratori IT accedano alle risorse nell'infrastruttura locale o nel cloud. AWS
- Puoi utilizzare AD Connector per abilitare l'autenticazione a più fattori integrandosi con l'infrastruttura MFA esistente basata su RADIUS per fornire un ulteriore livello di sicurezza quando gli utenti accedono alle applicazioni. AWS

Continua a leggere gli argomenti contenuti in questa sezione per ulteriori informazioni su come stabilire una connessione a una directory e sfruttare al massimo le caratteristiche di AD Connector.

Argomenti

Nozioni di base su AD Connector

Con AD Connector puoi connetterti Directory Service all'Active Directory aziendale esistente. Quando si è connessi a una directory esistente, tutti i dati della directory rimangono sui controller dei domini. Directory Service non replica alcun dato della directory.

Argomenti

Prerequisiti di AD Connector

Per collegare la directory esistente a AD Connector, è necessario quanto segue:

Amazon VPC

Impostare un VPC con quanto segue:

- Almeno due sottoreti. Ciascuna sottorete deve trovarsi in una zona di disponibilità diversa e deve appartenere allo stesso tipo di rete.

Puoi usarlo IPv6 per il tuo VPC. Per ulteriori informazioni, consulta il IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

- Il VPC deve essere connesso alla rete esistente tramite una connessione VPN (rete privata virtuale) o Direct Connect.
- Il VPC deve disporre di una tenancy hardware predefinita.

Directory Service utilizza una struttura a due VPC. Le EC2 istanze che compongono la directory vengono eseguite all'esterno dell' AWS account e sono gestite da. AWS Hanno due schede di rete, `ETH0` e `ETH1`. `ETH0` è la scheda di gestione ed è al di fuori del tuo account. `ETH1` viene creata all'interno dell'account.

L'intervallo IP di gestione della rete `ETH0` della directory viene scelto a livello di codice per garantire che non sia in conflitto con il VPC in cui è distribuita la directory. Questo intervallo IP può trovarsi in una delle seguenti coppie (poiché le directory vengono eseguite in due sottoreti):

- 10.0.1.0/24 e 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 e 192.168.2.0/24

Evitiamo i conflitti controllando il primo ottetto del CIDR. `ETH1`. Se inizia con un 10, scegliamo un VPC 192.168.0.0/16 con le sottoreti 192.168.1.0/24 e 192.168.2.0/24. Se il primo ottetto è diverso da un 10, scegliamo un VPC 10.0.0.0/16 con le sottoreti 10.0.1.0/24 e 10.0.2.0/24.

L'algoritmo di selezione non include i percorsi del VPC. È quindi possibile avere un conflitto di routing IP da questo scenario.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di Amazon VPC:

- Cos'è Amazon VPC?
- Le sottoreti nel proprio VPC
- Aggiunta di un gateway privato virtuale hardware al proprio VPC

Per ulteriori informazioni in merito AWS Direct Connect, consulta la Guida per l'AWS Direct Connect utente.

Active Directory esistente

Dovrai connetterti a una rete esistente con un dominio Active Directory.

> **Note**
>
> AD Connector non supporta i domini con etichetta singola.

Il livello di funzionalità di questo dominio Active Directory deve essere pari `Windows Server 2003` o superiore. AD Connector supporta anche la connessione a un dominio ospitato su un' EC2 istanza Amazon.

> **Note**
>
> AD Connector non supporta i controller di dominio di sola lettura (RODC) se utilizzati in combinazione con la funzionalità Amazon domain-join. EC2

Account del servizio

È necessario disporre delle credenziali di un account del servizio nella directory esistente a cui sono stati assegnati i seguenti privilegi:

- Leggi utenti e gruppi - Obbligatorio
- Unisci computer al dominio: richiesto solo quando si utilizza Seamless Domain Join e WorkSpaces
- Creazione di oggetti informatici - Obbligatorio solo quando si utilizza Seamless Domain Join e WorkSpaces
- La password dell'account del servizio deve essere conforme AWS ai requisiti in materia di password. AWS le password devono essere:
  - Tra 8 e 128 caratteri di lunghezza, inclusi.
  - Contengono almeno un carattere di tre delle quattro categorie seguenti:
    - Lettere minuscole (a-z)
    - Lettere maiuscole (A-Z)
    - Numeri (0-9)
    - Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Per ulteriori informazioni, consulta Delegare privilegi all'account del servizio.

> **Note**
>
> AD Connector utilizza Kerberos per l'autenticazione e l'autorizzazione delle applicazioni AWS . LDAP viene utilizzato solo per la ricerca di oggetti di utenti e gruppi (operazioni di lettura). Con le transazioni LDAP, nulla è mutabile e le credenziali non vengono passate in testo non crittografato. L'autenticazione è gestita da un servizio AWS interno, che utilizza i ticket Kerberos per eseguire operazioni LDAP come utente.

Autorizzazioni degli utenti

Tutti gli utenti di Active Directory devono avere le autorizzazioni necessarie per leggere i propri attributi, in particolare, quelli elencati di seguito:

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Per impostazione predefinita, gli utenti di Active Directory dispongono dell'autorizzazione in lettura per questi attributi. Queste autorizzazioni potrebbero essere modificate nel tempo dagli amministratori, quindi è opportuno verificare che gli utenti le abbiano prima di configurare AD Connector per la prima volta.

Indirizzi IP

Ottenere gli indirizzi IP di due server DNS o controller del dominio nella directory esistente.

AD Connector ottiene i record SRV `_ldap._tcp.<DnsDomainName>` e `_kerberos._tcp.<DnsDomainName>` da questi server durante la connessione alla directory, quindi questi server devono contenere questi record SRV. AD Connector cerca di trovare un controller del dominio comune che fornirà entrambi i servizi LDAP e Kerberos, quindi questi record SRV devono comprendere almeno un controller del dominio comune. Per ulteriori informazioni sui record SRV, consultate SRV Resource Records su Microsoft. TechNet

Porte per sottoreti

Affinché AD Connector reindirizzi le richieste di directory ai controller di dominio Active Directory esistenti, il firewall della rete esistente deve avere le seguenti porte aperte CIDRs per entrambe le sottoreti del tuo Amazon VPC.

- TCP/UDP 53 - DNS
- TCP/UDP 88 - autenticazione Kerberos
- TCP/UDP 389 - LDAP

Queste sono le porte minime necessarie prima che AD Connector possa connettersi alla directory. La propria configurazione specifica potrebbe richiedere l'apertura di porte aggiuntive.

Se desideri utilizzare AD Connector e Amazon WorkSpaces, l'attributo Disable VLVSupport LDAP deve essere impostato su 0 per i controller di dominio. Questa è l'impostazione predefinita per i controller di dominio. AD Connector non sarà in grado di interrogare gli utenti nella directory se l'attributo Disable VLVSupport LDAP è abilitato. Ciò impedisce il funzionamento di AD Connector con Amazon WorkSpaces.

> **Note**
>
> Se i server DNS o i server del controller di dominio per il dominio Active Directory esistente si trovano all'interno del VPC, i gruppi di sicurezza associati a tali server devono avere le porte di cui sopra aperte a entrambe CIDRs le sottoreti del VPC.

Per requisiti di porta aggiuntivi, consulta Requisiti delle porte AD e AD DS nella documentazione. Microsoft

Preautenticazione Kerberos

I tuoi account utente devono avere la preautenticazione Kerberos abilitata. Per istruzioni dettagliate su come abilitare questa impostazione, vedi Assicurarsi che la preautenticazione di Kerberos sia abilitata. Per informazioni generali su questa impostazione, vai a Preautenticazione attiva Microsoft TechNet.

Tipi di crittografia

AD Connector supporta i seguenti tipi di crittografia durante l'autenticazione via Kerberos ai controller dei domini Active Directory:

- AES-256-HMAC

- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center prerequisiti

Se prevedi di utilizzare il Centro identità IAM con AD Connector, devi assicurarti che le seguenti condizioni siano vere:

- L'AD Connector è configurato nell'account di gestione della tua AWS organizzazione.
- L'istanza del Centro identità IAM si trova nella stessa regione in cui è impostato AD Connector.

Per ulteriori informazioni, consulta i prerequisiti di IAM Identity Center nella Guida per l' AWS IAM Identity Center utente.

Prerequisiti dell'autenticazione a più fattori

Per supportare l'autenticazione a più fattori con la directory AD Connector, è necessario quanto segue:

- Un server Remote Authentication Dial-In User Service (RADIUS) nella rete esistente che disponga di due endpoint client. Gli endpoint client RADIUS hanno i seguenti requisiti:
  - Per creare gli endpoint, sono necessari gli indirizzi IP dei server Directory Service . Questi indirizzi IP possono essere ottenuti dal campo Directory IP Address (Indirizzo IP della directory) dei dettagli della directory.
  - Entrambi gli endpoint RADIUS devono utilizzare lo stesso codice segreto condiviso.
- La rete esistente deve consentire il traffico in entrata attraverso la porta predefinita del server RADIUS (1812) dai server. Directory Service
- I nomi utente tra il server RADIUS e la directory esistente devono essere identici.

Per ulteriori informazioni sull'uso di AD Connector con l'MFA, consulta Abilitazione dell'autenticazione a più fattori per AD Connector.

Delegare privilegi all'account del servizio

Per connettersi alla directory esistente, è necessario disporre delle credenziali per l'account del servizio AD Connector nella directory esistente con determinati privilegi. Anche se i membri del gruppo Domain Admins (Amministratori del dominio) dispongono di privilegi sufficienti per connettersi

alla directory, come best practice è consigliabile utilizzare un account del servizio che disponga solo dei privilegi minimi necessari per connettersi alla directory. La procedura seguente illustra come creare un nuovo gruppo chiamato`Connectors`, delegare i privilegi necessari per connettersi a questo gruppo e quindi aggiungere un nuovo account di servizio Directory Service a questo gruppo.

Questa procedura deve essere eseguita su un computer che sia collegato alla directory e che abbia installato lo snap-in di MMC Utenti e computer di Active Directory. Inoltre, è necessario aver eseguito l'accesso come amministratore del dominio.

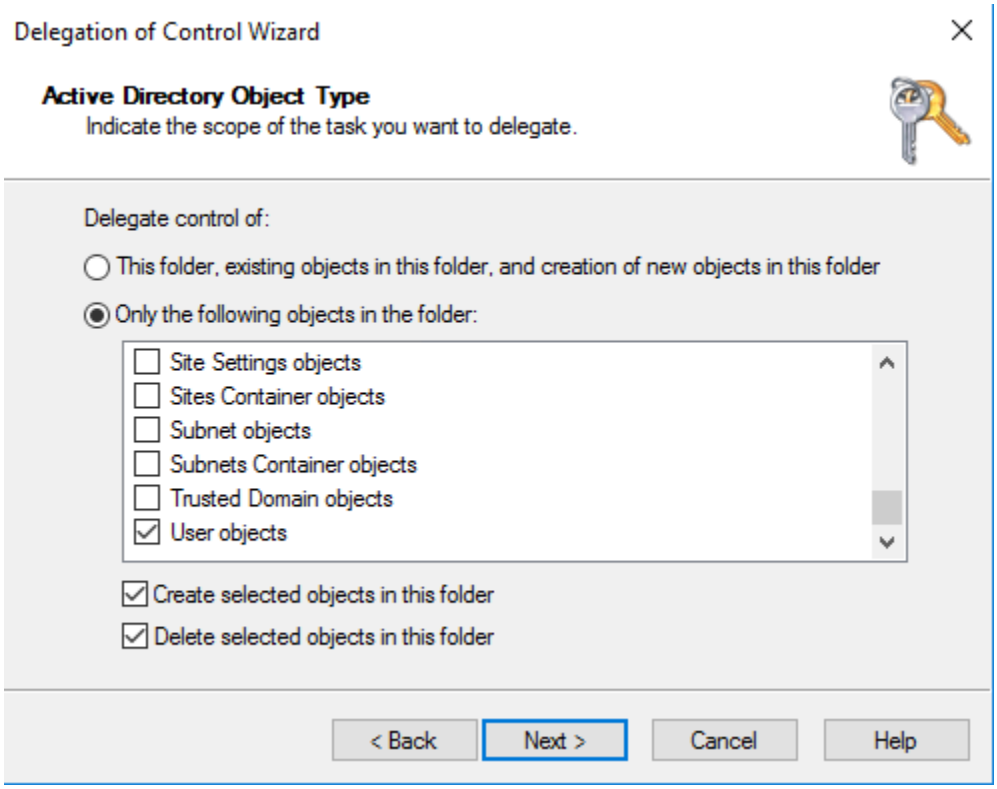
Delegare privilegi all'account del servizio

1. Apri Active Directory User and Computers (Utenti e computer di Active Directory) e seleziona la radice del dominio nell'albero di spostamento.
2. Nell'elenco nel riquadro a sinistra, fare clic con il pulsante destro del mouse su Utenti, selezionare Nuovo, quindi selezionare Gruppo.
3. Nella finestra di dialogo Nuovo oggetto Gruppo, inserire quanto segue e fare clic su OK.

Campo	Valore/Selezione
Group name (Nome gruppo)	`Connectors`
Ambito del gruppo	Globale
Tipo gruppo	Sicurezza

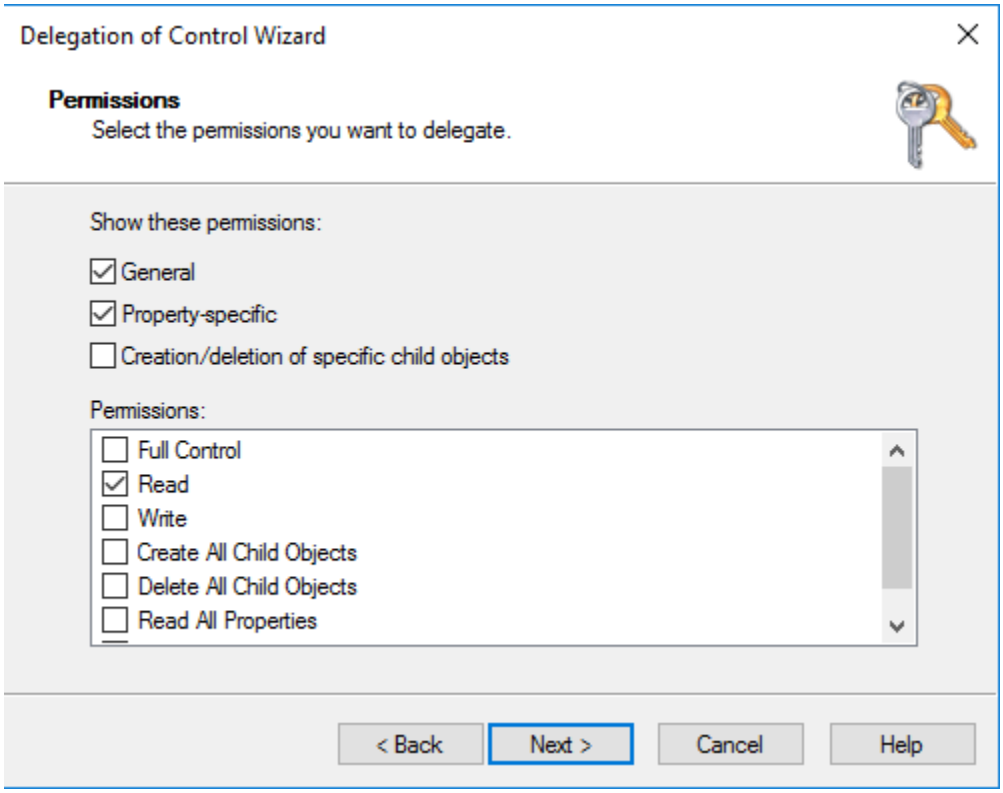
4. Nell'albero di navigazione Utenti e computer di Active Directory, selezionare Identifica l'unità organizzativa (OU) in cui verranno creati gli account dei computer. Nel menu, selezionare Azione e quindi Delega controllo. È possibile selezionare un'unità organizzativa principale fino al dominio in modo che le autorizzazioni si propaghino al figlio. OUs Se il tuo AD Connector è connesso a AWS Managed Microsoft AD, non avrai accesso al controllo delegato a livello di radice del dominio. In questo caso, per delegare il controllo, seleziona l'unità organizzativa nella directory OU in cui verranno creati gli oggetti computer.
5. Nella pagina Delega guidata del controllo, fare clic su Avanti, quindi fare clic su Aggiungi.
6. Nella finestra di dialogo Seleziona utenti, computer o gruppi, immettere `Connectors` e fare clic su OK. Se viene trovato più di un oggetto, selezionare il gruppo `Connectors` creato sopra. Fai clic su Next (Successivo).
7. Nella pagina Operazioni da delegare, selezionare Crea un'operazione personalizzata per eseguire la delega, quindi scegliere Avanti.

8. Selezionare Solo i seguenti oggetti contenuti nella cartella, quindi selezionare Oggetti computer e Oggetti utente.
9. Selezionare Crea gli oggetti selezionati in questa cartella e Elimina gli oggetti selezionati in questa cartella. Quindi scegli Successivo.



10. Seleziona Read (Lettura), quindi scegli Next (Avanti).

> **Note**
>
> Se utilizzerai Seamless Domain Join oppure WorkSpaces, devi anche abilitare le autorizzazioni di scrittura in modo che Active Directory possa creare oggetti informatici.



11. Verificare le informazioni sulla pagina Completamento di Delega guidata del controllo e fare clic su Fine.
12. Creare un account utente con una password complessa e aggiungerlo al gruppo `Connectors`. Questo utente sarà noto come account del servizio AD Connector e, poiché ora è membro del `Connectors` gruppo, dispone ora di privilegi sufficienti per connettersi Directory Service alla directory.

Test di un AD Connector

Affinché AD Connector si connetta alla directory esistente, il firewall della rete esistente deve avere determinate porte aperte CIDRs per entrambe le sottoreti del VPC. Per verificare se tali requisiti sono soddisfatti, eseguire i passaggi che seguono:

Per verificare la connessione

1. Lanciare un'istanza di Windows nel VPC e collegarla tramite RDP. L'istanza deve essere un membro del dominio esistente. I passaggi rimanenti vengono eseguiti su questa istanza VPC.

2. Scaricate e decomprimete l'applicazione di prova. DirectoryServicePortTest Il codice sorgente e i file di progetto Visual Studio sono inclusi, per cui è possibile modificare l'applicazione per i test, se necessario.

> **Note**
>
> Questo script non è supportato su Windows Server 2003 o sistemi operativi precedenti.

3. Da un prompt dei comandi di Windows, eseguire l'applicazione per i test DirectoryServicePortTest con le seguenti opzioni:

> **Note**
>
> L'applicazione di DirectoryServicePortTest test può essere utilizzata solo quando i livelli di funzionalità del dominio e della foresta sono impostati su Windows Server 2012 R2 e versioni precedenti.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,389" -udp "53,88,389"
```

<domain_name>

Il nome di dominio completo. Questo viene utilizzato per testare la foresta e i livelli funzionali del dominio. Se si esclude il nome del dominio, non sarà effettuato alcun test sui livelli funzionali.

<server_IP_address>

L'indirizzo IP di un controller di dominio nel dominio esistente. Le porte saranno testate usando questo indirizzo IP. Se si esclude l'indirizzo IP, non sarà effettuato alcun test sulle porte.

Questa applicazione di test determina se le porte necessarie sono aperte dal VPC al dominio e, inoltre, verifica i livelli funzionali di dominio e di foresta minimi.

L'output sarà simile al seguente:

```
Testing forest functional level.
```

```
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED

Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
Checking TCP port 88: PASSED
Checking TCP port 389: PASSED

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
Checking UDP port 88: PASSED
Checking UDP port 389: PASSED
```

Il seguente è il codice di origine per il modulo di risposta per l'applicazione DirectoryServicePortTest.

```
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;
```

```
        static void Main(string[] args)
        {
            if (ParseArgs(args))
            {
                try
                {
                    if (_domain.Length > 0)
                    {
                        try
                        {
                            TestForestFunctionalLevel();

                            TestDomainFunctionalLevel();
                        }
                        catch (ActiveDirectoryObjectNotFoundException)
                        {
                            Console.WriteLine("The domain {0} could not be found.\n",
_domain);
                        }
                    }

                    if (null != _ipAddr)
                    {
                        if (_tcpPorts.Count > 0)
                        {
                            TestTcpPorts(_tcpPorts);
                        }

                        if (_udpPorts.Count > 0)
                        {
                            TestUdpPorts(_udpPorts);
                        }
                    }
                }
                catch (AuthenticationException ex)
                {
                    Console.WriteLine(ex.Message);
                }
            }
            else
            {
                PrintUsage();
            }
```

```
            Console.Write("Press <enter> to continue.");
            Console.ReadLine();
        }

        static void PrintUsage()
        {
            string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
            Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
        }

        static bool ParseArgs(string[] args)
        {
            bool fReturn = false;
            string ipAddress = "";

            try
            {
                _tcpPorts = new List<int>();
                _udpPorts = new List<int>();

                for (int i = 0; i < args.Length; i++)
                {
                    string arg = args[i];

                    if ("-tcp" == arg | "/tcp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _tcpPorts = ParsePortList(portList);
                    }

                    if ("-udp" == arg | "/udp" == arg)
                    {
                        i++;
                        string portList = args[i];
                        _udpPorts = ParsePortList(portList);
                    }

                    if ("-d" == arg | "/d" == arg)
                    {
```

```
                    i++;
                    _domain = args[i];
                }

                if ("-ip" == arg | "/ip" == arg)
                {
                    i++;
                    ipAddress = args[i];
                }
            }
        }
        catch (ArgumentOutOfRangeException)
        {
            return false;
        }

        if (_domain.Length > 0 || ipAddress.Length > 0)
        {
            fReturn = true;
        }

        if (ipAddress.Length > 0)
        {
            _ipAddr = IPAddress.Parse(ipAddress);
        }

        return fReturn;
    }

    static List<int> ParsePortList(string portList)
    {
        List<int> ports = new List<int>();

        char[] separators = {',', ';', ':'};

        string[] portStrings = portList.Split(separators);
        foreach (string portString in portStrings)
        {
            try
            {
                ports.Add(Convert.ToInt32(portString));
            }
            catch (FormatException)
            {
```

```
                }
            }

            return ports;
        }

        static void TestForestFunctionalLevel()
        {
            Console.WriteLine("Testing forest functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
            Forest forestContext = Forest.GetForest(dirContext);

            Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

            if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static void TestDomainFunctionalLevel()
        {
            Console.WriteLine("Testing domain functional level.");

            DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
            Domain domainObject = Domain.GetDomain(dirContext);

            Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

            if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
            {
                Console.WriteLine("PASSED");
            }
            else
```

```
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static List<int> TestTcpPorts(List<int> portList)
        {
            Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking TCP port {0}: ", port);

                TcpClient tcpClient = new TcpClient();

                try
                {
                    tcpClient.Connect(_ipAddr, port);

                    tcpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }

        static List<int> TestUdpPorts(List<int> portList)
        {
            Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();
```

```
            foreach (int port in portList)
            {
                Console.Write("Checking UDP port {0}: ", port);

                UdpClient udpClient = new UdpClient();

                try
                {
                    udpClient.Connect(_ipAddr, port);
                    udpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }
    }
}
```

Creazione di un AD Connector

Per collegarti alla tua directory esistente con AD Connector, procedi come segue. Prima di iniziare la procedura, assicurati di soddisfare i prerequisiti illustrati in Prerequisiti di AD Connector.

> **Note**
>
> Non è possibile creare un AD Connector con un modello Cloud Formation.

Per connettersi con AD Connector

1. Nel riquadro di navigazione della Console AWS Directory Service, scegli Directory, quindi seleziona Configura directory.
2. Nella pagina Seleziona il tipo di directory, scegli AD Connector, quindi seleziona Successivo.

3. Nella pagina Enter AD Connector information (Inserisci le informazioni su AD Connector), fornire le seguenti informazioni:

   Dimensione della directory

   Scegliere tra l'opzione di dimensione Small (Piccola) o Large (Grande). Per ulteriori informazioni sulle dimensioni, consulta AD Connector.

   Descrizione della directory

   Descrizione opzionale della directory.

4. Nella pagina Choose VPC and subnets (Scegli VPC e sottoreti) fornire le seguenti informazioni, quindi selezionare Next (Successivo).

   VPC

   VPC per la directory.

   Sottoreti

   Scegli le sottoreti per i controller di dominio. Le due sottoreti devono trovarsi in diverse zone di disponibilità.

5. Nella pagina Connect to AD (Connettiti ad AD), fornire le seguenti informazioni:

   Nome DNS directory

   Il nome completo della directory esistente, ad esempio `corp.example.com`.

   Nome NetBIOS della directory

   Il nome breve della directory esistente, ad esempio `CORP`.

   Indirizzi IP DNS

   L'indirizzo IP di almeno un server DNS nella directory esistente. Questi server devono essere accessibili da ciascuna sottorete specificata nella fase 4. Questi server possono essere posizionati all'esterno AWS, purché vi sia connettività di rete tra le sottoreti specificate e gli indirizzi IP del server DNS.

   Nome utente dell'account del servizio

   Il nome utente di un utente nella directory esistente. Per ulteriori informazioni su questo account, consultare Prerequisiti di AD Connector.

Password dell'account del servizio

La password per l'account dell'utente esistente. Questa password distingue tra maiuscole e minuscole e deve essere di lunghezza compresa tra 8 e 128 caratteri. Deve anche contenere un carattere di almeno tre delle seguenti quattro categorie:

- Lettere minuscole (a-z)
- Lettere maiuscole (A-Z)
- Numeri (0-9)
- Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Conferma la password

Immettere nuovamente la password per l'account dell'utente esistente.

6. Nella pagina Review & create (Rivedi e crea), esaminare le informazioni relative alla directory ed eseguire eventuali modifiche. Quando le informazioni sono corrette, scegli Create Directory (Crea directory). Per creare la directory sono necessari alcuni minuti. Una volta creato, il valore Status cambia in Active (Attivo).

Per ulteriori informazioni su ciò che viene creato con il tuo AD Connector, consultaCosa viene creato con il tuo AD Connector.

Cosa viene creato con il tuo AD Connector

Quando crei un AD Connector, crea e associa Directory Service automaticamente un'interfaccia di rete elastica (ENI) a ciascuna delle tue istanze di AD Connector. Ognuno di questi ENIs elementi è essenziale per la connettività tra il VPC e Directory Service AD Connector e non deve mai essere eliminato. È possibile identificare tutte le interfacce di rete riservate all'uso Directory Service mediante la descrizione: "interfaccia di rete AWS creata per directory directory-id». Per ulteriori informazioni, consulta Elastic Network Interfaces nella Amazon EC2 User Guide.

> **Note**
>
> Per impostazione predefinita, le istanze AD Connector sono implementate in due zone di disponibilità in una regione e connesse al tuo cloud privato virtuale (VPC) di Amazon. Le istanze AD Connector che non funzionano vengono automaticamente sostituite nella stessa zona di disponibilità utilizzando lo stesso indirizzo IP.

Quando accedi a qualsiasi AWS applicazione o servizio integrato con un AD Connector (AWS IAM Identity Center incluso), l'app o il servizio inoltra la richiesta di autenticazione ad AD Connector, che a sua volta inoltra la richiesta a un controller di dominio nel tuo Active Directory autogestito per l'autenticazione. Se l'autenticazione è avvenuta correttamente nell'Active Directory autogestita, AD Connector restituisce quindi un token di autenticazione all'app o al servizio (simile a un token Kerberos). A questo punto, ora puoi accedere all'app o al AWS servizio.

Best practice per AD Connector

Di seguito alcuni suggerimenti e linee guida da tenere in considerazione per evitare problemi e sfruttare al massimo AD Connector.

Configurazione: prerequisiti

Tieni presenti queste linee guida prima di creare la directory.

Verifica di avere il tipo di directory corretto

Directory Service offre diverse modalità di utilizzo Microsoft Active Directory con altri AWS servizi. Puoi scegliere il servizio di directory con le caratteristiche di cui hai bisogno a un costo che si adatta al tuo budget:

- AWS Directory Service per Microsoft Active Directory è un servizio gestito ricco di funzionalità Microsoft Active Directory ospitato sul AWS cloud. AWS Microsoft AD gestito è la scelta migliore se hai più di 5.000 utenti e hai bisogno di impostare una relazione di fiducia tra una directory AWS ospitata e le directory locali.
- AD Connector collega semplicemente l'Active Directory locale esistente a AWS. Il connettore AD rappresenta la scelta migliore quando vuoi utilizzare la tua directory on-premise esistente tramite i servizi AWS .
- Simple AD è una directory a basso costo su scala ridotta con compatibilità di base con Active Directory. Supporta fino a 5.000 utenti, applicazioni compatibili con Samba 4 e compatibilità LDAP per applicazioni compatibili con LDAP.

Per un confronto più dettagliato delle Directory Service opzioni, consultaQuale scegliere.

Assicurati che le tue istanze VPCs e siano configurate correttamente

Per connetterti, gestire e utilizzare le tue directory, devi configurare correttamente le directory a VPCs cui sono associate. Consulta Prerequisiti per la creazione di un AWS Managed Microsoft AD, Prerequisiti di AD Connector o Prerequisiti di Simple AD per informazioni sulla sicurezza del VPC e sui requisiti di rete.

Se aggiungi un'istanza al dominio, assicurati di disporre della connessione e dell'accesso remoto all'istanza, come descritto in Modi per aggiungere un' EC2 istanza Amazon al tuo AWS Managed Microsoft AD.

Sii consapevole dei limiti

Scopri i vari limiti per il tuo tipo di directory specifico. Lo spazio di archiviazione disponibile e la dimensione aggregata degli oggetti sono le uniche limitazioni al numero di oggetti che puoi archiviare nella directory. Consulta, AWS Quote Microsoft AD gestite, Quote di AD Connector o Quote di Simple AD per maggiori dettagli sulla directory scelta.

Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory

AWS crea un gruppo di sicurezza e lo collega alle interfacce di rete elastiche della directory, accessibili tramite peering o ridimensionamento. VPCs AWS configura il gruppo di sicurezza per bloccare il traffico non necessario verso la directory e consente il traffico necessario.

Modifica del gruppo di sicurezza della directory

Per modificare la sicurezza delle directory dei tuoi gruppi di sicurezza, puoi farlo. Apporta tali modifiche solo se hai compreso a pieno come funziona il filtraggio del gruppo di sicurezza. Per ulteriori informazioni, consulta i gruppi EC2 di sicurezza Amazon per le istanze Linux nella Amazon EC2 User Guide. Modifiche improprie possono causare la perdita delle comunicazioni con i computer e le istanze previsti. AWS consiglia di non tentare di aprire porte aggiuntive nella directory in quanto ciò riduce la sicurezza della directory. Verifica attentamente il modello di responsabilità condivisa di AWS.

> **Warning**
>
> È tecnicamente possibile associare il gruppo di sicurezza della directory ad altre EC2 istanze create dall'utente. Tuttavia, AWS sconsiglia questa pratica. AWS può avere motivi per

modificare il gruppo di sicurezza senza preavviso per soddisfare le esigenze funzionali o di sicurezza della directory gestita. Tali modifiche influiscono sulle eventuali istanze con cui viene associato il gruppo di sicurezza della directory e possono interrompere il funzionamento delle istanze associate. Inoltre, l'associazione del gruppo di sicurezza della directory EC2 alle istanze può creare un potenziale rischio per la EC2 sicurezza delle istanze.

Configura i siti e le sottoreti on-premise correttamente quando utilizzi AD Connector

Se la tua rete on-premise ha siti di Active Directory definiti, è necessario accertarsi che le sottoreti nel VPC in cui AD Connector risiede siano definite in un sito Active Directory e che non vi siano conflitti tra le sottoreti del VPC e le sottoreti di altri siti.

Per individuare i controller di dominio, AD Connector utilizza il sito Active Directory i cui intervalli di indirizzi IP della sottorete sono vicini a quelli del VPC contenente AD Connector. Se disponi di un sito le cui sottoreti hanno gli stessi intervalli di indirizzi IP di quelli nel VPC, AD Connector individuerà i controller di dominio di tale sito, che potrebbero non essere fisicamente vicini alla tua regione.

Comprendi le restrizioni relative al nome utente per le applicazioni AWS

Directory Service fornisce supporto per la maggior parte dei formati di caratteri che possono essere utilizzati nella creazione di nomi utente. Tuttavia, vengono applicate restrizioni sui caratteri ai nomi utente che verranno utilizzati per l'accesso ad AWS applicazioni WorkSpaces, come WorkDocs Amazon WorkMail o Quick Suite. Queste limitazioni richiedono che non vengano utilizzati i seguenti caratteri:

- Spazi
- Caratteri multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Il simbolo @ è consentito purché preceda un suffisso UPN.

Programmazione delle applicazioni

Prima di programmare le applicazioni, valuta quanto segue:

Esecuzione di test di caricamento prima della produzione

Assicurati di effettuare test di laboratorio con le applicazioni e le richieste più importanti del tuo carico di lavoro di produzione per confermare che la directory si adatti al carico dell'applicazione. Se necessiti di ulteriore capacità, distribuisci i carichi su più directory AD Connector.

Utilizzo della directory

Di seguito sono elencati alcuni suggerimenti da tenere a mente quando utilizzi la directory.

Modifica periodica delle credenziali dell'amministratore

Modifica periodicamente la password dell'amministratore dell'account di servizio AD Connector e assicurati che sia coerente con le policy esistenti delle password di Active Directory. Per istruzioni su come modificare la password dell'account di servizio, consulta Aggiornamento delle credenziali dell'account del servizio AD Connector in Console di gestione AWS.

Utilizza AD Connectors univoci per ciascun dominio

AD Connectors e i domini AD on-premise hanno una relazione uno-a-uno. Ovvero per ciascun dominio on-premise, compresi i domini figlio in una foresta AD dove si desidera autenticarsi, devi creare un AD Connector univoco. Ogni AD Connector creato deve utilizzare un diverso account del servizio, anche se è connesso alla stessa directory.

Controlla la compatibilità

Quando si utilizza AD Connector, è necessario assicurarsi che la directory locale sia e rimanga compatibile con Directory Service. Per ulteriori informazioni sulle proprie responsabilità, consultare il nostro modello sulla responsabilità condivisa.

Gestione della directory AD Connector

Puoi utilizzarlo Console di gestione AWS per gestire il tuo AD Connector e completare le attività day-to-day amministrative. I modi in cui puoi gestire la tua directory includono:

- Visualizza i dettagli sul tuo AD Connector.
- Aggiorna l'indirizzo DNS a cui punta il tuo AD Connector.
- Elimina il tuo AD Connector quando non è più necessario.

Visualizzazione delle informazioni sulla directory AD Connector

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory. Le informazioni sulla directory vengono visualizzate nella sezione Dettagli della directory.

Per ulteriori informazioni sul campo Status (Stato), consultare Comprendere lo stato della directory.

Aggiornamento del tipo di rete di directory

Puoi aggiornare il tipo di rete della tua Directory Service directory da IPv4 a Dual-stack (and). IPv4 IPv6 L'aggiornamento del tipo di rete per includere gli indirizzi IPv6 IP offre uno spazio di indirizzi più ampio di. IPv4 IPv4 e le IPv6 comunicazioni sono indipendenti l'una dall'altra.

Per i dettagli, consulta la sezione Confronta IPv4 e IPv6 nella Amazon Virtual Private Cloud User Guide.

> **Important**
>
> Si tratta di un'operazione unidirezionale che non può essere annullata. Esegui prima il test in un ambiente non di produzione.

Prerequisiti

Prima di aggiornare il tipo di rete di directory, assicuratevi che siano soddisfatti i seguenti requisiti:

- Il tuo VPC deve essere configurato con intervalli IPv6 CIDR. Per i dettagli, consulta il IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
- Hai accesso amministrativo a. Console di gestione AWS
- La tua directory deve essere in stato attivo.
- Disponi delle autorizzazioni IAM appropriate per modificare Directory Service le impostazioni.

Per aggiornare il tipo di rete delle directory

Per aggiornare la directory alla rete dual-stack

> **Note**
>
> Se la directory viene replicata in più regioni, esegui questo aggiornamento in ciascuna regione.

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Seleziona la directory di destinazione.
3. Vai alla scheda Rete e sicurezza.
4. Scegli Aggiungi IPv6 supporto. Questa opzione è disponibile solo per le directory IPv4 -only.
5. Consulta le informazioni di aggiornamento e i dettagli sui prezzi.
6. Scegli Aggiungi per confermare l'aggiornamento.

Dopo aver avviato l'aggiornamento, lo stato della directory passa a Aggiornamento durante il processo di aggiornamento. Il completamento dell'aggiornamento richiede in genere 15-30 minuti. Una volta completato, lo stato della directory torna ad Attivo.

Aggiornamento dell'indirizzo DNS per il tuo AD Connector

Utilizza i passaggi seguenti per aggiornare gli indirizzi DNS ai quali punta AD Connector.

> **Note**
>
> Se è in corso un aggiornamento, è necessario attenderne il completamento prima di avviare un altro aggiornamento.
> Se lo utilizzi WorkSpaces con il tuo AD Connector, assicurati che anche gli indirizzi DNS del tuo WorkSpace account siano aggiornati. Per ulteriori informazioni, consulta Aggiornare i server DNS per. WorkSpaces

Per aggiornare le impostazioni DNS per AD Connector

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Dettagli della directory selezionare la scheda Reti e sicurezza.
4. Nella sezione Impostazioni DNS esistenti, scegli Aggiorna.
5. Nella finestra di dialogo Aggiornamento di indirizzi DNS esistenti, digita gli indirizzi IP DNS aggiornati, quindi scegli Aggiorna.

Per ulteriori informazioni sulla risoluzione dei problemi di AD Connector, consulta Risoluzione dei problemi di AD Connector.

Eliminazione di AD Connector

Quando una directory del connettore AD viene eliminata, quella on-premise rimane intatta. Anche tutte le istanze collegate alla directory rimangono intatte e collegate alla tua directory on-premise. Puoi, tuttavia, utilizzare le credenziali della directory per accedere a queste istanze.

Eliminare AD Connector

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory. Assicurati di trovarti nel Regione AWS luogo in cui è distribuito il tuo AD Connector. Per ulteriori informazioni, consulta Scelta di una regione.
2. Assicurati che nessuna AWS applicazione sia abilitata per l'AD Connector che intendi eliminare. AWSLe applicazioni abilitate ti impediranno di eliminare il tuo AD Connector.

    a. Nella pagina Directories (Directory), scegli l'ID della directory.

    b. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione). Nella sezione AWSapp e servizi, puoi vedere quali AWS applicazioni sono abilitate per il tuo AD Connector.

    - Disabilita Console di gestione AWS l'accesso. Per ulteriori informazioni, consulta Disabilitazione dell'accesso Console di gestione AWS.
    - Per disabilitare Amazon WorkSpaces, devi annullare la registrazione del servizio dalla directory nella WorkSpaces console. Per ulteriori informazioni, consulta Eliminare una directory nella Amazon WorkSpaces Administration Guide.

- Per disabilitarlo WorkDocs, devi eliminare il WorkDocs sito nella WorkDocs console. Per ulteriori informazioni, consulta Eliminare un sito nella Amazon WorkDocs Administration Guide.
- Per disabilitare Amazon WorkMail, devi rimuovere l' WorkMail organizzazione Amazon dalla WorkMail console Amazon. Per ulteriori informazioni, consulta Rimuovere un'organizzazione nella Amazon WorkMail Administrator Guide.
- Per disabilitare Amazon FSx for Windows File Server, devi rimuovere il FSx file system Amazon dal dominio. Per ulteriori informazioni, consulta Working with Active Directory in FSx for Windows File Server nella Amazon FSx for Windows File Server User Guide.
- Per disabilitare Amazon Relational Database Service, devi rimuovere l'istanza Amazon RDS dal dominio. Per ulteriori informazioni, consulta Gestione di un'istanza database in un dominio nella Guida per l'utente di Amazon RDS.
- Per disabilitare AWS Client VPN il servizio, è necessario rimuovere il servizio di directory dall'endpoint Client VPN. Per ulteriori informazioni, consulta Work with Client VPN nella AWS Client VPNAdministrator Guide.
- Per disabilitare Amazon Connect, è necessario eliminare l'istanza di Amazon Connect. Per ulteriori informazioni, consulta Eliminare l'istanza Amazon Connect nella Amazon Connect Administration Guide.
- Per disabilitare Amazon Quick Suite, devi annullare l'iscrizione ad Amazon Quick Suite. Per ulteriori informazioni, consulta Chiusura Amazon Quick Suite dell'account nella Guida per l'utente di Amazon Quick Suite.

> **Note**
>
> Se la utilizzi AWS IAM Identity Center e la hai precedentemente connessa alla directory AWS Managed Microsoft AD che intendi eliminare, devi prima modificare l'origine dell'identità prima di poterla eliminare. Per ulteriori informazioni, consulta Modifica della fonte di identità nella Guida per l'utente del Centro identità IAM.

3. Nel riquadro di navigazione, seleziona Directory.
4. Seleziona solo l'AD Connector da eliminare, quindi fai clic su Elimina. Sono necessari alcuni minuti per l'eliminazione dell'AD Connector. Una volta eliminato, AD Connector viene rimosso dal tuo elenco di directory.

Protezione della directory AD Connector

Puoi utilizzare funzionalità come l'autenticazione a più fattori (MFA), il Lightweight Directory Access Protocol over Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) sul lato client e proteggere il tuo AD Connector. AWS Autorità di certificazione privata I modi per proteggere il tuo AD Connector includono:

- Abilita l'MFA per aumentare la sicurezza di AD Connector.
- Abilita il Lightweight Directory Access Protocol over Secure Socket Layer (SSL) /Transport Layer Security (TLS) (LDAPS) sul lato client in modo che le comunicazioni su LDAP siano crittografate e migliorino la sicurezza.
- Abilita l'autenticazione Mutual Transport Layer Security (MTLS) basata su certificati con smart card che consente agli utenti di autenticarsi in Amazon Web Services tramite Active Directory e AD Connector.
- Aggiorna le credenziali dell'account del servizio AD Connector.
- Configura AWS Private CA Connector for AD in modo da poter emettere e gestire i certificati per il tuo AD Connector.

Attività per proteggere il tuo AD Connector

- Abilitazione dell'autenticazione a più fattori per AD Connector
- Abilitazione di LDAPS lato client tramite AD Connector
- Abilitazione dell'autenticazione MTLS in AD Connector per l'utilizzo con smart card
- Aggiornamento delle credenziali dell'account del servizio AD Connector in Console di gestione AWS
- Configurare AWS Private CA Connector for AD

Abilitazione dell'autenticazione a più fattori per AD Connector

Puoi abilitare l'autenticazione a più fattori per AD Connector quando Active Directory è in esecuzione in locale o in istanze Amazon EC2 . Per ulteriori informazioni sull'utilizzo dell'autenticazione a più fattori con, consulta. Directory ServicePrerequisiti di AD Connector

> **Note**
>
> L'autenticazione a più fattori non è disponibile per Simple AD. Tuttavia, l'MFA può essere abilitata per la directory AWS Managed Microsoft AD. Per ulteriori informazioni, consulta Abilitazione dell'autenticazione a più fattori per AWS Managed Microsoft AD.

Per abilitare l'autenticazione a più fattori per AD Connector

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Scegli il link ID directory per la directory AD Connector.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Multi-factor authentication (Autenticazione a più fattori) selezionare Actions (Operazioni), quindi Enable (Abilita).
5. Fornire i seguenti valori nella pagina Enable multi-factor authentication (MFA) (Abilita l'autenticazione a più fattori (MFA)):

   Display label (Visualizza etichetta)

   Indicare un nome per l'etichetta.

   RADIUS server DNS name or IP addresses (Indirizzi IP o nome DNS del server RADIUS)

   Gli indirizzi IP degli endpoint del server RADIUS o l'indirizzo IP del sistema di bilanciamento del carico del server RADIUS. Puoi inserire più indirizzi IP separandoli con una virgola, ad esempio `192.0.0.0,192.0.0.12`.

   > **Note**
   >
   > RADIUS MFA è applicabile solo per autenticare l'accesso a o ad applicazioni e servizi Amazon Enterprise come Amazon Quick Suite o WorkSpaces Amazon Chime. Console di gestione AWS Non fornisce MFA ai carichi di lavoro Windows in esecuzione su EC2 istanze o per l'accesso a un'istanza. EC2 Directory Service non supporta l'autenticazione RADIUS. Challenge/Response
   > Quando inseriscono nome utente e password, gli utenti devono disporre del proprio codice MFA. In alternativa, è necessario utilizzare una soluzione che esegua l'autenticazione a più fattori, out-of-band ad esempio la verifica del testo tramite SMS

per l'utente. Nelle soluzioni out-of-band MFA, è necessario assicurarsi di impostare il valore di timeout RADIUS in modo appropriato per la soluzione in uso. Quando si utilizza una soluzione out-of-band MFA, la pagina di accesso richiederà all'utente un codice MFA. In questo caso, la best practice per gli utenti è inserire la loro password nel campo password e nel campo MFA.

Porta

La porta utilizzata dal server RADIUS per le comunicazioni. La rete locale deve consentire il traffico in entrata attraverso la porta server RADIUS predefinita (UDP:1812) dai server. Directory Service

Shared secret code (Codice segreto condiviso)

Il codice segreto condiviso specificato quando sono stati creati gli endpoint RADIUS.

Confirm shared secret code (Conferma codice segreto condiviso)

Conferma il codice segreto condiviso per gli endpoint RADIUS.

Protocollo

Seleziona il protocollo specificato quando sono stati creati gli endpoint RADIUS.

Server timeout (in seconds) (Timeout del server (in secondi))

Il periodo di tempo, in secondi, per cui il server RADIUS attende una risposta. Il valore deve essere compreso tra 1 e 50.

Max RADIUS request retries (Numero massimo di tentativi di richieste RADIUS)

Il numero di volte per cui viene tentata la comunicazione con il server RADIUS. Il valore deve essere compreso tra 0 e 10.

L'autenticazione a più fattori è disponibile se RADIUS Status (Stato RADIUS) viene modificato in Enabled (Abilitato).

6. Scegli Abilita .

Abilitazione di LDAPS lato client tramite AD Connector

Il supporto LDAPS lato client in AD Connector crittografa le comunicazioni tra Microsoft Active Directory (AD) e le applicazioni. AWS Esempi di tali applicazioni includono WorkSpaces AWS IAM Identity Center, Quick Suite e Amazon Chime. Questa crittografia ti aiuta a proteggere meglio i dati di identità della tua organizzazione e a soddisfare i tuoi requisiti di sicurezza.

È inoltre possibile annullare la registrazione e disabilitare il protocollo LDAPS lato client.

Argomenti

Prerequisiti

Prima di abilitare LDAPS lato client, è necessario soddisfare i seguenti requisiti.

Prerequisiti:

- Distribuire certificati server in Active Directory
- Requisiti del certificato CA
- Requisiti di rete

Distribuire certificati server in Active Directory

Per abilitare LDAPS lato client, è necessario ottenere e installare i certificati server per ogni controller di dominio in Active Directory. Questi certificati verranno utilizzati dal servizio LDAP per ascoltare e accettare automaticamente connessioni SSL dai client LDAP. È possibile utilizzare certificati SSL emessi da una distribuzione interna di Active Directory Certificate Services (ADCS) o acquistati da un'emittente commerciale. Per ulteriori informazioni sui requisiti dei certificati server Active Directory, vedere il certificato LDAP su SSL (LDAPS) sul sito Web Microsoft.

Requisiti del certificato CA

Un certificato di autorità di certificazione (CA), che rappresenta l'emittente dei certificati server, è necessario per l'operazione LDAPS lato client. I certificati CA sono abbinati ai certificati server

presentati dai controller di dominio Active Directory per crittografare le comunicazioni LDAP. Tenere presenti i seguenti requisiti del certificato CA:

- Per registrare un certificato, sono necessari più di 90 giorni dalla scadenza.
- I certificati devono essere in formato PEM (Privacy-Enhanced Mail). Se si esportano certificati CA da Active Directory, scegliere il formato di file di esportazione con codifica Base64 X.509 (.CER).
- È possibile archiviare un massimo di cinque (5) certificati CA per la directory AD Connector.
- I certificati che utilizzano l'algoritmo di firma RSASSA-PSS non sono supportati.

Requisiti di rete

AWS il traffico LDAP dell'applicazione verrà eseguito esclusivamente sulla porta TCP 636, senza alcun fallback sulla porta LDAP 389. Tuttavia, le comunicazioni LDAP di Windows che supportano replica, trust e altro ancora continueranno a utilizzare la porta LDAP 389 con protezione nativa di Windows. Configura i gruppi AWS di sicurezza e i firewall di rete per consentire le comunicazioni TCP sulla porta 636 in AD Connector (in uscita) e Active Directory autogestita (in entrata).

Abilitazione del protocollo LDAPS lato client

Per abilitare LDAPS lato client, è possibile importare il certificato di autorità di certificazione (CA) in AD Connector e quindi abilitare LDAPS nella directory. Una volta abilitato, tutto il traffico LDAP tra le AWS applicazioni e l'Active Directory autogestito fluirà con la crittografia dei canali Secure Sockets Layer (SSL).

Sono disponibili due metodi diversi per abilitare LDAPS lato client per la directory. È possibile utilizzare il metodo o il Console di gestione AWS metodo. AWS CLI

Registrazione del certificato in Directory Service

Utilizza uno dei seguenti metodi per registrare un certificato in Directory Service.

Metodo 1: Per registrare il certificato in Directory Service (Console di gestione AWS)

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Client-side LDAPS (LDAPS lato client) selezionare il menu Actions (Operazioni) e quindi selezionare Register certificate (Registra certificato).

5. Nella finestra di dialogo Register a CA certificate (Registra un certificato CA) selezionare Browse (Sfoglia), quindi selezionare il certificato e scegliere Open (Apri).
6. Scegliere Register certificate (Registra certificato).

Metodo 2: registrare il certificato in Directory Service (AWS CLI)

- Esegui il comando seguente. Per i dati del certificato, scegliere il percorso del file del certificato CA. Nella risposta verrà fornito un ID certificato.

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

Verifica dello stato della registrazione

Per visualizzare lo stato di una registrazione di certificati o di un elenco di certificati registrati, utilizzare uno dei seguenti metodi.

Metodo 1: per controllare lo stato di registrazione del certificato in Directory Service (Console di gestione AWS)

1. Andare alla sezione Client-side LDAPS (LDAPS lato client) nella pagina dei Directory details (Dettagli della directory).
2. Esaminare lo stato di registrazione del certificato corrente visualizzato nella colonna Registration status (Stato registrazione). Quando il valore dello stato di registrazione cambia in Registered (Registrato), il certificato è stato registrato.

Metodo 2: Per controllare lo stato di registrazione del certificato in Directory Service (AWS CLI)

- Esegui il comando seguente. Se il valore dello stato restituisce `Registered`, il certificato è stato registrato.

```
aws ds list-certificates --directory-id your_directory_id
```

Abilitazione del protocollo LDAPS lato client

Utilizzate uno dei seguenti metodi per abilitare l'accesso LDAPS lato client. Directory Service

> **Note**
>
> Devi aver registrato almeno un certificato prima di poter abilitare LDAPS lato client.

Metodo 1: Per abilitare LDAPS lato client in () Directory ServiceConsole di gestione AWS

1. Andare alla sezione Client-side LDAPS (LDAPS lato client) nella pagina dei Directory details (Dettagli della directory).
2. Scegli Abilita . Se questa opzione non è disponibile, verificare che un certificato valido sia stato registrato e riprovare.
3. Nella finestra di dialogo Enable client-side LDAPS (Abilita LDAPS lato client) scegliere Enable (Abilita).

Metodo 2: Per abilitare LDAPS lato client in () Directory ServiceAWS CLI

- Esegui il comando seguente.

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

Verifica dello stato LDAPS

Utilizzate uno dei seguenti metodi per verificare lo stato LDAPS. Directory Service

Metodo 1: per controllare lo stato LDAPS in Directory Service ()Console di gestione AWS

1. Andare alla sezione Client-side LDAPS (LDAPS lato client) nella pagina dei Directory details (Dettagli della directory).
2. Se il valore dello stato visualizzato è Enabled (Abilitato), LDAPS è stato configurato.

Metodo 2: Per controllare lo stato LDAPS in Directory Service ()AWS CLI

- Esegui il comando seguente. Se il valore di stato restituisce `Enabled`, LDAPS è stato configurato.

```
aws ds describe-ldaps-settings -directory-id your_directory_id
```

Per ulteriori informazioni sulla visualizzazione del certificato LDAPS sul lato client, sull'annullamento della registrazione o sulla disabilitazione del certificato LDAPS, consulta. Gestione del protocollo LDAPS lato client

Gestione del protocollo LDAPS lato client

Utilizzare questi comandi per gestire la configurazione LDAPS.

Sono disponibili due metodi diversi per gestire le impostazioni LDAPS lato client. È possibile utilizzare il Console di gestione AWS metodo o il metodo. AWS CLI

Visualizzare i dettagli del certificato

Utilizza uno dei seguenti metodi per vedere quando scade un certificato.

Metodo 1: per visualizzare i dettagli del certificato in Directory Service (Console di gestione AWS)

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Client-side LDAPS (LDAPS lato client), le informazioni sul certificato verranno visualizzate in CA certificates (Certificati CA).

Metodo 2: Per visualizzare i dettagli del certificato in Directory Service (AWS CLI)

- Esegui il comando seguente. Per l'ID del certificato, utilizzare l'identificatore restituito da `register-certificate` o `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Annullare la registrazione di un certificato

Utilizza uno dei seguenti metodi per annullare la registrazione di un certificato.

> **Note**
>
> Se è registrato un solo certificato, è necessario disabilitare LDAPS prima di poter annullare la registrazione del certificato.

Metodo 1: annullare la registrazione di un certificato in Directory Service ()Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Client-side LDAPS (LDAPS lato client) selezionare il menu Actions (Operazioni) e quindi selezionare Deregister certificate (Annulla registrazione certificato).
5. Nella finestra di dialogo Deregister a CA certificate (Annulla la registrazione di un certificato CA) scegliere Deregister (Annulla registrazione).

Metodo 2: annullare la registrazione di un certificato in () Directory ServiceAWS CLI

- Esegui il comando seguente. Per l'ID del certificato, utilizzare l'identificatore restituito da `register-certificate` o `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Disabilitare LDAPS lato client

Utilizza uno dei seguenti metodi per disabilitare LDAPS lato client.

Metodo 1: disabilitare LDAPS lato client in () Directory ServiceConsole di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Client-side LDAPS (LDAPS lato client) scegliere Disable (Disabilita).

5. Nella finestra di dialogo Disable client-side LDAPS (Disabilita LDAPS lato client) scegliere Disable (Disabilita).

Metodo 2: disabilitare LDAPS lato client in () Directory ServiceAWS CLI

- Esegui il comando seguente.

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

Abilitazione dell'autenticazione MTLS in AD Connector per l'utilizzo con smart card

Puoi utilizzare l'autenticazione Mutual Transport Layer Security (MTLS) basata su certificati con smart card per autenticare gli utenti in WorkSpaces Amazon tramite Active Directory (AD) e AD Connector autogestiti. Se abilitata, gli utenti selezionano la propria smart card nella schermata di WorkSpaces accesso e inseriscono un PIN per l'autenticazione, anziché utilizzare nome utente e password. Da lì, il desktop virtuale Windows o Linux utilizza la smart card per autenticarsi in AD dal sistema operativo desktop nativo.

> **Note**
>
> L'autenticazione con smart card in AD Connector è disponibile solo nei seguenti Regioni AWS casi e solo con WorkSpaces. Al momento non sono supportate altre AWS applicazioni.
>
> - Stati Uniti orientali (Virginia settentrionale)
> - Stati Uniti occidentali (Oregon)
> - Asia Pacifico (Sydney)
> - Asia Pacifico (Tokyo)
> - Europa (Irlanda)
> - AWSGovCloud (Stati Uniti occidentali)
> - AWSGovCloud (Stati Uniti orientali)

Puoi anche annullare la registrazione e disabilitare i certificati.

Argomenti

- Prerequisiti
- Attivazione dell'autenticazione con smart card
- Gestione delle impostazioni di autenticazione delle smart card

Prerequisiti

Per abilitare l'autenticazione Mutual Transport Layer Security (mTLS) basata su certificati utilizzando smart card per il WorkSpaces client Amazon, è necessaria un'infrastruttura smart card operativa integrata con Active Directory autogestita. Per ulteriori informazioni su come configurare l'autenticazione con smart card con Amazon WorkSpaces e Active Directory, consulta la Amazon WorkSpaces Administration Guide.

Prima di abilitare l'autenticazione con smart card per WorkSpaces, consulta i seguenti prerequisiti:

- Requisiti del certificato CA
- Requisiti in termini di certificato utente
- Processo di verifica della revoca del certificato
- Considerazioni

Requisiti del certificato CA

AD Connector richiede un certificato dell'autorità di certificazione (CA), che rappresenta l'emittente dei certificati utente, per l'autenticazione con smart card. AD Connector abbina i certificati CA a quelli presentati dagli utenti con le loro smart card. Tenere presenti i seguenti requisiti del certificato CA:

- Per registrare un certificato CA, sono necessari più di 90 giorni dalla scadenza.
- I certificati CA devono essere in formato PEM (Privacy-Enhanced Mail). Se esporti certificati CA da Active Directory, scegliere come formato di file di esportazione X.509 (.CER) con codifica Base64.
- Affinché l'autenticazione con smart card abbia esito positivo, è necessario caricare tutti i certificati CA root e intermediari che collegano la CA emittente ai certificati utente.
- È possibile archiviare un massimo di 100 certificati CA per la directory AD Connector
- AD Connector non supporta l'algoritmo di firma RSASSA-PSS per i certificati CA.
- Verifica che il servizio di propagazione dei certificati sia impostato su Automatico e in esecuzione.

Requisiti in termini di certificato utente

Di seguito sono riportati alcuni dei requisiti per il certificato utente:

- Il certificato smart card dell'utente ha un nome alternativo del soggetto (SAN) dell'utente userPrincipalName (UPN).
- Il certificato smart card dell'utente dispone di Enhanced Key Usage come accesso tramite smart card (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2).
- Le informazioni OCSP (Online Certificate Status Protocol) per il certificato smart card dell'utente devono essere Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) nell'Authority Information Access.

Per ulteriori informazioni sui requisiti di autenticazione ad Connector e smart card, consulta Requisiti nella Amazon WorkSpaces Administration Guide. Per assistenza nella risoluzione dei WorkSpaces problemi di Amazon, come l'accesso WorkSpaces, la reimpostazione della password o la connessione a WorkSpaces, consulta Risolvere i WorkSpaces problemi dei client nella Amazon User Guide. WorkSpaces

Processo di verifica della revoca del certificato

Per eseguire l'autenticazione con smart card, AD Connector deve verificare lo stato di revoca dei certificati utente utilizzando il protocollo OCSP (Online Certificate Status Protocol). Per eseguire il controllo della revoca dei certificati, l'URL del risponditore OCSP deve essere accessibile da Internet. Se utilizzi un nome DNS, l'URL del risponditore OCSP deve utilizzare un dominio di primo livello trovato nel database della zona radice dell'IANA (Internet Assigned Numbers Authority).

Il controllo della revoca dei certificati di AD Connector utilizza il seguente processo:

- AD Connector deve verificare l'estensione AIA (Authority Information Access) nel certificato utente per l'URL del risponditore OCSP e poi utilizzare l'URL per verificare la revoca.
- Se non riesce a risolvere l'URL trovato nell'estensione AIA del certificato utente né a trovare l'URL del risponditore OCSP nel certificato utente, AD Connector utilizza l'URL OCSP opzionale fornito durante la registrazione del certificato CA root.

  Se l'URL nell'estensione AIA del certificato utente si risolve ma non risponde, l'autenticazione dell'utente non va a buon fine.

- Se l'URL del risponditore OCSP fornito durante la registrazione del certificato CA root non può essere risolto o non risponde, oppure se non è stato fornito alcun URL del risponditore OCSP, l'autenticazione dell'utente non va a buon fine.
- Il server OCSP deve essere conforme alla RFC 6960. Inoltre, il server OCSP deve supportare le richieste che utilizzano il metodo GET per richieste inferiori o uguali a 255 byte in totale.

> **Note**
>
> AD Connector richiede un URL HTTP per l'URL del risponditore OCSP.

Considerazioni

Prima di abilitare l'autenticazione con smart card in AD Connector, considera i seguenti elementi:

- AD Connector utilizza l'autenticazione mTLS (Mutual Transport Layer Security) basata su certificati per autenticare gli utenti su Active Directory utilizzando certificati smart card basati su hardware o software. Al momento sono supportate solo le carte di accesso comune (CAC) e quelle di verifica dell'identità personale (PIV). Altri tipi di smart card basate su hardware o software potrebbero funzionare ma non sono state testate per l'uso con lo Streaming Protocol. WorkSpaces
- L'autenticazione con smart card sostituisce l'autenticazione di nome utente e password con. WorkSpaces

  Se nella directory AD Connector sono configurate altre AWS applicazioni con l'autenticazione smart card abilitata, tali applicazioni presentano ancora la schermata di immissione del nome utente e della password.
- L'attivazione dell'autenticazione con smart card limita la durata della sessione utente alla durata massima dei ticket di assistenza Kerberos. È possibile configurare questa impostazione utilizzando una policy del gruppo e, per impostazione predefinita, è impostata su 10 ore. Per ulteriori informazioni sulle impostazioni, consulta la documentazione di Microsoft.
- Il tipo di crittografia Kerberos supportato dall'account del servizio AD Connector deve corrispondere a ogni tipo di crittografia Kerberos supportato dal controller di dominio.

Attivazione dell'autenticazione con smart card

Per abilitare l'autenticazione con smart card WorkSpaces sul tuo AD Connector, devi prima importare i certificati dell'autorità di certificazione (CA) in AD Connector. Puoi importare i tuoi certificati CA in

AD Connector utilizzando AWS Directory Service console, API o CLI. Utilizza i seguenti passaggi per importare i certificati CA e successivamente abilitare l'autenticazione con smart card.

Fasi

- Abilitazione della delega vincolata Kerberos per l'account del servizio AD Connector
- Registrazione del certificato CA in AD Connector
- Abilitazione dell'autenticazione tramite smart card per AWS le applicazioni e i servizi supportati

Abilitazione della delega vincolata Kerberos per l'account del servizio AD Connector

Per utilizzare l'autenticazione con smart card con AD Connector, è necessario abilitare la delega vincolata Kerberos (KCD) per l'account del servizio AD Connector al servizio LDAP nella directory AD autogestita.

La delega vincolata Kerberos è una funzionalità di Windows Server. Questa funzionalità consente agli amministratori di specificare e far rispettare i limiti di fiducia delle applicazioni limitando l'ambito in cui i servizi applicativi possono agire per conto di un utente. Per ulteriori informazioni, consulta Delega vincolata Kerberos.

> **Note**
>
> Kerberos Constrained Delegation (KCD) richiede che la parte relativa al nome utente dell'account del servizio AD Connector corrisponda al AMAccount nome s dello stesso utente. Il AMAccount nome s è limitato a 20 caratteri. s AMAccount Name è un attributo di Microsoft Active Directory utilizzato come nome di accesso per le versioni precedenti di client e server Windows.

1. Utilizza il comando `SetSpn` per impostare un nome principale del servizio (SPN) per l'account del servizio AD Connector nell'AD autogestito. Questo permette all'account del servizio di configurare la delega.

   L'SPN può essere una qualsiasi combinazione di servizi o nomi, ma non un duplicato di un SPN esistente. I controlli `-s` per i duplicati.

   ```
   setspn -s my/spn service_account
   ```

2. In Utenti e computer AD, apri il menu contestuale (pulsante destro del mouse), seleziona l'account del servizio AD Connector e scegli Proprietà.
3. Scegli la scheda Delega.
4. Scegli le opzioni Affidati a questo utente per la delega solo al servizio specificato e Utilizza qualsiasi protocollo di autenticazione.
5. Scegli Aggiungi e poi Utenti o Computer per individuare il controller di dominio.
6. Scegli OK per visualizzare un elenco dei servizi disponibili utilizzati per la delega.
7. Scegli il tipo di servizio ldap e seleziona OK.
8. Scegli Salva per salvare la nuova configurazione.
9. Ripetere questa procedura per altri controller di dominio in Active Directory. In alternativa è possibile automatizzare il processo utilizzando. PowerShell

Registrazione del certificato CA in AD Connector

Utilizza uno dei seguenti metodi per registrare un certificato CA per la tua directory AD Connector.

Metodo 1: registrare il certificato CA in AD Connector (Console di gestione AWS)

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Autenticazione con smart card, scegli Operazioni, quindi Registra certificato.
5. Nella finestra di dialogo Registra un certificato CA, seleziona Sfoglia, poi scegli il certificato e seleziona Apri. Come opzione facoltativa, puoi scegliere di eseguire il controllo di revoca per il certificato fornendo un URL del risponditore OCSP (Online Certificate Status Protocol). Per ulteriori informazioni su OCSP, consulta Processo di verifica della revoca del certificato.
6. Scegliere Register certificate (Registra certificato). Quando lo stato del certificato passa a Registrato, il processo di registrazione è stato completato con successo.

Metodo 2: registrare il certificato CA in AD Connector (AWS CLI)

- Eseguire il seguente comando seguente. Per i dati del certificato, scegliere il percorso del file del certificato CA. Per fornire un indirizzo del risponditore OCSP secondario, utilizza l'oggetto `ClientCertAuthSettings` opzionale.

```
aws ds register-certificate --directory-id your_directory_id --certificate-
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings
 OCSPUrl=http://your_OCSP_address
```

In caso di successo, la risposta fornisce un ID certificato. Puoi anche verificare che il tuo certificato CA sia stato registrato correttamente eseguendo il seguente comando CLI:

```
aws ds list-certificates --directory-id your_directory_id
```

Se il valore dello stato restituisce `Registered`, hai registrato correttamente il certificato.

Abilitazione dell'autenticazione tramite smart card per AWS le applicazioni e i servizi supportati

Utilizza uno dei seguenti metodi per registrare un certificato CA per la tua directory AD Connector.

Metodo 1: abilitare l'autenticazione con smart card in AD Connector (Console di gestione AWS)

1. Vai alla sezione Autenticazione con smart card nella pagina Dettagli della directory e scegli Abilita. Se questa opzione non è disponibile, verificare che un certificato valido sia stato registrato e riprovare.
2. Nella finestra di dialogo Abilita l'autenticazione con smart card, seleziona Abilita.

Metodo 2: abilitare l'autenticazione con smart card in AD Connector (AWS CLI)

- Eseguire il seguente comando seguente.

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

In caso di successo, AD Connector restituisce una risposta `HTTP 200` con un corpo HTTP vuoto.

Per ulteriori informazioni sulla visualizzazione del certificato, l'annullamento della registrazione o la disabilitazione del certificato, consulta. Gestione delle impostazioni di autenticazione delle smart card

Gestione delle impostazioni di autenticazione delle smart card

Sono disponibili due metodi diversi per gestire le impostazioni delle smart card. È possibile utilizzare il Console di gestione AWS metodo o il AWS CLI metodo.

Argomenti

Visualizzare i dettagli del certificato

Utilizza uno dei seguenti metodi per vedere quando scade un certificato.

Metodo 1: per visualizzare i dettagli del certificato in Directory Service (Console di gestione AWS)

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Scegli il link ID directory per la directory AD Connector.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Autenticazione con smart card, in Certificati CA, scegli l'ID certificato per visualizzare i dettagli su quel certificato.

Metodo 2: Per visualizzare i dettagli del certificato in Directory Service (AWS CLI)

- Eseguire il seguente comando seguente. Per l'ID del certificato, utilizzare l'identificatore restituito da `register-certificate` o `list-certificates`.

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Annullare la registrazione di un certificato

Utilizza uno dei seguenti metodi per annullare la registrazione di un certificato.

> **Note**
>
> Se è registrato un solo certificato, è necessario disabilitare l'autenticazione con smart card prima di poter annullare la registrazione.

Metodo 1: annullare la registrazione di un certificato in Directory Service () Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Scegli il link ID directory per la directory AD Connector.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Autenticazione con smart card, in Certificati CA, seleziona il certificato di cui vuoi annullare la registrazione, scegli Operazioni e poi Annulla la registrazione del certificato.

   > **Important**
   >
   > Assicurati che il certificato di cui stai per annullare la registrazione non sia attivo o sia attualmente utilizzato come parte di una catena di certificati CA per l'autenticazione con smart card.

5. Nella finestra di dialogo Deregister a CA certificate (Annulla la registrazione di un certificato CA) scegliere Deregister (Annulla registrazione).

Metodo 2: annullare la registrazione di un certificato in () Directory ServiceAWS CLI

- Eseguire il seguente comando seguente. Per l'ID del certificato, utilizzare l'identificatore restituito da `register-certificate` o `list-certificates`.

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

Disattivare l'autenticazione con smart card

Utilizza uno dei seguenti metodi per disattivare l'autenticazione con smart card.

Metodo 1: disabilitare l'autenticazione tramite smart card in Directory Service () Console di gestione AWS

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Scegli il link ID directory per la directory AD Connector.
3. Nella pagina Directory details (Dettagli della directory) selezionare la scheda Networking & security (Reti e sicurezza).
4. Nella sezione Autenticazione con smart card, scegli Disabilita.
5. Nella finestra di dialogo Disabilita autenticazione con smart card, scegli Disabilita.

Metodo 2: per disabilitare l'autenticazione tramite smart card in Directory Service (AWS CLI)

- Eseguire il seguente comando seguente.

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Aggiornamento delle credenziali dell'account del servizio AD Connector in Console di gestione AWS

Le credenziali AD Connector fornite Directory Service rappresentano l'account di servizio utilizzato per accedere alla directory locale esistente. È possibile modificare le credenziali dell'account di servizio Directory Service eseguendo le seguenti operazioni.

> **Note**
>
> Se AWS IAM Identity Center è abilitato per la directory, Directory Service deve trasferire il nome principale del servizio (SPN) dall'account di servizio corrente al nuovo account di servizio. Se l'account del servizio non dispone dell'autorizzazione per eliminare l'SPN, oppure il nuovo account del servizio non dispone dell'autorizzazione per aggiungere un SPN, ti verranno richieste le credenziali di un account di directory che dispone dell'autorizzazione per eseguire entrambe le operazioni. Queste credenziali vengono utilizzate solo per trasferire l'SPN e non vengono archiviate dal servizio.

Per aggiornare le credenziali dell'account del servizio AD Connector in Directory Service

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory.
3. Nella pagina Dettagli della directory, scorri verso il basso fino alla sezione Credenziali dell'account del servizio.
4. Nella sezione Credenziali account del servizio scegliere Aggiorna.
5. Nella finestra di dialogo Aggiorna le credenziali dell'account del servizio, digita il nome utente e la password dell'account del servizio. Inserisci nuovamente la password per confermarla, quindi seleziona Aggiorna.

Configurare AWS Private CA Connector for AD

Puoi integrare la tua Active Directory autogestita con AWS Autorità di certificazione privata l'utilizzo di AD Connector per emettere e gestire certificati per utenti, gruppi e computer aggiunti al dominio AD. AWS Private CA Connector for AD fornisce una soluzione completamente gestita AWS Private CA che sostituisce direttamente l'azienda autogestita CAs senza che sia necessario distribuire, applicare patch o aggiornare agenti locali o server proxy.

Puoi configurare questa integrazione tramite la Directory Service console, la console AWS Private CA Connector for AD o chiamando l'API. `CreateTemplate` Per utilizzare la console AWS Private CA Connector for Active Directory, vedi AWS Private CA Connettore per Active Directory. Le sezioni seguenti descrivono come configurare questa integrazione dalla Directory Service console.

Prerequisiti

Per le istruzioni di configurazione, consulta Configurare Connector for AD nella Guida per l'utente di AWS Private CA Connector for AD.

Configurazione di AWS Private CA Connector for AD

Per creare un connettore CA privato per Active Directory

1. Accedi a Console di gestione AWS e apri la Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.

3. Nella scheda Gestione delle AWS applicazioni e nella sezione App e servizi, scegli AWS Private CA Connector for AD.
4. Nella pagina Crea certificato CA privato per Active Directory, completa i passaggi per creare il connettore CA privata per Active Directory.

Per ulteriori informazioni, consulta Creazione di un connettore.

Visualizza il tuo AWS Private CA Connector for AD

Per visualizzare i dettagli del connettore CA privato

1. Accedi a Console di gestione AWS e apri la Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella scheda Gestione delle AWS applicazioni e nella sezione app e servizi, visualizza i connettori CA privati e la CA privata associata. Vengono visualizzati i seguenti campi:
   a. AWS Private CA ID connettore: l'identificatore univoco di un AWS Private CA connettore. Sceglilo per visualizzare la pagina dei dettagli.
   b. AWS Private CA oggetto: informazioni relative al nome distinto della CA. Sceglilo per visualizzare la pagina dei dettagli.
   c. Status: risultati del controllo dello stato del AWS Private CA Connector e AWS Private CA:
      - Attivo: entrambi i controlli vengono superati
      - 1/2 controlli non riusciti: un controllo fallisce
      - Fallito: entrambi i controlli hanno esito negativo

      Per informazioni sullo stato dell'operazione non riuscita, passa il mouse sul collegamento ipertestuale per vedere quale controllo non è riuscito.
   d. Stato di registrazione dei certificati DC: verifica dello stato dello stato del certificato del controller di dominio:
      - Abilitato: la registrazione dei certificati è abilitata
      - Disabilitata: la registrazione dei certificati è disabilitata
   e. Data di creazione: quando è stato creato il AWS Private CA connettore.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli del connettore.

Verifica l'emissione del certificato agli utenti AD

Completa i seguenti passaggi per confermare che AWS Private CA stai emettendo certificati per il tuo Active Directory autogestito:

- Riavvia i controller di dominio locali.
- Visualizza i tuoi certificati con. Microsoft Management Console Per ulteriori informazioni, consulta Microsoftla documentazione.

Monitoraggio della directory AD Connector

Puoi ottenere il massimo dal tuo AD Connector scoprendo di più sui diversi stati di AD Connector e sul loro significato per il tuo AD Connector. Puoi anche utilizzare Amazon Simple Notification Service per ricevere notifiche sullo stato del tuo AD Connector.

Attività per monitorare il tuo AD Connector:

- Comprendere lo stato della directory
- Abilitazione delle notifiche sullo stato della directory AD Connector con Amazon SNS

Comprendere lo stato della directory

Di seguito sono elencati i diversi stati per una directory.

Active (Attivo)

La directory funziona normalmente. Nessun problema è stato rilevato da Directory Service per la directory.

Creating (Creazione in corso)

La directory è attualmente in fase di creazione. Solitamente la creazione di una directory può richiedere da 20 a 45 minuti, ma può variare in base al carico di sistema.

Deleted (Eliminato)

La directory è stata eliminata. Tutte le risorse per la directory sono state rilasciate. Una volta che una directory entra in questo stato, non può essere ripristinata.

Deleting (Eliminazione in corso)

La directory è attualmente in fase di eliminazione. La directory rimarrà in questo stato finché non sarà completamente eliminata. Una volta che una directory entra in questo stato, l'operazione di eliminazione non può essere annullata e la directory non può essere ripristinata.

Failed (Non riuscito)

Impossibile creare la directory. Elimina questa directory. Se questo problema persiste, contatta il Centro Supporto AWS.

Impaired (Insufficiente)

La directory è in esecuzione in uno stato danneggiato. Uno o più problemi sono stati rilevati e non tutte le operazioni di directory potrebbero lavorare alla massima capacità operativa. Ci sono molti motivi per cui la directory può trovarsi in questo stato. Questi includono le normali attività di manutenzione operativa, ad esempio l'applicazione di patch o la rotazione delle EC2 istanze, l'hot spot temporaneo da parte di un'applicazione su uno dei controller di dominio o le modifiche apportate alla rete che interrompono inavvertitamente le comunicazioni tra gli elenchi. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi AWS a Managed Microsoft AD, Risoluzione dei problemi di AD Connector, Risoluzione dei problemi di Simple AD. Per i normali problemi relativi alla manutenzione, AWS risolve questi problemi entro 40 minuti. Se dopo aver esaminato l'argomento di risoluzione dei problemi, la directory è in stato Danneggiato per più di 40 minuti, consigliamo di contattare il Centro Supporto AWS.

> **Important**
>
> Non ripristinare uno snapshot mentre la directory è in stato danneggiato. Raramente è necessario ripristinare uno snapshot per risolvere dei danni. Per ulteriori informazioni, consulta Ripristino di AWS Managed Microsoft AD con istantanee.

Inoperable (Inutilizzabile)

La directory non è funzionale. Sono stati segnalati problemi per tutti gli endpoint della directory.

Requested (Richiesta)

Una richiesta di creazione della directory è attualmente in sospeso.

Abilitazione delle notifiche sullo stato della directory AD Connector con Amazon SNS

Tramite Amazon Simple Notification Service (Amazon SNS), puoi ricevere messaggi e-mail o di testo (SMS) quando lo stato della directory cambia. Ricevi una notifica se la directory passa da uno stato Attivo a uno stato Danneggiato o Inutilizzabile. Puoi anche ricevere una notifica quando la directory torna a uno stato Active (Attivo).

Come funziona

Amazon SNS utilizza "argomenti" per raccogliere e distribuire i messaggi. Ogni argomento ha uno o più abbonati che ricevono i messaggi che sono stati pubblicati su quell'argomento. Utilizzando i passaggi seguenti puoi aggiungere Directory Service come editore a un argomento di Amazon SNS. Quando Directory Service rileva una modifica nello stato della tua directory, pubblica un messaggio su quell'argomento, che viene quindi inviato ai sottoscrittori dell'argomento.

Puoi associare più directory come editori a un singolo argomento. Puoi anche aggiungere messaggi di stato della directory agli argomenti che hai precedentemente creato in Amazon SNS. Hai un controllo dettagliato su chi può pubblicare ed effettuare la sottoscrizione a un argomento. Per informazioni complete su Amazon SNS, consulta Cos'è Amazon SNS?.

Per abilitare la messaggistica SNS per la directory

1. Accedi a Console di gestione AWS e apri la console. Directory Service
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Seleziona la scheda Manutenzione.
4. Nella sezione Monitoraggio della directory, scegli Azioni, quindi seleziona Crea notifica.
5. Nella pagina Crea notifica, seleziona Scegli un tipo di notifica, quindi scegli Crea una nuova notifica. In alternativa, se disponi già di un argomento SNS, puoi scegliere Associa ad argomento SNS esistente per l'invio di messaggi di stato da questa directory a tale argomento.

> **Note**
>
> Se scegli Crea una nuova notifica, ma utilizzerai lo stesso nome dell'argomento per un argomento SNS già esistente, Amazon SNS non crea un nuovo argomento, ma aggiunge semplicemente le nuove informazioni di abbonamento a quello esistente.

Se scegli Associa ad argomento SNS esistente, potrai solo scegliere un argomento SNS presente nella stessa regione della directory.

6. Scegli il Tipo di destinatario e inserisci le informazioni di contatto del Destinatario. Se inserisci un numero di telefono per SMS, utilizza solo numeri. Non includere trattini, spazi o parentesi.
7. (Facoltativo) Fornisci un nome per l'argomento SNS e un relativo nome visualizzato. Il nome visualizzato è un nome breve di massimo 10 caratteri incluso in tutti i messaggi SMS di questo argomento. Quando utilizzi l'opzione SMS, il nome visualizzato è obbligatorio.

> **Note**
>
> Se hai effettuato l'accesso utilizzando un utente o un ruolo IAM con solo la policy DirectoryServiceFullAccessgestita, il nome dell'argomento deve iniziare con «DirectoryMonitoring». Se desideri personalizzare ulteriormente il nome dell'argomento, avrai bisogno di ulteriori privilegi per SNS.

8. Scegli Create (Crea).

Se desideri designare abbonati SNS aggiuntivi, ad esempio un indirizzo e-mail aggiuntivo, code Amazon SQS oppureAWS Lambda, puoi farlo dalla console Amazon SNS.

Per rimuovere i messaggi di stato della directory da un argomento

1. Accedi e apri la console. Console di gestione AWSDirectory Service
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Seleziona la scheda Manutenzione.
4. Nella sezione Monitoraggio delle directory, seleziona il nome di un argomento SNS nell'elenco, scegli Operazioni, quindi seleziona Rimuovi.
5. Scegli Rimuovi.

Questa operazione rimuove la directory come editore per l'argomento SNS selezionato. Se desideri eliminare l'intero argomento, puoi farlo dalla console Amazon SNS.

> **Note**
>
> Prima di eliminare un argomento Amazon SNS tramite la console di SNS, devi accertarti che una directory non stia inviando messaggi di stato a tale argomento.

Se elimini un argomento Amazon SNS tramite la console di SNS, questa modifica non si rifletterà immediatamente nella console Servizio di directory. Riceverai una notifica solo la prossima volta che una directory pubblica una notifica all'argomento eliminato, nel qual caso visualizzerai uno stato aggiornato nella scheda Monitoring (Monitoraggio) della directory che indica che l'argomento non è stato trovato.
Pertanto, per evitare di perdere importanti messaggi sullo stato della directory, prima di eliminare qualsiasi argomento da cui vengono ricevuti messaggiDirectory Service, associa la directory a un argomento Amazon SNS diverso.

Accesso ad AWS applicazioni e servizi da AD Connector

Puoi consentire ad AD Connector di accedere ad AWS applicazioni e servizi per l'Active Directory connessa. Alcune delle AWS applicazioni e dei servizi supportati includono:

- Amazon Chime
- Amazon WorkSpaces
- Centro identità IAM
- Console di gestione AWS

Non esistono applicazioni di terze parti che funzionano con AD Connector.

Attività per accedere ad AWS applicazioni e servizi da AD Connector

- Policy di compatibilità delle applicazioni per AD connector
- Consentire l'accesso ad AWS applicazioni e servizi da AD Connector

Policy di compatibilità delle applicazioni per AD connector

In alternativa a AWS Directory Service for Microsoft Active Directory (AWSMicrosoft AD gestito), AD Connector è un proxy Active Directory solo per applicazioni e servizi AWS creati. Puoi configurare il proxy per l'uso di un dominio Active Directory specificato. Quando l'applicazione deve cercare un utente o un gruppo in Active Directory, AD Connector trasmette la richiesta alla directory. Analogamente, quando un utente accede all'applicazione, AD Connector trasmette la richiesta di autenticazione alla directory. Non esistono applicazioni di terze parti che funzionano con AD Connector.

Di seguito è riportato un elenco di AWS applicazioni e servizi compatibili:

- Amazon Chime: per istruzioni dettagliate, consulta Connessione ad Active Directory.
- Amazon Connect: per ulteriori informazioni, consulta Come funziona Amazon Connect.
- Amazon EC2 per Windows o Linux: puoi utilizzare la semplice funzionalità di aggiunta al dominio Active Directory di Amazon EC2 Windows o Linux per aggiungere la tua istanza alla tua Active Directory autogestita (locale). Una volta completata l'unione, l'istanza comunica direttamente con l'Active Directory e ignora AD Connector. Per ulteriori informazioni, consulta Modi per aggiungere un' EC2 istanza Amazon alla tua Active Directory.
- Console di gestione AWS — Puoi utilizzare AD Connector per autenticare Console di gestione AWS gli utenti con le loro credenziali di Active Directory senza configurare l'infrastruttura SAML. Per ulteriori informazioni, consulta Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite.
- Quick Suite - Per ulteriori informazioni, consulta Gestione degli account utente in Quick Suite Enterprise Edition.
- AWS IAM Identity Center - Per istruzioni dettagliate, consulta Connect IAM Identity Center a un Active Directory locale.
- AWS Transfer Family - Per istruzioni dettagliate, vedere Lavorare con Directory Service Microsoft Active Directory.
- AWS Client VPN: per istruzioni dettagliate, consulta Autenticazione e autorizzazione del client.
- WorkDocs - Per istruzioni dettagliate, consulta Connessione alla directory locale con AD Connector.
- Amazon WorkMail : per istruzioni dettagliate, consulta Integrare Amazon WorkMail con una directory esistente (configurazione standard).
- WorkSpaces - Per istruzioni dettagliate, consulta Avviare un ad Connector WorkSpace utilizzando AD Connector.

> **Note**
>
> Amazon RDS è compatibile solo con AWS Managed Microsoft AD e non è compatibile con AD Connector. Per ulteriori informazioni, consulta la sezione AWS Managed Microsoft AD della Directory Service FAQspagina.

Consentire l'accesso ad AWS applicazioni e servizi da AD Connector

Gli utenti possono autorizzare AD Connector a fornire ad AWS applicazioni e servizi, come Amazon WorkSpaces, l'accesso al tuo Active Directory. Le seguenti AWS applicazioni e servizi possono essere abilitati o disabilitati per funzionare con AD Connector.

AWS applicazione/servizio	Ulteriori informazioni…
Amazon Chime	Per ulteriori informazioni, vedere Connessione ad Active Directory.
Amazon Connect	Per ulteriori informazioni, consulta la Guida all'amministrazione di Amazon Connect.
Amazon WorkDocs	Per ulteriori informazioni, consulta la Guida introduttiva ad Amazon WorkDocs.
Amazon WorkMail	Per ulteriori informazioni, consulta la sezione Creazione di un'organizzazione.
Amazon WorkSpaces	Puoi creare un Simple AD, AWS Managed Microsoft AD o AD Connector direttamente da WorkSpaces. È sufficiente avviare Advanced Setup (Impostazioni avanzate) durante la creazione del Workspace. Per ulteriori informazioni, consulta la Amazon WorkSpaces Administration Guide.
AWS Client VPN	Per ulteriori informazioni, consulta la AWS Client VPN Guida per l'utente di .
AWS IAM Identity Center	Per ulteriori informazioni, consulta la AWS IAM Identity Center Guida per l'utente di .
Console di gestione AWS	Per ulteriori informazioni, consulta Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite.

AWS applicazione/servizio	Ulteriori informazioni…
AWS Transfer Family	Per ulteriori informazioni, consulta la AWS Transfer Family Guida per l'utente di .

Una volta abilitato, puoi gestire l'accesso alle directory nella console dell'applicazione o del servizio a cui intendi consentire l'accesso alla directory. Per trovare i link AWS alle applicazioni e ai servizi sopra descritti nella Directory Service console, procedi nel seguente modo.

Visualizzazione dei servizi e applicazioni di una directory

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Consulta l'elenco nella sezione app e servizi AWS .

Per ulteriori informazioni su come autorizzare o rimuovere l'autorizzazione all'utilizzo Directory Service di AWS applicazioni e servizi, vedere. Autorizzazione per l'AWSutilizzo di applicazioni e servizi Directory Service

Modi per aggiungere un' EC2 istanza Amazon alla tua Active Directory

AD Connector è un gateway di directory con cui è possibile reindirizzare le richieste di directory all'MicrosoftActive Directory locale senza memorizzare nella cache alcuna informazione nel cloud. Ecco ulteriori informazioni su come aggiungere un Amazon EC2 a un dominio Active Directory:

- Puoi aggiungere senza problemi un' EC2 istanza Amazon al tuo dominio Active Directory all'avvio dell'istanza. Per ulteriori informazioni sull'aggiunta di un'istanza di EC2 Windows a un AWS Managed Microsoft AD, vedereUnire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory.
- Se è necessario aggiungere manualmente un' EC2 istanza al dominio Active Directory, è necessario avviare l'istanza nel gruppo o nella sottorete appropriata Regione AWS e di sicurezza, quindi aggiungere l'istanza al dominio Active Directory.

- Per essere in grado di connettersi in remoto a queste istanze, è necessario disporre di connettività IP per le istanze dalla rete da cui ti connetti. Nella maggior parte dei casi, questo richiede che un gateway Internet sia associato ad Amazon VPC e che l'istanza disponga di un indirizzo IP pubblico. Per ulteriori informazioni sulla connessione a Internet utilizzando un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.

> **Note**
>
> Una volta aggiunta a un'istanza ad Active Directory autogestito (on-premise), l'istanza comunica direttamente con Active Directory e ignora AD Connector.

Quote di AD Connector

Di seguito sono elencate le quote predefinite per AD Connector. Salvo ove diversamente specificato, ogni quota si applica a una regione.

Quote di AD Connector

Risorsa	Quota predefinita
Directory AD Connector	10
Numero massimo di certificati emessi da una CA registrati per directory	5

Risoluzione dei problemi di AD Connector

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potresti riscontrare durante la creazione o l'utilizzo di AD Connector.

Argomenti

- Problemi di creazione
- Problemi di connettività
- Problemi di autenticazione
- Problemi di manutenzione

- Non riesco a eliminare il mio AD Connector
- Strumenti generali per l'analisi degli emittenti di AD Connector

Problemi di creazione

Di seguito sono riportati i problemi di creazione più comuni per AD Connector

- Visualizzo un messaggi odi errore "AZ Constrained" (AZ vincolata) quando creo una directory
- Ricevo l'errore «Rilevati problemi di connettività» quando tento di creare AD Connector

Visualizzo un messaggi odi errore "AZ Constrained" (AZ vincolata) quando creo una directory

Alcuni AWS account creati prima del 2012 potrebbero avere accesso alle zone di disponibilità nelle regioni Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale) o Asia Pacifico (Tokyo) che non supportano Directory Service le directory. Se ricevi un errore come questo durante la creazione di Active Directory, scegli una sottorete in una zona di disponibilità diversa e prova a creare nuovamente la directory.

Ricevo l'errore «Rilevati problemi di connettività» quando tento di creare AD Connector

Se ricevi l'errore «Rilevato problema di connettività» durante il tentativo di creare un connettore AD, l'errore potrebbe essere dovuto alla disponibilità delle porte o alla complessità della password di AD Connector. Puoi testare la connessione del tuo AD Connector per vedere se sono disponibili le seguenti porte:

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Per testare la connessione, consultaTest di un AD Connector. Il test di connessione deve essere eseguito sull'istanza unita a entrambe le sottoreti a cui sono associati gli indirizzi IP del connettore AD.

Se il test di connessione ha esito positivo e l'istanza si unisce al dominio, controlla la password di AD Connector. AD Connector deve soddisfare i requisiti di complessità delle AWS password. Per ulteriori informazioni, consulta Account di servizio inPrerequisiti di AD Connector.

Se il tuo AD Connector non soddisfa questi requisiti, ricrea il tuo AD Connector con una password conforme a questi requisiti.

Ricevo il messaggio «È stato riscontrato un errore interno del servizio durante la connessione della directory. Riprova l'operazione». errore durante la creazione di un AD Connector

Questo errore si verifica in genere quando AD Connector non riesce a creare e non riesce a connettersi a un controller di dominio valido per il dominio Active Directory autogestito.

> **Note**
>
> Come procedura consigliata, se nella rete autogestita sono stati definiti Active Directory Sites, è necessario verificare quanto segue:
>
> - Le sottoreti VPC in cui risiede l'AD Connector sono definite in un sito di Active Directory.
> - Non esistono conflitti tra le sottoreti VPC e le sottoreti degli altri siti.

AD Connector utilizza il sito di Active Directory i cui intervalli di indirizzi IP di sottorete sono vicini a quelli del VPC che contiene AD Connector per individuare i controller di dominio AD. Se hai un sito le cui sottoreti hanno gli stessi intervalli di indirizzi IP di quelli del tuo VPC, AD Connector individuerà i controller di dominio in quel sito. Il controller di dominio potrebbe non essere fisicamente vicino alla regione in cui risiede il tuo AD Connector.

- Incoerenze nei record DNS SRV (questi record utilizzano la seguente sintassi: `_ldap._tcp.<DnsDomainName>` e `_kerberos._tcp.<DnsDomainName>`) creati nel dominio Active Directory gestito dal cliente. Ciò può verificarsi quando AD Connector non riesce a trovare e connettersi a un controller di dominio valido basato su questi record SRV.
- Problemi di rete tra AD Connector e AD gestito dal cliente, come i dispositivi firewall.

È possibile utilizzare l'acquisizione di pacchetti di rete sui controller di dominio, sui server DNS e sui log di flusso VPC delle interfacce di rete delle directory per esaminare questo problema. Contatta per ulteriore assistenza. Supporto AWS

Problemi di connettività

Di seguito sono riportati i problemi di connettività più comuni per AD Connector

- Ricevo un messaggio di errore "Connectivity issues detected" (Problemi di connettività rilevati) quando cerco di connettermi alla mia directory in locale
- Ricevo un messaggio di errore "DNS unavailable" (DNS non disponibile) quando cerco di connettermi alla mia directory in locale
- Ricevo un messaggio di errore "SRV record" (record SRV) quando cerco di connettermi alla mia directory in locale

Ricevo un messaggio di errore "Connectivity issues detected" (Problemi di connettività rilevati) quando cerco di connettermi alla mia directory in locale

Quando ti connetti alla tua directory locale, ricevi un messaggio di errore simile al seguente: Problemi di connettività rilevati: LDAP non disponibile (porta TCP 389) per IP: *<IP address>* Kerberos/ authentication non disponibile (porta TCP 88) per IP: *<IP address>* Verifica che le porte elencate siano disponibili e riprova l'operazione.

AD Connector deve essere in grado di comunicare con i controller dei domini on-premise tramite TCP e UDP attraverso le seguenti porte. Verifica che i gruppi di sicurezza e i firewall in locale permettano la comunicazione TCP e UDP su queste porte. Per ulteriori informazioni, consulta Prerequisiti di AD Connector.

- 88 (Kerberos)
- 389 (LDAP)

Potrebbero essere necessarie porte aggiuntive TCP/UDP a seconda delle esigenze. Consulta l'elenco seguente per alcune di queste porte. Per ulteriori informazioni sulle porte utilizzate da Active Directory, vedi Come configurare un firewall per i domini e i trust di Active Directory nella Microsoft documentazione.

- 135 (RPC Endpoint Mapper)
- 646 (SSL LDAP)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

Ricevo un messaggio di errore "DNS unavailable" (DNS non disponibile) quando cerco di connettermi alla mia directory in locale

Ricevi un messaggio di errore simile al seguente quando ti connetti alla tua directory in locale:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector deve essere in grado di comunicare con i tuoi server DNS on-premise tramite TCP e UDP attraverso la porta 53. Verifica che i gruppi di sicurezza e i firewall in locale permettano la comunicazione TCP e UDP su questa porta. Per ulteriori informazioni, consulta Prerequisiti di AD Connector.

Ricevo un messaggio di errore "SRV record" (record SRV) quando cerco di connettermi alla mia directory in locale

Ricevi un messaggio di errore simile a uno o più dei seguenti quando ti connetti alla tua directory in locale:

```
SRV record for LDAP does not exist for IP: <DNS IP address> SRV record for Kerberos
 does not exist for IP: <DNS IP address>
```

AD Connector deve ottenere i record SRV `_ldap._tcp.<DnsDomainName>` e `_kerberos._tcp.<DnsDomainName>` quando si connette alla tua directory. Riceverai questo messaggio di errore se il servizio non è in grado di ottenere questi record dai server DNS che hai specificato al momento della connessione alla tua directory. Per ulteriori informazioni su questi record SRV, consulta SRV record requirements.

Problemi di autenticazione

Ecco alcuni problemi di autenticazione comuni con AD Connector:

- Ricevo il messaggio di errore «Convalida del certificato non riuscita» quando tento di accedere Amazon WorkSpaces con una smart card
- Ricevo un messaggio errore "Credenziali non valide" quando l'account del servizio utilizzato da AD Connector cerca di eseguire l'autenticazione
- Ricevo un errore «Impossibile autenticare» quando utilizzo AWS le applicazioni per cercare utenti o gruppi

- Ricevo un errore relativo alle mie credenziali di directory quando tento di aggiornare l'account del servizio AD Connector
- Alcuni dei miei utenti non possono eseguire l'autenticazione con la mia directory

Ricevo il messaggio di errore «Convalida del certificato non riuscita» quando tento di accedere Amazon WorkSpaces con una smart card

Quando si tenta di accedere WorkSpaces con una smart card, viene visualizzato un messaggio di errore simile al seguente: ERRORE: Convalida del certificato non riuscita. Riprova riavviando il browser o l'applicazione e assicurati di selezionare il certificato corretto. L'errore si verifica se il certificato della smart card non è archiviato correttamente nel client che utilizza i certificati. Per ulteriori informazioni sui requisiti di AD Connector e smart card, consultaPrerequisiti.

Utilizzare le seguenti procedure per risolvere i problemi relativi alla capacità della smart card di memorizzare i certificati nell'archivio certificati dell'utente:

1. Sul dispositivo che presenta problemi di accesso ai certificati, accedi a Microsoft Management Console (MMC).

   > **Important**
   >
   > Prima di procedere, crea una copia del certificato della smart card.

2. Accedere all'archivio dei certificati nella MMC. Eliminare il certificato smart card dell'utente dall'archivio certificati. Per ulteriori informazioni sulla visualizzazione dell'archivio certificati nella MMC, vedere Procedura: Visualizzazione dei certificati con lo snap-in MMC nella documentazione. Microsoft
3. Rimuovere la smart card.
4. Reinserire la smart card in modo che possa ripopolare il certificato della smart card nell'archivio certificati dell'utente.

   > **Warning**
   >
   > Se la smart card non ripopola il certificato nell'archivio utenti, non può essere utilizzata per l'autenticazione tramite smart card. WorkSpaces

L'account di servizio di AD Connector deve avere quanto segue:

- `my/spn`aggiunto al nome principale del servizio
- Delegato per il servizio LDAP

Dopo aver ripopolato il certificato sulla smart card, è necessario controllare il controller di dominio locale per determinare se è bloccato dalla mappatura UPN (User Principal Name) per Subject Alternative Name. Per ulteriori informazioni su questa modifica, vedi Come disabilitare la mappatura Subject Alternative Name for UPN nella documentazione. Microsoft

Utilizza la seguente procedura per controllare la chiave di registro del controller di dominio:

- Nell'editor del registro, accedi alla seguente chiave hive

  HKEY_LOCAL_MACHINE\ SYSTEM\\ Services\ Kdc\ CurrentControlSet UseSubjectAltName

  - Ispeziona UseSubjectAltName il valore di:

    i. Se il valore è impostato su 0, la mappatura del nome alternativo del soggetto è disabilitata ed è necessario mappare esplicitamente un determinato certificato a un solo utente. Se un certificato è mappato a più utenti e questo valore è 0, l'accesso con quel certificato avrà esito negativo.

    ii. Se il valore non è impostato o impostato su 1, è necessario mappare esplicitamente un determinato certificato a un solo utente o utilizzare il campo Subject Alternative Name per l'accesso.

    A. Se il campo Subject Alternative Name esiste nel certificato, gli verrà assegnata la priorità.

    B. Se il campo Subject Alternative Name non esiste nel certificato e il certificato è mappato in modo esplicito a più di un utente, l'accesso con quel certificato avrà esito negativo.

> **Note**
>
> Se la chiave di registro è impostata sui controller di dominio locali, AD Connector non sarà in grado di localizzare gli utenti in Active Directory e genererà il messaggio di errore sopra riportato.

I certificati Certificate Authority (CA) devono essere caricati nel certificato smart card AD Connector. Il certificato deve contenere informazioni OCSP. Di seguito sono elencati i requisiti aggiuntivi per la CA:

- Il certificato deve trovarsi nella Trusted Root Authority del controller di dominio, nel server dell'autorità di certificazione e nel WorkSpaces.
- I certificati CA offline e root non conterranno le informazioni OSCP. Questi certificati contengono informazioni sulla loro revoca.
- Se si utilizza un certificato CA di terze parti per l'autenticazione con smart card, è necessario pubblicare la CA e i certificati intermedi nell'archivio di Active Directory NTAuth . Devono essere installati nell'autorità principale attendibile per tutti i controller di dominio, i server delle autorità di certificazione e. WorkSpaces
  - È possibile utilizzare il comando seguente per pubblicare certificati nell' NTAuth archivio di Active Directory:

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

Per ulteriori informazioni sulla pubblicazione dei certificati nello NTAuth store, consulta Importazione del certificato CA emittente nell'Enterprise NTAuth store nella Guida all'installazione di Access Amazon WorkSpaces with Common Access Cards.

Puoi verificare se il certificato utente o i certificati della catena CA sono verificati da OCSP seguendo questa procedura:

1. Esporta il certificato della smart card in una posizione sul computer locale come l'unità C:.
2. Aprire un prompt della riga di comando e accedere alla posizione in cui è archiviato il certificato smart card esportato.
3. Immetti il comando seguente:

```
certutil -URL Certficate_name.cer
```

4. Dopo il comando dovrebbe apparire una finestra pop-up. Seleziona l'opzione OCSP nell'angolo destro e seleziona Recupera. Lo stato dovrebbe tornare come verificato.

Per ulteriori informazioni sul comando certutil, vedere certutil nella documentazione Microsoft

Ricevo un messaggio errore "Credenziali non valide" quando l'account del servizio utilizzato da AD Connector cerca di eseguire l'autenticazione

Questo può verificarsi se il disco rigido sul tuo controller dei domini esaurisce lo spazio. Verifica che i dischi rigidi del tuo controller dei domini non siano pieni.

Ricevo «Si è verificato un errore» o «Un errore imprevisto» quando tento di aggiornare l'account del servizio AD Connector

I seguenti errori o sintomi si verificano durante la ricerca di utenti in applicazioni AWS aziendali come Amazon WorkSpaces Console Launch Wizard:

- Si è verificato un errore. Se continui a riscontrare un problema, contatta il Supporto AWS Team sui forum della community e tramite AWS Premium Support.
- Si è verificato un errore. La tua directory necessita di un aggiornamento delle credenziali. Aggiorna le credenziali della directory.

Se tenti di aggiornare le credenziali dell'account del servizio AD Connector in AD Connector, potresti ricevere i seguenti messaggi di errore:

- Errore imprevisto. Si è verificato un errore imprevisto.
- Si è verificato un errore. Si è verificato un errore nella account/password combinazione di servizi. Per favore riprova.

L'account di servizio della directory AD Connector risiede nell'Active Directory gestito dal cliente. L'account viene utilizzato come identità per eseguire query e operazioni sul dominio Active Directory gestito dal cliente tramite AD Connector per conto di AWS Enterprise Applications. AD Connector utilizza Kerberos e LDAP per eseguire queste operazioni.

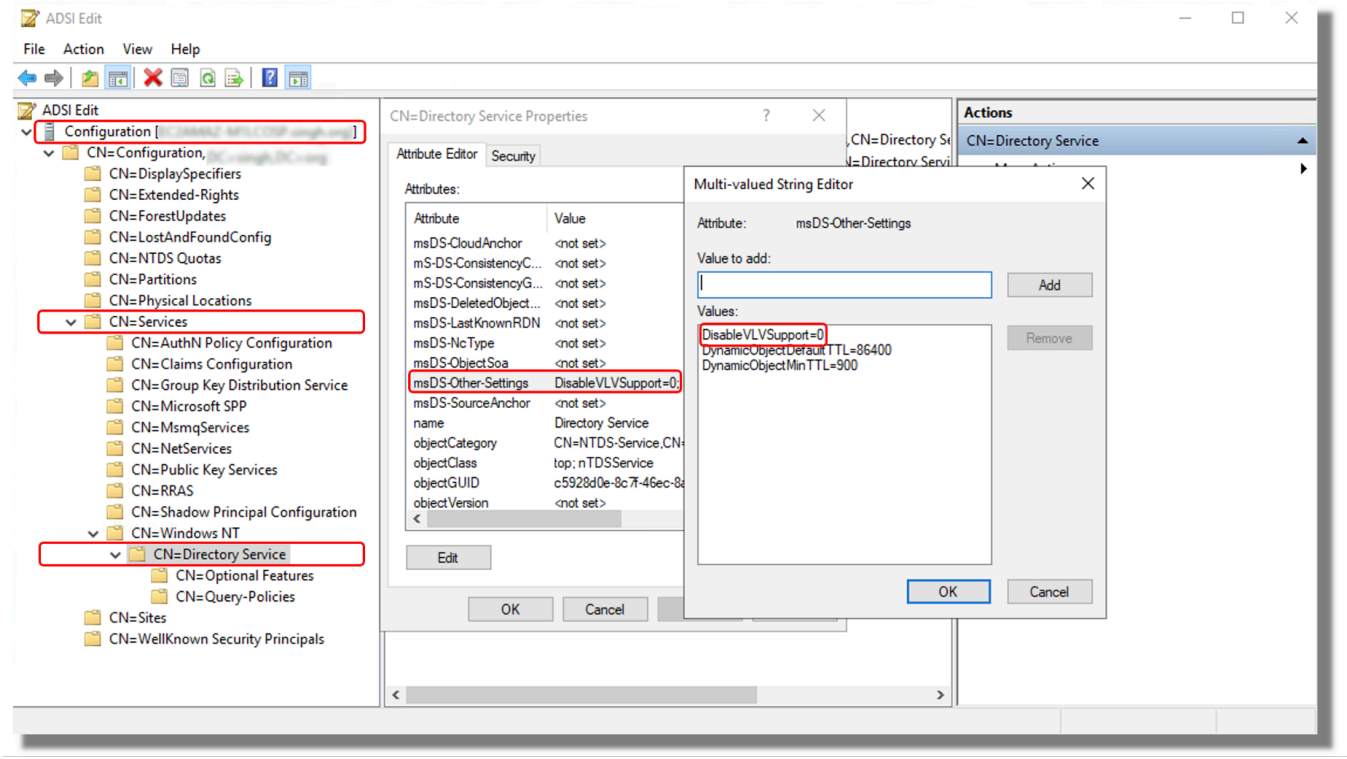
L'elenco seguente spiega il significato di questi messaggi di errore:

- Potrebbe esserci un problema con la sincronizzazione dell'ora e Kerberos. AD Connector invia le richieste di autenticazione Kerberos ad Active Directory. Queste richieste richiedono un intervallo di tempo limitato e, se vengono ritardate, avranno esito negativo. Assicurati che non vi siano problemi di sincronizzazione temporale tra i controller di dominio gestiti dal cliente. Per risolvere questo problema, consulta la sezione Raccomandazione: configurare il Root PDC con un'origine temporale autorevole ed evitare una distorsione temporale diffusa nella documentazione. Microsoft Per ulteriori informazioni sul servizio orario e sulla sincronizzazione, consulta quanto segue:

  - Come funziona il servizio Windows Time
  - Tolleranza massima per la sincronizzazione dell'orologio del computer
  - WindowsStrumenti e impostazioni del servizio orario
- Un dispositivo di rete intermedio, con una restrizione MTU di rete, come configurazioni hardware Firewall o VPN, tra AD Connector e controller di dominio gestiti dal cliente, può causare questo errore a causa della frammentazione della rete.
  - Per verificare la restrizione MTU, puoi eseguire un test Ping tra il controller di dominio gestito dal cliente e un' EC2 istanza Amazon lanciata in una delle tue sottoreti di directory connessa tramite AD Connector. La dimensione del frame non deve essere superiore alla dimensione predefinita di 1500 byte
  - Il test ping ti aiuterà a capire se la dimensione del frame è superiore a 1500 byte (noti anche come frame Jumbo) e se sono in grado di raggiungere il VPC e la sottorete AD Connector senza bisogno di frammentazione. Verifica ulteriormente con il team di rete e assicurati che i frame Jumbo siano consentiti sui dispositivi di rete intermedi.
- Potresti riscontrare questo problema se LDAPS lato client è abilitato su AD Connector e i certificati sono scaduti. Assicurati che sia il certificato lato server che il certificato CA siano validi, non scaduti e soddisfino i requisiti indicati nella documentazione. LDAPs
- Se il supporto Virtual List View Support è disabilitato nel dominio Active Directory gestito dal cliente, AWS le applicazioni non saranno in grado di cercare gli utenti perché AD Connector utilizza la ricerca VLV nelle query LDAP. Virtual List View Support è disabilitato quando Disable VLVSupport è impostato su un valore diverso da zero. Assicurati che il supporto Virtual List View (VLV) sia abilitato in Active Directory utilizzando i seguenti passaggi:

  1. Accedi al controller di dominio come proprietario del ruolo principale dello schema utilizzando un account con credenziali di amministratore dello schema.
  2. Seleziona Start, quindi Esegui, quindi inserisci**`Adsiedit.msc`**.
  3. Nello strumento ADSI Edit, fate clic su Connect to Configuration Partition ed espandete il nodo Configuration [DomainController].
  4. Espandi il contenitore CN=Configuration, DC=. DomainName
  5. Espandi l'oggetto CN=Services.
  6. Espandere l'oggetto CN=Windows NT.
  7. Seleziona l'oggetto CN=Directory Service. Seleziona Proprietà.
  8. Nell'elenco Attributi, selezionare msDS-Other-Settings. Seleziona Edit (Modifica).

9. Nell'elenco Valori, seleziona qualsiasi istanza di Disable VLVSupport =x in cui x non è uguale a 0 e seleziona Rimuovi.
10. Dopo la rimozione, inserisci**`DisableVLVSupport=0`**. Selezionare Aggiungi.
11. Seleziona OK. È possibile chiudere lo strumento ADSI Edit. L'immagine seguente mostra la finestra di dialogo Multivalore di stringhe nella finestra ADSI Edit:



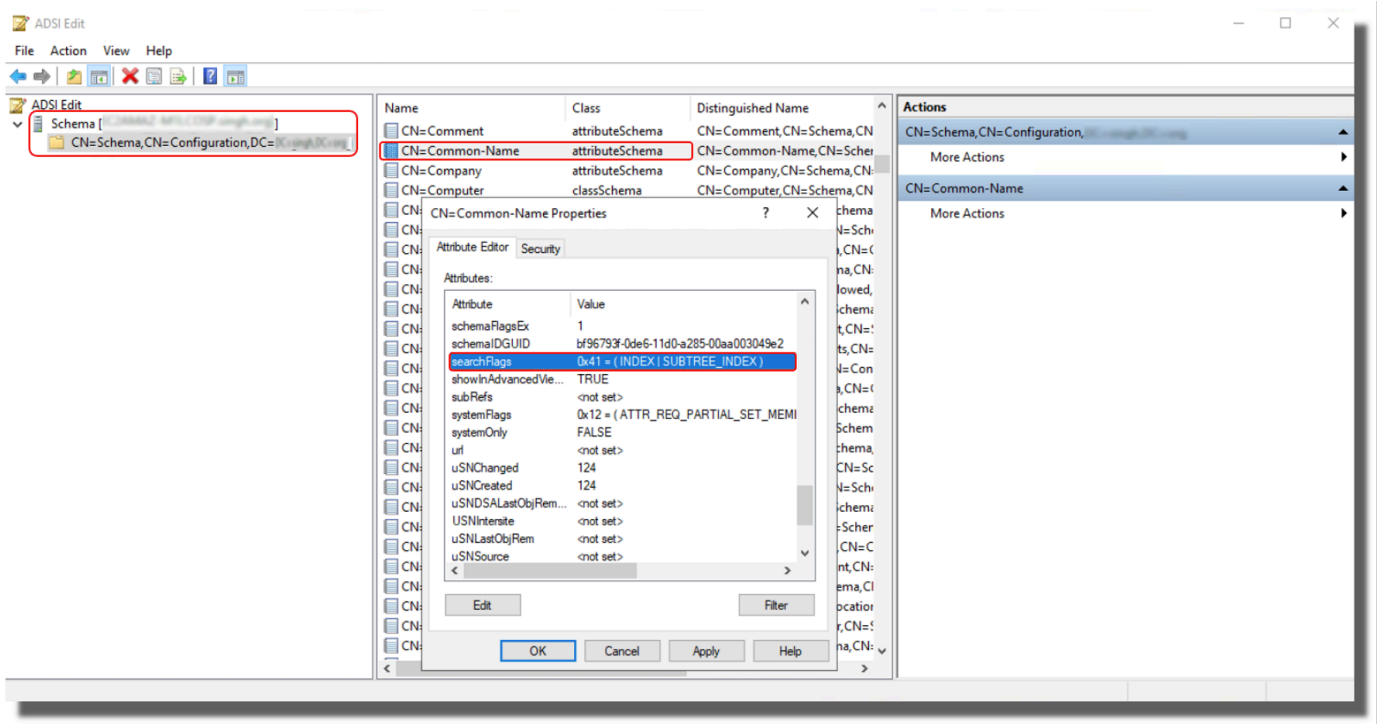
> **Note**
>
> In un'infrastruttura Active Directory di grandi dimensioni con più di 100.000 utenti, potresti essere in grado di cercare solo utenti specifici. Tuttavia, se si tenta di elencare tutti gli utenti (ad esempio, Show All Users in WorkSpaces Launch Wizard) contemporaneamente, potrebbe verificarsi lo stesso errore anche se VLV Support è abilitato. AD Connector richiede che i risultati vengano ordinati per l'attributo «CN» utilizzando Subtree Index. Il Subtree Index è il tipo di indice che prepara i controller di dominio all'esecuzione di un'operazione di ricerca LDAP (Virtual List View) che consente ad AD Connector di completare una ricerca ordinata. Questo indice migliora la ricerca VLV e impedisce l'uso della tabella temporanea del database chiamata. MaxTempTableSize La dimensione di questa tabella può variare, ma per impostazione predefinita il numero massimo di voci è 10000 (l' MaxTempTableSize impostazione della Default Query Policy). L'aumento di

MaxTempTableSize è meno efficiente rispetto all'utilizzo dell'indicizzazione dei sottoalberi. Per evitare questi errori in ambienti AD di grandi dimensioni, si consiglia di utilizzare Subtree Indexing.

È possibile abilitare l'indice Subtree modificando l'attributo searchflags nella definizione dell'attributo, nello schema di Active Directory, con un valore di 65 (0x41), procedendo come segue: ADSEdit

1. Accedere al controller di dominio come proprietario del ruolo principale dello schema utilizzando un account con credenziali di amministratore dello schema.
2. Seleziona Avvia ed esegui, inserisci**`Adsiedit.msc`**.
3. Nello strumento ADSI Edit, connettiti a Schema Partition.
4. Espandi il contenitore CN=Schema, CN=Configuration, DC=. DomainName
5. Individua l'attributo "Common-Name", fai clic con il pulsante destro del mouse e seleziona Proprietà.
6. Individua l'attributo SearchFlags e modificane il valore in modo da abilitare **`65 (0x41)`** l' SubTree indicizzazione insieme al normale indice.

   L'immagine seguente mostra la finestra di dialogo delle proprietà CN=Common-Name nella finestra ADSI Edit:



7. Seleziona OK. È possibile chiudere lo strumento ADSI Edit.
8. Per la conferma, dovresti essere in grado di visualizzare un ID evento 1137 (Fonte: Active Directory_DomainServices), che indica che l'AD ha creato con successo il nuovo indice per l'attributo specificato.

Per ulteriori informazioni, consulta la documentazione di Microsoft.

Ricevo un errore «Impossibile autenticare» quando utilizzo AWS le applicazioni per cercare utenti o gruppi

Potresti riscontrare errori durante la ricerca di utenti o l'accesso ad AWS applicazioni, come WorkSpaces Quick Suite, anche quando lo stato AD Connector era attivo. Se la password dell'account di servizio di AD Connector è stata modificata o è scaduta, AD Connector non può più interrogare il dominio Active Directory. Contatta il tuo amministratore AD e verifica quanto segue:

- Verifica che la password dell'account del servizio AD Connector non sia scaduta
- Selezionato, l'account del servizio AD Connector non ha l'opzione L'utente deve cambiare la password al prossimo accesso abilitata.
- Verifica che l'account del servizio AD Connector non sia bloccato.
- Se non sei sicuro che la password sia scaduta o modificata, puoi reimpostare la password dell'account del servizio e aggiornare la stessa password in AD Connector.

Ricevo un errore relativo alle mie credenziali di directory quando tento di aggiornare l'account del servizio AD Connector

Quando tenti di aggiornare l'account del servizio AD Connector, ricevi un messaggio di errore simile a uno o più dei seguenti:

Messaggio:Si è verificato un errore La directory richiede un aggiornamento delle credenziali. Aggiorna le credenziali della directory. Si è verificato un errore La directory richiede un aggiornamento delle credenziali. Aggiorna le credenziali della directory dopo il messaggio Aggiorna le credenziali dell'account del servizio AD Connector: Si è verificato un errore La richiesta ha un problema. Consulta i seguenti dettagli. Si è verificato un errore nella combinazione account di servizio/password

Potrebbe esserci un problema con la sincronizzazione dell'ora e Kerberos. AD Connector invia le richieste di autenticazione Kerberos ad Active Directory. Queste richieste richiedono un intervallo

di tempo limitato e, se vengono ritardate, avranno esito negativo. Per risolvere questo problema, vedi Raccomandazione: configurare il Root PDC con un'origine temporale autorevole ed evitare una distorsione temporale diffusa nella documentazione. Microsoft Per ulteriori informazioni sul servizio orario e sulla sincronizzazione, vedi sotto:

- Come funziona il Windows Time Service
- Tolleranza massima per la sincronizzazione dell'orologio del computer
- WindowsStrumenti e impostazioni del servizio orario

Alcuni dei miei utenti non possono eseguire l'autenticazione con la mia directory

I tuoi account utente devono avere la preautenticazione Kerberos abilitata. Questa è l'impostazione predefinita per i nuovi account utente e non deve essere modificata. Per ulteriori informazioni su questa impostazione, vai a Preautenticazione attiva Microsoft TechNet.

Problemi di manutenzione

Di seguito sono riportati i problemi di manutenzione più comuni per AD Connector

- La mia directory è bloccata nello stato "Requested" (Richiesta)
- L'aggiunta fluida al dominio per le EC2 istanze Amazon ha smesso di funzionare

La mia directory è bloccata nello stato "Requested" (Richiesta)

Se disponi di una directory che è stata nello stato "Richiesta" per più di cinque minuti, prova a eliminare la directory e a ricrearla. Se il problema persiste, contatta Supporto AWS.

L'aggiunta fluida al dominio per le EC2 istanze Amazon ha smesso di funzionare

Se Seamless Domain Join for EC2 Instances funzionava e poi si è interrotto mentre AD Connector era attivo, le credenziali per il tuo account di servizio AD Connector potrebbero essere scadute. Le credenziali scadute possono impedire a AD Connector di creare oggetti computer in Active Directory.

Per risolvere questo problema, aggiorna le password dell'account del servizio nell'ordine seguente, in modo che corrispondano:

1. Aggiorna la password per l'account di servizio in Active Directory.

2. Aggiorna la password per l'account di servizio nel tuo AD Connector inDirectory Service. Per ulteriori informazioni, consulta Aggiornamento delle credenziali dell'account del servizio AD Connector in Console di gestione AWS.

> **Important**
>
> L'aggiornamento della password solo in Directory Service non comporta il trasferimento della modifica della password all'Active Directory locale esistente, quindi è importante farlo nell'ordine mostrato nella procedura precedente.

Non riesco a eliminare il mio AD Connector

Se il tuo AD Connector passa a uno stato non funzionante, non hai più accesso ai controller di dominio. Blocchiamo l'eliminazione di un AD Connector quando ci sono ancora applicazioni ad esso collegate perché una di queste applicazioni potrebbe ancora utilizzare la directory. Per un elenco delle applicazioni che devi disabilitare per eliminare il tuo AD Connector, consultaEliminazione di AD Connector. Se ancora non riesci a eliminare il tuo AD Connector, puoi richiedere assistenza tramite Supporto AWS.

Strumenti generali per l'analisi degli emittenti di AD Connector

I seguenti strumenti possono essere utilizzati per risolvere vari problemi di AD Connector relativi alla creazione, all'autenticazione e alla connettività:

DirectoryServicePortTest strumento

Lo strumento DirectoryServicePortTestdi test può essere utile per la risoluzione dei problemi di connettività tra AD Connector e i server Active Directory o DNS gestiti dal cliente. Per ulteriori informazioni su come utilizzare lo strumento, consultaTest di un AD Connector.

Strumento di acquisizione dei pacchetti

È possibile utilizzare l'utilità integrata di acquisizione dei Windows pacchetti (netsh) per analizzare e risolvere potenziali problemi di rete o di comunicazione con Active Directory (ldap e kerberos). Per ulteriori informazioni, consulta Acquisizione di una traccia di rete senza installare nulla.

Log di flusso VPC

Per comprendere meglio quali richieste vengono ricevute e inviate da AD Connector, puoi configurare i log di flusso VPC per le interfacce di rete delle directory. È possibile identificare tutte le interfacce di rete riservate all'uso Directory Service tramite la descrizione:. `AWSCreated network interface for directory` *`your-directory-id`*

Un caso d'uso semplice è rappresentato dalla creazione di AD Connector con un dominio Active Directory gestito dal cliente con un gran numero di controller di dominio. Puoi utilizzare i log di flusso VPC e filtrare in base alla porta Kerberos (88) per scoprire quali controller di dominio nell'Active Directory gestita dal cliente vengono contattati per l'autenticazione.

Simple AD

Simple AD è una directory indipendente gestita supportata da un server compatibile con Active Directory di Samba 4. È disponibile in due dimensioni.

- Piccola: supporta fino a 500 utenti (circa 2.000 oggetti, inclusi utenti, gruppi e computer).
- Grande: supporta fino a 5.000 utenti (circa 20.000 oggetti, inclusi utenti, gruppi e computer).

Simple AD offre un sottoinsieme delle funzionalità offerte da AWS Managed Microsoft AD, tra cui la possibilità di gestire gli account utente e le appartenenze ai gruppi, creare e applicare policy di gruppo, connettersi in modo sicuro alle EC2 istanze Amazon e fornire il Single Sign-On (SSO) basato su Kerberos. Tuttavia, tieni presente che Simple AD non supporta funzionalità come l'autenticazione a più fattori (MFA), le relazioni di fiducia con altri domini, il Centro PowerShell di amministrazione di Active Directory, il supporto, il cestino di riciclaggio di Active Directory, gli account di servizio gestiti di gruppo e le estensioni dello schema per le applicazioni POSIX e Microsoft.

Simple AD offre diversi vantaggi:

- Simple AD semplifica la gestione EC2 delle istanze Amazon che eseguono Linux e Windows e la distribuzione di applicazioni Windows nel AWS cloud.
- Molte delle applicazioni e degli strumenti che utilizzi oggi e che richiedono il supporto Microsoft Active Directory possono essere utilizzati con Simple AD.
- Gli account utente in Simple AD consentono l'accesso ad AWS applicazioni come WorkSpaces WorkDocs, o Amazon WorkMail.
- Puoi gestire AWS le risorse tramite l'accesso basato sui ruoli IAM a. Console di gestione AWS
- Le istantanee automatiche giornaliere consentono il ripristino. point-in-time

Simple AD non supporta:

- WorkSpaces Applicazioni Amazon
- Amazon Chime
- Amazon FSx
- Amazon RDS per SQL Server
- Amazon RDS per Oracle

- AWS IAM Identity Center
- Relazioni di trust con altri domini
- Centro di amministrazione di Active Directory
- PowerShell
- Cestino di Active Directory
- Account del servizio gestito del gruppo
- Estensioni dello schema per applicazioni Microsoft e POSIX

Continua a leggere gli argomenti di questa sezione per sapere come creare il tuo Simple AD.

Argomenti

Nozioni di base su Simple AD

Simple AD crea una directory completamente gestita basata su Samba nel cloud. AWS Quando crei una directory con Simple AD, Directory Service crea due controller di dominio e server DNS per tuo conto. I controller di dominio vengono creati in diverse sottoreti in un Amazon VPC. Questa ridondanza aiuta a garantire che la directory rimanga accessibile anche in caso di errore.

Argomenti

- Cosa viene creato con il tuo Simple AD

Prerequisiti di Simple AD

Per creare un Simple AD Active Directory, è necessario un Amazon VPC con quanto segue:

- Il VPC deve disporre di una tenancy hardware predefinita.

  Puoi usarlo IPv6 per il tuo VPC. Per ulteriori informazioni, consulta il IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
- Almeno due sottoreti in due zone di disponibilità diverse e devono essere dello stesso tipo di rete. Le sottoreti devono appartenere allo stesso intervallo CIDR (Classless Inter-Domain Routing). Se si desidera estendere o ridimensionare il VPC per la directory, assicurarsi di selezionare entrambe le sottoreti dei controller di dominio per l'intervallo CIDR VPC esteso. Quando crei un Simple AD, Directory Service crea due controller di dominio e server DNS per tuo conto.
  - Per ulteriori informazioni sulla gamma CIDR, consulta la sezione Indirizzamento IP per le sottoreti VPCs e le sottoreti nella Amazon VPC User Guide.
- Se hai bisogno del supporto LDAPS con Simple AD, consigliamo di configurarlo utilizzando un Network Load Balancer collegato alla porta 389. Questo modello consente di utilizzare un certificato sicuro per la connessione LDAPS, di semplificare l'accesso a LDAPS attraverso un solo indirizzo IP NLB e di avere il failover automatico nell'NLB. Simple AD non supporta l'uso di certificati autofirmati sulla porta 636. Per ulteriori informazioni su come configurare LDAPS con Simple AD, consulta Come configurare un endpoint LDAPS per Simple AD nel Blog di AWS sulla sicurezza.
- I seguenti tipi di crittografia devono essere abilitati nella directory:
  - RC4_HMAC_ MD5
  - AES128_HMAC_ SHA1
  - AES256_HMAC_ SHA1
  - Tipi di crittografia futuri

> **Note**
>
> La disabilitazione di questi tipi di crittografia può causare problemi di comunicazione tra RSAT (Remote Server Administration Tools) e può influire sulla disponibilità della directory.

- Per ulteriori informazioni, consultare Che cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC

Directory Serviceutilizza una struttura a due VPC. Le EC2 istanze che compongono la directory vengono eseguite all'esterno dell'AWSaccount e sono gestite da. AWS Hanno due schede di rete, `ETH0` e `ETH1`. `ETH0` è la scheda di gestione ed è al di fuori del tuo account. `ETH1` viene creata all'interno dell'account.

L'intervallo IP di gestione della rete `ETH0` della directory viene scelto a livello di codice per garantire che non sia in conflitto con il VPC in cui è distribuita la directory. Questo intervallo IP può trovarsi in una delle seguenti coppie (poiché le directory vengono eseguite in due sottoreti):

- 10.0.1.0/24 e 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 e 192.168.2.0/24

Evitiamo i conflitti controllando il primo ottetto del CIDR. `ETH1`. Se inizia con un 10, scegliamo un VPC 192.168.0.0/16 con le sottoreti 192.168.1.0/24 e 192.168.2.0/24. Se il primo ottetto è diverso da un 10, scegliamo un VPC 10.0.0.0/16 con le sottoreti 10.0.1.0/24 e 10.0.2.0/24.

L'algoritmo di selezione non include i percorsi del VPC. È quindi possibile avere un conflitto di routing IP da questo scenario.

> **Important**
>
> Se uno qualsiasi dei prerequisiti di Simple AD viene modificato dopo la creazione di Simple AD, il Simple AD può non funzionare. Per risolvere il tuo stato di Simple AD Impaired, dovrai contattare Supporto AWS.

Crea il tuo Simple AD

Questa procedura illustra tutti i passaggi necessari per creare un Simple AD. È stato progettato per consentirti di iniziare a usare Simple AD in modo rapido e semplice, ma non è destinato all'uso in un ambiente di produzione su larga scala.

Fasi

- Prerequisiti
- Creazione e configurazione di Amazon VPC per il tuo Simple AD
- Creare il tuo Simple AD

Prerequisiti

Questa procedura presuppone quanto segue:

- Ne hai uno attivoAccount AWS.
- Il tuo account non ha raggiunto il limite di Amazon VPCs per la regione in cui desideri utilizzare Simple AD. Per ulteriori informazioni su VPC, consulta What is Amazon VPC? e sottoreti nel tuo VPC nella Amazon VPC User Guide.
- Non disponi di un VPC esistente nella regione con un CIDR di. `10.0.0.0/16`
- Ti trovi in una regione in cui è disponibile Simple AD. Per ulteriori informazioni, consulta Disponibilità regionale per Directory Service.

Per ulteriori informazioni, consulta Prerequisiti di Simple AD.

Creazione e configurazione di Amazon VPC per il tuo Simple AD

Innanzitutto, creerai e configurerai un Amazon VPC da utilizzare con Simple AD. Prima di iniziare la procedura, assicurati di soddisfare i Prerequisiti.

Il VPC che creerai avrà due sottoreti pubbliche. Directory Servicerichiede due sottoreti nel VPC e ogni sottorete deve trovarsi in una zona di disponibilità diversa.

Crea un VPC

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di controllo VPC, scegli Crea VPC.
3. In Impostazioni VPC, scegli VPC e altro.
4. Completa i campi come segue:

    - Mantieni selezionata l'opzione Generato automaticamente in Generazione automatica del tag nome. Modifica progetto in `ADS VPC`.
    - Il blocco IPv4 CIDR dovrebbe essere. `10.0.0.0/16`
    - Mantieni selezionata l'opzione Nessun blocco IPv6 CIDR.

- La Tenancy deve rimanere Predefinita.
- Seleziona 2 per il numero di zone di disponibilità (AZs).
- Seleziona 2 in Numero di sottoreti pubbliche. Il numero di sottoreti private può essere modificato a 0.
- Scegli Personalizza i blocchi CIDR della sottorete per configurare l'intervallo di indirizzi IP della sottorete pubblica. I blocchi CIDR della sottorete pubblica devono essere `10.0.0.0/20` e `10.0.16.0/20`.

5. Seleziona Crea VPC. La creazione del VPC richiede diversi minuti.

Creare il tuo Simple AD

Per creare un nuovo Simple AD, procedi nel seguente modo. Prima di iniziare questa procedura, assicurati di aver completato quanto segue in Prerequisiti eCreazione e configurazione di Amazon VPC per il tuo Simple AD.

Crea un Simple AD

1. Nel riquadro di navigazione della console AWS Directory Service, scegli Directory, quindi seleziona Configura directory.
2. Nella pagina Seleziona il tipo di directory, scegli Simple AD, quindi seleziona Successivo.
3. Nella pagina Enter directory information (Inserisci le informazioni sulla directory) inserisci le seguenti informazioni:

   Dimensione della directory

   Scegliere tra l'opzione di dimensione Small (Piccola) o Large (Grande). Per ulteriori informazioni sulle dimensioni, consulta Simple AD.

   Nome organizzazione

   Un nome dell'organizzazione univoco per la directory che viene utilizzato per registrare i dispositivi client.

   Questo campo è disponibile solo se stai creando la tua directory durante il lancio WorkSpaces.

   Nome DNS directory

   Il nome completo della directory, ad esempio `corp.example.com`.

Nome NetBIOS della directory

Nome breve per la directory, ad esempio `CORP`.

Administrator password (Password dell'amministratore)

La password dell'amministratore della directory. Durante il processo di creazione della directory viene generato un account amministratore con nome utente `Administrator` e questa password.

La password dell'amministratore della directory applica la distinzione tra maiuscole e minuscole e deve contenere tra 8 e 64 caratteri. Deve anche contenere un carattere di almeno tre delle seguenti quattro categorie:

- Lettere minuscole (a-z)
- Lettere maiuscole (A-Z)
- Numeri (0-9)
- Caratteri non alfanumerici (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Conferma la password

Digitare di nuovo la password dell'amministratore.

> **Important**
>
> Assicurati di salvare questa password. Directory Servicenon memorizza questa password e non può essere recuperata. Tuttavia, è possibile reimpostare una password dalla Directory Service console o utilizzando l'ResetUserPasswordAPI.

Descrizione della directory

Descrizione opzionale della directory.

4. Nella pagina Choose VPC and subnets (Scegli VPC e sottoreti) fornire le seguenti informazioni, quindi selezionare Next (Successivo).

   VPC

   VPC per la directory.

Sottoreti

Scegli le sottoreti per i controller di dominio. Le due sottoreti devono trovarsi in diverse zone di disponibilità.

5. Nella pagina Review & create (Rivedi e crea), esaminare le informazioni relative alla directory ed eseguire eventuali modifiche. Quando le informazioni sono corrette, scegli Create Directory (Crea directory). Per creare la directory sono necessari alcuni minuti. Una volta creato, il valore Status cambia in Active (Attivo).

Per ulteriori informazioni su ciò che viene creato con Simple AD, consultaCosa viene creato con il tuo Simple AD.

Cosa viene creato con il tuo Simple AD

Quando crei un Active Directory con Simple AD, Directory Service esegue le seguenti attività per tuo conto:

- Configura una directory basata su Samba all'interno del VPC.
- Crea un account amministratore della directory con il nome utente `Administrator` e la password specificata. Puoi utilizzare questo account per gestire le directory.

> **Important**
>
> Assicurati di salvare questa password. Directory Service non memorizza questa password e non può essere recuperata. Tuttavia, è possibile reimpostare una password dalla Directory Service console o utilizzando l'ResetUserPasswordAPI.

- Crea un gruppo di sicurezza per i controller della directory.
- Crea l'account `AWSAdminD-`*`xxxxxxxx`* con privilegi di amministratore del dominio. Questo account viene utilizzato per Directory Service eseguire operazioni automatizzate per le operazioni di manutenzione delle directory, come l'acquisizione di istantanee delle directory e il trasferimento di ruoli FSMO. Le credenziali di questo account vengono archiviate in modo sicuro da Directory Service.
- crea e associa automaticamente una interfaccia di rete elastica (ENI) a ciascuno dei controller di dominio. Ciascuno di ENIs questi è essenziale per la connettività tra il VPC e i controller di Directory Service dominio e non deve mai essere eliminato. È possibile identificare tutte le interfacce di rete riservate all'uso Directory Service mediante la descrizione: "interfaccia di

rete AWS creata per directory directory-id». Per ulteriori informazioni, consulta Elastic Network Interfaces nella Amazon EC2 User Guide. Il server DNS predefinito di AWS Managed Microsoft AD Active Directory è il server DNS VPC at Classless Inter-Domain Routing (CIDR) +2. Per ulteriori informazioni, consulta Amazon DNS server nella Amazon VPC User Guide.

> **Note**
>
> Per impostazione predefinita, i controller di dominio sono distribuiti in due zone di disponibilità in una regione e connessi al tuo cloud privato virtuale (VPC) Amazon. I backup vengono eseguiti automaticamente una volta al giorno e i volumi Amazon Elastic Block Store (EBS) sono crittografati per garantire che i dati siano protetti quando sono inattivi. In caso di guasto, i controller di dominio vengono sostituiti automaticamente nella stessa zona di disponibilità utilizzando lo stesso indirizzo IP ed è possibile eseguire un ripristino di emergenza completo utilizzando il backup più recente.

Best practice per Simple AD

Ecco alcuni suggerimenti e linee guida da prendere in considerazione per evitare problemi e ottenere il massimo da Simple AD.

Configurazione: prerequisiti

Tieni presenti queste linee guida prima di creare la directory.

Verifica di avere il tipo di directory corretto

Directory Service offre diverse modalità di utilizzo Microsoft Active Directory con altri AWS servizi. Puoi scegliere il servizio di directory con le caratteristiche di cui hai bisogno a un costo che si adatta al tuo budget:

- AWS Directory Service per Microsoft Active Directory è un servizio gestito ricco di funzionalità Microsoft Active Directory ospitato sul AWS cloud. AWS Microsoft AD gestito è la scelta migliore se hai più di 5.000 utenti e hai bisogno di impostare una relazione di fiducia tra una directory AWS ospitata e le directory locali.
- AD Connector collega semplicemente l'Active Directory locale esistente a AWS. Il connettore AD rappresenta la scelta migliore quando vuoi utilizzare la tua directory on-premise esistente tramite i servizi AWS .

- Simple AD è una directory a basso costo su scala ridotta con compatibilità di base con Active Directory. Supporta fino a 5.000 utenti, applicazioni compatibili con Samba 4 e compatibilità LDAP per applicazioni compatibili con LDAP.

Per un confronto più dettagliato delle Directory Service opzioni, consultaQuale scegliere.

Assicurati che le tue istanze VPCs e siano configurate correttamente

Per connetterti, gestire e utilizzare le tue directory, devi configurare correttamente le directory a VPCs cui sono associate. Consulta Prerequisiti per la creazione di un AWS Managed Microsoft AD, Prerequisiti di AD Connector o Prerequisiti di Simple AD per informazioni sulla sicurezza del VPC e sui requisiti di rete.

Se aggiungi un'istanza al dominio, assicurati di disporre della connessione e dell'accesso remoto all'istanza, come descritto in Modi per aggiungere un' EC2 istanza Amazon al tuo AWS Managed Microsoft AD.

Sii consapevole dei limiti

Scopri i vari limiti per il tuo tipo di directory specifico. Lo spazio di archiviazione disponibile e la dimensione aggregata degli oggetti sono le uniche limitazioni al numero di oggetti che puoi archiviare nella directory. Consulta, AWS Quote Microsoft AD gestite, Quote di AD Connector o Quote di Simple AD per maggiori dettagli sulla directory scelta.

Comprendi la configurazione e l'utilizzo del gruppo AWS di sicurezza della tua directory

AWS crea un gruppo di sicurezza e lo collega alle interfacce di rete elastiche del controller di dominio della directory. AWS configura il gruppo di sicurezza per bloccare il traffico non necessario verso la directory e consente il traffico necessario.

Modifica del gruppo di sicurezza della directory

Puoi modificare i gruppi di sicurezza per le tue directory, ma solo se conosci appieno il filtraggio dei gruppi di sicurezza. Per ulteriori informazioni, consulta i gruppi EC2 di sicurezza Amazon per le istanze Linux nella Amazon EC2 User Guide. Modifiche improprie possono interrompere le comunicazioni con i computer e le istanze previsti. AWS sconsiglia l'apertura di porte aggiuntive nella directory in quanto ciò riduce la sicurezza. Esamina il modello di responsabilitàAWS condivisa prima di apportare modifiche.

> **Warning**
>
> È tecnicamente possibile associare il gruppo di sicurezza della directory ad altre EC2 istanze create dall'utente. Tuttavia, AWS sconsiglia questa pratica. AWS può avere motivi per modificare il gruppo di sicurezza senza preavviso per soddisfare le esigenze funzionali o di sicurezza della directory gestita. Tali modifiche influiscono sulle eventuali istanze con cui viene associato il gruppo di sicurezza della directory e possono interrompere il funzionamento delle istanze associate. Inoltre, l'associazione del gruppo di sicurezza della directory EC2 alle istanze può creare un potenziale rischio per la EC2 sicurezza delle istanze.

Usa AWS Managed Microsoft AD se sono richiesti trust

Simple AD non supporta relazioni di trust. Se è necessario stabilire un trust tra la propria Directory Service directory e un'altra directory, è necessario utilizzare AWS Directory Service per Microsoft Active Directory.

Configurazione: creazione della directory

Di seguito sono elencati alcuni suggerimenti da considerare durante la creazione della directory.

Ricorda l'ID amministratore e la password

Quando configuri la directory, fornisci una password per l'account amministratore. Questo ID account è Amministratore per Simple AD. Ricorda la password creata per questo account; altrimenti sarai in grado di aggiungere oggetti alla directory.

Comprendi le restrizioni relative al nome utente per AWS le applicazioni

Directory Service fornisce supporto per la maggior parte dei formati di caratteri che possono essere utilizzati nella creazione di nomi utente. Tuttavia, vengono applicate restrizioni sui caratteri ai nomi utente che verranno utilizzati per l'accesso ad AWS applicazioni WorkSpaces, come WorkDocs Amazon WorkMail o Quick Suite. Queste limitazioni richiedono che non vengano utilizzati i seguenti caratteri:

- Spazi
- Caratteri multibyte
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> Il simbolo @ è consentito purché preceda un suffisso UPN.

Programmazione delle applicazioni

Prima di programmare le applicazioni, valuta quanto segue:

Utilizzo del servizio di localizzazione DC di Windows

Durante lo sviluppo di applicazioni, utilizza il servizio di localizzazione di Windows DC o il servizio DNS dinamico (DDNS) di Managed AWS Microsoft AD per individuare i controller di dominio (). DCs Non effettuare l'hard coding delle applicazioni con l'indirizzo di un DC. Il servizio di localizzazione DC garantisce che il carico della directory venga distribuito e ti consente di sfruttare i vantaggi della scalabilità orizzontale aggiungendo i controller dei domini alla distribuzione. Se colleghi l'applicazione a un DC fisso e il DC viene sottoposto a patch o ripristino, l'applicazione perderà l'accesso al DC anziché utilizzare uno dei controller rimanenti. DCs Inoltre, l'hard coding di un DC può provocare la creazione di "hot spot" su un solo DC. In casi gravi, gli hot spot possono provocare un blocco del DC. In questi casi, inoltre, l'automazione delle AWS directory potrebbe contrassegnare la directory come danneggiata e avviare processi di ripristino che sostituiscono il controller di dominio che non risponde.

Esecuzione di test di caricamento prima della produzione

Assicurati di effettuare test di laboratorio con gli oggetti e le richieste più importanti del tuo carico di lavoro di produzione per confermare che la directory si adatti al carico dell'applicazione. Se è necessaria una capacità aggiuntiva, è consigliabile utilizzare Directory Service Microsoft Active Directory, che consente di aggiungere controller di dominio per prestazioni elevate. Per ulteriori informazioni, consulta Implementazione di controller di dominio aggiuntivi per Managed AWS Microsoft AD.

Utilizzo delle query LDAP

Query LDAP estese su un controller di dominio e migliaia di oggetti possono consumare cicli di CPU significativi in un singolo DC e generare così hot spot. L'operazione potrebbe incidere sulle applicazioni che condividono lo stesso DC durante la query.

Gestione della directory Simple AD

Puoi utilizzarlo Console di gestione AWS per gestire il tuo Simple AD e completare le attività day-to-day amministrative. I modi in cui puoi mantenere il tuo Simple AD includono:

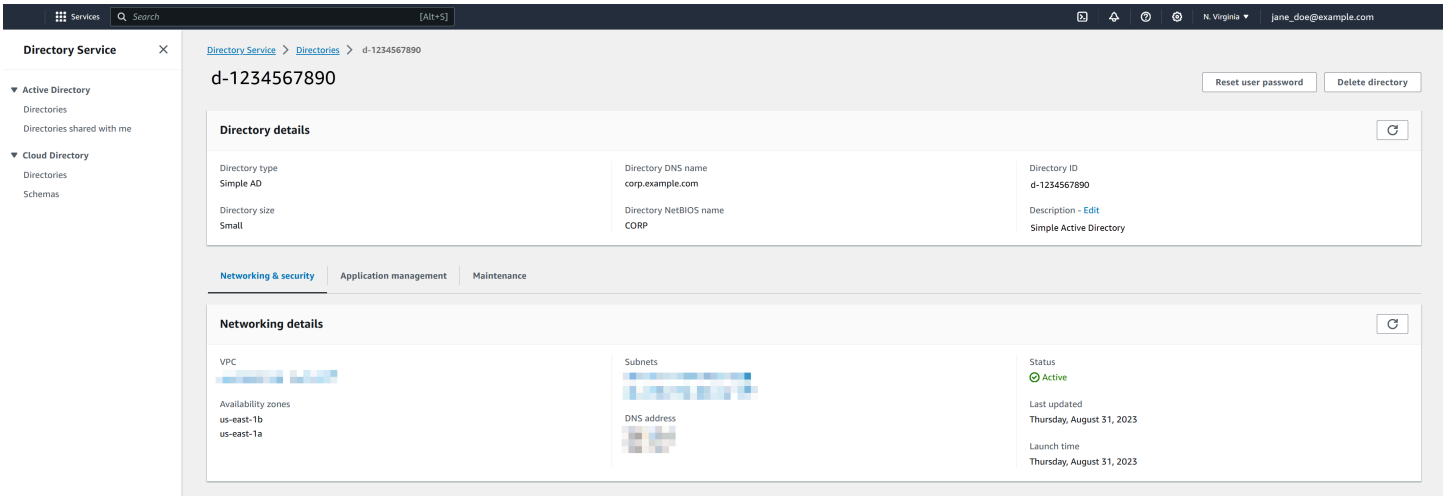
- Visualizza i dettagli sul tuo Simple AD come il nome DNS, l'ID della directory e lo stato della directory.
- Aggiorna l'indirizzo DNS per il tuo Simple AD.
- Ripristina il tuo Simple AD con istantanee. Puoi anche creare istantanee ed eliminare istantanee.
- Elimina il tuo Simple AD quando non è più necessario.

Visualizzazione delle informazioni sulla directory Simple AD

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione della console AWS Directory Service, in Active Directory, seleziona Directory.
2. Seleziona il collegamento dell'ID per la tua directory. Le informazioni sulla directory vengono visualizzate nella sezione Dettagli della directory.

Per ulteriori informazioni sul campo Status (Stato), consultare Comprendere lo stato della directory Simple AD.



Aggiornamento del tipo di rete di directory

Puoi aggiornare il tipo di rete della tua Directory Service directory da IPv4 a Dual-stack (and). IPv4 IPv6 L'aggiornamento del tipo di rete per includere gli indirizzi IPv6 IP offre uno spazio di indirizzi più ampio di. IPv4 IPv4 e le IPv6 comunicazioni sono indipendenti l'una dall'altra.

Per i dettagli, consulta la sezione Confronta IPv4 e IPv6 nella Amazon Virtual Private Cloud User Guide.

> **Important**
>
> Si tratta di un'operazione unidirezionale che non può essere annullata. Effettua prima il test in un ambiente non di produzione.

Prerequisiti

Prima di aggiornare il tipo di rete di directory, assicuratevi che siano soddisfatti i seguenti requisiti:

- Il tuo VPC deve essere configurato con intervalli IPv6 CIDR. Per i dettagli, consulta il IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
- Hai accesso amministrativo a. Console di gestione AWS
- La tua directory deve essere in stato attivo.
- Disponi delle autorizzazioni IAM appropriate per modificare Directory Service le impostazioni.

Per aggiornare il tipo di rete delle directory

Per aggiornare la directory alla rete dual-stack

> **Note**
>
> Se la directory viene replicata in più regioni, esegui questo aggiornamento in ciascuna regione.

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Seleziona la directory di destinazione.
3. Vai alla scheda Rete e sicurezza.

4. Scegli Aggiungi IPv6 supporto. Questa opzione è disponibile solo per le directory IPv4 -only.

   IPv6 solo le directory non sono supportate.
5. Consulta le informazioni di aggiornamento e i dettagli sui prezzi.
6. Scegli Aggiungi per confermare l'aggiornamento.

Dopo aver avviato l'aggiornamento, lo stato della directory passa a Aggiornamento durante il processo di aggiornamento. Il completamento dell'aggiornamento richiede in genere 15-30 minuti. Una volta completato, lo stato della directory torna ad Attivo.

Configurazione dei server DNS per Simple AD

Simple AD inoltra le richieste DNS all'indirizzo IP dei server DNS forniti da Amazon VPC. Questi server DNS risolvono i nomi configurati nelle zone ospitate private Amazon Route 53. Puntando i computer on-premise a Simple AD, ora puoi risolvere le richieste DNS nella zona ospitata privata. Per ulteriori informazioni su Route 53, consulta Che cos'è Amazon Route 53?.

Per abilitare il Simple AD alla risposta a query DNS esterne, devi configurare la lista di controllo degli accessi (ACL) di rete per il VPC contenente il Simple AD per consentire il traffico dall'esterno del VPC.

- Se non utilizzi le zone ospitate private Route 53, le richieste DNS vengono inoltrate a server DNS pubblici.
- Se utilizzi server DNS personalizzati esterni al tuo VPC e desideri utilizzare DNS privato, devi riconfigurarlo per utilizzare server DNS personalizzati su EC2 istanze all'interno del tuo VPC. Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private.
- Se desideri che il Simple AD risolva i nomi utilizzando sia i server DNS all'interno del VPC sia quelli privati al di fuori del VPC, puoi utilizzare un set di opzioni DHCP. Per un esempio dettagliato, consulta questo articolo.
- Integrando i tuoi Directory Service'una risoluzione DNS con. Amazon Route 53 Resolver

> **Note**
>
> Gli aggiornamenti dinamici del DNS non sono supportati nei domini di Simple AD. È invece possibile apportare direttamente le modifiche collegandosi alla directory utilizzando DNS Manager su un'istanza che è stata aggiunta al dominio.

Ripristino di Simple AD con snapshot

AWS Directory Service offre la possibilità di scattare istantanee manuali dei dati per la directory Simple AD. Queste istantanee possono essere utilizzate per eseguire un point-in-time ripristino della directory. Non è possibile acquisire snapshot del connettore AD.

Argomenti

Creazione di uno snapshot della directory

Uno snapshot può essere utilizzato per riportare la tua directory a quello che era nel momento in cui è stato creato lo snapshot. Per creare uno snapshot manuale della tua directory, esegui la procedura seguente.

> **Note**
>
> Hai un limite di 5 snapshot manuali per ogni directory. Se hai già raggiunto questo limite, devi eliminare uno degli snapshot manuali esistenti prima di crearne un altro.

Creazione di uno snapshot manuale

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Maintenance (Manutenzione).
4. Nella sezione Snapshots (Snapshot) scegliere Actions (Operazioni), quindi selezionare Create snapshot (Crea snapshot).
5. Se lo si desidera, nella finestra di dialogo Create directory snapshot (Crea snapshot della directory) è possibile dare un nome allo snapshot. Quando pronto, scegli Create (Crea).

A seconda delle dimensioni della directory, possono essere necessari alcuni minuti per creare lo snapshot. Quando lo snapshot è pronto, il valore Status (Stato) cambia in `Completed`.

Ripristino della directory da uno snapshot

Il ripristino di una directory da uno snapshot equivale a spostare la directory indietro nel tempo. Gli snapshot di directory sono univoci nella directory da cui sono stati creati. È possibile ripristinare uno snapshot solo nella directory da cui è stato creato. Inoltre, l'età massima supportata di un'istantanea manuale è di 180 giorni. Per ulteriori informazioni, consulta Useful shelf life of a system-state backup of Active Directory nel sito Web Microsoft.

> **Warning**
>
> Consigliamo di contattare il centro del Supporto AWS prima che uno snapshot venga ripristinato, potremmo essere in grado di aiutarti per non dover ripristinare uno snapshot. Ogni ripristino da uno snapshot può risultare in perdita di dati come sono in un momento specifico. È importante comprendere che tutti i server DNS associati alla directory saranno offline fino al completamento dell'operazione di ripristino. DCs

Per ripristinare la tua directory da uno snapshot, segui la seguente procedura.

Ripristino di una directory da uno snapshot

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Maintenance (Manutenzione).
4. Nella sezione Snapshots (Snapshot) selezionare uno snapshot dall'elenco, scegliere Actions (Operazioni), quindi selezionare Restore snapshot (Ripristina snapshot).
5. Verificare le informazioni nella finestra di dialogo Restore directory snapshot (Ripristina snapshot di directory), quindi scegliere Restore (Ripristina).

Per una directory Simple AD, possono essere necessari alcuni minuti per il suo ripristino. Una volta ripristinato correttamente, il valore Status (Stato) della directory passa a `Active`. Qualsiasi modifica apportata alla directory dopo la data di snapshot verrà sovrascritta.

Eliminazione di uno snapshot

Per eliminare uno snapshot

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Maintenance (Manutenzione).
4. Nella sezione Snapshots (Snapshot) scegliere Actions (Operazioni), quindi selezionare Delete snapshot (Elimina snapshot).
5. Verificare di voler eliminare lo snapshot, quindi scegliere Delete (Elimina).

Eliminare il tuo Simple AD

Quando si elimina un Simple AD, tutti i dati di directory e le istantanee vengono eliminati e non possono essere recuperati. Dopo l'eliminazione della directory, tutte le istanze collegate alla directory rimangono intatte. Tuttavia, non puoi utilizzare le credenziali della directory per accedere a queste istanze. È necessario accedere a queste istanze con un account utente che è in locale all'istanza.

Quando si elimina una directory AWS Managed Microsoft AD, Simple AD o ibrida, tutti i dati e le istantanee della directory vengono eliminati e non possono essere recuperati. Dopo l'eliminazione della directory, tutte le istanze collegate alla directory rimangono intatte. Tuttavia, non puoi utilizzare le credenziali della directory per accedere a queste istanze. È necessario accedere a queste istanze con un account utente che è in locale all'istanza.

Quando una directory del connettore AD viene eliminata, quella on-premise rimane intatta. Anche tutte le istanze collegate alla directory rimangono intatte e collegate alla tua directory on-premise. Puoi, tuttavia, utilizzare le credenziali della directory per accedere a queste istanze.

Eliminazione di una directory

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory. Assicurati di trovarti nel Regione AWS luogo in cui è distribuito Active Directory. Per ulteriori informazioni, consulta Scelta di una regione.
2. Assicurati che nessuna AWS applicazione sia abilitata per la directory che intendi eliminare. AWSLe applicazioni abilitate impediranno l'eliminazione di AWS Managed Microsoft AD o Simple AD.

a. Nella pagina Directories (Directory), scegli l'ID della directory.

b. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione). Nella sezione AWSapp e servizi, puoi vedere quali AWS applicazioni sono abilitate per la tua directory.

- Disabilita Console di gestione AWS l'accesso. Per ulteriori informazioni, consulta Disabilitazione dell'accesso Console di gestione AWS.
- Per disabilitare Amazon WorkSpaces, devi annullare la registrazione del servizio dalla directory nella WorkSpaces console. Per ulteriori informazioni, consulta Eliminare una directory nella Amazon WorkSpaces Administration Guide.
- Per disabilitarlo WorkDocs, devi eliminare il WorkDocs sito nella WorkDocs console. Per ulteriori informazioni, consulta Eliminare un sito nella Amazon WorkDocs Administration Guide.
- Per disabilitare Amazon WorkMail, devi rimuovere l' WorkMail organizzazione Amazon dalla WorkMail console Amazon. Per ulteriori informazioni, consulta Rimuovere un'organizzazione nella Amazon WorkMail Administrator Guide.
- Per disabilitare Amazon FSx for Windows File Server, devi rimuovere il FSx file system Amazon dal dominio. Per ulteriori informazioni, consulta Working with Active Directory in FSx for Windows File Server nella Amazon FSx for Windows File Server User Guide.
- Per disabilitare Amazon Relational Database Service, devi rimuovere l'istanza Amazon RDS dal dominio. Per ulteriori informazioni, consulta Gestione di un'istanza database in un dominio nella Guida per l'utente di Amazon RDS.
- Per disabilitare AWS Client VPN il servizio, è necessario rimuovere il servizio di directory dall'endpoint Client VPN. Per ulteriori informazioni, consulta Work with Client VPN nella AWS Client VPNAdministrator Guide.
- Per disabilitare Amazon Connect, è necessario eliminare l'istanza di Amazon Connect. Per ulteriori informazioni, consulta Eliminare l'istanza Amazon Connect nella Amazon Connect Administration Guide.
- Per disabilitare Amazon Quick Suite, devi annullare l'iscrizione ad Amazon Quick Suite. Per ulteriori informazioni, consulta Chiusura Amazon Quick Suite dell'account nella Guida per l'utente di Amazon Quick Suite.

> **Note**
>
> Se la utilizzi AWS IAM Identity Center e la hai precedentemente connessa alla directory AWS Managed Microsoft AD che intendi eliminare, devi prima modificare l'origine dell'identità prima di poterla eliminare. Per ulteriori informazioni, consulta Modifica della fonte di identità nella Guida per l'utente del Centro identità IAM.

3. Nel riquadro di navigazione, seleziona Directory.
4. Seleziona solo la directory da eliminare, quindi fai clic su Elimina. Sono necessari alcuni minuti per l'eliminazione della directory. Una volta eliminata la directory, viene rimossa dal tuo elenco di directory.

Proteggi la tua directory Simple AD

Questa sezione descrive le considerazioni per proteggere l'ambiente Simple AD.

Argomenti

- Come reimpostare la password di un account Simple AD krbtgt

Come reimpostare la password di un account Simple AD krbtgt

L'account krbtgt svolge un ruolo importante negli scambi di biglietti Kerberos. L'account krbtgt è un account speciale utilizzato per la crittografia Kerberos ticket-granting ticket (TGT) e svolge un ruolo cruciale nella sicurezza del protocollo di autenticazione Kerberos. In Samba AD, krbtgt è rappresentato come un account utente (disabilitato). La password di questo account viene generata casualmente al momento del provisioning del dominio. L'accesso a questo segreto può comportare una compromissione totale e non rilevabile del dominio, poiché i nuovi ticket Kerberos possono essere stampati senza alcun controllo. Per ulteriori informazioni, consulta la documentazione di Samba.

Si consiglia di cambiare questa password regolarmente ogni 90 giorni. Puoi reimpostare la password dell'account krbtgt da un' EC2 Windowsistanza Amazon aggiunta a Simple AD.

> **Note**
>
> AWS Simple AD è alimentato da Samba-AD. Samba-AD non memorizza l'hash N-1 per l'account krbtgt. Pertanto, quando la password dell'account krbtgt viene reimpostata, al client Kerberos verrà richiesto di negoziare un nuovo Ticket Granting Ticket (TGT) durante la successiva richiesta di Service Ticket (ST). Per ridurre al minimo le potenziali interruzioni del servizio, è necessario pianificare la reimpostazione della password dell'account krbtgt al di fuori dell'orario lavorativo. Questo approccio mitiga gli impatti sulle operazioni in corso e garantisce una continuità dell'autenticazione senza intoppi.

Le seguenti procedure mostrano come reimpostare la password dell'account krbtgt da un'istanza Amazon EC2Windows.

Prerequisiti

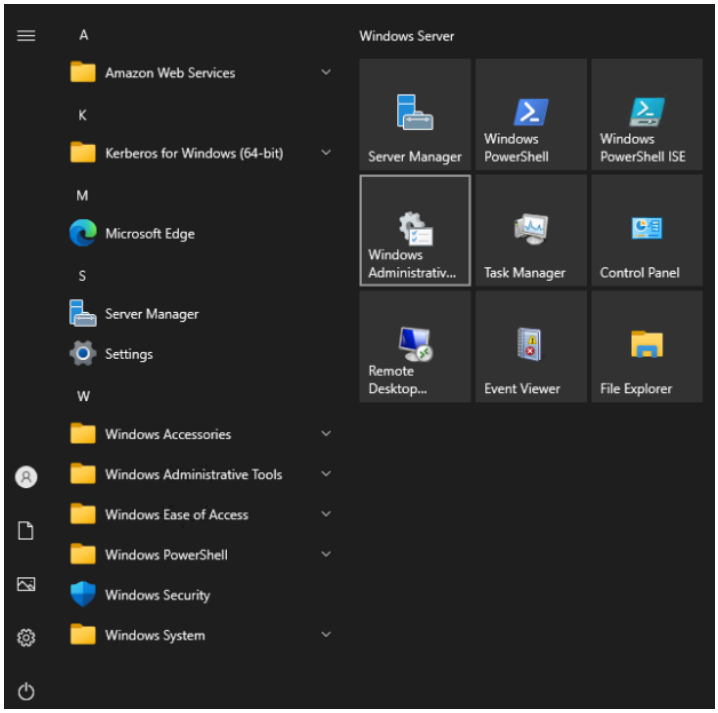
- Prima di iniziare questa procedura, completa quanto segue:
  - Il dominio ha aggiunto un' EC2 istanza alla directory Simple AD.
    - Per ulteriori informazioni su come aggiungere un' EC2 Windowsistanza a un Simple AD, vederethe section called “Unire un'istanza Windows”.
  - Hai le credenziali di amministratore della directory Simple AD. Effettuerai l'accesso come amministratore della directory Simple AD per questa procedura.

> **Note**
>
> Alcuni, Servizi AWS come Amazon WorkDocs e Amazon WorkSpaces, creeranno un Simple AD per tuo conto.

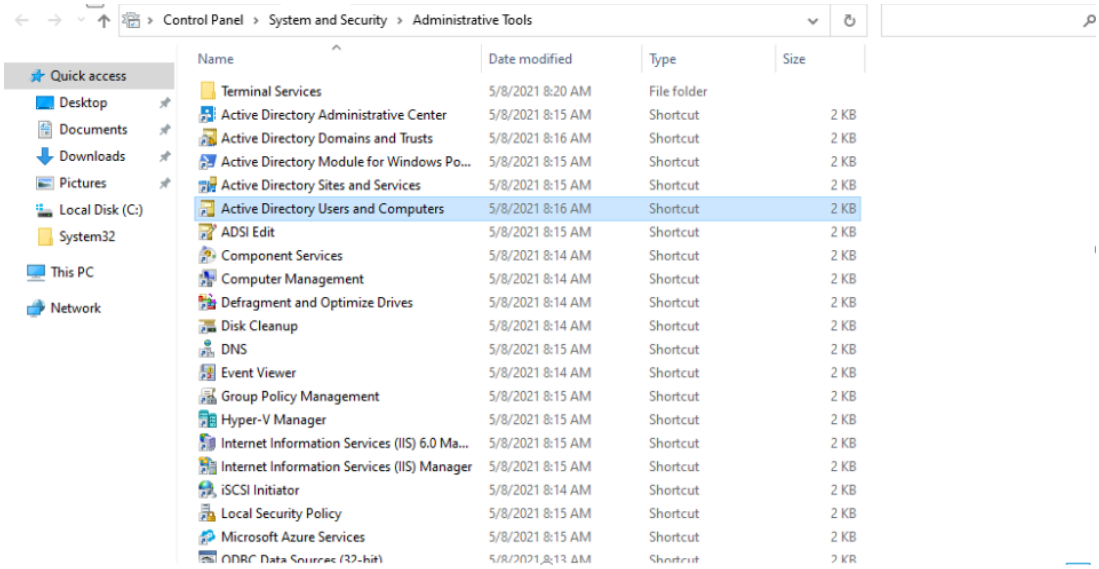
Reimpostazione della password dell'account Simple AD krbtgt

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella EC2 console Amazon, scegli Istanze e seleziona l'istanza Windows Server. Quindi scegliere Connetti.
3. Nella pagina Collega all'istanza, scegli Client RDP.

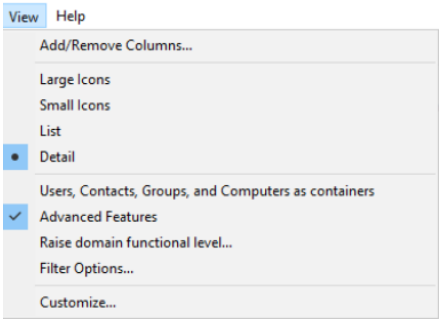
4. Nella finestra di dialogo Sicurezza di Windows, copia le credenziali di amministratore locale per il computer Windows Server a cui accedere. Il nome utente può avere i seguenti formati: `NetBIOS-Name\administrator` o`DNS-Name\administrator`. Ad esempio, `corp\administrator` sarebbe il nome utente se hai seguito la procedura inthe section called “Crea il tuo Simple AD”.
5. Una volta effettuato l'accesso al computer Windows Server, apri Strumenti di Windows amministrazione dal menu Start scegliendo la cartella Strumenti di Windows amministrazione.



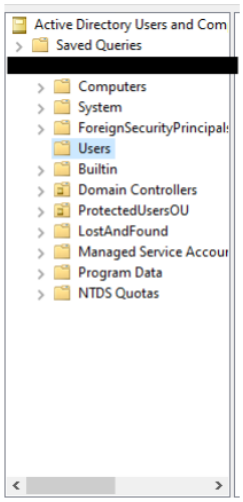
6. Nella dashboard Strumenti di Windows amministrazione, apri Utenti e computer di Active Directory scegliendo Utenti e computer di Active Directory.



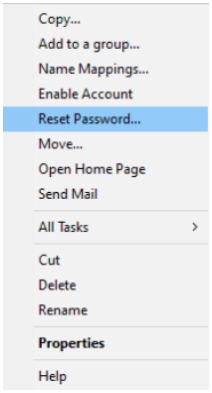
7. Nella finestra Utenti e computer di Active Directory, seleziona Visualizza, quindi scegli Abilita funzionalità avanzate.



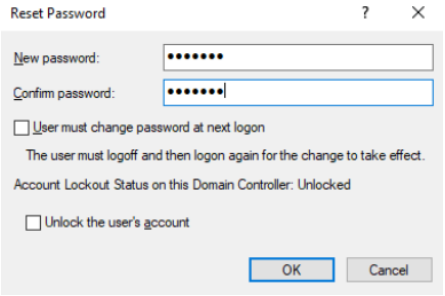
8. Nella finestra Utenti e computer di Active Directory, seleziona Utenti dal pannello di sinistra.



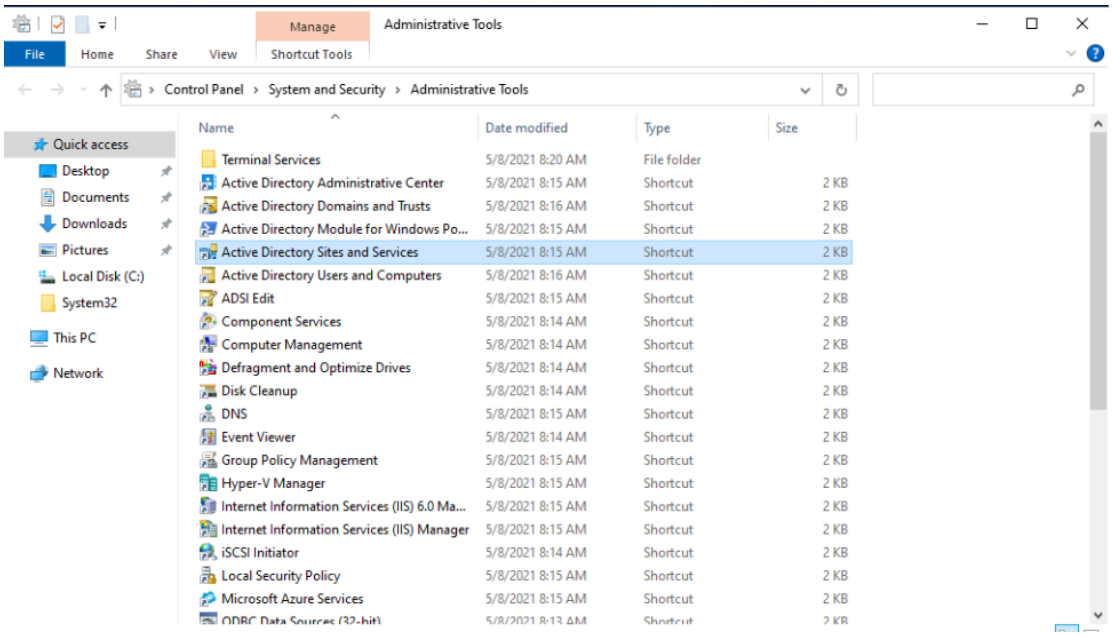
9. Trova l'utente denominato krbtgt, fai clic con il pulsante destro del mouse su di esso e seleziona Reimposta password.



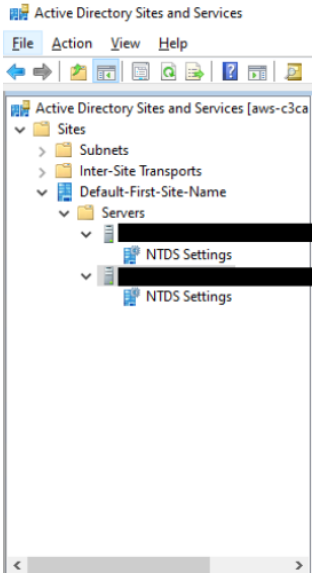
10. Nella nuova finestra, inserisci la nuova password, inseriscila di nuovo, quindi scegli OK per reimpostare la password dell'account krbtgt.



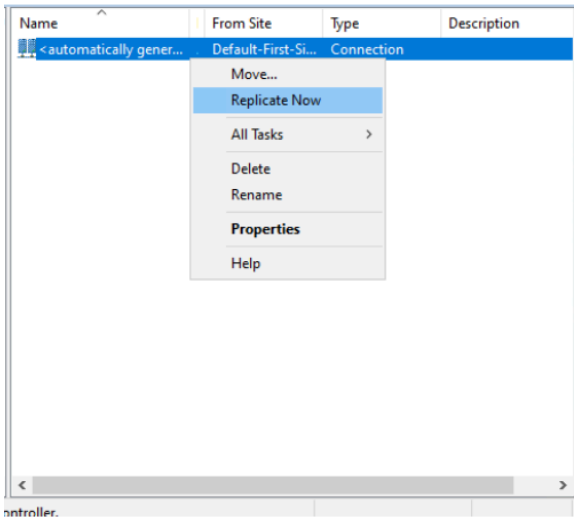
11. Nella dashboard Strumenti di Windows amministrazione, scegli Siti e servizi di Active Directory.



12. Nella finestra Siti e servizi di Active Directory, espandi Site, Default-First-Site-Name e Servers.



13. Nella finestra Impostazioni NTDS, fai clic con il pulsante destro del mouse sul server e seleziona Replica ora.



14. Ripeti i passaggi da 13 a 14 per gli altri server.

Monitoraggio della directory Simple AD

Puoi ottenere il massimo dal tuo Simple AD scoprendo di più sui diversi stati di Simple AD e sul loro significato per il tuo Simple AD. Puoi anche utilizzare AWS servizi come Amazon Simple Notification Service per monitorare il tuo Simple AD. Amazon Simple Notification Service può inviarti notifiche sullo stato della tua directory Simple AD.

Attività per monitorare il tuo Simple AD

- Comprendere lo stato della directory Simple AD
- Attivazione delle notifiche sullo stato delle directory Simple AD con Amazon Simple Notification Service

Comprendere lo stato della directory Simple AD

Di seguito sono elencati i diversi stati per una directory.

Active (Attivo)

La directory funziona normalmente. Nessun problema è stato rilevato da Directory Service per la directory.

Creating (Creazione in corso)

La directory è attualmente in fase di creazione. Solitamente la creazione di una directory può richiedere da 20 a 45 minuti, ma può variare in base al carico di sistema.

Deleted (Eliminato)

La directory è stata eliminata. Tutte le risorse per la directory sono state rilasciate. Una volta che una directory entra in questo stato, non può essere ripristinata.

Deleting (Eliminazione in corso)

La directory è attualmente in fase di eliminazione. La directory rimarrà in questo stato finché non sarà completamente eliminata. Una volta che una directory entra in questo stato, l'operazione di eliminazione non può essere annullata e la directory non può essere ripristinata.

Failed (Non riuscito)

Impossibile creare la directory. Elimina questa directory. Se questo problema persiste, contatta il Centro Supporto AWS.

Impaired (Insufficiente)

La directory è in esecuzione in uno stato danneggiato. Uno o più problemi sono stati rilevati e non tutte le operazioni di directory potrebbero lavorare alla massima capacità operativa. Ci sono molti motivi per cui la directory può trovarsi in questo stato. Questi includono le normali attività di manutenzione operativa, come l'applicazione di patch o la rotazione delle EC2 istanze, l'hot spot temporaneo da parte di un'applicazione su uno dei controller di dominio o le modifiche apportate alla rete che interrompono inavvertitamente le comunicazioni tra le directory. Lo stato della directory può essere compromesso se si modificano le impostazioni descritte in. Prerequisiti di Simple AD Per ulteriori informazioni, consulta Risoluzione dei problemi relativi AWS a Managed Microsoft AD, Risoluzione dei problemi di AD Connector, Risoluzione dei problemi di Simple AD. Per i normali problemi relativi alla manutenzione, AWS risolve questi problemi entro 40 minuti. Se dopo aver esaminato l'argomento di risoluzione dei problemi, la directory è in stato Danneggiato per più di 40 minuti, consigliamo di contattare il Centro Supporto AWS.

> **Important**
>
> Non ripristinare uno snapshot mentre la directory è in stato danneggiato. Raramente è necessario ripristinare uno snapshot per risolvere dei danni. Per ulteriori informazioni, consulta Ripristino di AWS Managed Microsoft AD con istantanee.

Inoperable (Inutilizzabile)

La directory non è funzionale. Sono stati segnalati problemi per tutti gli endpoint della directory.

Requested (Richiesta)

Una richiesta di creazione della directory è attualmente in sospeso.

RestoreFailed

Ripristino della directory da uno snapshot non riuscito. Riprova l'operazione di ripristino. Se il problema persiste, prova un altro snapshot oppure contatta il Centro Supporto AWS.

Restoring (Ripristino)

La directory è attualmente in corso di ripristino da uno snapshot automatico o manuale. Il ripristino da uno snapshot richiede solitamente alcuni minuti, a seconda delle dimensioni dei dati della directory nello snapshot.

Per ulteriori informazioni, consulta Risoluzione dei problemi relativi ai messaggi di stato della directory Simple AD.

Attivazione delle notifiche sullo stato delle directory Simple AD con Amazon Simple Notification Service

Tramite Amazon Simple Notification Service (Amazon SNS), puoi ricevere messaggi e-mail o di testo (SMS) quando lo stato della directory cambia. Ricevi una notifica se la directory passa da uno stato Attivo a uno stato Danneggiato o Inutilizzabile. Puoi anche ricevere una notifica quando la directory torna a uno stato Active (Attivo).

Come funziona

Amazon SNS utilizza "argomenti" per raccogliere e distribuire i messaggi. Ogni argomento ha uno o più abbonati che ricevono i messaggi che sono stati pubblicati su quell'argomento. Utilizzando i passaggi seguenti puoi aggiungere Directory Service come editore a un argomento di Amazon SNS. Quando Directory Service rileva una modifica nello stato della tua directory, pubblica un messaggio su quell'argomento, che viene quindi inviato ai sottoscrittori dell'argomento.

Puoi associare più directory come editori a un singolo argomento. Puoi anche aggiungere messaggi di stato della directory agli argomenti che hai precedentemente creato in Amazon SNS. Hai un controllo dettagliato su chi può pubblicare ed effettuare la sottoscrizione a un argomento. Per informazioni complete su Amazon SNS, consulta Cos'è Amazon SNS?.

Per abilitare la messaggistica SNS per la directory

1. Accedi a Console di gestione AWS e apri la console. Directory Service
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Seleziona la scheda Manutenzione.
4. Nella sezione Monitoraggio della directory, scegli Azioni, quindi seleziona Crea notifica.
5. Nella pagina Crea notifica, seleziona Scegli un tipo di notifica, quindi scegli Crea una nuova notifica. In alternativa, se disponi già di un argomento SNS, puoi scegliere Associa ad argomento SNS esistente per l'invio di messaggi di stato da questa directory a tale argomento.

   > **Note**
   >
   > Se scegli Crea una nuova notifica, ma utilizzerai lo stesso nome dell'argomento per un argomento SNS già esistente, Amazon SNS non crea un nuovo argomento, ma aggiunge semplicemente le nuove informazioni di abbonamento a quello esistente.
   > Se scegli Associa ad argomento SNS esistente, potrai solo scegliere un argomento SNS presente nella stessa regione della directory.

6. Scegli il Tipo di destinatario e inserisci le informazioni di contatto del Destinatario. Se inserisci un numero di telefono per SMS, utilizza solo numeri. Non includere trattini, spazi o parentesi.
7. (Facoltativo) Fornisci un nome per l'argomento SNS e un relativo nome visualizzato. Il nome visualizzato è un nome breve di massimo 10 caratteri incluso in tutti i messaggi SMS di questo argomento. Quando utilizzi l'opzione SMS, il nome visualizzato è obbligatorio.

   > **Note**
   >
   > Se hai effettuato l'accesso utilizzando un utente o un ruolo IAM con solo la policy DirectoryServiceFullAccessgestita, il nome dell'argomento deve iniziare con «DirectoryMonitoring». Se desideri personalizzare ulteriormente il nome dell'argomento, avrai bisogno di ulteriori privilegi per SNS.

8. Scegli Create (Crea).

Se desideri designare abbonati SNS aggiuntivi, ad esempio un indirizzo e-mail aggiuntivo, code Amazon SQS oppureAWS Lambda, puoi farlo dalla console Amazon SNS.

Per rimuovere i messaggi di stato della directory da un argomento

1. Accedi e apri la console. Console di gestione AWSDirectory Service
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Seleziona la scheda Manutenzione.
4. Nella sezione Monitoraggio delle directory, seleziona il nome di un argomento SNS nell'elenco, scegli Operazioni, quindi seleziona Rimuovi.
5. Scegli Rimuovi.

Questa operazione rimuove la directory come editore per l'argomento SNS selezionato. Se desideri eliminare l'intero argomento, puoi farlo dalla console Amazon SNS.

> **Note**
>
> Prima di eliminare un argomento Amazon SNS tramite la console di SNS, devi accertarti che una directory non stia inviando messaggi di stato a tale argomento.
> Se elimini un argomento Amazon SNS tramite la console di SNS, questa modifica non si rifletterà immediatamente nella console Servizio di directory. Riceverai una notifica solo la prossima volta che una directory pubblica una notifica all'argomento eliminato, nel qual caso visualizzerai uno stato aggiornato nella scheda Monitoring (Monitoraggio) della directory che indica che l'argomento non è stato trovato.
> Pertanto, per evitare di perdere importanti messaggi sullo stato della directory, prima di eliminare qualsiasi argomento da cui vengono ricevuti messaggiDirectory Service, associa la directory a un argomento Amazon SNS diverso.

Accesso ad AWS applicazioni e servizi dal tuo Simple AD

Puoi concedere l'accesso ai tuoi utenti di Simple AD per accedere ad AWS applicazioni e servizi. Alcune di queste AWS applicazioni e servizi includono:

- Amazon WorkDocs
- Console di gestione AWS
- Amazon WorkSpaces

Puoi anche utilizzare l'accesso URLs e il single sign-on con Simple AD.

Argomenti

Policy di compatibilità delle applicazioni per Simple AD

Simple AD è un'implementazione di Samba che offre molte delle funzionalità di base di Active Directory. A causa della vastità delle off-the-shelf applicazioni personalizzate e commerciali che utilizzano Active Directory, non esegue e AWS non può eseguire verifiche formali o ampie della compatibilità delle applicazioni di terze parti con Simple AD. Sebbene AWS collabori con i clienti nel tentativo di superare eventuali problemi di installazione delle applicazioni che potrebbero incontrare, non siamo in grado di garantire che qualsiasi applicazione sia o continuerà a essere compatibile con Simple AD.

Le seguenti applicazioni di terze parti sono compatibili con Simple AD:

- Microsoft Internet Information Services (IIS) sulle seguenti piattaforme:
  - Windows Server 2003 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Microsoft SQL Server:
  - SQL Server 2005 R2 (edizioni Express, Web e Standard)
  - SQL Server 2008 R2 (edizioni Express, Web e Standard)
  - SQL Server 2012 (edizioni Express, Web e Standard)
  - SQL Server 2014 (edizioni Express, Web e Standard)
- Microsoft SharePoint:
  - SharePoint Fondazione 2010
  - SharePoint Impresa 2010

- SharePoint Impresa 2013

I clienti possono scegliere di utilizzare AWS Directory Service per Microsoft Active Directory (AWSMicrosoft AD gestito) per un livello di compatibilità più elevato basato su Active Directory effettivo.

Consentire l'accesso ad AWS applicazioni e servizi per Simple AD

Gli utenti possono autorizzare Simple AD a fornire ad AWS applicazioni e servizi, come Amazon WorkSpaces, l'accesso al tuo Active Directory. Le seguenti AWS applicazioni e servizi possono essere abilitati o disabilitati per funzionare con Simple AD.

AWS applicazione/servizio	Ulteriori informazioni…
Amazon WorkDocs	Per ulteriori informazioni, consulta la Amazon WorkDocs Administration Guide
Amazon WorkMail	Per ulteriori informazioni, consulta l'Amazon WorkMail Administrator Guide.
Amazon WorkSpaces	Puoi creare un Simple AD, AWS Managed Microsoft AD o AD Connector direttamente da WorkSpaces. È sufficiente avviare Advanced Setup (Impostazioni avanzate) durante la creazione del Workspace. Per ulteriori informazioni, consulta la Amazon WorkSpaces Administration Guide.
Console di gestione AWS	Per ulteriori informazioni, consulta Abilitazione Console di gestione AWS dell'accesso con credenziali Microsoft AD AWS gestite.

Una volta abilitato, puoi gestire l'accesso alle directory nella console dell'applicazione o del servizio a cui intendi consentire l'accesso alla directory. Per trovare i link AWS alle applicazioni e ai servizi sopra descritti nella Directory Service console, procedi nel seguente modo.

Visualizzazione dei servizi e applicazioni di una directory

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Consulta l'elenco nella sezione app e servizi AWS .

Per ulteriori informazioni su come autorizzare o rimuovere l'autorizzazione all'utilizzo Directory Service di AWS applicazioni e servizi, vedere. Autorizzazione per l'AWSutilizzo di applicazioni e servizi Directory Service

Abilitazione dell'accesso alle credenziali Console di gestione AWS with Simple AD

Directory Service ti consente di concedere ai membri della tua directory l'accesso a Console di gestione AWS. Per impostazione predefinita, i membri della directory non hanno accesso ad alcuna AWS risorsa. Assegni ruoli IAM ai membri della tua directory per consentire loro di accedere ai vari AWS servizi e risorse. Il ruolo IAM definisce i servizi, le risorse e il livello di accesso dei membri della directory.

Prima di poter concedere l'accesso alla console ai membri della directory, la directory deve disporre di un URL di accesso. Per ulteriori informazioni su come visualizzare i dettagli della directory e ottenere l'URL di accesso, consulta Visualizzazione delle informazioni sulla directory AWS Managed Microsoft AD. Per ulteriori informazioni su come creare un URL di accesso, consulta Creazione di un URL di accesso per AWS Managed Microsoft AD.

Per ulteriori informazioni su come creare e assegnare ruoli IAM ai membri della directory, consulta Concedere agli utenti e ai gruppi di AWS Managed Microsoft AD l'accesso alle AWS risorse con ruoli IAM.

Argomenti

- Abilitare l'accesso Console di gestione AWS
- Disabilitazione dell'accesso Console di gestione AWS
- Impostazione della durata della sessione di accesso

Articolo correlato del blog AWS sulla sicurezza

- Come accedere all' Console di gestione AWS utilizzo di Microsoft AD AWS gestito e alle credenziali locali

Articolo correlato AWS re:Post

- Come posso concedere l'accesso a un Console di gestione AWS utente di Active Directory locale?

Abilitare l'accesso Console di gestione AWS

Per impostazione predefinita, l'accesso alla console non è abilitato per tutte le directory. Per abilitare l'accesso alla console dei membri e dei gruppi della directory, segui la procedura indicata:

Abilitazione dell'accesso alla console

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Nella sezione Console di gestione AWS, scegli Abilita. Ora l'accesso alla console è abilitato per la tua directory.

> **Important**
>
> Prima che gli utenti possano accedere alla console con il tuo URL di accesso, devi prima aggiungere gli utenti al ruolo IAM. Per ulteriori informazioni sull'assegnazione di ruoli IAM agli utenti, consulta Assegnazione di utenti o gruppi a un ruolo IAM esistente. Dopo l'assegnazione dei ruoli IAM, gli utenti possono accedere alla console utilizzando l'URL di accesso. Ad esempio, se l'URL di accesso alla directory è example-corp.awsapps.com, l'URL per accedere alla console è. https://example-corp.awsapps.com/console/

Disabilitazione dell'accesso Console di gestione AWS

Per disabilitare l'accesso alla console per i membri e i gruppi della directory, segui la procedura indicata:

Disabilitare l'accesso alla console

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Nella sezione Console di gestione AWS, scegli Disabilita. Ora l'accesso alla console è disabilitato per la tua directory.
5. Se nella directory sono stati assegnati ruoli IAM a utenti o gruppi, il pulsante Disabilita potrebbe non essere disponibile. In questo caso, devi rimuovere tutte le assegnazioni dei ruoli IAM per la directory prima di procedere, tra cui quelle per gli utenti o i gruppi della directory che sono stati eliminati, che saranno visualizzati come Utente eliminato o Gruppo eliminato.

   Una volta rimosse tutte le assegnazioni dei ruoli IAM, ripeti le fasi indicate precedentemente.

Impostazione della durata della sessione di accesso

Per impostazione predefinita, gli utenti dispongono di 1 ora per utilizzare la sessione dopo aver effettuato correttamente l'accesso alla console, prima che venga eseguita la disconnessione. Successivamente, gli utenti devono accedere nuovamente per avviare la prossima sessione di 1 ora prima che venga effettuato nuovamente il logout. Puoi utilizzare la procedura seguente per modificare il periodo di tempo fino a 12 ore per ogni sessione.

Impostazione del periodo di sessione di login

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Nella sezione App e servizi AWS , scegli Console di gestione AWS .
5. Nella finestra di dialogo Gestisci l'accesso alle AWS risorse, scegli Continua.
6. Nella pagina Assign users and groups to IAM roles (Assegna utenti e gruppi a ruoli IAM), in Set login session length (Imposta periodo di sessione di login) modifica il valore numerato, quindi seleziona Save (Salva).

Creazione di un URL di accesso per Simple AD

Un URL di accesso viene utilizzato con AWS applicazioni e servizi, come Amazon WorkDocs, per raggiungere una pagina di accesso associata alla tua directory. L'URL deve essere univoco a livello globale. Puoi creare un URL di accesso per la tua directory eseguendo la procedura seguente.

> **Warning**
>
> Una volta creato, l'URL di accesso all'applicazione per questa directory non potrà essere modificato. Dopo aver creato un URL di accesso, non può essere utilizzato da altri utenti. Se cancelli la tua directory, anche l'URL di accesso viene eliminato e può quindi essere utilizzato da qualsiasi altro account.

Per creare un URL di accesso

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Nella sezione URL di accesso all'applicazione, se un URL di accesso non è stato assegnato alla directory, viene visualizzato il pulsante Crea. Inserisci un alias di directory e scegli Crea. Se viene restituito un errore Entità già esistente, l'alias di directory specificato è già stato allocato. Scegli un altro alias e ripeti questa procedura.

   L'URL di accesso viene visualizzato nel formato *<alias>* .awsapps.com.

Abilitazione di Single Sign-On

AWS Directory Service offre la possibilità di consentire agli utenti di accedere WorkDocs da un computer aggiunto alla directory senza dover inserire le proprie credenziali separatamente.

Prima di abilitare l'accesso single sign-on, è necessario eseguire operazioni aggiuntive per abilitare il browser Web dei tuoi utenti a supportare l'accesso single sign-on. Gli utenti potrebbero dover modificare le proprie impostazioni del browser Web per abilitare l'accesso single sign-on.

> **Note**
>
> L'accesso single sign-on funziona solo quando viene utilizzato su un computer collegato alla directory Directory Service e non può essere utilizzato sui computer che non sono collegati alla directory.

Se la directory è una directory del connettore AD e l'account del servizio Connettore AD non dispone dell'autorizzazione per aggiungere o rimuovere l'attributo nome dell'entità servizio, per i passaggi 5 e 6 seguenti sono disponibili due opzioni:

1. È possibile procedere e verrà richiesto il nome utente e la password per un utente di directory che dispone di questa autorizzazione per aggiungere o rimuovere l'attributo nome dell'entità servizio nell'account del servizio Connettore AD. Queste credenziali vengono utilizzate solo per abilitare l'accesso single sign-on e non vengono archiviate dal servizio. Le autorizzazioni dell'account del servizio Connettore AD non vengono modificate.
2. Puoi delegare le autorizzazioni per consentire all'account del servizio AD Connector di aggiungere o rimuovere l'attributo del nome principale del servizio su se stesso, puoi eseguire i PowerShell comandi seguenti da un computer aggiunto al dominio utilizzando un account che dispone delle autorizzazioni per modificare le autorizzazioni sull'account del servizio AD Connector. Il comando seguente darà all'account del servizio Connettore AD la possibilità di aggiungere e rimuovere un attributo nome dell'entità servizio solo per se stesso.

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
```

```
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

Per abilitare o disabilitare il single sign-on con WorkDocs

1. Nel riquadro di navigazione della console AWS Directory Service, seleziona Directory.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella pagina Directory details (Dettagli della directory), seleziona la scheda Application management (Gestione dell'applicazione).
4. Nella sezione URL di accesso all'applicazione, scegli Abilita per abilitare il single sign-on per. WorkDocs

   Se non visualizzi il pulsante Enable (Abilita), potresti dover creare un URL di accesso prima che questa opzione venga visualizzata. Per ulteriori informazioni su come creare un URL di accesso, consulta Creazione di un URL di accesso per AWS Managed Microsoft AD.
5. Nella finestra di dialogo Enable Single Sign-On for this directory (Abilita accesso single sign-on per questa directory) scegli Enable (Abilita). L'accesso single sign-on è abilitato per la directory.
6. Se in seguito desiderate disabilitare il Single Sign-On con WorkDocs, scegliete Disabilita, quindi nella finestra di dialogo Disabilita il Single Sign-On per questa directory, scegliete nuovamente Disabilita.

Argomenti

- Accesso con autenticazione unica per IE e Chrome
- Accesso con autenticazione unica per Firefox

Accesso con autenticazione unica per IE e Chrome

Per permettere ai browser Internet Explorer (IE) e Google Chrome di Microsoft di supportare l'accesso single sign-on, è necessario eseguire le attività seguenti sul computer client:

- Aggiungi il tuo URL di accesso (ad esempio, https://*<aliias>*.awsapps.com) all'elenco dei siti approvati per il Single Sign-On.

- Abilita lo scripting attivo (). JavaScript
- Permetti l'accesso automatico.
- Abilita l'autenticazione integrata.

Tu o i tuoi utenti potete eseguire queste attività manualmente oppure potete modificare queste impostazioni usando le impostazioni delle policy di gruppo.

Argomenti

Aggiornamento manuale per l'accesso con autenticazione unica su Windows

Per abilitare manualmente l'accesso single sign-on su un computer Windows, esegui la procedura seguente sul computer client. Alcune di queste impostazioni possono essere già impostate correttamente.

Abilitazione manuale dell'accesso single sign-on per Internet Explorer e Chrome su Windows

1. Per aprire la finestra di dialogo Internet Properties (Proprietà Internet), seleziona il menu Start, digita `Internet Options` nella casella di ricerca e seleziona Internet Options (Opzioni Internet).
2. Aggiungi il tuo URL di accesso all'elenco dei siti approvati per l'accesso single sign-on eseguendo le fasi seguenti:
    a. Nella finestra di dialogo Internet Properties (Proprietà Internet), seleziona la scheda Security (Sicurezza).
    b. Seleziona Local Intranet (Intranet locale) e scegli Sites (Siti).
    c. Nella finestra di dialogo Local intranet (Intranet locale) scegli Advanced (Opzioni avanzate).
    d. Aggiungi il tuo URL di accesso all'elenco di siti Web e scegli Close (Chiudi).
    e. Nella finestra di dialogo Local intranet (Intranet locale) scegli OK.
3. Per abilitare lo scripting attivo, segui la procedura seguente:
    a. Nella scheda Security (Sicurezza) della finestra di dialogo Internet Properties (Proprietà Internet), scegli Custom level (Livello personalizzato).

b. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale), scorri verso il basso a Scripting e seleziona Enable (Abilita) sotto Active scripting (Scripting attivo).

c. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale) scegli OK.

4. Per abilitare l'accesso automatico, segui la procedura seguente:

a. Nella scheda Security (Sicurezza) della finestra di dialogo Internet Properties (Proprietà Internet), scegli Custom level (Livello personalizzato).

b. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale), scorri verso il basso a User Authentication (Autenticazione utenti) e seleziona Automatic logon only in Intranet zone (Accesso automatico solo in area intranet) sotto Logon (Accesso).

c. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale) scegli OK.

d. Nella finestra di dialogo Security Settings - Local Intranet Zone (Impostazioni di sicurezza - Area Intranet locale) scegli OK.

5. Per abilitare l'autenticazione integrata, segui la procedura seguente:

a. Nella finestra di dialogo Internet Properties (Proprietà Internet), seleziona la scheda Advanced (Opzioni avanzate).

b. Scorri verso il basso a Security (Sicurezza) e seleziona Enable Integrated Windows Authentication (Abilita autenticazione di Windows integrata).

c. Nella finestra di dialogo Internet Properties (Proprietà Internet) scegli OK.

6. Chiudi e riapri il browser perché queste modifiche diventino effettive.

Aggiornamento manuale per l'accesso con autenticazione unica su OS X

Per abilitare manualmente l'accesso single sign-on a Chrome su OS X, esegui la procedura seguente sul computer client. Dovrai disporre di diritti di amministratore sul tuo computer per completare questa procedura.

Abilitazione manuale dell'accesso single sign-on a Chrome su OS X

1. Aggiungi l'URL di accesso alla AuthServerAllowlistpolicy eseguendo il comando seguente:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Apri System Preferences (Preferenze di sistema), vai al pannello Profiles (Profili) ed elimina il profilo `Chrome Kerberos Configuration`.
3. Riavvia Chrome e apri chrome://policy in Chrome per confermare che le nuove impostazioni siano effettive.

Impostazioni delle policy di gruppo per l'accesso con autenticazione unica

L'amministratore di dominio può implementare le impostazioni delle policy di gruppo per effettuare le modifiche dell'accesso single sign-on su computer client collegati al dominio.

> **Note**
>
> Se gestisci i browser web Chrome sui computer del tuo dominio con i criteri di Chrome, devi aggiungere il tuo URL di accesso alla AuthServerAllowlistpolitica. Per ulteriori informazioni su come impostare le policy di Chrome, vai all'argomento relativo alle Impostazioni delle policy in Chrome.

Abilitazione manuale dell'accesso single sign-on per Internet Explorer e Chrome utilizzando le impostazioni delle policy di gruppo

1. Crea un nuovo oggetto Group Policy seguendo questa procedura:
   a. Apri lo strumento di gestione di Group Policy, vai al tuo dominio e seleziona Group Policy Objects (Oggetti Group Policy).
   b. Dal menu principale, seleziona Action (Operazione) e quindi New (Nuovo).
   c. Nella finestra di dialogo New GPO (Nuovo GPO) digita un nome descrittivo per l'oggetto Group Policy, ad esempio `IAM Identity Center Policy` e lascia Source Starter GPO (GPO Starter di origine) impostato su (none) (nessuno). Fai clic su OK.
2. Aggiungi l'URL di accesso all'elenco dei siti approvati per l'accesso single sign-on eseguendo la procedura seguente:
   a. Nello strumento di gestione di policy di gruppo, vai al tuo dominio, seleziona Oggetti di policy di gruppo, apri il menu contestuale (pulsante destro del mouse) per la tua policy Centro identità IAM e scegli Modifica.

b. Nella struttura della policy, seleziona User Configuration (Configurazione utente) > Preferences (Preferenze) > Windows Settings (Impostazioni di Windows).

c. Nell'elenco Windows Settings (Impostazioni di Windows), apri il menu contestuale (pulsante destro del mouse) per Registry (Registro di sistema) e seleziona New registry item (Nuovo elemento di registro di sistema).

d. Nella finestra di dialogo New Registry Properties (Nuove proprietà di registro di sistema), inserisci le impostazioni seguenti e scegli OK:

   Azione

   ```
   Update
   ```

   Hive

   ```
   HKEY_CURRENT_USER
   ```

   Path

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   \ZoneMap\Domains\awsapps.com\<alias>
   ```

   Il valore per *<alias>* è derivato dal tuo URL di accesso. Se il tuo URL di accesso è `https://examplecorp.awsapps.com`, l'alias è `examplecorp` e la chiave di registro sarà `Software\Microsoft\Windows\CurrentVersion\Internet Settings \ZoneMap\Domains\awsapps.com\examplecorp`.

   Value name (Nome valore)

   ```
   https
   ```

   Value type (Tipo di valore)

   ```
   REG_DWORD
   ```

   Value data (Dati valore)

   ```
   1
   ```

3. Per abilitare lo scripting attivo, segui la procedura seguente:

   a. Nello strumento di gestione di policy di gruppo, vai al tuo dominio, seleziona Oggetti di policy di gruppo, apri il menu contestuale (pulsante destro del mouse) per la tua policy Centro identità IAM e scegli Modifica.

b. Nella struttura della policy, passa a Computer Configuration (Configurazione computer) > Policies (Policy) > Administrative Templates (Modelli amministrativi) > Windows Components (Componenti di Windows) > Internet Explorer > Internet Control Panel (Pannello di controllo Internet) > Security Page (Pagina protezione) > Intranet Zone (Area Intranet).

c. Nell'elenco Intranet Zone (Area Intranet), apri il menu contestuale (pulsante destro del mouse) per Allow active scripting (Consenti scripting attivo) e scegli Modifica (Edit).

d. Nella finestra di dialogo Allow active scripting (Consenti scripting attivo), inserisci le impostazioni seguenti e scegli OK:

- Seleziona il pulsante di opzione Enabled (Abilitato).
- In Options (Opzioni) imposta Allow active scripting (Consenti scripting attivo) su Enable (Abilita).

4. Per abilitare l'accesso automatico, segui la procedura seguente:

a. Nello strumento di gestione di Group Policy, passa al tuo dominio, seleziona Group Policy Objects (Oggetti Group Policy), apri il menu contestuale (pulsante destro del mouse) della policy SSO e scegli Edit (Modifica).

b. Nella struttura della policy, passa a Computer Configuration (Configurazione computer) > Policies (Policy) > Administrative Templates (Modelli amministrativi) > Windows Components (Componenti di Windows) > Internet Explorer > Internet Control Panel (Pannello di controllo Internet) > Security Page (Pagina protezione) > Intranet Zone (Area Intranet).

c. Nell'elenco Intranet Zone (Area Intranet), apri il menu contestuale (pulsante destro del mouse) per Logon options (Opzioni di accesso) e scegli Modifica (Edit).

d. Nella finestra di dialogo Logon options (Opzioni di accesso), inserisci le impostazioni seguenti e scegli OK:

- Seleziona il pulsante di opzione Enabled (Abilitato).
- In Options (Opzioni) imposta Logon options (Opzioni di accesso) su Automatic logon only in Intranet zone (Accesso automatico solo nell'area Intranet).

5. Per abilitare l'autenticazione integrata, segui la procedura seguente:

a. Nello strumento di gestione di policy di gruppo, vai al tuo dominio, seleziona Oggetti di policy di gruppo, apri il menu contestuale (pulsante destro del mouse) per la tua policy Centro identità IAM e scegli Modifica.

b. Nella struttura della policy, seleziona User Configuration (Configurazione utente) > Preferences (Preferenze) > Windows Settings (Impostazioni di Windows).

c. Nell'elenco Windows Settings (Impostazioni di Windows), apri il menu contestuale (pulsante destro del mouse) per Registry (Registro di sistema) e seleziona New registry item (Nuovo elemento di registro di sistema).

d. Nella finestra di dialogo New Registry Properties (Nuove proprietà di registro di sistema), inserisci le impostazioni seguenti e scegli OK:

   Azione

   ```
   Update
   ```

   Hive

   ```
   HKEY_CURRENT_USER
   ```

   Path

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   ```

   Value name (Nome valore)

   ```
   EnableNegotiate
   ```

   Value type (Tipo di valore)

   ```
   REG_DWORD
   ```

   Value data (Dati valore)

   ```
   1
   ```

6. Chiudi la finestra Group Policy Management Editor (Editor gestione di Group Policy) se è ancora aperta.

7. Assegna la nuova policy al tuo dominio seguendo questa procedura:

   a. Nella struttura di gestione di Group Policy, apri il menu contestuale (pulsante destro del mouse) del tuo dominio e scegli Link an Existing GPO (Collega un GPO esistente).

   b. Nell'elenco Oggetti policy di gruppo, seleziona la policy Centro identità IAM e scegli OK.

Queste modifiche diventeranno effettive dopo l'aggiornamento successivo della policy di gruppo sul client, oppure all'accesso successivo da parte dell'utente.

Accesso con autenticazione unica per Firefox

Per consentire al browser Mozilla Firefox di supportare il single sign-on, aggiungi l'URL di accesso (ad esempio, https://*<alias>*.awsapps.com) all'elenco dei siti approvati per il single sign-on. Puoi eseguire questa operazione manualmente oppure in maniera automatizzata con uno script.

Argomenti

- Aggiornamento manuale dell'accesso con autenticazione unica
- Aggiornamento automatico dell'accesso con autenticazione unica

Aggiornamento manuale dell'accesso con autenticazione unica

Per aggiungere manualmente l'URL di accesso all'elenco dei siti approvati in Firefox, esegui la seguente procedura sul computer client.

Aggiunta manuale dell'URL di accesso all'elenco dei siti approvati in Firefox

1. Apri Firefox e apri la pagina `about:config`.
2. Apri la preferenza `network.negotiate-auth.trusted-uris` e aggiungi il tuo URL di accesso all'elenco dei siti. Utilizza una virgola (,) per separare più voci.

Aggiornamento automatico dell'accesso con autenticazione unica

In qualità di amministratore di dominio, puoi utilizzare uno script per aggiungere l'URL di accesso alla preferenza utente `network.negotiate-auth.trusted-uris` di Firefox su tutti i computer della rete. Per ulteriori informazioni, visita https://support.mozilla. org/en-US/questions/939037.

Modi per aggiungere un' EC2 istanza Amazon al tuo Simple AD

Puoi aggiungere senza problemi un' EC2 istanza Amazon al tuo dominio Active Directory all'avvio dell'istanza. Per ulteriori informazioni, consulta Unire un'istanza Amazon EC2 Windows al tuo AWS Managed Microsoft AD Active Directory. Puoi anche avviare un' EC2 istanza e aggiungerla a un dominio Active Directory direttamente dalla Directory Service console con AWS Systems ManagerAutomation.

Se devi aggiungere manualmente un' EC2 istanza al tuo dominio Active Directory, devi avviare l'istanza nella regione e nel gruppo di sicurezza o nella sottorete appropriati, quindi aggiungere l'istanza al dominio.

Per essere in grado di connettersi in remoto a queste istanze, è necessario disporre di connettività IP per le istanze dalla rete da cui ti connetti. Nella maggior parte dei casi, questo richiede che un gateway Internet sia associato al VPC e che l'istanza disponga di un indirizzo IP pubblico.

Argomenti

Unire un'istanza Amazon EC2 Windows al tuo Simple AD Active Directory

Puoi avviare e unire un' EC2 Windowsistanza Amazon a un Simple AD. In alternativa, puoi aggiungere manualmente un' EC2 Windowsistanza esistente a un Simple AD

Seamlessly join an EC2 Windows

Per aggiungere facilmente un dominio a un' EC2 istanza, devi completare quanto segue:

Prerequisiti

- Crea un Simple AD Per saperne di più, vediCrea il tuo Simple AD.
- Avrai bisogno delle seguenti autorizzazioni IAM per unirti senza problemi a un' EC2Windowsistanza:
  - Profilo di istanza IAM con le seguenti autorizzazioni IAM:
    - `AmazonSSMManagedInstanceCore`
    - `AmazonSSMDirectoryServiceAccess`
  - Il dominio utente che si unisce perfettamente a Simple EC2 AD necessita delle seguenti autorizzazioni IAM:
    - Directory ServiceAutorizzazioni:
      - `"ds:DescribeDirectories"`
      - `"ds:CreateComputer"`
    - Autorizzazioni Amazon VPC:
      - `"ec2:DescribeVpcs"`
      - `"ec2:DescribeSubnets"`

    - `"ec2:DescribeNetworkInterfaces"`
    - `"ec2:CreateNetworkInterface"`
    - `"ec2:AttachNetworkInterface"`
  - EC2 Autorizzazioni:
    - `"ec2:DescribeInstances"`
    - `"ec2:DescribeImages"`
    - `"ec2:DescribeInstanceTypes"`
    - `"ec2:RunInstances"`
    - `"ec2:CreateTags"`
  - AWS Systems ManagerAutorizzazioni:
    - `"ssm:DescribeInstanceInformation"`
    - `"ssm:SendCommand"`
    - `"ssm:GetCommandInvocation"`
    - `"ssm:CreateBatchAssociation"`

Quando viene creato Simple AD, viene creato un gruppo di sicurezza con regole in entrata e in uscita. Per ulteriori informazioni su queste regole e porte, consulta. Cosa viene creato con il tuo Simple AD Per aggiungere facilmente un dominio a un' EC2 Windowsistanza, il VPC su cui stai lanciando l'istanza deve consentire le stesse porte consentite nelle regole in entrata e in uscita del gruppo di sicurezza Simple AD.

- A seconda della sicurezza di rete e delle impostazioni del firewall, potrebbe esserti richiesto di consentire traffico in uscita aggiuntivo. Questo traffico sarebbe destinato a HTTPS (porta 443) verso i seguenti endpoint:

Endpoint	Ruolo
`ec2messages.` *`region`*`.amazonaws.com`	Crea ed elimina i canali di sessione con il servizio Session Manager. Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.

Endpoint	Ruolo
`ssm.region.amazonaws.com`	Endpoint per. AWS Systems Manager Session Manager Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ssmmessages. region.amazonaws.com`	Crea ed elimina i canali di sessione con il servizio Session Manager. Per ulteriori informazioni, consulta Endpoint e quote per AWS Systems Manager.
`ds.region.amazonaws.com`	Endpoint per. Directory Service Per ulteriori informazioni, consulta Disponibilità regionale per Directory Service.

- Ti consigliamo di utilizzare un server DNS che risolva il tuo nome di dominio Simple AD. A tale scopo, è possibile creare un set di opzioni DHCP. Per ulteriori informazioni, consulta Creazione di un set di opzioni DHCP per Simple AD.
  - Se scegli di non creare un set di opzioni DHCP, i tuoi server DNS saranno statici e configurati dal tuo Simple AD.

1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nella EC2 Dashboard, nella sezione Launch instance, scegli Launch instance.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per l' EC2 istanza di Windows.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivi per aggiungere una o più coppie chiave-valore di tag per organizzare, tracciare o controllare l'accesso per questa EC2 istanza.
6. Nella sezione Applicazione e immagine del sistema operativo (Amazon Machine Image), scegli Windows nel riquadro Guida rapida. Puoi modificare l'Amazon Machine Image (AMI) di Windows dall'elenco a discesa Amazon Machine Image (AMI).
7. Nella sezione Tipo di istanza, scegli il tipo di istanza che desideri utilizzare dall'elenco a discesa Tipo di istanza.

8. Nella sezione Coppia di chiavi (accesso), puoi scegliere se creare una nuova coppia di chiavi o selezionare una coppia di chiavi esistente.

   a. Per creare una nuova coppia di chiavi, scegli Crea nuova coppia di chiavi.

   b. Inserisci un nome per la coppia di chiavi e seleziona un'opzione per il Tipo di coppia di chiavi e il Formato del file della chiave privata.

   c. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegli .pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegli .ppk.

   d. Scegli crea coppia di chiavi.

   e. Il file della chiave privata viene automaticamente scaricato dal browser. Salvare il file della chiave privata in un luogo sicuro.

   > **Important**
   >
   > Questo è l'unico momento in cui salvare il file della chiave privata.

9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.

10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto il traffico esterno instradato a un gateway Internet. In caso contrario, non potrai connetterti in remoto all'istanza.

    Per ulteriori informazioni su come connettersi a un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.

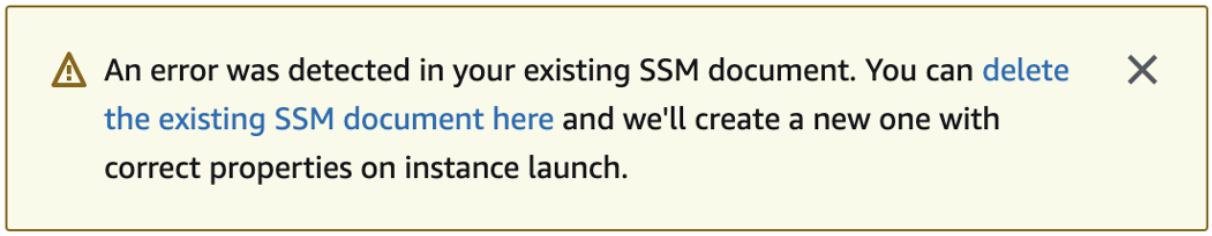
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta l'indirizzo IP delle EC2 istanze Amazon nella Amazon EC2 User Guide.

12. Nelle impostazioni Firewall (gruppi di sicurezza), puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.

13. Nelle impostazioni Configurazione dell'archiviazione, puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.

14. Seleziona la sezione Dettagli avanzati, scegli il tuo dominio dall'elenco a discesa Directory di aggiunta al dominio.

> **Note**
>
> Dopo aver scelto la directory di accesso al dominio, potresti vedere:
>
> 
>
>
> Questo errore si verifica se la procedura guidata di EC2 avvio identifica un documento SSM esistente con proprietà impreviste. Puoi effettuare una delle seguenti operazioni:
>
> - Se in precedenza hai modificato il documento SSM e le proprietà sono previste, scegli chiudi e procedi all'avvio dell' EC2 istanza senza modifiche.
> - Seleziona qui il link Elimina il documento SSM esistente per eliminare il documento SSM. Ciò consentirà la creazione di un documento SSM con le proprietà corrette. Il documento SSM verrà creato automaticamente all'avvio dell' EC2 istanza.

15. In Profilo dell'istanza IAM, puoi selezionare un profilo dell'istanza IAM esistente o crearne uno nuovo. Seleziona un profilo di istanza IAM a cui sono SSMDirectory ServiceAccess associate le policy AWS gestite Amazon SSMManaged InstanceCore e Amazon dall'elenco a discesa del profilo dell'istanza IAM. Per crearne uno nuovo, scegli il link Crea nuovo profilo IAM, quindi procedi come segue:

    1. Scegli Crea ruolo.
    2. In Seleziona entità attendibile, scegli Servizio AWS.
    3. In Use case (Caso d'uso), scegli EC2.
    4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le SSMDirectory ServiceAccess politiche di Amazon SSMManaged InstanceCore e Amazon. Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Scegli Next (Successivo).

    > **Note**
    >
    > Amazon SSMDirectory ServiceAccess fornisce le autorizzazioni per unire le istanze a un Active Directory gestito da. Directory Service Amazon SSMManaged InstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il AWS

Systems Manager servizio. Per ulteriori informazioni sulla creazione di un ruolo con queste autorizzazioni e per informazioni su altre autorizzazioni e policy che puoi assegnare al tuo ruolo IAM, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager.

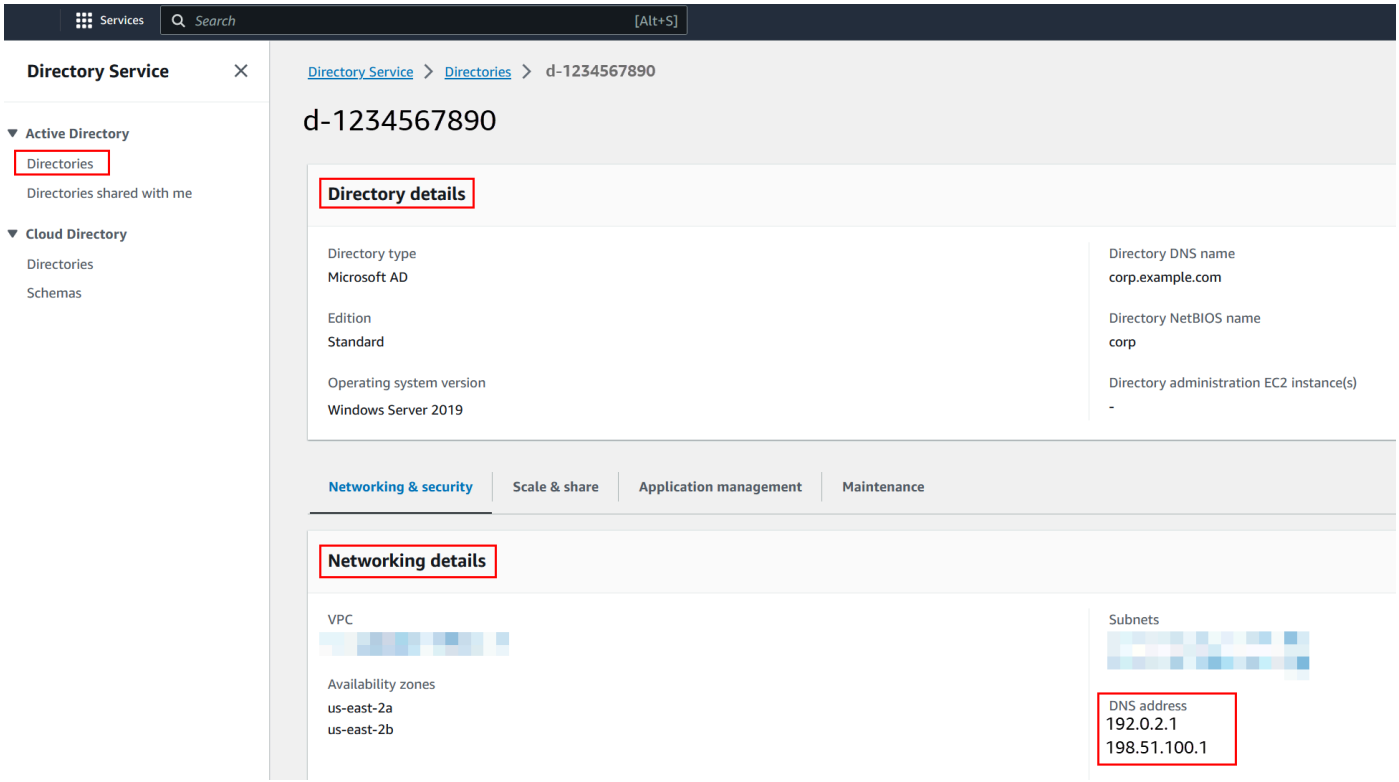
5. Nella pagina Denomina, rivedi e crea inserisci un Nome ruolo. Avrai bisogno di questo nome di ruolo da associare all' EC2istanza.
6. (Facoltativo) Puoi fornire una descrizione del profilo dell'istanza IAM nel campo Descrizione.
7. Scegli Crea ruolo.
8. Torna alla pagina Avvia un'istanza e scegli l'icona di aggiornamento accanto al profilo dell'istanza IAM. Il tuo nuovo profilo dell'istanza IAM dovrebbe essere visibile nell'elenco a discesa Profilo dell'istanza IAM. Scegli il nuovo profilo e lascia il resto delle impostazioni con i valori predefiniti.

16. Scegliere Launch Instance (Avvia istanza).

Manually join an EC2 Windows

Per aggiungere manualmente un'istanza Amazon EC2 Windows esistente a un Simple AD Active Directory, l'istanza deve essere avviata utilizzando i parametri specificati inUnire un'istanza Amazon EC2 Windows al tuo Simple AD Active Directory.

Avrai bisogno degli indirizzi IP dei server DNS Simple AD. Queste informazioni sono disponibili nelle sezioni Servizi di directory > Directory > ID directory relativo alla directory > Dettagli della directory e Rete e sicurezza.



Per aggiungere un'istanza di Windows a un Active Directory Simple AD

1. Connettiti all'istanza utilizzando qualsiasi client Remote Desktop Protocol.
2. Aprire la finestra di dialogo TCP/ IPv4 properties sull'istanza.
   a. Apri Network Connections (Connessioni di rete).

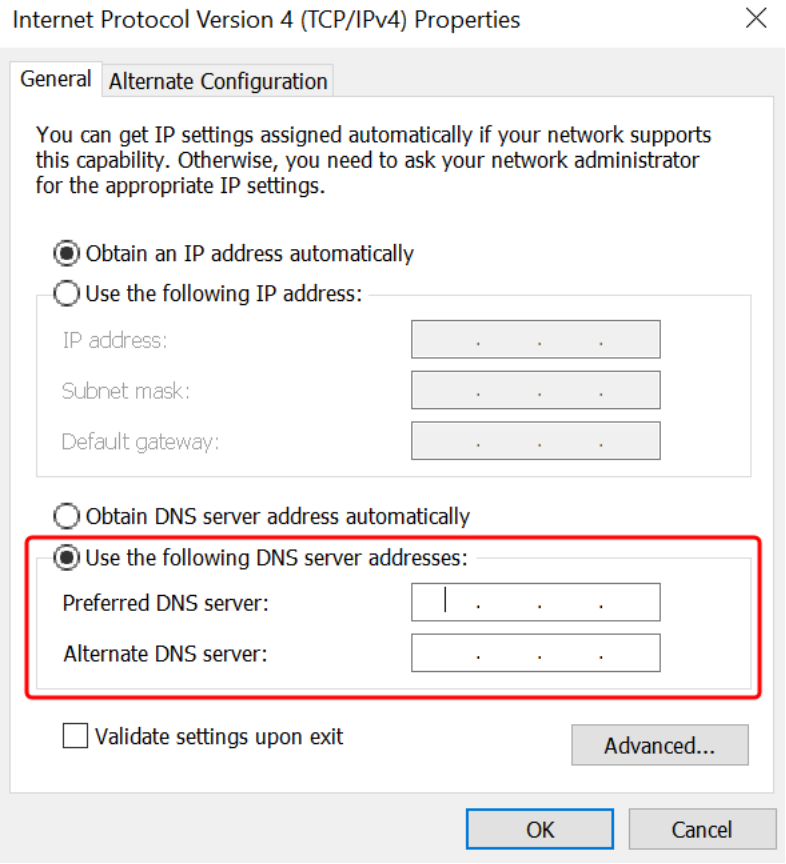
      Tip

      Puoi aprire le Network Connections (Connessioni di rete) direttamente eseguendo quanto segue da un prompt del comando sull'istanza.

      ```
      %SystemRoot%\system32\control.exe ncpa.cpl
      ```

   b. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per qualsiasi connessione di rete abilitata e scegli Properties (Proprietà).
   c. Nella finestra di dialogo delle proprietà di connessione, apri (doppio clic) Internet Protocol Version 4 (Protocollo Internet versione 4).

3. Seleziona Utilizza i seguenti indirizzi di server DNS, modifica gli indirizzi del server DNS preferito e del server DNS alternativo con gli indirizzi IP dei server DNS forniti da Simple AD e scegli OK.



4. Apri la finestra di dialogo System Properties (Proprietà del sistema) per l'istanza, seleziona la scheda Computer Name (Nome computer) e scegli Change (Modifica).

> **Tip**
>
> Puoi aprire la finestra di dialogo System Properties (Proprietà di sistema) direttamente eseguendo quanto segue da un prompt del comando sull'istanza.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Nel campo Membro di, seleziona Dominio, inserisci il nome completo del tuo Simple AD Active Directory e scegli OK.
6. Quando viene richiesto di specificare il nome e la password per l'amministratore del dominio, immetti il nome utente e la password di un account che dispone di privilegi di aggiunta di

dominio. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Simple AD.

> **Note**
>
> È possibile immettere il nome completo del dominio o il nome NetBIOS, seguito da una barra rovesciata (\) e quindi dal nome utente. Il nome utente sarebbe Administrator. Ad esempio **`corp.example.com\administrator`** o **`corp\administrator`**.

7. Dopo aver ricevuto il messaggio che ti invita al dominio, riavvia l'istanza perché le modifiche diventino effettive.

Ora che l'istanza è stata aggiunta al dominio Simple AD Active Directory, puoi accedere all'istanza in remoto e installare le utilità per gestire la directory, ad esempio aggiungere utenti e gruppi. Gli strumenti di amministrazione di Active Directory possono essere utilizzati per creare utenti e gruppi. Per ulteriori informazioni, consulta Installazione degli strumenti di amministrazione di Active Directory per Simple AD.

Unisci un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory

Puoi avviare e aggiungere un'istanza Amazon EC2 Linux al tuo Simple AD inConsole di gestione AWS. Puoi anche aggiungere manualmente un'istanza EC2 Linux al tuo Simple AD.

Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le distribuzioni precedenti a Ubuntu 14 e Red Hat Enterprise Linux 7 e 8 non supportano la funzionalità seamless domain join.

Modi per aggiungere un dominio a un'istanza EC2 Linux:

- Unisci senza problemi un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory
- Unisci manualmente un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory

Unisci senza problemi un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory

Questa procedura unisce senza problemi un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory.

Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64-bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le distribuzioni precedenti a Ubuntu 14 e Red Hat Enterprise Linux 7 e 8 non supportano la funzionalità seamless domain join.

Prerequisiti

Prima di poter configurare Seamless Domain Join su un'istanza Linux, è necessario completare le procedure descritte in questa sezione.

Selezione dell'account del servizio di aggiunta ottimizzata del dominio

Puoi aggiungere in modo ottimizzato computer Linux al tuo dominio Simple AD. A tale scopo, devi creare un account utente con le autorizzazioni di creazione di account di computer per aggiungere i computer al dominio. Sebbene i membri degli Amministratori di dominio o di altri gruppi possano disporre di privilegi sufficienti per aggiungere computer al dominio, questa operazione non è consigliata. Come procedura consigliata, suggeriamo di utilizzare un account del servizio con i privilegi minimi necessari per aggiungere i computer al dominio.

Per informazioni su come elaborare e delegare le autorizzazioni all'account del servizio per la creazione di account del computer, consulta Delegare privilegi all'account del servizio.

Creazione dei segreti per archiviare l'account del servizio di dominio

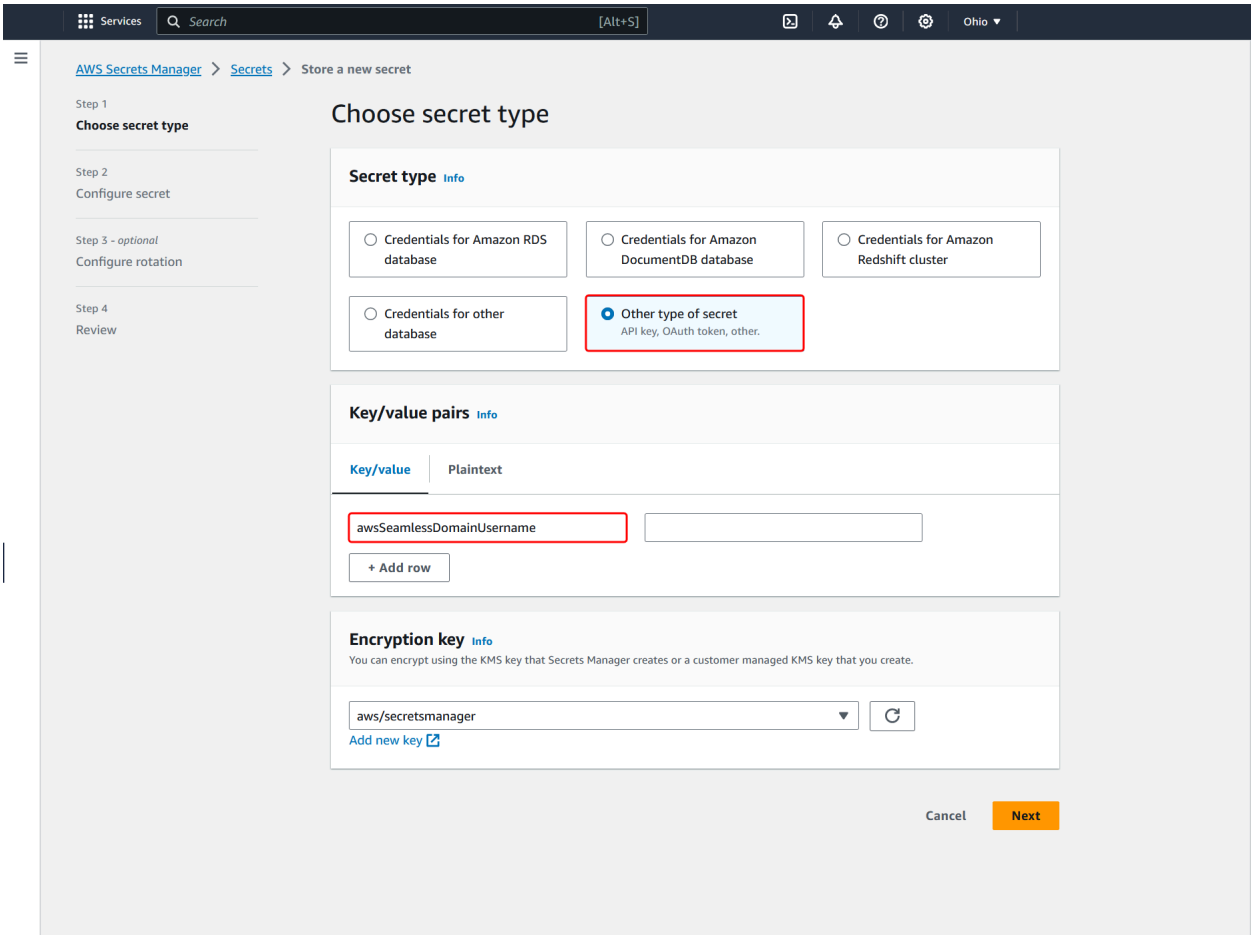
È possibile utilizzare Gestione dei segreti AWS per archiviare l'account del servizio di dominio. Per ulteriori informazioni, consulta Creare un Gestione dei segreti AWS segreto.

> **Note**
>
> Secrets Manager è a pagamento. Per ulteriori informazioni, consulta la sezione Prezzi nella Guida Gestione dei segreti AWS per l'utente.

Per creare segreti e archiviare le informazioni sull'account del servizio di dominio

1. Accedi Console di gestione AWS e apri la Gestione dei segreti AWS console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Archivia un nuovo segreto, procedere nel seguente modo:
    a. In Tipo segreto, scegli Altro tipo di segreti.
    b. In Coppie chiave/valore, procedi come segue:
        i. Nella prima casella, inserisci **`awsSeamlessDomainUsername`**. Nella stessa riga, nella casella successiva, inserisci il nome utente per il tuo account di servizio. Ad esempio, se hai utilizzato il PowerShell comando in precedenza, il nome dell'account del servizio sarebbe**`awsSeamlessDomain`**.

> **Note**
>
> Devi inserire **`awsSeamlessDomainUsername`** esattamente come è. Assicurati che non vi siano spazi iniziali o finali. In caso contrario, l'aggiunta del dominio avrà esito negativo.



ii. Scegli Aggiungi riga.

iii. Nella nuova riga, nella prima casella, inserisci **`awsSeamlessDomainPassword`**. Nella stessa riga, nella casella successiva, inserisci la password per il tuo account del servizio.

> **Note**
>
> Devi inserire **awsSeamlessDomainPassword** esattamente come è. Assicurati che non vi siano spazi iniziali o finali. In caso contrario, l'aggiunta del dominio avrà esito negativo.

iv. In Chiave di crittografia, lascia il valore predefinito`aws/secretsmanager`. Gestione dei segreti AWScrittografa sempre il segreto quando scegli questa opzione. Puoi anche scegliere una chiave creata da te.

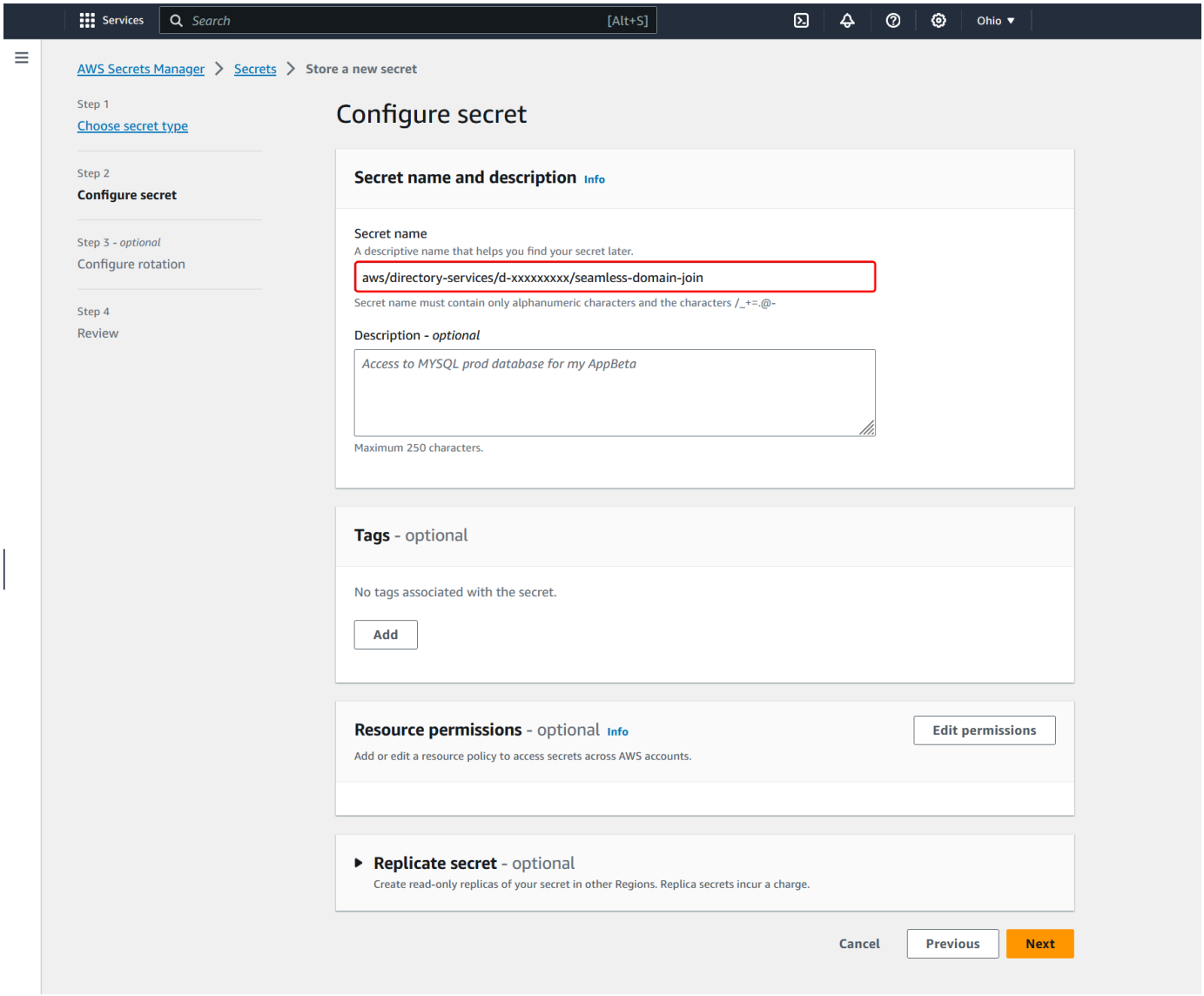
v. Scegli Next (Successivo).

4. In Nome segreto, inserisci un nome segreto che includa l'ID della tua directory utilizzando il seguente formato, sostituendolo *d-xxxxxxxxx* con il tuo ID di directory:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Questo nome viene utilizzato per recuperare i segreti nell'applicazione.

> **Note**
>
> Devi inserirlo **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** esattamente così com'è, ma sostituirlo *d-xxxxxxxxx* con l'ID della tua directory. Assicurati che non vi siano spazi iniziali o finali. In caso contrario, l'aggiunta del dominio avrà esito negativo.



5. Lascia tutto il resto impostato sui valori predefiniti, quindi scegli Avanti.
6. In Configura rotazione automatica, lascia selezionata Disabilita rotazione automatica e scegli Successivo.

   Puoi attivare la rotazione di questo segreto dopo averlo archiviato.
7. Controlla le impostazioni, quindi scegli Archivia per salvare le modifiche. La console Secrets Manager restituisce l'elenco dei segreti nel tuo account con il nuovo segreto ora incluso nell'elenco.
8. Scegli il nome segreto appena creato dall'elenco e prendi nota del valore ARN segreto. Lo utilizzerai nella sezione successiva.

Attiva la rotazione per il segreto dell'account del servizio di dominio

Ti consigliamo di modificare regolarmente i segreti per migliorare il tuo livello di sicurezza.

Per attivare la rotazione per il segreto dell'account del servizio di dominio

- Segui le istruzioni in Configurare la rotazione automatica per Gestione dei segreti AWS i segreti nella Guida per l'Gestione dei segreti AWSutente.

  Per il passaggio 5, utilizzare il modello di rotazione Microsoft Active Directory credenziali nella Guida per l'Gestione dei segreti AWSutente.

  Per assistenza, consulta Risoluzione dei problemi di Gestione dei segreti AWS rotazione nella Guida per l'Gestione dei segreti AWSutente.

Creazione della policy e del ruolo IAM richiesti

Utilizza i seguenti passaggi preliminari per creare una policy personalizzata che consenta l'accesso in sola lettura al tuo Secrets Manager seamless domain join secret (che hai creato in precedenza) e per creare un nuovo ruolo Linux IAM. EC2 DomainJoin

Creazione della policy di lettura IAM di Secrets Manager

Utilizzi la console IAM per creare una policy che conceda l'accesso in sola lettura al segreto di Secrets Manager.

Per creare la policy di lettura IAM di Secrets Manager

1. Accedi Console di gestione AWS come utente autorizzato a creare policy IAM. Quindi apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro di navigazione, Gestione degli accessi, scegli Politiche.
3. Scegli Crea policy.
4. Seleziona la scheda JSON e copia il testo dal documento della seguente policy JSON. Quindi incollalo nella casella di testo JSON.

> **Note**
>
> Assicurati di sostituire l'ARN della regione e della risorsa con la regione e l'ARN effettivi del segreto che hai creato in precedenza.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. Quando hai terminato, seleziona Successivo. In Validatore di policy vengono segnalati eventuali errori di sintassi. Per ulteriori informazioni, consulta Convalida delle policy IAM.
6. Nella pagina Verifica policy, inserisci un nome per la policy, ad esempio **`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. Consulta la sezione Riepilogo per visualizzare le autorizzazioni concesse dalla policy. Seleziona Crea policy per salvare le modifiche. La nuova policy appare nell'elenco delle policy gestite ed è pronta a collegarsi a un'identità.

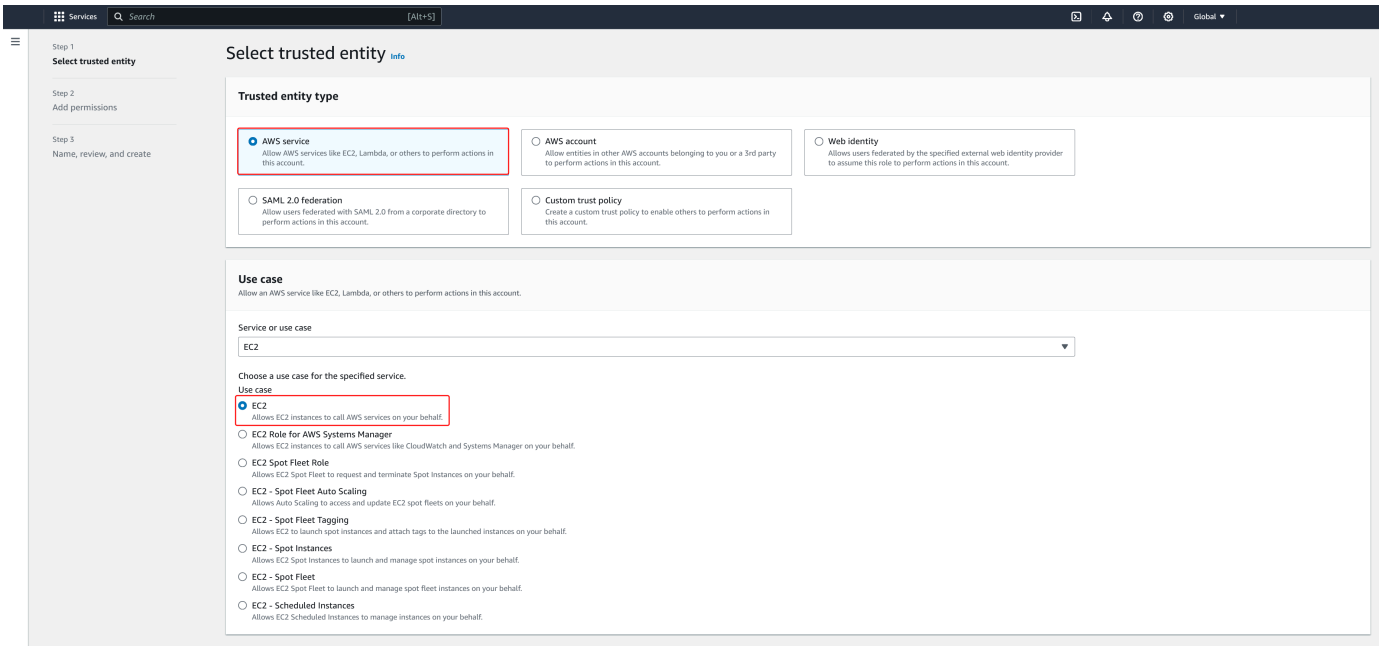
> **Note**
>
> Consigliamo di creare una policy per ogni segreto. In questo modo, ti assicuri che le istanze abbiano accesso solo al segreto in questione e riduci al minimo l'impatto se un'istanza viene compromessa.

Crea il ruolo Linux EC2 DomainJoin

Utilizzi la console IAM per creare il ruolo che utilizzerai per aggiungere il dominio alla tua EC2 istanza Linux.

Per creare il EC2 DomainJoin ruolo Linux

1. Accedi Console di gestione AWS come utente autorizzato a creare policy IAM. Quindi apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione, in Gestione degli accessi, scegli Ruoli.
3. Nel riquadro del contenuto seleziona Crea ruolo.
4. In Select type of trusted entity (Seleziona tipo di entità attendibile), scegli AWS service (Servizio).
5. In Caso d'uso, scegli EC2, quindi scegli Avanti.



6. In Filtra policy, procedi come segue:

   a. Specificare **`AmazonSSMManagedInstanceCore`**. Dopodiché, seleziona la casella di controllo per tale elemento nell'elenco.

   b. Specificare **`AmazonSSMDirectoryServiceAccess`**. Dopodiché, seleziona la casella di controllo per tale elemento nell'elenco.

   c. Inserisci **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** (o il nome della policy creata nella procedura precedente). Dopodiché, seleziona la casella di controllo per tale elemento nell'elenco.

   d. Dopo aver aggiunto le tre politiche sopra elencate, seleziona Crea ruolo.

> **Note**
>
> Amazon SSMDirectory ServiceAccess fornisce le autorizzazioni per unire le istanze a un Active Directory gestito da. Directory Service Amazon SSMManaged InstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il AWS Systems Manager servizio. Per ulteriori informazioni sulla creazione di un ruolo con queste autorizzazioni e per informazioni su altre autorizzazioni e policy che puoi assegnare al tuo ruolo IAM, consulta Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager.

7. Inserisci un nome per il tuo nuovo ruolo, ad esempio **`LinuxEC2DomainJoin`** o un altro nome che preferisci nel campo Nome del ruolo.
8. (Facoltativo) Per Role Description (Descrizione ruolo), immetti una descrizione.
9. (Facoltativo) Scegli Aggiungi nuovo tag nel Passaggio 3: Aggiungi tag per aggiungere tag. Le coppie chiave-valore dei tag vengono utilizzate per organizzare, tracciare o controllare l'accesso per questo ruolo.
10. Scegli Crea ruolo.

Unisci senza problemi un'istanza Linux al tuo Simple AD Active Directory

Per unire senza problemi la tua istanza Linux

1. Accedi a Console di gestione AWS e apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal selettore della regione nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nella EC2 Dashboard, nella sezione Launch instance, scegli Launch instance.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua EC2 istanza Linux.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivi per aggiungere una o più coppie chiave-valore di tag per organizzare, tracciare o controllare l'accesso per questa EC2 istanza.
6. Nella sezione Applicazione e immagine del sistema operativo (Amazon Machine Image), scegli un'AMI Linux che desideri avviare.

> **Note**
>
> L'AMI utilizzato deve avere AWS Systems Manager (SSM Agent) la versione 2.3.1644.0 o successiva. Per verificare la versione dell'Agente SSM installata nell'AMI avviando un'istanza da quest'ultima, consulta Ottenere la versione dell'Agente SSM attualmente installata. Se è necessario aggiornare l'agente SSM, vedere Installazione e configurazione dell'agente SSM su istanze per Linux. EC2
> SSM utilizza il `aws:domainJoin` plug-in quando aggiunge un'istanza Linux a un dominio Active Directory. Il plugin cambia il nome host per le istanze Linux nel formato EC2 AMAZ-. *XXXXXXX* Per ulteriori informazioni in merito*`aws:domainJoin`*, consultate AWS Systems ManagerCommand Document Plugin reference nella Guida per l'AWS Systems Managerutente.

7. Nella sezione Tipo di istanza, scegli il tipo di istanza che desideri utilizzare dall'elenco a discesa Tipo di istanza.
8. Nella sezione Coppia di chiavi (accesso), puoi scegliere se creare una nuova coppia di chiavi o selezionare una coppia di chiavi esistente. Per creare una nuova coppia di chiavi, scegli Crea nuova coppia di chiavi. Inserisci un nome per la coppia di chiavi e seleziona un'opzione per il Tipo di coppia di chiavi e il Formato del file della chiave privata. Per salvare la chiave privata in un formato che può essere utilizzato con OpenSSH, scegli .pem. Per salvare la chiave privata in un formato che può essere utilizzato con PuTTY, scegli .ppk. Scegli crea coppia di chiavi. Il file della chiave privata viene automaticamente scaricato dal browser. Salvare il file della chiave privata in un luogo sicuro.

> **Important**
>
> Questo è l'unico momento in cui salvare il file della chiave privata.

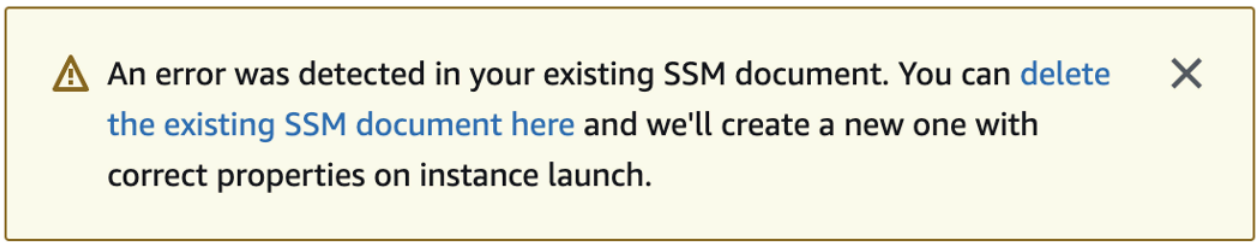
9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto il traffico esterno instradato a un gateway Internet. In caso contrario, non potrai connetterti in remoto all'istanza.

    Per ulteriori informazioni su come connettersi a un gateway Internet, consulta Eseguire la connessione a Internet utilizzando un gateway Internet nella Guida per l'utente di Amazon VPC.

11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta l'indirizzo IP delle EC2 istanze Amazon nella Amazon EC2 User Guide.

12. Nelle impostazioni Firewall (gruppi di sicurezza), puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
13. Nelle impostazioni Configurazione dell'archiviazione, puoi utilizzare le impostazioni predefinite o apportare modifiche per soddisfare le tue esigenze.
14. Seleziona la sezione Dettagli avanzati, scegli il tuo dominio dall'elenco a discesa Directory di aggiunta al dominio.

> **Note**
>
> Dopo aver scelto la directory di accesso al dominio, potresti vedere:
>
> 
>
>
> Questo errore si verifica se la procedura guidata di EC2 avvio identifica un documento SSM esistente con proprietà impreviste. Puoi effettuare una delle seguenti operazioni:
>
> - Se in precedenza hai modificato il documento SSM e le proprietà sono previste, scegli chiudi e procedi all'avvio dell' EC2 istanza senza modifiche.
> - Seleziona qui il link Elimina il documento SSM esistente per eliminare il documento SSM. Ciò consentirà la creazione di un documento SSM con le proprietà corrette. Il documento SSM verrà creato automaticamente all'avvio dell' EC2 istanza.

15. Per il profilo dell'istanza IAM, scegli il ruolo IAM creato in precedenza nella sezione dei prerequisiti Step 2: Creazione del ruolo Linux EC2 DomainJoin .
16. Scegliere Launch Instance (Avvia istanza).

> **Note**
>
> Se stai eseguendo l'aggiunta ottimizzata di un dominio con SUSE Linux, è necessario un riavvio prima che le autenticazioni funzionino. Per riavviare SUSE dal terminale Linux, digita sudo reboot.

Unisci manualmente un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory

Oltre alle istanze Amazon EC2 Windows, puoi anche aggiungere determinate istanze Amazon EC2 Linux al tuo Simple AD Active Directory. Sono supportate le seguenti distribuzioni e versioni di istanze Linux:

- AMI Amazon Linux 2018.03.0
- Amazon Linux 2 (64-bit x86)
- AMI Amazon Linux 2023
- Red Hat Enterprise Linux 8 (HVM) (64-bit x86)
- Ubuntu Server 18.04 LTS e Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Le altre distribuzioni e versioni di Linux potrebbero non funzionare, sebbene non siano state testate.

Prerequisiti

Prima di poter collegare un'istanza Amazon Linux, CentOS, Red Hat o Ubuntu alla tua directory, l'istanza deve essere avviata come specificato in Unisci senza problemi un'istanza Amazon EC2 Linux al tuo Simple AD Active Directory.

> **Important**
>
> Alcune delle procedure seguenti, se non eseguite correttamente, possono rendere l'istanza non raggiungibile o inutilizzabile. Pertanto, ti consigliamo vivamente di effettuare un backup o effettuare uno snapshot dell'istanza prima di eseguire queste procedure.

Per collegare un'istanza Linux alla tua directory

Segui i passaggi descritti per l'istanza Linux specifica utilizzando una delle seguenti schede:

Amazon Linux

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP dei server DNS dei server DNS Directory Service forniti. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza di Amazon Linux a 64 bit sia aggiornata.

   ```
   sudo yum -y update
   ```

4. Installa i pacchetti Amazon Linux necessari sull'istanza Linux.

   > **Note**
   >
   > Alcuni di questi pacchetti potrebbero essere già installati.
   > Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

   Amazon Linux

   ```
   sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
    krb5-workstation
   ```

> **Note**
>
> Per assistenza nella determinazione della versione di Amazon Linux che stai utilizzando, consulta Identificazione delle immagini Amazon Linux nella Amazon EC2 User Guide for Linux Instances.

5. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

6. Imposta il servizio SSH per permettere l'autenticazione della password.
   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

```
sudo vi /etc/ssh/sshd_config
```

   b. Imposta `PasswordAuthentication` su `yes`.

```
PasswordAuthentication yes
```

   c. Riavvia il servizio SSH.

```
sudo systemctl restart sshd.service
```

   In alternativa:

```
sudo service sshd restart
```

7. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi il gruppo di amministratori di dominio all'elenco dei sudoers seguendo la procedura seguente:

   a. Apri il file `sudoers` tramite il comando seguente:

   ```
   sudo visudo
   ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

CentOS

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP del server DNS dei server DNS Directory Service forniti. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza di CentOS 7 sia aggiornata.

   ```
   sudo yum -y update
   ```

4. Installa i pacchetti CentOS 7 necessari sull'istanza Linux.

   > **Note**
   >
   > Alcuni di questi pacchetti potrebbero essere già installati.

Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

6. Imposta il servizio SSH per permettere l'autenticazione della password.
   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

```
sudo vi /etc/ssh/sshd_config
```

   b. Imposta `PasswordAuthentication` su `yes`.

```
PasswordAuthentication yes
```

   c. Riavvia il servizio SSH.

```
sudo systemctl restart sshd.service
```

In alternativa:

```
sudo service sshd restart
```

7. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi il gruppo di amministratori di dominio all'elenco dei sudoers seguendo la procedura seguente:
   a. Apri il file `sudoers` tramite il comando seguente:

   ```
   sudo visudo
   ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

Red hat

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP del server DNS dei server DNS Directory Service forniti. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Red Hat - 64bit sia aggiornata.

   ```
   sudo yum -y update
   ```

4. Installa i pacchetti Red Hat necessari nell'istanza Linux.

   > **Note**
   >
   > Alcuni di questi pacchetti potrebbero essere già installati.

Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

Il AMAccountnome s di un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

6. Imposta il servizio SSH per permettere l'autenticazione della password.
   a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

```
sudo vi /etc/ssh/sshd_config
```

   b. Imposta `PasswordAuthentication` su `yes`.

```
PasswordAuthentication yes
```

   c. Riavvia il servizio SSH.

```
sudo systemctl restart sshd.service
```

In alternativa:

```
sudo service sshd restart
```

7. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi il gruppo di amministratori di dominio all'elenco dei sudoers seguendo la procedura seguente:

   a. Apri il file `sudoers` tramite il comando seguente:

   ```
   sudo visudo
   ```

   b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

Ubuntu

1. Connettiti all'istanza tramite qualsiasi client SSH.
2. Configura l'istanza Linux per utilizzare gli indirizzi IP dei server DNS dei server DNS Directory Service forniti. A tale scopo, puoi configurare l'istanza nel set di opzioni DHCP collegato al VPC o effettuare la configurazione manualmente sull'istanza. Se desideri impostarlo manualmente, consulta Come posso assegnare un server DNS statico a un' EC2 istanza Amazon privata nel AWS Knowledge Center per indicazioni sull'impostazione del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Ubuntu - 64bit sia aggiornata.

   ```
   sudo apt-get update
   sudo apt-get -y upgrade
   ```

4. Installa i pacchetti Ubuntu necessari nell'istanza Linux.

   > **Note**
   >
   > Alcuni di questi pacchetti potrebbero essere già installati.

Quando installi i pacchetti, potrebbero essere visualizzate diverse schermate popup di configurazione. In generale, puoi lasciare vuoti i campi di queste schermate.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Disattivare la risoluzione DNS inversa e impostare l'area di autenticazione predefinita sul nome di dominio completo del dominio. Perché un realm possa funzionare, le istanze Ubuntu devono essere risolvibili in modo inverso nel DNS. In caso contrario, dovrai disabilitare il DNS inverso in /etc/krb5.conf come segue:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Collega l'istanza alla directory tramite il comando seguente.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

Il AMAccountnome s di un account nel *example.com* dominio che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delega dei privilegi di accesso alle directory per Managed AWS Microsoft AD.

example.com

Il nome completo del DNS della directory.

```
...
 * Successfully enrolled machine in realm
```

7. Imposta il servizio SSH per permettere l'autenticazione della password.

a. Apri il file `/etc/ssh/sshd_config` in un editor di testo.

```
sudo vi /etc/ssh/sshd_config
```

b. Imposta `PasswordAuthentication` su `yes`.

```
PasswordAuthentication yes
```

c. Riavvia il servizio SSH.

```
sudo systemctl restart sshd.service
```

In alternativa:

```
sudo service sshd restart
```

8. Dopo il riavvio dell'istanza, connettiti a essa tramite qualsiasi client SSH, quindi aggiungi il gruppo di amministratori di dominio all'elenco dei sudoers seguendo la procedura seguente:

a. Apri il file `sudoers` tramite il comando seguente:

```
sudo visudo
```

b. Aggiungi il codice seguente alla fine del file `sudoers` e salva il file.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(L'esempio precedente utilizza "\<space>" per creare il carattere di spazio di Linux).

> **Note**
>
> Quando si utilizza Simple AD, se crei un account utente su un'istanza Linux con l'opzione "Richiedi all'utente di modificare la password al primo accesso", tale utente non sarà in grado di modificare inizialmente la password utilizzando kpasswd. Per modificare la password la prima volta, un amministratore del dominio deve aggiornare la password utente tramite gli strumenti di gestione di Active Directory.

Gestione di account da un'istanza Linux

Per gestire gli account in Simple AD da un'istanza Linux, è necessario aggiornare file di configurazione specifici dell'istanza Linux come segue:

1. Imposta krb5_use_kdcinfo su False nel file/.conf. etc/sssd/sssd Esempio:

   ```
   [domain/example.com]
       krb5_use_kdcinfo = False
   ```

2. Perché la configurazione diventi effettiva, devi riavviare il servizio sssd:

   ```
   $ sudo systemctl restart sssd.service
   ```

   In alternativa, puoi usare:

   ```
   $ sudo service sssd start
   ```

3. Se si gestiscono utenti da un'istanza Linux CentOS, è anche necessario modificare il file /etc/smb.conf per includere:

   ```
   [global]
     workgroup = EXAMPLE.COM
     realm = EXAMPLE.COM
     netbios name = EXAMPLE
     security = ads
   ```

Limitazioni di accesso all'account

Poiché tutti gli account vengono definiti in Active Directory, per impostazione predefinita tutti gli utenti nella directory possono accedere all'istanza. Puoi permettere solo a utenti specifici di accedere all'istanza con ad_access_filter in sssd.conf. Esempio:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Indica che agli utenti è consentito solo l'accesso all'istanza se membri di un determinato gruppo.

cn

Il nome canonico del gruppo a cui è consentito l'accesso. In questo esempio, il nome del gruppo *admins* è.

ou

È l'unità organizzativa in cui si trova il gruppo di cui sopra. In questo esempio, l'unità organizzativa è*Testou*.

dc

È il componente di dominio del tuo dominio. In questo esempio, *example*.

dc

È un componente di dominio aggiuntivo. In questo esempio, *com*.

È necessario aggiungere manualmente ad_access_filter a /etc/sssd/sssd.conf.

Apri il file /etc/sssd/sssd.conf in un editor di testo.

```
sudo vi /etc/sssd/sssd.conf
```

A questo punto, il tuo sssd.conf potrebbe avere questo aspetto:

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

Perché la configurazione diventi effettiva, devi riavviare il servizio sssd:

```
sudo systemctl restart sssd.service
```

In alternativa, puoi usare:

```
sudo service sssd restart
```

Mappatura degli ID

La mappatura degli ID può essere eseguita con due metodi per mantenere un'esperienza unificata tra le identità UNIX/Linux User Identifier (UID) e Group Identifier (GID) e le identità SID (Windows e Active Directory Security Identifier). Questi metodi sono:

1. Centralizzato
2. Distribuito

> **Note**
>
> La mappatura centralizzata dell'identità degli utenti in Active Directory richiede l'interfaccia del sistema operativo portatile o POSIX.

Mappatura centralizzata delle identità degli utenti

Active Directory o un altro servizio LDAP (Lightweight Directory Access Protocol) fornisce UID e GID agli utenti Linux. In Active Directory, questi identificatori vengono memorizzati negli attributi degli utenti se l'estensione POSIX è configurata:

- UID: il nome utente Linux (String)
- Numero UID: il numero ID utente Linux (numero intero)
- Numero GID: il numero ID del gruppo Linux (numero intero)

Per configurare un'istanza Linux per utilizzare l'UID e il GID di Active Directory, impostali `ldap_id_mapping = False` nel file sssd.conf. Prima di impostare questo valore, verifica di aver aggiunto un UID, un numero UID e un numero GID agli utenti e ai gruppi in Active Directory.

Mappatura distribuita delle identità degli utenti

Se Active Directory non ha l'estensione POSIX o se scegli di non gestire centralmente la mappatura delle identità, Linux può calcolare i valori UID e GID. Linux utilizza l'identificatore di sicurezza (SID) univoco dell'utente per mantenere la coerenza.

Per configurare la mappatura distribuita degli ID utente, impostala `ldap_id_mapping = True` nel file sssd.conf.

Problemi comuni

Se lo impostil`dap_id_mapping = False`, a volte l'avvio del servizio SSSD fallirà. Il motivo di questo errore è dovuto al fatto che le modifiche UIDs non sono supportate. Ti consigliamo di eliminare la cache SSSD ogni volta che passi dalla mappatura degli ID agli attributi POSIX o dagli attributi POSIX alla mappatura degli ID. Per ulteriori dettagli sulla mappatura degli ID e sui parametri ldap_id_mapping, consultate la pagina man sssd-ldap (8) nella riga di comando di Linux.

Connect all'istanza Linux

Quando un utente effettua la connessione all'istanza tramite un client SSH, gli verrà richiesto di inserire il proprio nome utente. L'utente può immettere il nome utente nei formati `username@example.com` o `EXAMPLE\username` . La risposta apparirà simile alla seguente, a seconda della distribuzione Linux utilizzata:

Amazon Linux, Red Hat Enterprise Linux e CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01              Processes:           102
  Usage of /:   18.6% of 7.69GB   Users logged in:     2
  Memory usage: 16%               IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

Delega dei privilegi di accesso alle directory per Simple AD

Per unire un computer alla directory, devi disporre di un account con privilegi per aggiungere computer alla directory.

Con Simple AD, i membri del gruppo Amministratori di dominio dispongono di privilegi sufficienti per aggiungere computer alla directory.

Tuttavia, come best practice, dovresti utilizzare un account che disponga solo dei privilegi minimi necessari. La seguente procedura mostra come creare un nuovo gruppo denominato `Joiners` e delegare i privilegi necessari a questo gruppo per aggiungere i computer alla directory.

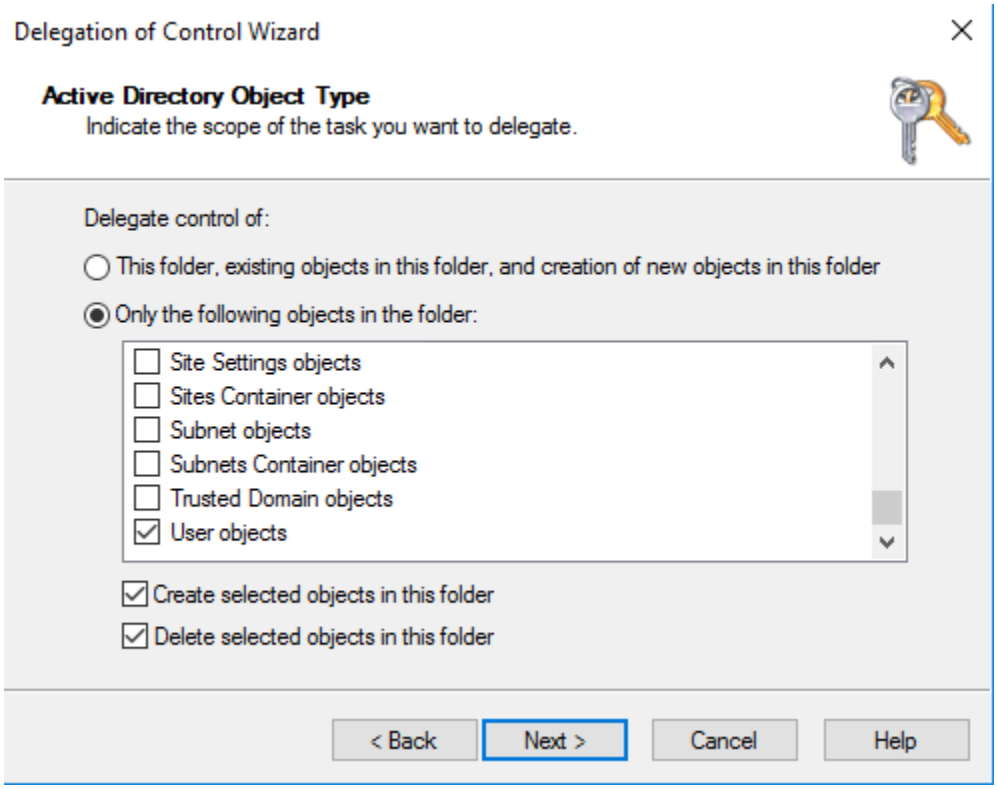
Devi eseguire questa procedura su un computer che è stato aggiunto alla directory e che abbia installato lo snap-in di MMC Utenti e computer di Active Directory. Inoltre, è necessario aver eseguito l'accesso come amministratore del dominio.

Per delegare i privilegi di aggiunta per Simple AD

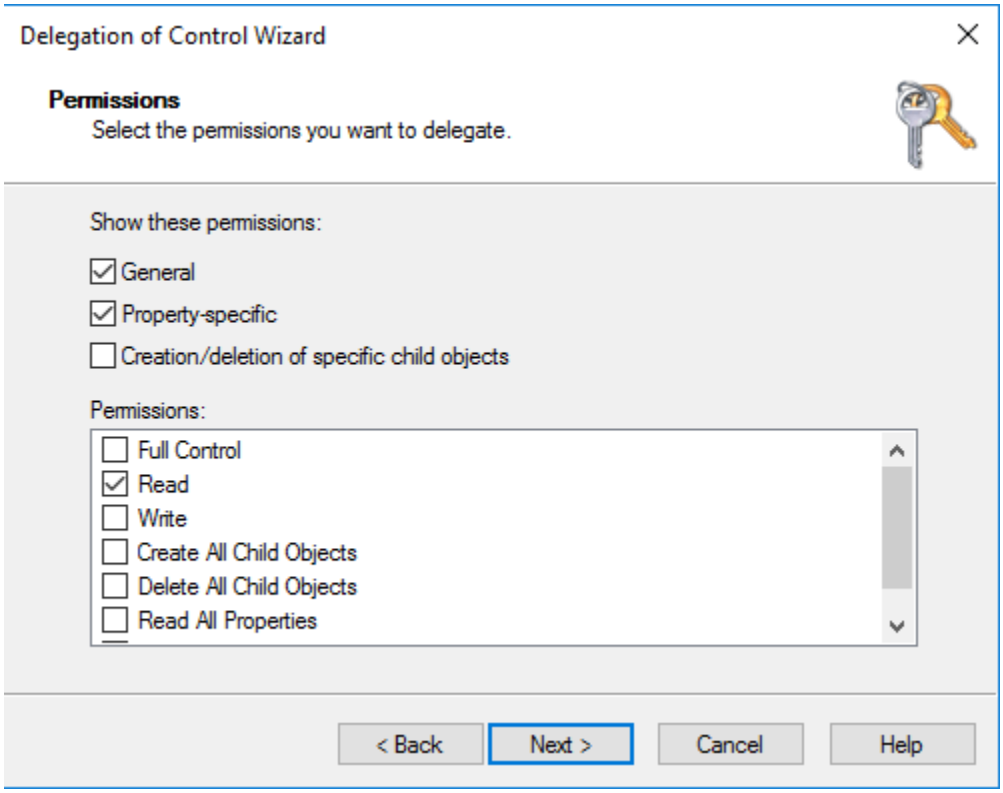
1. Apri Active Directory User and Computers (Utenti e computer di Active Directory) e seleziona la radice del dominio nell'albero di spostamento.
2. Nella struttura di navigazione a sinistra, fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida Users (Utenti), scegliere New (Nuovo), quindi Group (Gruppo).
3. Nella finestra New Object - Group (Nuovo oggetto - Gruppo), digita quanto segue e scegli OK.

- Per Group name (Nome gruppo), digita **`Joiners`**.
- In Group scope (Ambito del gruppo), scegli Global (Globale).
- Per Group type (Tipo gruppo), scegli Security (Sicurezza).

4. Nella struttura di navigazione, selezionare la radice del dominio. Nel menu Action (Operazione), scegli Delegate Control (Delega controllo).
5. Nella pagina Delegation of Control Wizard (Delega guidata del controllo), scegli Next (Avanti), quindi scegli Add (Aggiungi).
6. Nella finestra Select Users, Computers, or Groups (Seleziona utenti, computer o gruppi), digita `Joiners` e scegli OK. Se viene trovato più di un oggetto, selezionare il gruppo `Joiners` creato sopra. Scegli Next (Successivo).
7. Nella pagina Operazioni da delegare, selezionare Crea un'operazione personalizzata per eseguire la delega, quindi scegliere Avanti.
8. Seleziona Only the following objects in the folder (Solo i seguenti oggetti contenuti nella cartella), quindi Computer objects (Oggetti computer).
9. Selezionare Crea gli oggetti selezionati in questa cartella e Elimina gli oggetti selezionati in questa cartella. Quindi scegli Successivo.



10. Seleziona Read (Lettura) e Write (Scrittura), quindi scegli Next (Avanti).



11. Verificare le informazioni nella pagina Completing the Delegation of Control Wizard (Completamento della delega guidata del controllo) e scegli Finish (Termina).
12. Crea un utente con una password complessa e aggiungilo al gruppo `Joiners`. L'utente disporrà quindi di privilegi sufficienti per connettersi alla directory. Directory Service

Creazione di un set di opzioni DHCP per Simple AD

AWSconsiglia di creare un set di opzioni DHCP per la Directory Service directory e di assegnare le opzioni DHCP impostate al VPC in cui si trova la directory. Questo permette alle istanze in tale VPC di puntare al dominio e ai server DNS specificati per risolvere i propri nomi di dominio.

Per ulteriori informazioni sui set di opzioni DHCP, consulta Set di opzioni DHCP nella Guida per l'utente di Amazon VPC.

Creazione di un set opzioni DHCP per la tua directory

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel riquadro di navigazione, scegliere DHCP Options Sets (Set di opzioni DHCP), quindi selezionare Create DHCP options set (Crea set di opzioni DHCP).
3. Nella pagina Crea set di opzioni DHCP, fornisci i seguenti valori per la directory:

Nome

Un tag opzionale per il set di opzioni.

Nome dominio

Il nome completo della tua directory, ad esempio `corp.example.com`.

Server dei nomi di dominio (DNS)

Gli indirizzi IP dei server DNS della directory AWS fornita dall'utente.

> **Note**
>
> Puoi trovare questi indirizzi accedendo al riquadro di navigazione della console AWS Directory Service, selezionando Directory e quindi l'ID directory corretto.

Server NTP

Lasciare questo campo vuoto.

Server dei nomi NetBIOS

Lasciare questo campo vuoto.

Tipo di nodo NetBIOS

Lasciare questo campo vuoto.

4. Selezionare Create DHCP options set (Crea set di opzioni DHCP). Il nuovo set di opzioni DHCP viene visualizzato nell'elenco delle opzioni DHCP.
5. Prendi nota dell'ID del nuovo set di opzioni DHCP (dopt-). *xxxxxxxx* Devi utilizzarlo per associare il nuovo set di opzioni al tuo VPC.

Modifica del set opzioni DHCP associato a un VPC

Dopo aver creato un set di opzioni DHCP, non puoi modificarle. Se desideri che il tuo VPC utilizzi un altro set di opzioni DHCP, devi creare un nuovo set e associarlo al tuo VPC. Puoi anche impostare il tuo VPC senza utilizzare alcuna opzione DHCP.

1. Apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel riquadro di navigazione, scegli Your. VPCs
3. Seleziona il VPC, quindi scegli Azioni, Modifica impostazioni VPC.
4. Per il set di opzioni DHCP, seleziona un set di opzioni o scegli Nessun set di opzioni DHCP, quindi scegli Salva.

Per modificare il set di opzioni DHCP associato a un VPC utilizzando la riga di comando, vedere quanto segue:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Gestione di utenti e gruppi in Simple AD

Gli utenti possono essere individui singoli o entità che hanno accesso alla tua directory. I gruppi sono molto utili per concedere o negare privilegi ai gruppi di utenti, piuttosto che dover applicare tali privilegi a ogni singolo utente. Se un utente passa a un'altra organizzazione, sposta tale utente a un altro gruppo e riceverà automaticamente i privilegi necessari per la nuova organizzazione.

Per creare utenti e gruppi in una Directory Service directory, è necessario utilizzare qualsiasi istanza (locale o EC2) aggiunta alla Directory Service directory ed effettuare l'accesso come utente con privilegi per creare utenti e gruppi. È inoltre necessario installare gli strumenti di Active Directory sull' EC2istanza in modo da poter aggiungere utenti e gruppi con lo snap-in Utenti e computer di Active Directory. Per ulteriori informazioni su come configurare un' EC2 istanza e installare gli strumenti necessari, consultaModi per aggiungere un' EC2 istanza Amazon al tuo Simple AD.

> **Note**
>
> I tuoi account utente devono avere la preautenticazione Kerberos abilitata. Questa è l'impostazione predefinita per i nuovi account utente e non deve essere modificata. Per ulteriori informazioni su questa impostazione, vai a Preautenticazione su Microsoft TechNet.

Negli argomenti seguenti sono incluse istruzioni su come creare e gestire gli utenti e i gruppi.

Argomenti

- Installazione degli strumenti di amministrazione di Active Directory per Simple AD
- Creazione di un utente Simple AD

- Eliminazione di un utente Simple AD
- Reimpostazione di una password utente Simple AD
- Creazione di un gruppo Simple AD
- Aggiungere un utente Simple AD a un gruppo

Installazione degli strumenti di amministrazione di Active Directory per Simple AD

Per gestire Active Directory da un'istanza di Amazon EC2 Windows Server, devi installare gli strumenti Active Directory Domain Services e Active Directory Lightweight Directory Services sull'istanza. Utilizza la seguente procedura per installare questi strumenti su un'istanza EC2 Windows Server.

Prerequisiti

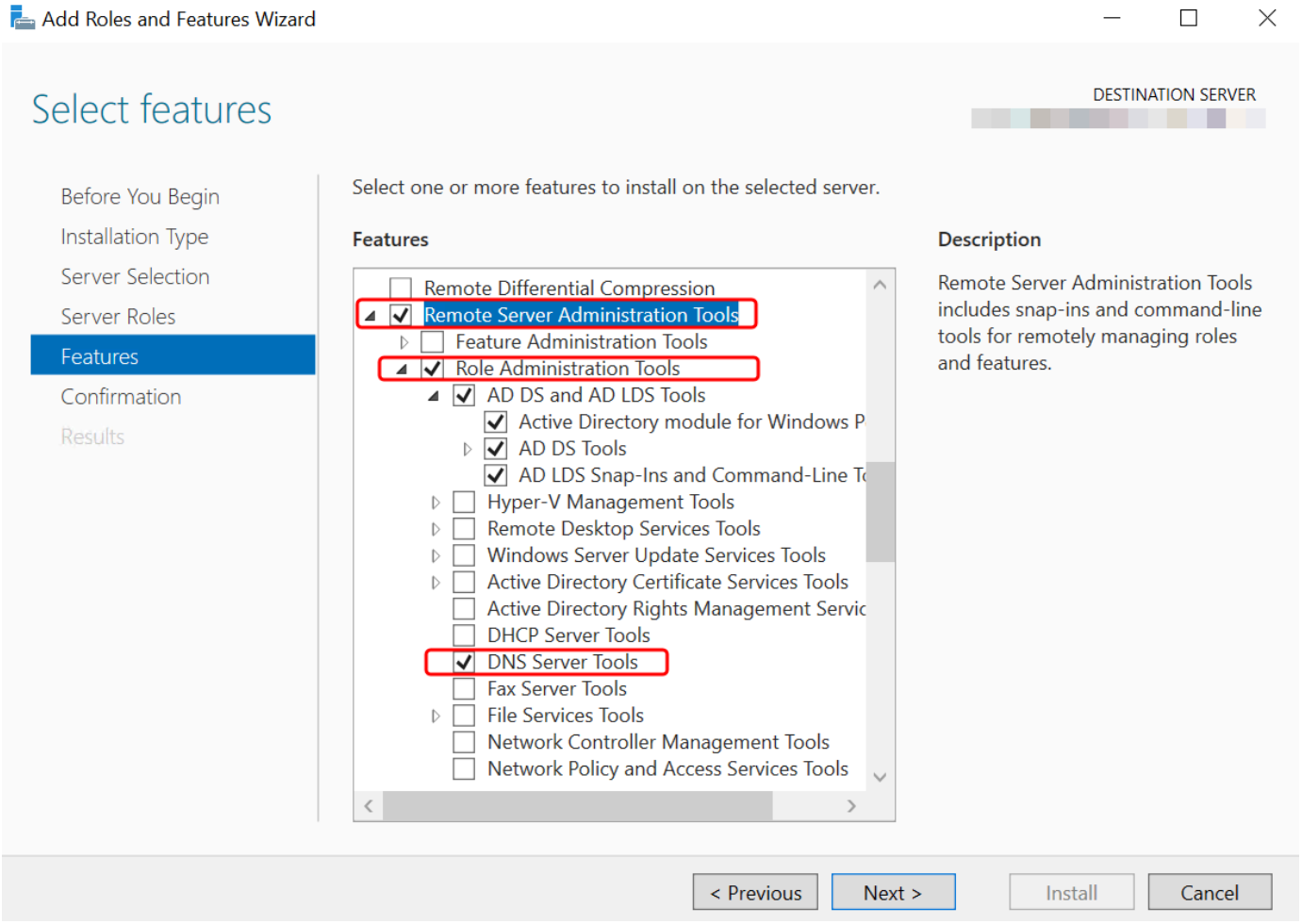
Prima di iniziare questa procedura, completa quanto segue:

1. Crea un Simple AD Active Directory. Per ulteriori informazioni, consulta Crea il tuo Simple AD.
2. Avvia e unisci un'istanza EC2 Windows Server al tuo Simple AD Active Directory. L' EC2 istanza necessita delle seguenti politiche per creare utenti e gruppi: **`AmazonSSMManagedInstanceCore`** e**`AmazonSSMDirectoryServiceAccess`**. Per ulteriori informazioni, consulta Unire un'istanza Amazon EC2 Windows al tuo Simple AD Active Directory.
3. Avrai bisogno delle credenziali per l'amministratore del dominio Active Directory. Queste credenziali sono state create al momento della creazione di Simple AD. Se hai seguito la procedura riportata inCrea il tuo Simple AD, il nome utente dell'amministratore include il nome NetBIOS,. **`corp\administrator`**

Per installare gli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

1. Apri la EC2 console Amazon all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella EC2 console Amazon, scegli Istanze, seleziona l'istanza di Windows Server, quindi scegli Connect.
3. Nella pagina Collega all'istanza, scegli Client RDP.
4. Nella scheda Client RDP, scegli Scarica il file del desktop remoto, quindi scegli Ottieni password per recuperare la password.

5. Nella sezione Ottieni la password di Windows, scegli Carica il file della chiave privata. Scegli il file della chiave privata .pem associato all'istanza di Windows Server. Dopo aver caricato il file della chiave privata, seleziona Decrittografa la password.
6. Nella finestra di dialogo Sicurezza di Windows, copia le credenziali di amministratore locale per il computer Windows Server a cui accedere. Il nome utente può avere i seguenti formati: ***NetBIOS-Name*****\administrator** o***DNS-Name*****\administrator**. Ad esempio, **corp \administrator** sarebbe il nome utente se hai seguito la procedura inCrea il tuo Simple AD.
7. Una volta effettuato l'accesso all'istanza di Windows Server, apri Server Manager dal menu Start scegliendo Server Manager.
8. Nel pannello di controllo Server Manager scegli Aggiungi ruoli e funzionalità.
9. In Aggiunta guidata ruoli e funzionalità scegliere Tipo di installazione, selezionare Installazione basata su ruoli o basata su funzionalità e scegliere Avanti.
10. In Selezione server verificare che sia selezionato il server locale, quindi scegliere Funzionalità nel riquadro di navigazione a sinistra.
11. Nell'albero Funzionalità, apri Strumenti di amministrazione remota del server, Strumenti di amministrazione del ruolo e Strumenti AD DS e AD LDS. Con AD DS e AD LDS Tools selezionati, vengono selezionati il modulo Active Directory per PowerShell, AD DS Tools, gli snap-in e gli strumenti da riga di comando di AD LDS. Scorri verso il basso e seleziona Strumenti server DNS, quindi scegli Successivo.



12. Verificare che le informazioni siano corrette e scegliere Installa. Quando l'installazione della funzionalità è terminata, Active Directory Domain Services e gli strumenti Active Directory Lightweight Directory Services sono disponibili nel menu Start nella cartella Strumenti di amministrazione.

Creazione di un utente Simple AD

Utilizza la seguente procedura per creare un utente con un' EC2 istanza Amazon aggiunta alla tua directory Simple AD. Prima di poter creare utenti, devi completare le procedure descritte in Installazione degli strumenti di amministrazione di Active Directory.

> **Note**
>
> Quando si utilizza Simple AD, se crei un account utente su un'istanza Linux con l'opzione "Richiedi all'utente di modificare la password al primo accesso", tale utente non sarà in grado di modificare inizialmente la password utilizzando kpasswd. Per modificare la password la

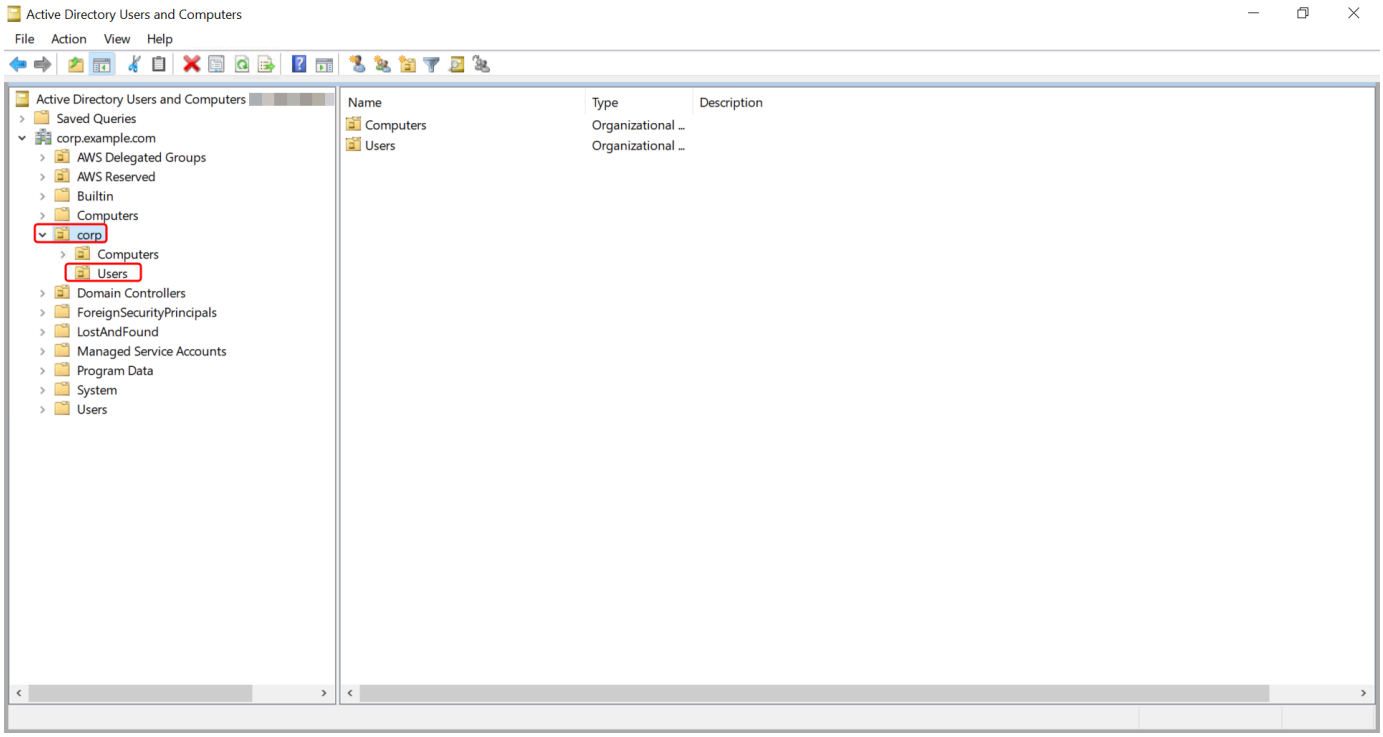
prima volta, un amministratore del dominio deve aggiornare la password utente tramite gli strumenti di gestione di Active Directory.

Creazione di un utente

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Apri lo strumento Utenti e computer di Active Directory dal menu Start di Windows. È disponibile un collegamento a questo strumento nella cartella Strumenti di amministrazione di Windows.

   > **Tip**
   >
   > Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Nell'albero delle directory, selezionare un'unità organizzativa sotto l'unità organizzativa con nome NetBIOS della directory in cui si desidera archiviare l'utente (ad esempio,**`corp\Users`**). Per ulteriori informazioni sulla struttura dell'unità organizzativa utilizzata dalle directory in AWS, vedere. Cosa viene creato con AWS Managed Microsoft AD



4. Nel menu Operazioni, scegli Nuovo, quindi Utente per aprire la nuova procedura guidata per un nuovo utente.
5. Nella prima pagina della procedura guidata, inserisci i valori per i campi seguenti, quindi scegli Successivo.
   - Nome
   - Cognome
   - User logon name (Nome di accesso dell'utente)
6. Nella seconda pagina della procedura guidata, inserisci una password temporanea in Password e Conferma password. Verifica che l'opzione L'utente deve modificare la password al prossimo accesso sia selezionata. Nessuna delle altre opzioni deve essere selezionata. Scegli Next (Successivo).
7. Nella terza pagina della procedura guidata, verifica che le informazioni del nuovo utente siano corrette e scegli Termina. Il nuovo utente verrà visualizzato nella cartella Users (Utenti).

Eliminazione di un utente Simple AD

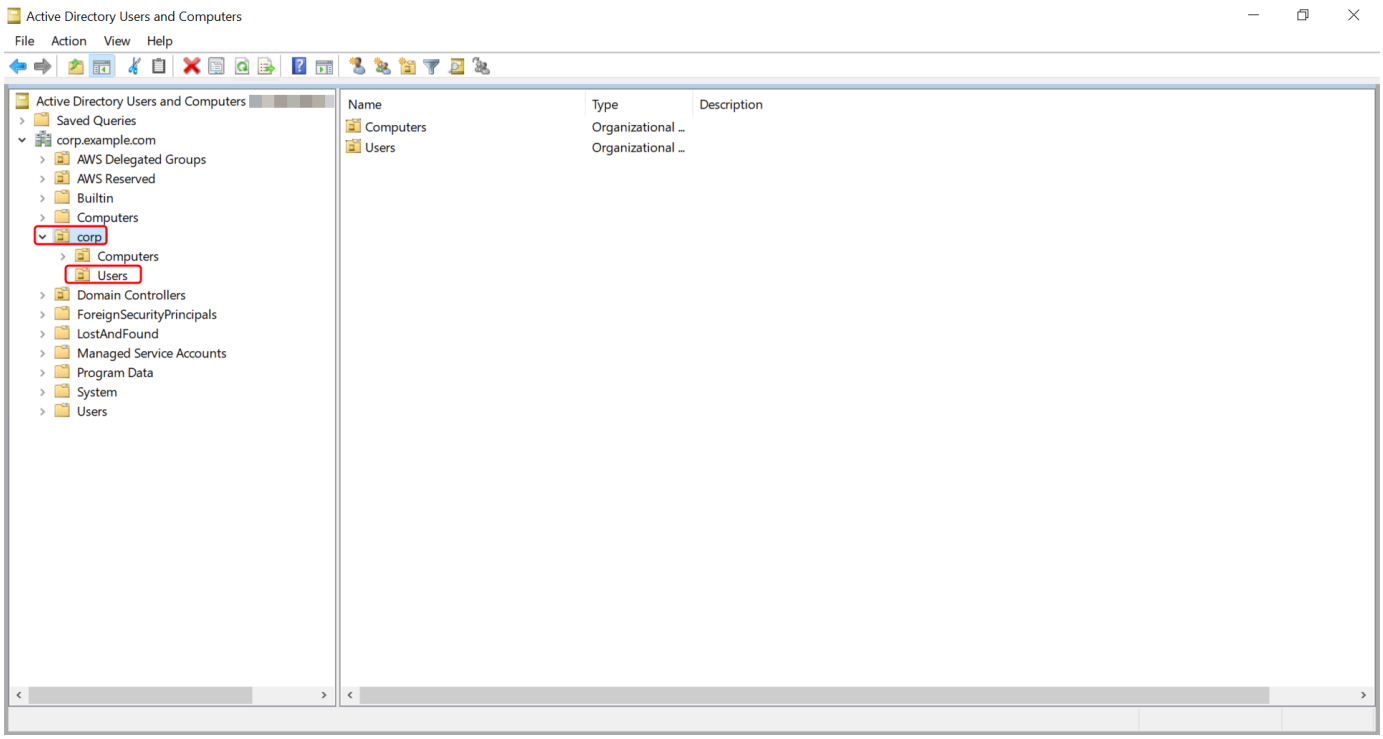
Utilizza la seguente procedura per eliminare un utente con un'istanza Amazon EC2 Windows aggiunta alla tua directory Simple AD.

Per eliminare un utente

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Apri lo strumento Utenti e computer di Active Directory dal menu Start di Windows. È disponibile un collegamento a questo strumento nella cartella Strumenti di amministrazione di Windows.

> **Tip**
>
> Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Nell'albero delle directory, selezionare l'unità organizzativa contenente l'utente che si desidera eliminare (ad esempio,**`corp\Users`**).



4. Seleziona l'utente che desideri eliminare. Dal menu Operazioni, scegli Elimina.
5. Viene visualizzata una finestra di dialogo che richiede di confermare se desideri eliminare l'utente. Scegli Sì per eliminare l'utente. Questa procedura elimina definitivamente l'utente selezionato.

Reimpostazione di una password utente Simple AD

Gli utenti devono rispettare le politiche in materia di password definite in Active Directory. A volte ciò può convincere gli utenti, incluso l'amministratore di Active Directory, a dimenticare la password. Quando ciò accade, puoi reimpostare rapidamente la password dell'utente utilizzando Directory Service if l'utente risiede in Simple AD.

Devi accedere come utente con le autorizzazioni necessarie per reimpostare le password. Per ulteriori informazioni sulle autorizzazioni, consultare Panoramica della gestione delle autorizzazioni di accesso alle risorse Directory Service.

Puoi reimpostare la password per qualsiasi utente in Active Directory con le seguenti eccezioni:

- È possibile reimpostare la password per qualsiasi utente all'interno dell'unità organizzativa (OU) basata sul nome NetBIOS utilizzato durante la creazione di Active Directory. Ad esempio, se si segue la procedura descritta inCrea il tuo Simple AD, il nome NetBIOS sarà CORP e le password degli utenti che è possibile reimpostare saranno membri dell'unità organizzativa. Corp/Users
- Non è possibile reimpostare la password di alcun utente al di fuori dell'unità organizzativa basata sul nome NetBIOS utilizzato durante la creazione di Active Directory. Per ulteriori informazioni sulla struttura dell'unità organizzativa per Simple AD, vedereCosa viene creato con il tuo Simple AD.
- Non è possibile reimpostare la password per nessun utente membro di due domini. Inoltre, non è possibile reimpostare la password di alcun utente membro del gruppo Domain Admins o Enterprise Admins, ad eccezione dell'utente Administrator.
- Non è possibile reimpostare la password per nessun utente membro del gruppo Domain Admins o Enterprise Admins ad eccezione dell'utente amministratore.

È possibile utilizzare uno dei seguenti metodi per reimpostare la password di un utente:

- Console di gestione AWS
- AWS CLI

Console di gestione AWS

1. Nel riquadro di navigazione della Directory Serviceconsole, in Active Directory, scegli Directory, quindi seleziona Active Directory nell'elenco in cui desideri reimpostare la password utente.

2. Nella pagina dei Dettagli della directory, scegli Operazioni, Reimposta password utente.
3. Nella finestra di dialogo Reimposta la password utente, in Nome utente digita il nome utente dell'utente la cui password deve essere modificata.
4. Digita una password in Nuova password e Conferma password, quindi scegli Reimposta password.

AWS CLI

1. Per installareAWS CLI, consulta Installare o aggiornare la versione più recente di AWS CLI.
2. Apri ilAWS CLI.
3. Digita il comando seguente e sostituisci l'ID di directory, il nome utente **`jane.doe`** e la password **`P@ssw0rd`** con l'ID di Active Directory e le credenziali desiderate. Per ulteriori informazioni reset-user-password, consulta la sezione AWS CLICommand Reference.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-password "P@ssw0rd"
```

Creazione di un gruppo Simple AD

Utilizza la seguente procedura per creare un gruppo di sicurezza con un' EC2 istanza Amazon aggiunta alla tua directory Simple AD. Prima di poter creare gruppi di sicurezza, è necessario completare le procedure descritte in Installazione degli strumenti di amministrazione di Active Directory.

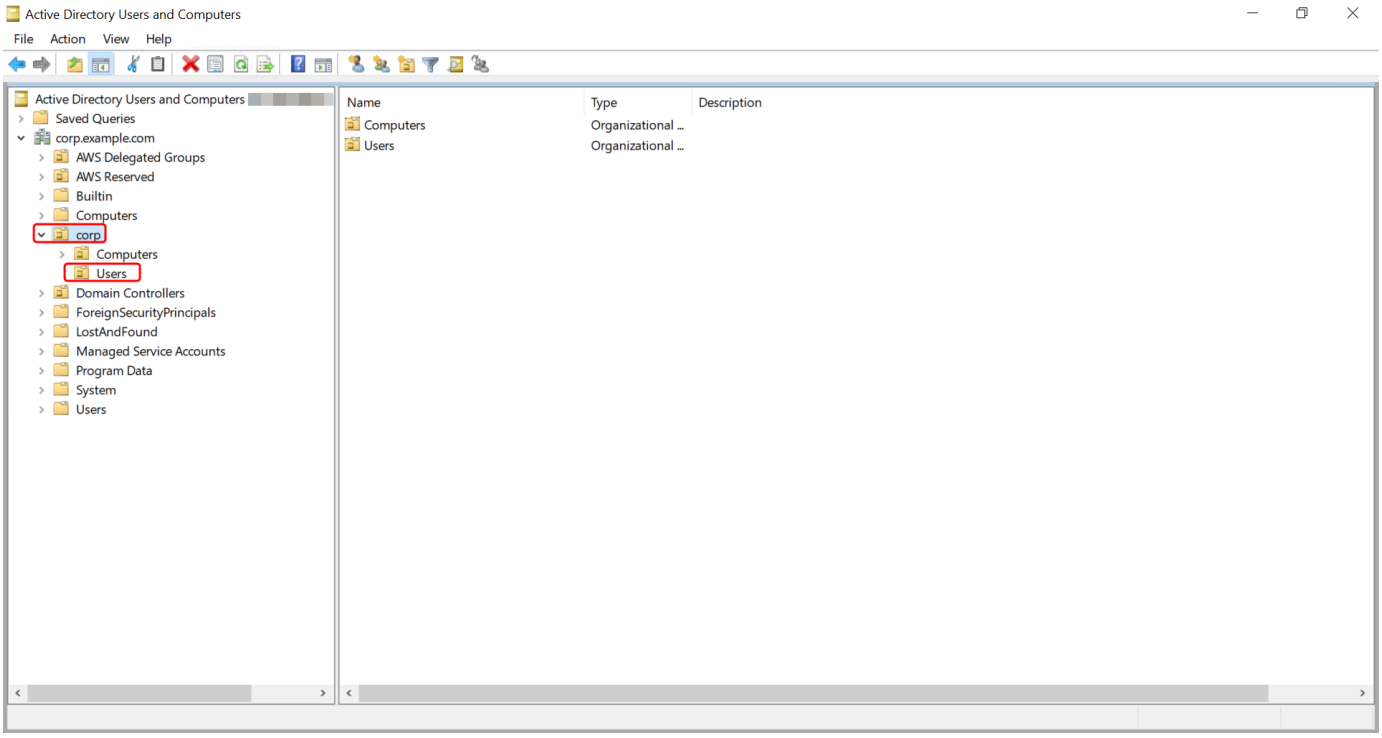
Creazione di un gruppo

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Apri lo strumento Utenti e computer di Active Directory. Trovi una scorciatoia a questo strumento nella cartella Administrative Tools (Strumenti amministrativi).

> **Tip**
>
> Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.

```
%SystemRoot%\system32\dsa.msc
```

3. Nell'albero delle directory, seleziona un'unità organizzativa sotto quella con nome NetBIOS della directory in cui desideri archiviare il gruppo (ad esempio, Corp\Users). Per ulteriori informazioni sulla struttura dell'unità organizzativa utilizzata dalle directory in AWS, consultaCosa viene creato con AWS Managed Microsoft AD.



4. Nel menu Action (Operazioni), fai clic su New (Nuovo), quindi fai clic su Group (Gruppo) per aprire la procedura guidata per un nuovo gruppo.
5. Digita un nome per il gruppo in Nome gruppo, seleziona un Ambito del gruppo che soddisfi le tue esigenze e seleziona Sicurezza per il Tipo di gruppo. Per ulteriori informazioni sull'ambito dei gruppi di Active Directory e sui gruppi di sicurezza, consulta Gruppi di sicurezza di Active Directory nella documentazione di Microsoft Windows Server.
6. Fai clic su OK. Il nuovo gruppo di sicurezza verrà visualizzato nella cartella Utenti.

Aggiungere un utente Simple AD a un gruppo

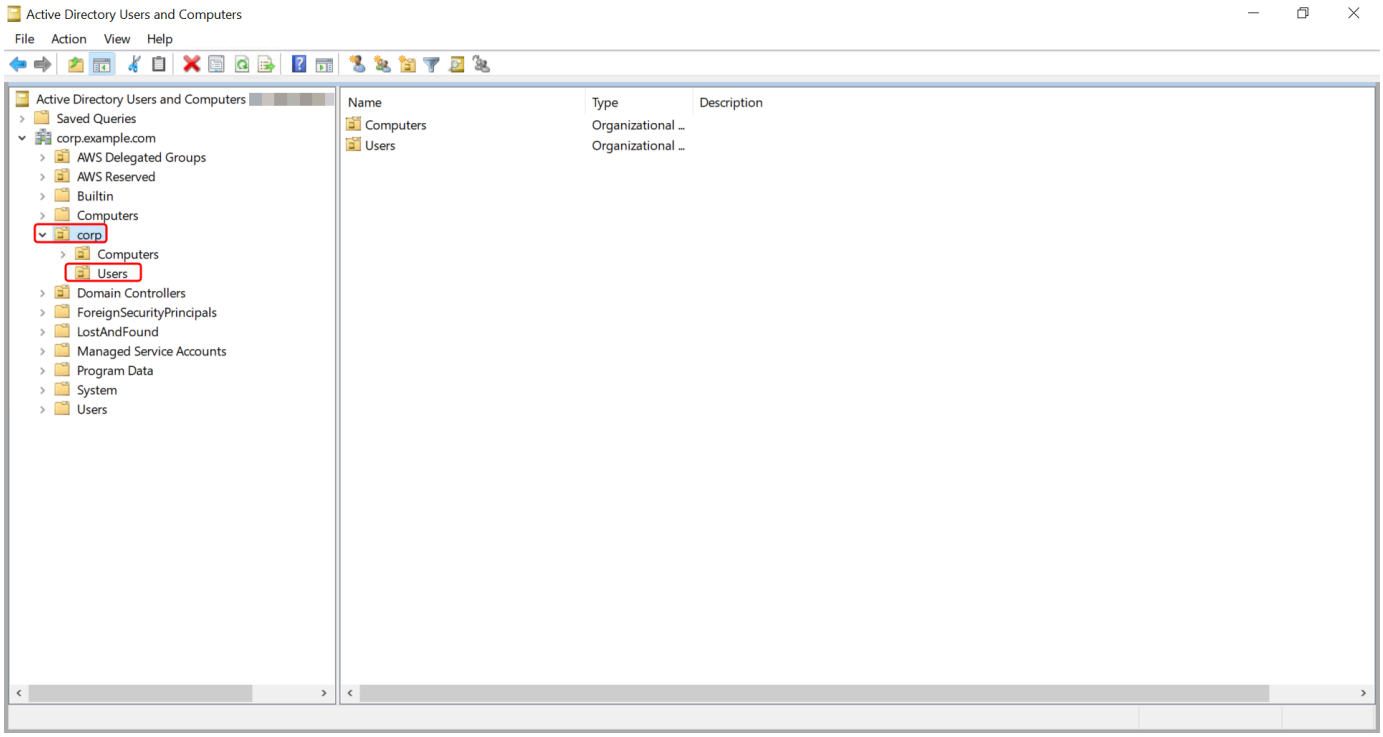
Utilizzare la procedura seguente per aggiungere un utente a un gruppo di sicurezza con un' EC2 istanza aggiunta alla directory Simple AD.

Aggiunta di un utente a un gruppo

1. Connettiti all'istanza in cui sono stati installati gli strumenti di amministrazione di Active Directory.
2. Apri lo strumento Utenti e computer di Active Directory. Trovi una scorciatoia a questo strumento nella cartella Administrative Tools (Strumenti amministrativi).

> **Tip**
>
> Puoi eseguire quanto segue da un prompt dei comandi sull'istanza per aprire direttamente la casella dello strumento Users and Computers (Utenti e computer) di Active Directory.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Nell'albero delle directory, seleziona l'unità organizzativa sotto quella con il nome NetBIOS della directory in cui è archiviato il gruppo e seleziona il gruppo a cui desideri aggiungere un utente come membro.



4. Nel menu Operazioni, fai clic su Proprietà per aprire la finestra di dialogo delle proprietà del gruppo.
5. Seleziona la scheda Membri e fai clic su Aggiungi….

6. Per Immettere i nomi degli oggetti da selezionare, digitare il nome utente che si desidera aggiungere e fare clic su OK. Il nome verrà visualizzato nell'elenco Membri. Fai nuovamente clic su OK per aggiornare l'appartenenza al gruppo.
7. Verifica che l'utente sia ora membro del gruppo selezionandolo nella cartella Utenti e facendo clic su Proprietà nel menu Operazioni per aprire la finestra di dialogo delle proprietà. Seleziona la scheda Membro di. Il nome del gruppo dovrebbe essere visualizzato nell'elenco dei gruppi a cui appartiene l'utente.

Quote di Simple AD

In generale, è opportuno non aggiungere più di 500 utenti a una directory Simple AD piccola e non più di 5.000 a una grande. Per opzioni di scalabilità più flessibili e funzionalità aggiuntive di Active Directory, prendi in considerazione l'utilizzo di AWS Directory Service per Microsoft Active Directory (Standard Edition o Enterprise Edition).

Di seguito sono elencati le quote predefinite per Simple AD. Salvo ove diversamente specificato, ogni quota si applica a una regione.

Quote di Simple AD

Risorsa	Quota predefinita
Directory Simple AD	10
Snapshot manuali *	5 per Simple AD

* La quota di snapshot manuali non può essere modificata.

> **Note**
>
> Non è possibile collegare un indirizzo IP pubblico alla propria AWS elastic network interface (ENI).

Risoluzione dei problemi di Simple AD

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potresti riscontrare durante la creazione o l'utilizzo di Simple AD Active Directory.

Argomenti

Recupero della password

Se un utente dimentica una password o riscontra problemi di accesso alla directory Simple AD, puoi reimpostarne la password utilizzando il Console di gestione AWS, PowerShell o il AWS CLI.

Per ulteriori informazioni, consulta Reimpostazione di una password utente Simple AD.

Ricevo un errore «KDC non può soddisfare l'opzione richiesta» quando aggiungo un utente a Simple AD

Ciò può verificarsi quando il client Samba CLI non invia correttamente i comandi a tutti i `net` controller di dominio. Se viene visualizzato questo messaggio di errore quando si utilizza il `net ads` comando per aggiungere un utente alla directory Simple AD, utilizzare l'`-S`argomento e specificare l'indirizzo IP di uno dei controller di dominio. Se l'errore persiste, provare l'altro controller di dominio. È anche possibile utilizzare gli strumenti di amministrazione di Active Directory per aggiungere utenti alla directory. Per ulteriori informazioni, consulta Installazione degli strumenti di amministrazione di Active Directory per Simple AD.

Non sono in grado di aggiornare il nome DNS o l'indirizzo IP di un'istanza collegata al mio dominio (aggiornamento dinamico DNS)

Gli aggiornamenti dinamici del DNS non sono supportati nei domini di Simple AD. È invece possibile apportare direttamente le modifiche collegandosi alla directory utilizzando DNS Manager su un'istanza che è stata aggiunta al dominio.

Non riesco ad accedere a SQL Server utilizzando un account SQL Server

Potresti ricevere un errore se tenti di utilizzare SQL Server Management Studio (SSMS) con un account SQL Server per accedere a SQL Server in esecuzione su un'istanza Amazon Windows EC2 2012 R2. Il problema si verifica quando SSMS viene eseguito come utente di dominio e può causare l'errore`Login failed for user`, anche quando vengono fornite credenziali valide. Si tratta di un problema noto e AWS si sta lavorando attivamente per risolverlo.

Per risolvere il problema, è possibile accedere a SQL Server con Windows l'autenticazione anziché l'autenticazione SQL. In alternativa, puoi avviare SSMS come utente locale anziché come utente di dominio Simple AD.

My Simple AD è bloccato nello stato «Richiesto»

Se hai un Simple AD che si trova nello `Requested` stato da più di cinque minuti, prova a eliminare la directory e a ricrearla. Se il problema persiste, contatta il centro Supporto AWS.

Ricevo un errore «AZ constrained» quando creo un Simple AD

Alcuni AWS account creati prima del 2012 potrebbero avere accesso alle zone di disponibilità nella regione Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale) o Asia Pacifico (Tokyo) che non supportano le directory. Directory Service Se ricevi un messaggio di errore di questo tipo quando crei una directory, seleziona una sottorete in un'altra zona di disponibilità e prova a creare di nuovo la directory.

Alcuni dei miei utenti non riescono ad autenticarsi con il mio Simple AD

I tuoi account utente devono avere la preautenticazione Kerberos abilitata. Questa è l'impostazione predefinita per i nuovi account utente e non dovrebbe essere modificata. Per ulteriori informazioni su questa impostazione, vai a Preauthentication on Simple AD TechNet.

Risorse aggiuntive

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

- AWS Knowledge Center: trova FAQs e collega altre risorse per aiutarti a risolvere i problemi.
- AWS Support Center: ottieni supporto tecnico.
- AWS Premium Support Center: ottieni supporto tecnico premium.

Argomenti

Risoluzione dei problemi relativi ai messaggi di stato della directory Simple AD

Quando un Simple AD è danneggiato o inutilizzabile, il messaggio di stato della directory contiene informazioni aggiuntive. Il messaggio di stato viene visualizzato nella Directory Service console o restituito al `DirectoryDescription.StageReason`membro dall'API. `DescribeDirectories` Per ulteriori informazioni sugli stati della directory, consulta Informazioni sullo stato della directory AWS Managed Microsoft AD.

Di seguito sono riportati i messaggi di stato di una directory Simple AD:

Argomenti

L'interfaccia di rete elastica del servizio di directory non è collegata

Descrizione

La critical elastic network interface (ENI) creata per tuo conto durante la creazione della directory per stabilire la connettività di rete con il tuo VPC non è collegata all'istanza della directory. AWS le applicazioni supportate da questa directory non funzioneranno. La directory non può connettersi alla rete on-premise.

Risoluzione dei problemi

Se l'ENI è distaccata ma esiste ancora, contatta Supporto. Se l'ENI viene eliminata, non c'è modo di risolvere il problema e la directory non può essere più utilizzata. Devi eliminare la directory e crearne una nuova.

Problemi rilevati dall'istanza

Descrizione

L'istanza ha rilevato un errore interno. Solitamente ciò indica che il servizio di monitoraggio sta tentando attivamente di ripristinare le istanze danneggiate.

Risoluzione dei problemi

Nella maggior parte dei casi, si tratta di un problema temporaneo e alla fine la directory torna allo stato Attivo. Se il problema persiste, contatta Supporto per ulteriore assistenza.

L'utente Directory Service riservato critico non è presente nella directory

Descrizione

Quando viene creato un Simple AD, Directory Service crea un account di servizio nella directory con il nome`AWSAdmin`*`D-xxxxxxxxx`*. Questo errore viene restituito quando è impossibile individuare l'account del servizio. Senza questo account, Directory Service non è in grado di eseguire funzioni amministrative sulla directory, rendendola inutilizzabile.

Risoluzione dei problemi

Per risolvere il problema, ripristinare la directory su una snapshot precedente, creata prima dell'eliminazione dell'account del servizio. Gli snapshot vengono acquisiti dalla tua directory Simple AD una volta al giorno. Se sono passati più di cinque giorni dall'eliminazione dell'account,

potrebbe non essere più possibile ripristinare lo stesso stato che la directory aveva nell'account. Se non è possibile ripristinare la directory da una snapshot in cui si trova questo account, la directory potrebbe diventare inutilizzabile definitivamente. In questo caso, è necessario eliminare la directory e crearne una nuova.

L'utente Directory Service riservato critico deve appartenere al gruppo Domain Admins

Descrizione

Quando viene creato un Simple AD, Directory Service crea un account di servizio nella directory con il nome`AWSAdmin`*`D-xxxxxxxxx`*. Questo errore viene ricevuto quando l'account del servizio non è un membro del gruppo `Domain Admins`. L'appartenenza a questo gruppo è necessaria per conferire Directory Service i privilegi necessari per eseguire operazioni di manutenzione e ripristino, come il trasferimento di ruoli FSMO, l'aggiunta di domini a nuovi controller di directory e il ripristino da istantanee.

Risoluzione dei problemi

Utilizzare lo strumento Users and Computers (Utenti e computer) di Active Directory per aggiungere nuovamente l'account del servizio al gruppo `Domain Admins`.

L'utente riservato critico è disabilitato Directory Service

Descrizione

Quando viene creato un Simple AD, Directory Service crea un account di servizio nella directory con il nome`AWSAdmin`*`D-xxxxxxxxx`*. Questo errore viene restituito quando l'account del servizio è disabilitato. Questo account deve essere abilitato in modo da Directory Service poter eseguire operazioni di manutenzione e ripristino sulla directory.

Risoluzione dei problemi

Utilizzare lo strumento Users and Computers (Utenti e computer) di Active Directory per abilitare nuovamente l'account del servizio.

Il controller di dominio principale non dispone di tutti i ruoli FSMO

Descrizione

Tutti i ruoli FSMO non sono di proprietà del controller della directory Simple AD. Il Directory Service non è in grado di garantire determinati comportamenti e funzionalità se i ruoli FSMO non appartengono al controller della directory Simple AD corretto.

Risoluzione dei problemi

Utilizzare gli strumenti di Active Directory per spostare nuovamente i ruoli FSMO nel controller della directory di lavoro originale. Per ulteriori informazioni sullo spostamento dei ruoli FSMO, vai a https://docs.microsoft.com/troubleshoot/windows- server/identity/transfer - or-seize-fsmo-roles - in-ad-ds. Se il problema persiste, contattateci Supporto per ricevere ulteriore assistenza.

Errori di replica del controller di dominio

Descrizione

I controller della directory Simple AD producono errori nel replicarsi tra loro. Questo può essere dovuto a uno o più dei problemi seguenti:

- I gruppi di sicurezza dei controller della directory non hanno le porte corrette aperte.
- La rete è ACLs troppo restrittiva.
- La tabella di routing VPC non instrada il traffico di rete in modo corretto tra i controller della directory.
- Un'altra istanza è stata promossa a controller di dominio nella directory.

Risoluzione dei problemi

Per ulteriori informazioni sui requisiti di rete VPC, consulta Microsoft AD gestito da AWS Prerequisiti per la creazione di un AWS Managed Microsoft AD, il connettore AD Prerequisiti di AD Connector o Simple AD Prerequisiti di Simple AD. Se è presente un controller di dominio sconosciuto nella directory, è necessario abbassarlo di livello. Se la configurazione della rete VPC è corretta ma l'errore persiste, contatta Supporto per ulteriore assistenza.

Sicurezza in AWS Directory Service

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWSti 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 applicabiliAWS Directory Service, consulta AWSServices 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 durante l'utilizzoDirectory Service. Negli argomenti seguenti viene illustrato come eseguire la configurazione Directory Service per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere Directory Service le tue risorse.

Argomenti relativi alla sicurezza

In questa sezione sono disponibili i seguenti argomenti relativi alla sicurezza:

- Gestione delle identità e degli accessi per Directory Service
- Registrazione e monitoraggio AWS Directory Service
- Convalida della conformità per AWS Directory Service
- Resilienza in AWS Directory Service
- Sicurezza dell'infrastruttura in AWS Directory Service

Ulteriori argomenti relativi alla sicurezza

In questa guida sono disponibili i seguenti argomenti aggiuntivi relativi alla sicurezza:

Account, trust e accesso alle AWS risorse

- AWS Account Microsoft AD Administrator gestito e autorizzazioni di gruppo
- Account del servizio gestito del gruppo
- Creazione di una relazione di fiducia tra AWS Managed Microsoft AD e AD autogestito
- Delega vincolata Kerberos
- Concedere agli utenti e ai gruppi di AWS Managed Microsoft AD l'accesso alle AWS risorse con ruoli IAM
- Autorizzazione per l'AWSutilizzo di applicazioni e servizi Directory Service

Protezione della directory

- Proteggi il tuo AWS Managed Microsoft AD
- Protezione della directory AD Connector

Registrazione e monitoraggio

- Monitora il tuo AWS Managed Microsoft AD
- Monitoraggio della directory AD Connector

Resilienza

- Applicazione di patch e manutenzione per Microsoft AD gestito da AWS

Gestione delle identità e degli accessi per Directory Service

L'accesso a Directory Service richiede credenziali che AWS possono essere utilizzate per autenticare le richieste. Tali credenziali devono disporre delle autorizzazioni per accedere alle AWS risorse, ad esempio una directory. Directory Service Le seguenti sezioni forniscono dettagli su come utilizzare AWS Identity and Access Management(IAM) e su come Directory Service proteggere le risorse controllando chi può accedervi:

- Autenticazione
- Controllo accessi

Autenticazione

Scopri come accedere AWS utilizzando le identità IAM.

Controllo accessi

Puoi avere credenziali valide per autenticare le tue richieste, ma a meno che tu non disponga delle autorizzazioni non puoi creare o accedere alle risorse. Directory Service Ad esempio, è necessario disporre delle autorizzazioni per creare una Directory Service directory o per creare uno snapshot della directory.

Le seguenti sezioni descrivono come gestire le autorizzazioni per. Directory Service Consigliamo di leggere prima la panoramica.

- Panoramica della gestione delle autorizzazioni di accesso alle risorse Directory Service
- Utilizzo di politiche basate sull'identità (politiche IAM) per Directory Service
- Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Panoramica della gestione delle autorizzazioni di accesso alle risorse Directory Service

Ogni AWS risorsa è di proprietà di un AWS account. Di conseguenza, le autorizzazioni per creare o accedere alle risorse sono regolate da politiche di autorizzazione. Tuttavia, un amministratore di account, ovvero un utente con autorizzazioni di amministratore, può assegnare autorizzazioni alle risorse. Hanno anche la possibilità di allegare politiche di autorizzazione alle identità IAM, come utenti, gruppi e ruoli, e alcuni servizi, ad esempio supportano AWS Lambda anche l'associazione di politiche di autorizzazione alle risorse.

> **Note**
>
> Per informazioni sul ruolo di amministratore dell'account, consulta le best practice di IAM nella IAM User Guide.

Argomenti

- Directory Servicerisorse e operazioni
- Informazioni sulla proprietà delle risorse

- Gestione dell'accesso alle risorse
- Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità
- Specifica delle condizioni in una policy

Directory Servicerisorse e operazioni

InDirectory Service, la risorsa principale è una directory. Poiché Directory Service supporta le risorse relative agli snapshot delle directory, è possibile creare istantanee solo nel contesto di una directory esistente. Questa istantanea viene definita sottorisorsa.

A queste risorse sono associati Amazon Resource Names (ARNs) univoci, come illustrato nella tabella seguente.

Tipo di risorsa	Formato ARN
Directory	`arn:aws:ds:` *`region`*`:`*`account-id`* `:directory/` *`external-directory-id`*
Istantanea	`arn:aws:ds:` *`region`*`:`*`account-id`* `:snapshot/` *`external-snapshot-id`*

Directory Serviceinclude due namespace di servizio in base al tipo di operazioni eseguite.

- Lo spazio dei nomi del `ds` servizio fornisce una serie di operazioni per lavorare con le risorse appropriate. Per un elenco delle operazioni disponibili, consulta la sezione relativa alle operazioni del servizio di directory.
- Lo spazio dei nomi del `ds-data` servizio fornisce una serie di operazioni agli oggetti di Active Directory. Per un elenco delle operazioni disponibili, consulta Directory Service Data API Reference.

Informazioni sulla proprietà delle risorse

Il proprietario della risorsa è l'AWSaccount che ha creato una risorsa. Cioè, il proprietario della risorsa è l'AWSaccount dell'entità principale (l'account root, un utente IAM o un ruolo IAM) che autentica la richiesta che crea la risorsa. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account root del tuo AWS account per creare una Directory Service risorsa, ad esempio una directory, l'AWSaccount è il proprietario di quella risorsa.
- Se crei un utente IAM nel tuo AWS account e concedi le autorizzazioni per creare Directory Service risorse a quell'utente, anche l'utente può creare Directory Service risorse. 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 Directory Service risorse, chiunque possa assumere il ruolo può creare Directory Service risorse. Il tuo AWS account, a cui appartiene il ruolo, possiede le Directory Service risorse.

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 diDirectory Service. 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, consulta Documentazioni di riferimento alle policy JSON IAM nella Guida per l'utente di IAM.

Le politiche collegate a un'identità IAM sono denominate politiche basate sull'identità (politiche IAM) e le politiche allegate a una risorsa sono denominate politiche basate sulle risorse. Directory Servicesupporta 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 collegare le policy 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: un amministratore dell'account può utilizzare una politica di autorizzazioni associata a un particolare utente per

concedere a quell'utente le autorizzazioni per creare una Directory Service risorsa, ad esempio una nuova directory.

- 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 `Describe`. Queste azioni mostrano informazioni su una Directory Service risorsa, ad esempio una directory o un'istantanea. Nota che il carattere jolly (*) nell'`Resource`elemento indica che le azioni sono consentite per tutte le Directory Service risorse di proprietà dell'account.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni sull'utilizzo di politiche basate sull'identità con, vedere. Directory Service Utilizzo di politiche basate sull'identità (politiche IAM) per Directory Service 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, puoi allegare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. Directory Servicenon supporta politiche basate sulle risorse.

Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità

Per ogni Directory Service risorsa, il servizio definisce una serie di operazioni API. Per ulteriori informazioni, consulta Directory Servicerisorse e operazioni. Per un elenco delle operazioni dell'API disponibili, consulta la sezione relativa alle operazioni del servizio di directory.

Per concedere le autorizzazioni per queste operazioni API, Directory Service definisce una serie di azioni che è possibile specificare in una politica. 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. Per Directory Service le risorse, usi sempre il carattere jolly (*) nelle policy IAM. Per ulteriori informazioni, consulta Directory Servicerisorse e operazioni.
- Operazione: utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, l'autorizzazione `ds:DescribeDirectories` concede all'utente le autorizzazioni per eseguire l'operazione Directory Service`DescribeDirectories`.
- Effetto: specifica l'effetto quando l'utente richiede l'operazione specifica. Può trattarsi di un'autorizzazione o di un rifiuto. USe non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.
- Principale: nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per le politiche basate sulle risorse, specifichi l'utente, l'account, il servizio o l'altra entità a cui desideri che riceva le autorizzazioni (si applica solo alle politiche basate sulle risorse). Directory Servicenon supporta le politiche basate sulle risorse.

Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consulta Documentazioni di riferimento alle policy JSON IAM nella Guida per l'utente di IAM.

Per una tabella che mostra tutte le azioni Directory Service API e le risorse a cui si applicano, consulta. Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Specifica delle condizioni in una policy

Quando concedi le autorizzazioni, puoi utilizzare la sintassi della policy di accesso per specificare le condizioni in base a cui la policy deve essere applicata. 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 Directory Service. 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.

AWSpolitiche gestite per AWS Directory Service

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

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

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

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

Le sezioni seguenti descrivono le politiche AWS gestite specifiche perDirectory Service. Puoi allegare queste politiche agli utenti del tuo account.

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

AWSpolitica gestita: AWSDirectoryServiceFullAccess

È possibile allegare la policy `AWSDirectoryServiceFullAccess` alle identità IAM. Per visualizzare le autorizzazioni complete per questa policy, consulta AWSDirectoryServiceFullAccessil AWSManaged Policy Reference.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo e principale a tutte le azioni. Directory Service I responsabili con queste autorizzazioni possono

creare, configurare e gestire directory, tra cui Simple AD, AD Connector e Managed Microsoft AD. Possono anche gestire la condivisione delle directory, le relazioni di fiducia e il monitoraggio delle configurazioni. Questa politica include le autorizzazioni per gestire l'infrastruttura di rete sottostante richiesta per i servizi di directory.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ds`— Consente ai responsabili l'accesso completo a tutte le Directory Service azioni.
- `ec2`— Consente ai responsabili di gestire interfacce di rete, gruppi di sicurezza e descrivere le risorse VPC necessarie per le operazioni di directory.
- `sns`— Consente ai responsabili di creare e gestire argomenti SNS per il monitoraggio delle directory, in particolare argomenti i cui nomi iniziano con "». DirectoryMonitoring
- `iam`— Consente ai responsabili di elencare i ruoli IAM per le operazioni dei servizi di directory.
- `organizations`— Consente ai responsabili di gestire l'integrazione di AWS Organizations e l'accesso ai enable/disable servizi per i servizi di directory.

AWSpolitica gestita: AWSDirectoryServiceReadOnlyAccess

È possibile allegare la policy `AWSDirectoryServiceReadOnlyAccess` alle identità IAM. Per visualizzare le autorizzazioni complete per questa policy, consulta AWSDirectoryServiceReadOnlyAccessil AWSManaged Policy Reference.

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni in. Directory Service I responsabili a cui è allegata questa politica non possono aggiornare le directory o le relative configurazioni. Ad esempio, gli amministratori con queste autorizzazioni possono visualizzare i dettagli delle directory, le relazioni di trust e le configurazioni di monitoraggio, ma non possono creare nuove directory o modificare quelle esistenti. Possono inoltre visualizzare le risorse di EC2 rete correlate e gli argomenti SNS associati alle directory.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ds`— Consente agli utenti di eseguire azioni di sola lettura che restituiscono informazioni sulla directory. Ciò include le operazioni API che iniziano con`Check`,, `Describe` `GetList`, o. `Verify`

- `ec2`— Consente agli utenti di descrivere interfacce di rete, sottoreti e servizi di directory VPCs associati.
- `sns`— Consente agli utenti di elencare e ottenere informazioni sugli argomenti e sugli abbonamenti SNS utilizzati per il monitoraggio delle directory.
- `organizations`— Consente agli utenti di descrivere gli AWS Organizations account e le configurazioni di accesso ai servizi di elenco.

AWSpolitica gestita: AWSDirectoryServiceDataFullAccess

È possibile allegare la policy `AWSDirectoryServiceDataFullAccess` alle identità IAM. Per visualizzare le autorizzazioni complete per questa policy, consulta AWSDirectoryServiceDataFullAccessil AWSManaged Policy Reference.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo principale alle operazioni dei dati del Directory Service. I responsabili con queste autorizzazioni possono creare, aggiornare ed eliminare utenti e gruppi di Active Directory all'interno delle directory gestite. Possono gestire le appartenenze ai gruppi, abilitare o disabilitare gli utenti ed eseguire operazioni complete di gestione di utenti e gruppi. Questa politica è progettata per gli amministratori che devono gestire gli oggetti di Active Directory a livello di programmazione.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ds`— Consente ai responsabili di accedere ai dati delle directory tramite l'API Directory Service Data.
- `ds-data`— Consente ai responsabili l'accesso completo a tutte le operazioni relative ai dati del Directory Service, tra cui la creazione, l'aggiornamento e l'eliminazione di utenti e gruppi, la gestione delle appartenenze ai gruppi e la ricerca di oggetti della directory.

Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess

È possibile allegare la policy `AWSDirectoryServiceDataReadOnlyAccess` alle identità IAM. Per visualizzare le autorizzazioni complete per questa politica, consulta il Managed Policy AWSDirectoryServiceDataReadOnlyAccessReference. AWS

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare e cercare oggetti Active Directory all'interno delle directory gestite. I responsabili a cui è allegato questo

criterio non possono apportare aggiornamenti a utenti, gruppi o appartenenze ai gruppi. Ad esempio, i responsabili con queste autorizzazioni possono cercare utenti e gruppi, visualizzare i dettagli di utenti e gruppi ed elencare le appartenenze ai gruppi, ma non possono creare, modificare o eliminare alcun oggetto di directory.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ds`— Consente ai responsabili di accedere ai dati delle directory tramite l'API Directory Service Data.
- `ds-data`— Consente agli utenti di eseguire azioni di sola lettura che restituiscono informazioni sugli oggetti della directory. Sono incluse le operazioni API che iniziano con `DescribeList`, o. `Search`

AWSDirectoryServiceServiceRolePolicy

Non puoi collegare la `AWSDirectoryServiceServiceRolePolicy` policy alle tue identità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a AWS Directory Service di eseguire azioni per conto dell'utente. Per vedere le autorizzazioni per questa policy, consulta AWSDirectoryServiceServiceRolePolicy nella Guida di riferimento sulle policy gestite da AWS.

Questa politica concede autorizzazioni che consentono di monitorare e valutare i controller Directory Service di dominio autogestiti in ambienti ibridi Active Directory. Il servizio utilizza queste autorizzazioni per eseguire valutazioni automatiche dello stato, eseguire PowerShell script per test di compatibilità e raccogliere informazioni sulla configurazione di rete per garantire una connettività ibrida adeguata e funzionalità di ripristino automatizzate.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `ssm`— Consente al servizio di inviare PowerShell comandi ai controller di dominio locali e recuperare i risultati dell'esecuzione dei comandi per scopi di monitoraggio e valutazione.
- `ec2`— Consente al servizio di descrivere risorse di rete come sottoreti VPCs, gruppi di sicurezza e interfacce di rete per convalidare le configurazioni di connettività ibrida.

IAM e aggiornamenti alle politiche gestite Directory ServiceAWS

Visualizza i dettagli sugli aggiornamenti a IAM e alle policy AWS gestite da quando il servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nelle pagine IAM e Directory Service Document history.

Modifica	Descrizione	Data
AWSDirectoryServiceServiceRolePolicy: nuova policy	Directory Serviceha aggiunto una nuova policy per consentire il monitoraggio dei AWS controller di dominio autogestiti del cliente.	30 luglio 2025
Policy gestita da AWS: AWSDirectoryServiceDataReadOnlyAccess: nuova policy	Directory Serviceha aggiunto una nuova politica per consentire a un utente o a un gruppo di accedere alla visualizzazione e alla ricerca di utenti, membri e gruppi di AD.	17 settembre 2024
AWSpolitica gestita: AWSDirectoryServiceDataFullAccess: nuova policy	Directory Serviceha aggiunto una nuova politica per consentire a un utente o un gruppo di accedere alla gestione degli oggetti integrata con Directory Service Data per creare, gestire e visualizzare utenti, membri e gruppi di AD.	17 settembre 2024
Directory Serviceha iniziato a tenere traccia delle modifiche	Directory Serviceha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	17 settembre 2024

Utilizzo di politiche basate sull'identità (politiche IAM) per Directory Service

In questo argomento vengono forniti esempi di policy basate su identità in cui un amministratore account può collegare policy di autorizzazione a identità IAM ovvero utenti, gruppi e ruoli. Questi esempi illustrano le politiche IAM in. Directory Service È necessario modificare e creare le proprie politiche in base alle proprie esigenze e al proprio ambiente.

> **Important**
>
> Si consiglia di esaminare innanzitutto gli argomenti introduttivi che spiegano i concetti e le opzioni di base disponibili per gestire l'accesso alle risorse. Directory Service Per ulteriori informazioni, consulta Panoramica della gestione delle autorizzazioni di accesso alle risorse Directory Service.

In questa sezione vengono trattati gli argomenti seguenti:

- Autorizzazioni necessarie per utilizzare la console Directory Service
- AWSpolitiche gestite (predefinite) per Directory Service
- Esempi di policy gestite dal cliente
- Utilizzo dei tag con policy IAM

Di seguito viene illustrato un esempio di policy di autorizzazione.

JSON

```
{
   "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDsEc2IamGetRole",
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeNetworkInterfaces",
```

```
                "ec2:DescribeVpcs",
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "iam:GetRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
        },
        {
            "Sid": "AllowPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/Your-Role-Name",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

Le tre istruzioni contenute nella politica concedono le autorizzazioni seguenti:

- La prima istruzione concede il permesso di creare una Directory Service directory. Poiché Directory Service non supporta le autorizzazioni a livello di risorsa, la policy specifica un carattere jolly (*) come valore. `Resource`
- La seconda istruzione concede le autorizzazioni per accedere alle azioni IAM, in modo che Directory Service possano leggere e creare ruoli IAM per tuo conto. Il carattere jolly (*) alla fine del valore `Resource` indica che l'istruzione concede l'autorizzazione alle operazioni IAM su qualsiasi

ruolo IAM. Per limitare questa autorizzazione a un determinato ruolo, sostituire il carattere jolly (*) nel nome ARN della risorsa con il nome del ruolo specifico. Per ulteriori informazioni, consulta la sezione relativa alle operazioni IAM.

- La terza istruzione concede le autorizzazioni a un insieme specifico di risorse in Amazon EC2 necessarie per consentire la creazione, Directory Service la configurazione e la distruzione delle relative directory. Sostituisci il ruolo ARN con il tuo ruolo. Per ulteriori informazioni, consulta Amazon EC2 Actions.

Non vedi alcun `Principal` elemento nella politica, perché in una politica basata sull'identità non specifichi il principale che ottiene l'autorizzazione. Quando alleghi la policy a un utente, l'utente è il principale implicito. Quando si collega una policy di autorizzazione a un ruolo IAM;, l'entità identificata nella policy di attendibilità del ruolo ottiene le autorizzazioni.

Per una tabella che mostra tutte le azioni Directory Service API e le risorse a cui si applicano, consulta. Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Autorizzazioni necessarie per utilizzare la console Directory Service

Affinché un utente possa utilizzare la Directory Service console, deve disporre delle autorizzazioni elencate nella politica precedente o delle autorizzazioni concesse dal ruolo Directory Service Full Access Role o Directory Service Read Only, descritto in. AWSpolitiche gestite (predefinite) per Directory Service

Se decidi di creare una policy IAM più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per gli utenti con tale policy IAM.

AWSpolitiche gestite (predefinite) per Directory Service

AWSaffronta molti casi d'uso comuni fornendo policy IAM predefinite o gestite create e amministrate da. AWS Le policy gestite concedono le autorizzazioni necessarie per i casi d'uso comuni, il che aiuta a decidere quali autorizzazioni sono necessarie. Per ulteriori informazioni, consulta AWSpolitiche gestite per AWS Directory Service.

Esempi di policy gestite dal cliente

In questa sezione, puoi trovare esempi di politiche utente che concedono autorizzazioni per varie azioni. Directory Service

> **Note**
>
> Tutti gli esempi utilizzano la regione degli Stati Uniti occidentali (Oregon) (`us-west-2`) e contengono account fittizi. IDs

Esempi

- Esempio 1: consentire a un utente di eseguire qualsiasi azione Descrivi su qualsiasi risorsa Directory Service
- Esempio 2: consentire a un utente di creare una directory

Esempio 1: consentire a un utente di eseguire qualsiasi azione Descrivi su qualsiasi risorsa Directory Service

La seguente politica di autorizzazioni concede a un utente le autorizzazioni per eseguire tutte le azioni che iniziano con `Describe` in un AWS Microsoft AD gestito con l'ID `d-1234567890` di directory in. Account AWS `111122223333` Queste operazioni riportano informazioni su una risorsa Directory Service, ad esempio una directory o una snapshot. Assicurati di modificare il Regione AWS numero di account in base alla regione che desideri utilizzare e al tuo numero di account.

JSON

```
{
"Version":"2012-10-17",
   "Statement":[
      {
"Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource": "arn:aws:ds:us-west-2:111122223333:directory/d-1234567890"
      }
   ]
}
```

Esempio 2: consentire a un utente di creare una directory

La seguente policy di autorizzazione concede autorizzazioni per permettere all'utente di creare una directory e tutte le altre risorse correlate, quali snapshot e trust. A tal fine, sono necessarie anche le autorizzazioni per determinati EC2 servizi Amazon.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ds:DescribeDirectories"
            ],
            "Resource": "arn:aws:ds:*:111122223333:*"
        }
    ]
}
```

Utilizzo dei tag con policy IAM

Puoi applicare autorizzazioni a livello di risorsa basate su tag nelle policy IAM che utilizzi per la maggior parte delle azioni API. Directory Service In questo modo è possibile controllare meglio le risorse che un utente può creare, modificare o utilizzare. Puoi utilizzare l'elemento `Condition` (denominato anche blocco `Condition`) con i seguenti valori e chiavi di contesto di condizione in una policy IAM per controllare l'accesso dell'utente (autorizzazione) in base ai tag della risorsa:

- Utilizza `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** per concedere o negare agli utenti operazioni su risorse con specifici tag.
- Utilizza `aws:ResourceTag/`**`tag-key`**`: `**`tag-value`** per richiedere che un tag specifico venga utilizzato (o non utilizzato) durante la creazione di una richiesta API per creare o modificare una risorsa che abilita i tag.
- Utilizza `aws:TagKeys: [`**`tag-key`**`, ...]` per richiedere che un set di tag specifico venga utilizzato (o non utilizzato) durante la creazione di una richiesta API per creare o modificare una risorsa che abilita i tag.

> **Note**
>
> Le chiavi di contesto della condizione e i valori all'interno di una policy IAM si applicano solo alle operazioni Directory Service in cui un identificatore per una risorsa in grado di essere taggata è un parametro obbligatorio.

Controllo dell'accesso mediante i tag nella Guida per l'utente di IAM contiene ulteriori informazioni sull'utilizzo dei tag. La sezione relativa alla documentazione di riferimento sulle policy JSON IAM della guida ha una sintassi dettagliata, descrizioni ed esempi di elementi, variabili e logica di valutazione delle policy JSON in IAM.

La seguente politica sui tag consente di creare una Directory Service directory purché vengano utilizzati i seguenti tag:

- Ambiente: produzione
- Proprietario: Infrastructure Team
- Centro di costo: 1234

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Environment": "Production",
                    "aws:RequestTag/Owner": "Infrastructure-Team",
                    "aws:RequestTag/CostCenter": "12345"
                }
            }
        }
    ]
}
```

La seguente politica sui tag consente l'aggiornamento e l'eliminazione Directory Service delle directory purché vengano utilizzati i seguenti tag:

- Progetto: Atlas
- Dipartimento: Ingegneria
- Ambiente: messa in scena

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ds:DeleteDirectory",
                "ds:UpdateDirectory"
```

```
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Project": "Atlas",
                    "aws:ResourceTag/Department": "Engineering",
                    "aws:ResourceTag/Environment": "Staging"
                }
            }
        }
    ]
}
```

La seguente politica di tag nega l'etichettatura delle risorse per i Directory Service casi in cui la risorsa ha uno dei seguenti tag:

- Produzione
- Sicurezza
- Riservato

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "ds:AddTagsToResource"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": ["Production", "Security", "Confidential"]
                }
            }
        }
    ]
}
```

Per ulteriori informazioni ARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Il seguente elenco di operazioni Directory Service API supporta le autorizzazioni a livello di risorsa basate su tag:

- AcceptSharedDirectory
- AddIpRoutes
- AddTagsToResource
- CancelSchemaExtension
- CreateAlias
- CreateComputer
- CreateConditionalForwarder
- CreateSnapshot
- CreateLogSubscription
- CreateTrust
- DeleteConditionalForwarder
- DeleteDirectory
- DeleteLogSubscription
- DeleteSnapshot
- DeleteTrust
- DeregisterEventTopic
- DescribeConditionalForwarders
- DescribeDomainControllers
- DescribeEventTopics
- DescribeSharedDirectories
- DescribeSnapshots
- DescribeTrusts
- DisableRadius
- DisableSso
- EnableRadius

- EnableSso
- GetSnapshotLimits
- ListIpRoutes
- ListSchemaExtensions
- ListTagsForResource
- RegisterEventTopic
- RejectSharedDirectory
- RemoveIpRoutes
- RemoveTagsFromResource
- ResetUserPassword
- RestoreFromSnapshot
- ShareDirectory
- StartSchemaExtension
- UnshareDirectory
- UpdateConditionalForwarder
- UpdateNumberOfDomainControllers
- UpdateRadius
- UpdateTrust
- VerifyTrust

Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Quando configuri Controllo accessi e scrivi policy di autorizzazione che puoi collegare a un'identità IAM (policy basate su identità), puoi usare la tabella Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni come riferimento. Ogni voce API nella include quanto segue:

- Il nome di ogni operazione API
- L'azione o le azioni corrispondenti di ogni operazione API in cui è possibile concedere le autorizzazioni per eseguire l'azione
- La AWS risorsa in cui è possibile concedere le autorizzazioni

Specifica le operazioni nel campo `Action` della policy e il valore della risorsa nel campo `Resource` della policy. Per specificare un'operazione, utilizza il prefisso `ds:` seguito dal nome dell'operazione API (ad esempio, `ds:CreateDirectory`). Alcune AWS applicazioni possono richiedere l'uso di operazioni Directory Service API non pubbliche come`ds:AuthorizeApplication`,,`ds:CheckAlias`, `ds:CreateIdentityPoolDirectory` `ds:GetAuthorizedApplicationDetails``ds:UpdateAuthorizedApplication`, e `ds:UnauthorizeApplication` nelle relative politiche.

Alcune Directory Service APIs possono essere richiamate solo tramite. Console di gestione AWS Non sono pubblici APIs, nel senso che non possono essere chiamati a livello di codice e non sono forniti da alcun SDK. Accettano le credenziali dell'utente. Queste operazioni API includono `ds:DisableRoleAccess``ds:EnableRoleAccess`, e`ds:UpdateDirectory`.

Puoi utilizzare le chiavi di condizione AWS globali nelle tue politiche Directory Service e in quelle relative ai dati di Directory Service per esprimere condizioni. Per un elenco completo delle AWS chiavi, consulta Available Global Condition Keys nella IAM User Guide.

Directory ServiceAPI e autorizzazioni richieste per le azioni

AWSAPI Directory Service Data e autorizzazioni richieste per le azioni

> **Note**
>
> Per specificare un'azione, utilizza il `ds-data:` prefisso seguito dal nome dell'operazione API (ad esempio,`ds-data:AddGroupMember`).

Operazioni dell'API dei dati del Directory Service	Autorizzazioni necessarie (azioni API)	Resources
AddGroupMember	`ds-data:AddGroupMember`	*
CreateGroup	`ds-data:CreateGroup`	*
CreateUser	`ds-data:CreateUser`	*
DeleteGroup	`ds-data:DeleteGroup`	*

Operazioni dell'API dei dati del Directory Service	Autorizzazioni necessarie (azioni API)	Resources
DeleteUser	`ds-data:DeleteUser`	*
DescribeGroup	`ds-data:DescribeGroup`	*
DescribeUser	`ds-data:DescribeUser`	*
DisableUser	`ds-data:DisableUser`	*
ListGroups	`ds-data:ListGroups`	*
ListGroupMembers	`ds-data:ListGroupMembers`	*
ListGroupsForMember	`ds-data:ListGroups ForMember`	*
ListUsers	`ds-data:ListUsers`	*
RemoveGroupMember	`ds-data:RemoveGroupMember`	*
SearchGroups	`ds-data:DescribeGroup` `ds-data:SearchGroups`	*
SearchUsers	`ds-data:DescribeUser` `ds-data:SearchUsers`	*
UpdateGroup	`ds-data:UpdateGroup`	*
UpdateUser	`ds-data:UpdateUser`	*

Argomenti correlati

- Controllo accessi

Chiavi delle condizioni di Directory Service Data

Utilizza le chiavi di condizione Directory Service Data per aggiungere istruzioni specifiche agli utenti e all'accesso a livello di gruppo. Ciò consente agli utenti di decidere quali responsabili possono eseguire azioni su quali risorse e in quali condizioni.

L'elemento Condition, o blocco Condition, consente di specificare le condizioni in cui un'istruzione è valida. L'elemento condizione è facoltativo. È possibile creare espressioni condizionali che utilizzano operatori di condizione, ad esempio equals (=) o less than (<), per abbinare la condizione nella politica ai valori della richiesta.

Se specificate più elementi Condition in un'istruzione o più chiavi in un singolo elemento Condition, li AWS valuta utilizzando un'operazione AND logica. Se specificate più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione OR logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse. È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi concedere a un utente IAM l'autorizzazione ad accedere a una risorsa solo se è contrassegnata con il suo nome utente. Per informazioni, consulta Condizione con più chiavi o valori nella Guida per l'utente IAM.

Per un elenco delle azioni che supportano queste chiavi di condizione, vedere Actions defined by AWS Directory Service Data nel Service Authorization Reference.

> **Note**
>
> Per informazioni sulle autorizzazioni a livello di risorsa basate su tag, consulta. Utilizzo dei tag con policy IAM

SAMAccountds-data: Nome

Funziona con gli operatori String.

Usa questa chiave per consentire o negare esplicitamente a un ruolo IAM di eseguire azioni su utenti e gruppi specifici.

> **Important**
>
> Quando usi `SAMAccountName` o`MemberName`, ti consigliamo di specificare `ds-data:Identifier` as. `SAMAccountName` In questo modo si evita che i futuri identificatori supportati da AWS Directory Service Data, ad esempio`SID`, violino le autorizzazioni esistenti.

La seguente policy impedisce al preside IAM di descrivere l'utente `joe` o il gruppo. `joegroup`

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDescribe",
      "Effect": "Deny",
      "Action": "ds-data:Describe*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe",
            "joegroup"
          ],
          "ds-data:identifier": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

> **Note**
>
> Questa condizione non fa distinzione tra maiuscole e minuscole. È necessario utilizzare `StringEqualsIgnoreCase` o `StringNotEqualsIgnoreCase` condizionare gli operatori per confrontare i valori delle stringhe indipendentemente dalle lettere maiuscole.

DS-Data: identificatore

Funziona con gli operatori String.

Usa questa chiave per definire quale identificatore utilizzare nelle autorizzazioni della policy IAM. Attualmente è supportato solo `SAMAccountName`.

La seguente policy consente al principale IAM di aggiornare l'utente. `joe`

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateJoe",
      "Effect": "Allow",
      "Action": "ds-data:UpdateUser",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe"
          ],
          "ds-data:identifier": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

ds-data: MemberName

Funziona con gli operatori String.

Utilizzate questa chiave per definire i membri su cui possono essere eseguite operazioni.

> **Important**
>
> Quando si utilizza `MemberName` o`SAMAccountName`, si consiglia di specificare `ds-data:Identifier` come`SAMAccountName`. In questo modo si evita che i futuri identificatori supportati da Directory Service Data, ad esempio`SID`, violino le autorizzazioni esistenti.

La seguente policy consente al principale IAM di eseguire operazioni `AddGroupMember` su un membro di qualsiasi `joe` gruppo.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
        "Sid": "AddJoe",
        "Effect": "Allow",
        "Action": "ds-data:AddGroupMember",
        "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
        "Condition": {
            "StringEqualsIgnoreCase": {
                "ds-data:MemberName": "joe"
            }
        }
    }
  ]
}
```

> **Note**
>
> Questa chiave condizionale non fa distinzione tra maiuscole e minuscole. È necessario utilizzare `StringEqualsIgnoreCase` o `StringNotEqualsIgnoreCase` condizionare gli operatori per confrontare i valori delle stringhe, indipendentemente dalle lettere maiuscole.

ds-data: MemberRealm

Funziona con gli operatori String.

Usa questa chiave per verificare se il `ds-data:MemberRealm` valore nella politica corrisponde all'area del membro nella richiesta.

> **Note**
>
> Questa chiave condizionale non fa distinzione tra maiuscole e minuscole. È necessario utilizzare `StringEqualsIgnoreCase` o `StringNotEqualsIgnoreCase` condizionare gli operatori per confrontare i valori delle stringhe, indipendentemente dalle lettere maiuscole.

La seguente policy consente al preside IAM di `AddGroupMember` richiedere un membro bob in realm. `ONE.TRU1.AMAZON.COM`

> **Note**
>
> L'esempio seguente utilizza solo la chiave di `ds-data:MemberName` contesto.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "addbob",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "bob",
          "ds-data:MemberRealm": "one.tru1.amazon.com"
        }
      }
    }
  ]
}
```

DS-Data: Realm

Funziona con gli operatori String.

Usa questa chiave per verificare se il `ds-data:Realm` valore della policy corrisponde al realm che un principale IAM può utilizzare per effettuare richieste ai Directory Service Data APIs.

> **Note**
>
> Questa chiave condizionale non fa distinzione tra maiuscole e minuscole. È necessario utilizzare `StringEqualsIgnoreCase` o `StringNotEqualsIgnoreCase` condizionare gli operatori per confrontare i valori delle stringhe indipendentemente dalle lettere maiuscole.

La seguente politica impedisce al preside IAM di fare riferimento `ListUsers` al `one.tru1.amazon.com` realm.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "DenyTrustedList",
      "Effect": "Deny",
      "Action": "ds-data:ListUsers",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:Realm": [
            "one.tru1.amazon.com"
          ]
        }
      }
    }
  ]
}
```

Autorizzazione per l'AWSutilizzo di applicazioni e servizi Directory Service

Questo argomento descrive l'autorizzazione per AWS applicazioni e servizi che utilizzano AWS Directory Service e AWS Directory Service Data.

Autorizzazione di un'AWSapplicazione su Active Directory

Directory Serviceconcede autorizzazioni specifiche per applicazioni selezionate per integrarsi perfettamente con Active Directory quando si autorizza un'applicazione. AWS AWSalle applicazioni viene concesso solo l'accesso necessario per i loro casi d'uso specifici. Di seguito è riportato un insieme di autorizzazioni interne concesse alle applicazioni e agli amministratori delle applicazioni dopo l'autorizzazione:

> **Note**
>
> L'`ds:AuthorizationApplication`autorizzazione è necessaria per autorizzare una nuova AWS applicazione per Active Directory. Le autorizzazioni per questa azione devono essere fornite solo agli amministratori che configurano le integrazioni con Directory Service.

- Accesso in lettura ai dati di utenti, gruppi, unità organizzative, computer o autorità di certificazione di Active Directory in tutte le unità organizzative (OU) delle directory AWS Managed Microsoft AD, Simple AD, AD Connector, nonché nei domini affidabili per Managed AWS Microsoft AD, se consentito da una relazione di trust.
- Scrivi l'accesso a utenti, gruppi, membri di gruppi, computer o dati dell'autorità di certificazione nell'unità organizzativa di AWS Managed Microsoft AD. Accesso in scrittura a tutte le unità organizzative di Simple AD.
- Autenticazione e gestione delle sessioni degli utenti di Active Directory per tutti i tipi di directory.

Alcune applicazioni AWS Managed Microsoft AD come Amazon RDS e Amazon si FSx integrano tramite una connessione di rete diretta al tuo Active Directory. In questo caso, le interazioni con le directory utilizzano protocolli nativi di Active Directory come LDAP e Kerberos. Le autorizzazioni di queste AWS applicazioni sono controllate da un account utente di directory creato nell'unità organizzativa AWS riservata (OU) durante l'autorizzazione dell'applicazione, che include la gestione DNS e l'accesso completo a un'unità organizzativa personalizzata creata per

l'applicazione. Per utilizzare questo account, l'applicazione richiede le autorizzazioni per operazioni `ds:GetAuthorizedApplicationDetails` tramite le credenziali del chiamante o un ruolo IAM.

Per ulteriori informazioni sulle autorizzazioni Directory Service API, vedere. Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Per ulteriori informazioni sull'abilitazione di AWS applicazioni e servizi per AWS Managed Microsoft AD, vedereAccesso ad AWS applicazioni e servizi dal tuo AWS Managed Microsoft AD. Per ulteriori informazioni sull'attivazione di AWS applicazioni e servizi per Simple AD, vedereAccesso ad AWS applicazioni e servizi dal tuo Simple AD. Per informazioni sull'abilitazione di AWS applicazioni e servizi per AD Connector, consultaAccesso ad AWS applicazioni e servizi da AD Connector.

Rimuovere l'autorizzazione di un'AWSapplicazione su Active Directory

L'`ds:UnauthorizedApplication`autorizzazione è necessaria per rimuovere le autorizzazioni affinché un'AWSapplicazione acceda a un Active Directory. Segui la procedura fornita dall'applicazione per disabilitarla.

AWSautorizzazione dell'applicazione con Directory Service Data

Per le directory Microsoft AD AWS gestite, l'API Directory Service Data (ds-data) fornisce l'accesso programmatico alle attività di gestione di utenti e gruppi. Il modello di autorizzazione delle AWS applicazioni è separato dai controlli di accesso di Directory Service Data, il che significa che le politiche di accesso per le azioni Directory Service Data non influiscono sull'autorizzazione per AWS le applicazioni. Negare l'accesso a una directory in ds-data non interromperà l'integrazione delle applicazioni o i casi d'AWSuso delle applicazioni. AWS

Quando scrivi criteri di accesso per le directory AWS Managed Microsoft AD che autorizzano AWS le applicazioni, tieni presente che le funzionalità di utenti e gruppi potrebbero essere disponibili chiamando un'API autorizzata di AWS Application o Directory Service Data. Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, Amazon Quick Suite e Amazon Chime forniscono tutte azioni di gestione di utenti e gruppi all'interno delle proprie. APIs Controlla l'accesso a questa funzionalità AWS dell'applicazione con le policy IAM.

Esempi

I seguenti frammenti mostrano i modi errati e corretti per negare `DeleteUser` la funzionalità quando AWS applicazioni, come WorkDocs Amazon WorkMail, sono autorizzate nella directory.

Errato

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "ds-data:DeleteUser"
            ],
            "Resource": "*"
        }
    ]
}
```

Corretto

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [{
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "ds-data:DeleteUser",
                "workmail:DeleteUser",
                "workdocs:DeleteUser"
            ],
            "Resource": "*"
        }
    ]
}
```

Utilizzo di ruoli collegati ai servizi per Directory Service

AWS Directory Serviceutilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM a cui è collegato direttamente. Directory

Service I ruoli collegati ai servizi sono predefiniti Directory Service e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione Directory Service perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Directory Servicedefinisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo può assumerne i ruoli. Directory Service Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni, che non possono essere collegate a un'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo si evita di perdere l'accesso alle Directory Service risorse perché non è possibile rimuovere inavvertitamente le autorizzazioni di accesso alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi consulta Servizi AWS che funzionano con IAM.

Argomenti

Autorizzazioni di ruolo collegate al servizio per Directory Service

Directory Serviceutilizza il ruolo collegato al servizio denominato AWSServiceRoleForDirectoryService: consente di monitorare i controller di dominio AWS autogestiti del cliente.

Ai fini dell'assunzione del ruolo, il ruolo collegato al servizio AWSServiceRoleForDirectoryService considera attendibili i seguenti servizi:

- `ds.amazonaws.com`

La politica di autorizzazione dei ruoli denominata AWSDirectory ServiceServiceRolePolicy consente di Directory Service completare le seguenti azioni sulle risorse specificate. Per le autorizzazioni

complete della policy, vedere AWSDirectoryServiceServiceRolePolicynel AWSManaged Policy Reference.

- `ec2`— Consente al servizio di descrivere risorse di rete come sottoreti VPCs, gruppi di sicurezza e interfacce di rete per convalidare le configurazioni di connettività ibrida:
  - `ec2:DescribeAvailabilityZones`
  - `ec2:DescribeDhcpOptions`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:DescribeVpcs`
- `ssm`— Consente al servizio di inviare e monitorare le PowerShell guilabel ai controller di dominio locali per scopi di monitoraggio e valutazione:
  - `ssm:Sendguilabel`
  - `ssm:Listguilabels`
  - `ssm:GetguilabelInvocation`
  - `ssm:DescribeInstanceInformation`
  - `ssm:GetConnectionStatus`

Per consentire a utenti, gruppi o ruoli di creare, modificare o eliminare un ruolo orientato ai servizi, devi configurare le 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 Directory Service

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando consenti di AWS monitorare i controller di dominio autogestiti del cliente nell'APIConsole di gestione AWS, l'o l'AWSAPIAWS CLI, Directory Service crea automaticamente il ruolo collegato al servizio. Per ulteriori informazioni su questa modifica, consulta Aggiornamenti delle politiche.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nell'account, se è stata completata un'operazione in un altro servizio che utilizza le caratteristiche supportate da questo

ruolo. Inoltre, se utilizzavi il Directory Service servizio prima del 1° gennaio 2017, quando ha iniziato a supportare i ruoli collegati al servizio, hai Directory Service creato il AWSServiceRoleForDirectoryServiceruolo nel tuo account. Per ulteriori informazioni, vedi A new role appeared in my. Account AWS

Modifica di un ruolo collegato al servizio per Directory Service

Directory Servicenon consente di modificare il ruolo collegato al AWSServiceRoleForDirectoryServiceservizio. 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 Directory Service

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

> **Note**
>
> Se il Directory Service servizio utilizza il ruolo nel momento in cui si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare Directory Service le risorse utilizzate da AWSService RoleForDirectoryService

- Per eliminare la tua directory, consultaEliminazione di AWS Managed Microsoft AD.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAMAWS CLI, o l'AWSAPI per eliminare il ruolo AWSServiceRoleForDirectoryServicecollegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente IAM.

Regioni supportate per i ruoli collegati ai servizi Directory Service

Directory Servicenon supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Tuttavia, Directory Service utilizza il AWSServiceRoleForDirectoryServiceruolo solo Regioni AWS quando è possibile attivare le directory ibride.

Supporto regionale con opt-in per le directory ibride

Nome della Regione	Identità della Regione	supporto opt-in
Stati Uniti orientali (Virginia settentri onale)	us-east-1	Sì
Stati Uniti orientali (Ohio)	us-east-2	Sì
Stati Uniti occidentali (California settentri onale)	us-west-1	Sì
Stati Uniti occidentali (Oregon)	us-west-2	Sì
Europa (Stoccolma)	eu-north-1	Sì
Medio Oriente (Bahrein)	me-south-1	Sì
Asia Pacifico (Mumbai)	ap-south-1	Sì
Europa (Parigi)	eu-west-3	Sì
Asia Pacifico (Giacarta)	ap-southeast-3	Sì
Africa (Città del Capo)	af-south-1	Sì
Europa (Irlanda)	eu-west-1	Sì
Medio Oriente (Emirati Arabi Uniti)	me-central-1	Sì
Europa (Francoforte)	eu-central-1	Sì
Sud America (San Paolo)	sa-east-1	Sì
Asia Pacific (Hong Kong)	ap-east-1	Sì

Nome della Regione	Identità della Regione	supporto opt-in
Asia Pacifico (Hyderabad)	ap-south-2	Sì
Asia Pacifico (Seoul)	ap-northeast-2	Sì
Asia Pacifico (Osaka)	ap-northeast-3	Sì
Europa (Londra)	eu-west-2	Sì
Asia Pacifico (Melbourne)	ap-southeast-4	Sì
Europe (Milan)	eu-south-1	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	Sì
Asia Pacifico (Singapore)	ap-southeast-1	Sì
Asia Pacifico (Sydney)	ap-southeast-2	Sì
Canada (Centrale)	ca-central-1	Sì
Europa (Spagna)	eu-south-2	Sì
Europa (Zurigo)	eu-central-2	Sì

Registrazione e monitoraggio AWS Directory Service

Come best practice, monitora la tua organizzazione per accertarti che le modifiche vengano registrate. Questo ti aiuta a garantire che eventuali modifiche impreviste possano essere esaminate e che le modifiche indesiderate possano essere ripristinate. AWS Directory Serviceattualmente supporta i due AWS servizi seguenti, quindi è possibile monitorare l'organizzazione e l'attività che si svolge al suo interno.

- Amazon CloudWatch : puoi utilizzare CloudWatch Events con il tipo di directory AWS Managed Microsoft AD. Per ulteriori informazioni, consulta Abilitazione dell'inoltro CloudWatch dei log di Amazon Logs per Managed Microsoft AD AWS. Inoltre, puoi utilizzare CloudWatch Metrics per monitorare le prestazioni dei controller di dominio. Per ulteriori informazioni, consulta Determinare quando aggiungere controller di dominio con metriche CloudWatch .

- AWS CloudTrail
  - È possibile utilizzarlo CloudTrail con tutti i tipi di Directory Service directory. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS Directory Service API utilizzando AWS CloudTrail.
  - Puoi utilizzarlo CloudTrail con AWS Managed Microsoft AD nell'API Directory Service Data. Per ulteriori informazioni, consulta Registrazione delle chiamate API dei dati del AWS Directory Service utilizzando AWS CloudTrail.

Registrazione delle chiamate AWS Directory Service API utilizzando AWS CloudTrail

L'API AWS Managed Microsoft AD è integrata conAWS CloudTrail, un servizio che acquisisce le chiamate API effettuate da o per conto di AWS Managed Microsoft AD nel tuo computer Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. CloudTrail acquisisce le chiamate API dalla console AWS Managed Microsoft AD e dalle chiamate di codice a AWS Managed Microsoft AD APIs. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare quale richiesta è stata effettuata a AWS Managed Microsoft AD, l'indirizzo IP di origine da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e così via. Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

AWSInformazioni Microsoft AD gestite in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività in AWS Managed Microsoft AD, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella Cronologia eventi. Puoi visualizzare, cercare e scaricare eventi recenti inAccount AWS. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuoAccount AWS, compresi gli eventi per AWS Managed Microsoft AD, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail

- 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 nel tuoAccount AWS, tutte le chiamate API effettuate alle azioni di AWS Managed Microsoft AD vengono tracciate nei file di registro. AWSI record Microsoft AD gestiti 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. Tutte le chiamate effettuate all'Directory ServiceAPI o alla CLI vengono registrate da. CloudTrail

Ogni voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni sull'identità dell'utente nel registro aiutano a determinare se la richiesta è stata effettuata con credenziali utente root o IAM, con credenziali di sicurezza temporanee per un ruolo o un utente federato o da un altro servizio. AWS Per ulteriori informazioni, consultare il campo userIdentity in Riferimento agli eventiCloudTrail .

È possibile archiviare i file di log nel bucket per un periodo di tempo indeterminato, ma è anche possibile definire regole per il ciclo di vita di Amazon S3 per archiviare o eliminare automaticamente i file di log. Per impostazione predefinita, i file di log sono crittografati mediante la crittografia lato server (SSE) di Amazon S3.

Puoi scegliere di CloudTrail pubblicare le notifiche di Amazon SNS quando vengono consegnati nuovi file di log se desideri intervenire rapidamente dopo la consegna dei file di log. Per ulteriori informazioni, consulta Configurazione delle notifiche Amazon SNS.

Puoi anche aggregare i file di log di Microsoft AD AWS gestiti da più AWS regioni e Account AWS in un unico bucket Amazon S3. Per ulteriori informazioni, consulta Aggregazione dei file di CloudTrail log in un singolo bucket Amazon S3.

Informazioni sulle voci AWS gestite dei file di registro di Microsoft AD

CloudTrail i file di registro possono contenere una o più voci di registro, ognuna delle quali è composta da più eventi in formato JSON. Una voce di log rappresenta una singola richiesta emessa da qualsiasi origine e include informazioni sull'operazione richiesta, eventuali parametri, la data e l'ora dell'operazione e così via. Non è garantito che le voci di registro siano in un ordine particolare; in altre parole, non sono una traccia ordinata dello stack delle chiamate API pubbliche.

Le informazioni sensibili, ad esempio le password, i token di autenticazione, i commenti e i contenuti dei file, vengono incluse nelle voci di log.

L'esempio seguente mostra un esempio di voce di CloudTrail registro per AWS Managed Microsoft AD:

```
{
  "Records" : [
    {
      "eventVersion" : "1.02",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "<user_id>",
        "arn" : "<user_arn>",
        "accountId" : "<account_id>",
        "accessKeyId" : "<access_key_id>",
        "userName" : "<username>"
      },
      "eventTime" : "<event_time>",
      "eventSource" : "ds.amazonaws.com",
      "eventName" : "CreateDirectory",
      "awsRegion" : "<region>",
      "sourceIPAddress" : "<IP_address>",
      "userAgent" : "<user_agent>",
      "requestParameters" :
      {
        "name" : "<name>",
        "shortName" : "<short_name>",
        "vpcSettings" :
        {
          "vpcId" : "<vpc_id>",
          "subnetIds" : [
            "<subnet_id_1>",
            "<subnet_id_2>"
          ]
        },
        "type" : "<size>",
        "setAsDefault" : <option>,
        "password" : "***OMITTED***"
      },
      "responseElements" :
      {
```

```
        "requestId" : "<request_id>",
        "directoryId" : "<directory_id>"
      },
      "requestID" : "<request_id>",
      "eventID" : "<event_id>",
      "eventType" : "AwsApiCall",
      "recipientAccountId" : "<account_id>"
    }
  ]
}
```

Registrazione delle chiamate API dei dati del AWS Directory Service utilizzando AWS CloudTrail

AWSDirectory Service Data si integra conAWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Directory Service Data. CloudTrail acquisisce tutte le chiamate API per i dati del Directory Service come eventi. Le chiamate acquisite includono chiamate dalla console Directory Service Data e chiamate in codice alle operazioni dell'API Directory Service Data. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per i dati dei Directory Service. Utilizzando le informazioni raccolte da CloudTrail, è possibile determinare la richiesta effettuata a Directory Service Data, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni sui dati del Directory Service in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività di evento supportata (eventi di gestione) in Directory Service Data, 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 ultimi 90 giorni di eventi di gestione nel tuoAccount AWS. Per ulteriori informazioni, vedere Visualizzazione degli eventi con la cronologia degli CloudTrail eventi. La visualizzazione della cronologia degli eventi è gratuita.

Per una registrazione continua degli eventi nel tuoAccount AWS, inclusi gli eventi per Directory Service Data, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare

ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le azioni di Directory Service Data vengono registrate CloudTrail e documentate nel Directory Service Data API Reference. Ad esempio, le chiamate alle `AddGroupMember` `SearchGroups` azioni `DescribeUser` e generano voci nei file di CloudTrail registro.

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 AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di log dei dati del Directory Service

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'CreateUserazione.

```
{
      "eventVersion": "1.08",
      "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "1234567890abcdef0",
            "arn": "arn:aws:iam::111222333444:role/AdAdmin",
            "accountId": "111222333444",
            "userName": "AdAdmin"
          },
          "attributes": {
            "creationDate": "2023-05-30T18:22:38Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2023-05-30T19:17:03Z",
      "eventSource": "ds.amazonaws.com",
      "eventName": "CreateUser",
      "awsRegion": "ap-northeast-2",
      "sourceIPAddress": ": 10.24.34.0",
      "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.create-user",
      "requestParameters": {
        "directoryId": "d-1234567890",
        "sAMAccountName": "johnsmith",
        "clientToken": "example_token"
        "emailAddress": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "surname": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "otherAttributes": {
          "physicalDeliveryOfficeName": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "telephoneNumber": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "streetAddress": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "displayName": {
```

```
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "homePhone": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "postalCode": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          },
          "description": {
            "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
          }
        },
        "clientToken": "createUserToken4"
      },
      "responseElements": {
        "directoryId": "d-1234567890",
        "sID": "S-1-5-21-1234567890-123456789-123456789-1234",
        "sAMAccountName": "johnsmith"
      },
      "additionalEventData": {
        "SID": "S-1-5-21-1234567890-123456789-123456789-1234"
      },
      "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
      "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
      "readOnly": false,
      "resources": [
        {
          "accountId": "111222333444",
          "type": "AWS::DirectoryService::MicrosoftAD",
          "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
      ],
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111222333444",
      "eventCategory": "Management",
      "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
      }
},
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListUsersazione.

Le azioni che non creano o modificano un oggetto restituiscono una risposta nulla.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T18:22:38Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-30T18:22:52Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "ListUsers",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.list-users",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "maxResults": 1
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1244",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
```

```
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ListGroupsazione.

> **Note**
>
> L'`NextToken`elemento viene rimosso da tutte le voci di registro.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T18:22:38Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-05-30T18:29:15Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "ListGroups",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.list-groups",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "nextToken": "REDACTED",
        "maxResults": 1
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```


Voci di registro per errori di eccezione

L'esempio seguente mostra una voce di CloudTrail registro per un errore di accesso negato. Per informazioni su questo errore, consulta Risoluzione dei messaggi di errore di accesso negato nella Guida per l'utente IAM.

> **Note**
>
> Il registro di accesso negato non mostra i parametri della richiesta.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-31T23:25:49Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-31T23:38:18Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "CreateUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.create-user",
    "errorCode": "AccessDenied",
    "errorMessage": "User: arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-
role is not authorized to perform: ds-data:CreateUser on resource: arn:aws:ds:ap-
northeast-2:111222333444:directory/d-1234567890 because no identity-based policy allows
 the ds-data:CreateUser action",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
```

```
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```

L'esempio seguente mostra una voce di CloudTrail registro per un errore Resource Not Found.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T20:41:50Z",
                "mfaAuthenticated": "false"
            }
        }
```

```
    },
    "eventTime": "2023-05-30T21:10:16Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "DescribeUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
 command/ds-data.describe-user",
    "errorCode": "ResourceNotFoundException",
    "errorMessage": "User not found in directory d-1234567890.",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "sAMAccountName": "nonExistingUser",
        "otherAttributes": [
            "co",
            "givenName",
            "sn",
            "telephoneNumber"
        ]
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444"
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}
```

Convalida della conformità per AWS Directory Service

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWSconformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzandoAWS 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'utilizzoServizi AWS, consulta AWSla documentazione sulla sicurezza.

Resilienza in AWS Directory Service

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWSLe 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

Oltre all'infrastruttura AWS globale, Directory Service offre la possibilità di scattare istantanee manuali dei dati in qualsiasi momento per supportare le esigenze di resilienza e backup dei dati. Per ulteriori informazioni, consulta Ripristino di AWS Managed Microsoft AD con istantanee.

Sicurezza dell'infrastruttura in AWS Directory Service

In quanto servizio gestito, AWS Directory Service è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi AWS di sicurezza e su come AWS protegge l'infrastruttura, consulta AWSCloud 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.

Utilizzate chiamate API AWS pubblicate per accedere Directory Service 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.

Prevenzione del confused deputy tra servizi

Il problema confused deputy è un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire un'azione può costringere un'entità maggiormente privilegiata a eseguire l'azione. NelAWS, l'impersonificazione tra servizi può portare al confuso problema del vicesceriffo. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse dell'account.

Si consiglia di utilizzare `aws:SourceArn`le chiavi di contesto della condizione `aws:SourceAccount`globale nelle politiche delle risorse per limitare le autorizzazioni che Directory Service per Microsoft Active Directory forniscono un altro servizio alla risorsa. Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un ARN di un bucket Amazon S3, è necessario utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` deve utilizzare lo stesso ID account nella stessa dichiarazione di policy. Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizzare `aws:SourceAccount` se si desidera consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

Per l'esempio seguente, il valore di `aws:SourceArn` deve essere un gruppo di CloudWatch log.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di

contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:servicename:*:123456789012:*`.

L'esempio seguente mostra come è possibile utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition in AWS Managed Microsoft AD per evitare il confuso problema del vice.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "logs:CreateLogStream",
            "logs:PutLogEvents"
        ],
        "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/
directoryservice/Log_Group_Name:*"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/Directory_Name"
             },
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            }
        }
    }
}
```

Per l'esempio seguente, il valore di `aws:SourceArn` deve essere un argomento SNS nel tuo account. Ad esempio, puoi usare qualcosa come `arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f` «ap-southeast-1" è la

tua regione, «123456789012" è il tuo ID cliente e" _d-966739499f» è il nome dell'argomento Amazon SNS che hai creato. DirectoryMonitoring

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

L'esempio seguente mostra come è possibile utilizzare le chiavi di contesto `aws:SourceArn` e `aws:SourceAccount` global condition in AWS Managed Microsoft AD per evitare il confuso problema del vice.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "SNS:GetTopicAttributes",
            "SNS:SetTopicAttributes",
            "SNS:AddPermission",
            "SNS:RemovePermission",
            "SNS:DeleteTopic",
            "SNS:Subscribe",
            "SNS:ListSubscriptionsByTopic",
            "SNS:Publish"
        ],
        "Resource": [
            "arn:aws:sns:us-east-1:111122223333:SNS_TOPIC_NAME"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/EXTERNAL_DIRECTORY_ID"
            },
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
```

```
            }
        }
    }
}
```

L'esempio seguente mostra una policy di attendibilità IAM per un ruolo a cui è stato delegato l'accesso alla console. Il valore di `aws:SourceArn` deve essere una risorsa di directory nel tuo account. Per ulteriori informazioni, vedere Tipi di risorse definiti da Directory Service. Ad esempio, puoi utilizzare `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890` dove `123456789012` è il tuo ID cliente e `d-1234567890` è l'ID directory.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole"
        ],
        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/YOUR_DIRECTORY_ID"
            },
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            }
        }
    }
}
```

Directory ServiceAPI e interfaccia tramite endpoint Amazon VPC AWS PrivateLink

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC Directory Service e i dati del Directory Service. APIs Ciò ti consente di accedere Directory Service ai dati del Directory Service APIs come se fossero nel tuo VPC e senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze del tuo Amazon VPC non richiedono indirizzi IP pubblici per Directory Service accedere ai dati dei Directory Service. APIs

Per stabilire una connessione privata, crei un'interfaccia Amazon VPC che alimenta. AWS PrivateLink In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti, che fungono da punto di ingresso per il traffico destinato ai Directory Service Data e ai Directory AWS Directory Service Service AWS Data.

Per ulteriori informazioni, consulta Access Servizi AWS through AWS PrivateLink nella Guida. AWS PrivateLink

Considerazioni relative ai dati Directory Service del Directory Service

Con Directory Service e Directory Service Data, puoi richiamare azioni API tramite gli endpoint dell'interfaccia. Per informazioni sui prerequisiti da considerare prima di creare un endpoint di interfaccia, consulta Accedere a un endpoint Amazon VPC Servizio AWS con interfaccia nella Guida. AWS PrivateLink

Directory Servicee disponibilità dei dati del Directory Service

Directory Servicee Directory Service Data supporta gli endpoint di interfaccia Regioni AWS ovunque siano disponibili. Per informazioni sul Regioni AWS supporto Directory Service e sui dati del Directory Service, vedere Disponibilità regionale per Directory Service.

Crea un'interfaccia, un endpoint Amazon VPC e i dati di Directory Directory Service Service

Puoi creare un endpoint di interfaccia per Directory Service e Directory Service Data APIs utilizzando la console Amazon VPC o AWS Command Line Interface il AWS CLI ().

Esempio:Directory Service

Crea un endpoint di interfaccia per Directory Service APIs utilizzare il seguente nome di servizio:

```
com.amazonaws.region.ds
```

Esempio: dati del Directory Service

Crea un endpoint di interfaccia per Directory Service Data APIs utilizzando il seguente nome di servizio:

```
com.amazonaws.region.ds-data
```

Per ulteriori informazioni sulla creazione di un endpoint di interfaccia, consulta Accedere a un endpoint Amazon VPC Servizio AWS con interfaccia nella Guida. AWS PrivateLink

Crea una policy di endpoint Amazon VPC per la tua interfaccia Amazon VPC endpoint

Una policy per gli endpoint è una politica delle risorse IAM che colleghi a un endpoint di interfaccia.

> **Note**
>
> Se non alleghi una policy di endpoint all'endpoint dell'interfaccia, AWS PrivateLink allega una policy endpoint predefinita all'endpoint di interfaccia per tuo conto. Per ulteriori informazioni, consulta Concetti di base di AWS PrivateLink.

Una policy di endpoint specifica le informazioni riportate di seguito:

- I principali (utenti IAM e Account AWS ruoli IAM) che possono eseguire azioni
- Le azioni che possono essere eseguite
- Le risorse su cui è possibile eseguire le azioni

Per ulteriori informazioni, consulta la sezione Controllo dell'accesso ai servizi con policy di endpoint nella Guida di AWS PrivateLink.

Puoi controllare l'accesso APIs dal tuo Amazon VPC allegando una policy personalizzata per gli endpoint all'endpoint di interfaccia.

Esempio: policy degli endpoint Amazon VPC per le azioni API Directory Service

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando colleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle Directory Service azioni elencate a tutti i principali su tutte le risorse.

Sostituisci *action-1* e *action-3* con le autorizzazioni richieste per quelle Directory Service APIs che desideri includere nella tua politica. *action-2* Per un elenco completo, consultare Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:action-1",
            "ds:action-2",
            "ds:action-3"
         ],
         "Resource":"*"
      }
   ]
}
```

Esempio: policy degli endpoint Amazon VPC per le azioni dell'API Directory Service Data

Di seguito è riportato l'esempio di una policy dell'endpoint personalizzata. Quando alleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni Directory Service Data elencate per tutti i principali su tutte le risorse.

Sostituisci *action-1* e *action-3* con le autorizzazioni richieste per i dati del Directory Service APIs che desideri includere nella tua politica. *action-2* Per un elenco completo, consultare Directory ServiceAutorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds-data:action-1",
            "ds-data:action-2",
            "ds-data:action-3"
```

```
         ],
         "Resource":"*"
      }
   ]
}
```

Accordo sul livello di servizio per Directory Service

Directory Service è un servizio ad alta disponibilità ed è basato su un'infrastruttura AWS gestita. È supportato da un accordo sul livello di servizio (SLA) che definisce la nostra politica di disponibilità del servizio.

- Lo SLA si applica a AWS Managed Microsoft AD, AD Connector e Simple AD.
- Lo SLA descrive i crediti di servizio, le esclusioni degli SLA e definisce termini come «Covered Directory», «Percentuale di uptime mensile» e «Richieste».
- Per ulteriori informazioni, consulta il Contratto sul livello di servizio per Directory Service.

Disponibilità regionale per Directory Service

La tabella riportata di seguito fornisce un elenco degli endpoint specifici della regione supportati in base al tipo di directory.

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
Stati Uniti orientali (Virginia settentrionale)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 Sì	 Sì	 Sì	 Sì
Stati Uniti orientali (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 Sì	 Sì	 Sì	 No
Stati Uniti occidentali (California settentrionale)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 Sì	 Sì	 Sì	 No
Stati Uniti	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 Sì	 Sì	 Sì	 Sì

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard ed Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
occidentali (Oregon)							
Africa (Città del Capo)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 S	 S	 S	 No
Asia Pacific (Hong Kong)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 S	 S	 S	 No
Asia Pacifico (Taipei)	ap-east-2	ds.ap-east-2.amazonaws.com	HTTPS	 S	 N	 S	 No
Asia Pacifico (Hyderad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 S	 S	 S	 No
Asia Pacifico (Giacarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 S	 S	 S	 No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard ed Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
Asia Pacifico (Malesia	ap-southeast-5	ds.ap-southeast-5.amazonaws.com	HTTPS	S	N	S	No
Asia Pacifico (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	S	S	S	No
Asia Pacifico (Thailandia)	ap-southeast-7	ds.ap-southeast-7.amazonaws.com	HTTPS	S	N	S	No
Asia Pacifico (Nuova Zelanda	ap-southeast-6	ds.ap-southeast-6.amazonaws.com	HTTPS	S	N	S	No
Asia Pacifico (Mumbai	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	S	S	S	No
Asia Pacifico (Osaka-Locale)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	S	S	S	No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard ed Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
Asia Pacific (Seoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Asia Pacifico (Singapore)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	Sì	Sì	Sì	Sì
Asia Pacifico (Sydney	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	Sì	Sì	Sì	Sì
Asia Pacifico (Tokyo)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	Sì	Sì	Sì	Sì
Canada (Central)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Canada occidentale (Calgary	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	Sì	No	Sì	No
Cina (Pechin	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	Sì	No	Sì	No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard ed Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
China (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	Sì	No	Sì	No
Europa (Francoforte)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Europa (Irlanda)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	Sì	Sì	Sì	Sì
Europe (Londra)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Europe (Milan)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Europa (Parigi)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Europa (Spagna)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	Sì	Sì	Sì	No
Europa (Stoccolma)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	Sì	Sì	Sì	No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard ed Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
Europa (Zurigo)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	 S	 S	 S	 No
Israele (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	 S	 N	 S	 No
Messico (Central)	mx-central-1	ds.mx-central-1.amazonaws.com	HTTPS	 S	 N	 S	 No
Medio Oriente (Bahrein)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	 S	 S	 S	 No
Medio Oriente (Emirati Arabi Uniti)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 S	 S	 S	 No
Sud America (San Paolo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 S	 S	 S	 No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicrosoft AD gestito (edizione Standard ed Enterprise)	AWSMicrosoft AD gestito (edizione ibrida)	AD Connector	Simple AD
AWSGovCloud (Stati Uniti occidentali)	us-gov-west-1	annunci. us-gov-west-1. amazonaws.com	HTTPS	S	N	S	No
AWSGovCloud (Stati Uniti orientali)	us-gov-east-1	annunci. us-gov-east-1. amazonaws.com	HTTPS	S	N	S	No

Per informazioni sull'utilizzo Directory Service nella regione AWS GovCloud (Stati Uniti occidentali) e AWS GovCloud nella regione (Stati Uniti orientali), consulta Service Endpoints nella Guida per l'utente. AWS GovCloud (US)

Per informazioni sull'utilizzo Directory Service nelle regioni di Pechino e Ningxia, consulta Endpoints e ARNs Amazon Web Services in Cina in Guida introduttiva in AWS Cina.

Per informazioni sugli endpoint FIPS supportati da Directory Service Data, vedere Endpoint e quote di Directory Service Data nella Guida di riferimento. Riferimenti generali di AWS

Supportato Regioni AWS per i dati del Directory Service

La tabella seguente fornisce un elenco degli endpoint specifici della regione supportati da Directory Service Data per tipo di directory.

Nome Regione	Regione	Endpoint	Protocollo	AWSMicroft AD gestito	AD Connect	Simple AD
Stati Uniti orientali (Ohio)	us-east-2	ds-data.us-east-2.amazonaws.com	HTTPS	S	N	No
Stati Uniti orientali (Virginia settentrionale)	us-east-1	ds-data.us-east-1.amazonaws.com	HTTPS	S	N	No
Stati Uniti occidentali (California settentrionale)	us-west-1	ds-data.us-west-1.amazonaws.com	HTTPS	S	N	No
Stati Uniti occidentali (Oregon)	us-west-2	ds-data.us-west-2.amazonaws.com	HTTPS	S	N	No
Asia Pacific (Hong Kong)	ap-east-1	ds-data.ap-east-1.amazonaws.com	HTTPS	S	N	No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicroft AD gestito	AD Connect	Simple AD
Asia Pacifico (Mumbai	ap-south-1	ds-data.ap-south-1.amazonaws.com	HTTPS	S	N	No
Asia Pacifico (Osaka-Locale)	ap-northeast-3	ds-data.ap-northeast-3.amazonaws.com	HTTPS	S	N	No
Asia Pacific (Seoul)	ap-northeast-2	ds-data.ap-northeast-2.amazonaws.com	HTTPS	S	N	No
Asia Pacifico (Singapore)	ap-southeast-1	ds-data.ap-southeast-1.amazonaws.com	HTTPS	S	N	No
Asia Pacifico (Sydney)	ap-southeast-2	ds-data.ap-southeast-2.amazonaws.com	HTTPS	S	N	No
Asia Pacifico (Tokyo)	ap-northeast-1	ds-data.ap-northeast-1.amazonaws.com	HTTPS	S	N	No
Canada (Central)	ca-central-1	ds-data.ca-central-1.amazonaws.com	HTTPS	S	N	No
Europa (Francoforte)	eu-central-1	ds-data.eu-central-1.amazonaws.com	HTTPS	S	N	No

Nome Regione	Regione	Endpoint	Protocollo	AWSMicroft AD gestito	AD Connect	Simple AD
Europa (Irlanda)	eu-west-1	ds-data.eu-west-1.amazonaws.com	HTTPS	S	N	No
Europe (London)	eu-west-2	ds-data.eu-west-2.amazonaws.com	HTTPS	S	N	No
Europa (Parigi)	eu-west-3	ds-data.eu-west-3.amazonaws.com	HTTPS	S	N	No
Europa (Stoccolma)	eu-north-1	ds-data.eu-north-1.amazonaws.com	HTTPS	S	N	No
Sud America (San Paolo)	sa-east-1	ds-data.sa-east-1.amazonaws.com	HTTPS	S	N	No

Per informazioni sugli endpoint FIPS supportati da Directory Service Data, vedere Endpoint e quote di Directory Service Data nella Guida di riferimento. Riferimenti generali di AWS

Compatibilità del browser per AWS Directory Service

AWSapplicazioni e servizi come Amazon WorkSpaces, Amazon Connect WorkMail, Amazon Chime e AWS IAM Identity Center tutti richiedono credenziali di accesso valide da un browser compatibile prima di potervi accedere. WorkDocs La tabella seguente descrive solo i browser e le versioni dei browser compatibili per gli accessi.

Browser	Versione	Compatibilità
Microsoft Edge	Ultime 3 versioni	Compatible
Mozilla Firefox	Ultime 3 versioni	Compatible
Google Chrome	Ultime 3 versioni	Compatible
Apple Safari	Ultime 3 versioni	Compatible

Ora che hai verificato che stai utilizzando una versione supportata del tuo browser, ti consigliamo di consultare anche la sezione seguente per verificare che il tuo browser sia stato configurato per utilizzare l'impostazione Transport Layer Security (TLS) richiesta daAWS.

Che cos'è TLS?

TLS è un protocollo utilizzato dai browser Web e da altre applicazioni per scambiare dati in modo sicuro su una rete. TLS garantisce che una connessione a un endpoint remoto avvenga all'endpoint previsto tramite la crittografia e la verifica dell'identità dell'endpoint. Le versioni di TLS, aggiornate, sono TLS 1.0, 1.1, 1.2 e 1.3.

Quali versioni TLS sono supportate dal Centro identità IAM

AWSle applicazioni e i servizi supportano TLS 1.1, 1.2 e 1.3 per accessi sicuri. A partire dal 30 ottobre 2019, TLS 1.0 non è più supportato, quindi è importante che tutti i browser siano configurati per supportare TLS 1.1 o versioni successive. Ciò significa che non sarà possibile accedere ad applicazioni e servizi AWS se vi accedi quando TLS 1.0 è abilitato. Per assistenza per apportare questa modifica, contattare l'amministratore.

Come abilito le versioni TLS supportate nel browser?

Dipende dal tuo browser. Di solito puoi trovare questa impostazione nell'area delle impostazioni avanzate del tuo browser. Ad esempio, in Internet Explorer sono disponibili diverse opzioni TLS in Proprietà Internet, nella scheda Avanzate e quindi nella sezione Sicurezza. Consultate il sito di assistenza del produttore del browser per istruzioni specifiche.

Cronologia dei documenti

La tabella seguente descrive le importanti modifiche apportate rispetto all'ultima versione della Guida per l'amministratore di AWS Directory Service.

Modifica	Descrizione	Data
Supporto per tipi di rete dual-stack	AWS Directory Serviceora supporta l'aggiornamento del tipo di rete di directory da IPv4 a dual stack (e). IPv4 IPv6 Questa funzionalità offre uno spazio di indirizzi più ampio e consente la IPv6 connettività per le directory. Puoi anche aggiornare le directory AD Connector e le directory Simple AD con il supporto dual stack.	30 settembre 2025
Nuovo ruolo collegato AWS al servizio	Directory Serviceaggiunge un nuovo ruolo collegato al AWS servizio AWSServiceRoleForDirectoryService e una politica AWS gestita,AWSDirectoryServiceServiceRolePolicy. La policy consente di AWS monitorare i controller di dominio gestiti dal cliente.	30 luglio 2025
AWSMicrosoft AD gestito (edizione ibrida)	AWSManaged Microsoft AD (Hybrid Edition) collega l'Active Directory autogestito con AWS Directory Service per Microsoft Active Directory, creando un ambiente di identità integrato	30 luglio 2025

	che copre sia l'infrastruttura che il. Cloud AWS	
Argomento aggiornato sulla registrazione e il monitoraggio: nuove sezioni	Sezioni incluse AWS Directory Service e AWS Directory Service Data nell'argomento di registrazione e monitoraggio.	18 settembre 2024
Nuova API e nuovi attributi per i dati del Directory Service	AWSDirectory Service Data fornisce una gestione integrata degli oggetti. Ora puoi trovare e aggiornare gli oggetti con un elenco di attributi AD supportati.	18 settembre 2024
AWSpolitiche gestite: nuove politiche	AWSDirectory Service Data aggiunge nuove politiche AWS gestite: AWSDirectoryServiceDataFullAccess eAWSDirectoryServiceDataReadOnlyAccess. Le politiche garantiscono l'accesso alla gestione degli oggetti Directory Service Data.	18 settembre 2024
Impostazioni di autenticazione basate sui certificati	Sono stati aggiunti contenuti su due nuove impostazioni di sicurezza per AWS Managed Microsoft AD.	11 aprile 2023
AWS PrivateLink	Sono stati aggiunti contenuti su AWS PrivateLink.	31 marzo 2023
Endpoint VPC Simple AD	Sono stati aggiunti contenuti su quali endpoint VPC non devono essere configurati.	25 agosto 2021

Endpoint VPC AD Connector	Sono stati aggiunti contenuti su quali endpoint VPC non devono essere configurati.	25 agosto 2021
Supporto per smart card	Aggiunti contenuti sul supporto per smart card e Amazon WorkSpaces Application Manager nella regione AWS GovCloud (Stati Uniti occidentali)	1 dicembre 2020
Reimpostazione della password	Sono stati aggiunti contenuti su come reimpostare le password degli utenti utilizzando Console di gestione AWS, PowerShell e. AWS CLI	2 gennaio 2019
Condivisione delle directory	Sono stati aggiunti contenuti su come utilizzare la condivisione di directory con AWS Managed Microsoft AD.	25 settembre 2018
Contenuti migrati nella nuova Guida per gli sviluppatori della directory del cloud Amazon	Il contenuto della directory del cloud Amazon è stato spostato da questa guida alla nuova Guida per gli sviluppatori della directory del cloud Amazon.	21 giugno 2018
Riorganizzazione completa del sommario della guida per l'amministratore	Sono stati riorganizzati i contenuti per concentrarci in modo più diretto sulle esigenze dei clienti. Inoltre, sono stati aggiunti nuovi contenuti laddove necessario.	5 Aprile 2018

AWSgruppi delegati	È stato aggiunto un elenco di gruppi AWS delegati che possono essere assegnati agli utenti locali.	8 marzo 2018
Policy granulari delle password	Sono stati aggiunti nuovi contenuti relativi alle nuove policy delle password.	5 luglio 2017
Controller di dominio aggiuntivi	Sono stati aggiunti contenuti su come aggiungere altri controller di dominio alla directory in Microsoft AD gestito da AWS.	30 giugno 2017
Tutorial	Aggiunti nuovi tutorial per testare un ambiente di laboratorio AWS Microsoft AD gestito.	21 giugno 2017
MFA con AWS Microsoft AD gestito	Sono stati aggiunti contenuti sull'utilizzo della MFA con Managed AWS Microsoft AD.	13 febbraio 2017
Directory del cloud Amazon	Sono stati aggiunti contenuti su un nuovo tipo di directory.	26 gennaio 2017
Estensioni dello schema	Aggiunto contenuto sulle estensioni dello schema con AWS Directory Service per Microsoft Active Directory.	14 novembre 2016
Riorganizzazione importante della Directory Service Guida per l'amministratore	Sono stati riorganizzati i contenuti per concentrarci in modo più diretto sulle esigenze dei clienti.	14 novembre 2016

Notifiche SNS	Sono stati aggiunti contenuti sulle notifiche SNS.	25 febbraio 2016
Autorizzazione e autenticazione	Sono stati aggiunti contenuti su come utilizzare IAM conDirectory Service.	25 febbraio 2016
AWSMicrosoft AD gestito	Sono stati aggiunti contenuti su AWS Managed Microsoft AD e guide combinate in un'unica guida.	17 Novembre 2015
Concedi alle istanze Linux di essere collegate a una directory Simple AD	Sono stati aggiunti contenuti su come collegare un'istanza Linux a una directory Simple AD.	23 luglio 2015
Separazione delle guide	Suddividi la Guida all'amministrazione di Directory Service in guide separate.	14 luglio 2015
Supporto Single Sign-On	Sono stati aggiunti contenuti sul supporto per il Single Sign-On.	31 marzo 2015
Nuova guida	Questa è la prima versione della Guida all'amministrazione di AWS Directory Service.	21 Ottobre 2014

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.