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 di utilizzare Microsoft Active Directory (AD) con altri AWS servizi. Le directory memorizzano 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.

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 l'opzione di AWS Directory Service directory 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 un servizio effettivo Microsoft Active Directory nel AWS cloud che supporti carichi di lavoro compatibili con Active Directory —aware o AWS applicazioni e servizi come Amazon e WorkSpaces Amazon QuickSight, oppure hai bisogno del supporto LDAP per applicazioni Linux. Usa AD Connector se devi solo consentire agli utenti locali di accedere ad AWS applicazioni e servizi con le proprie Active Directory credenziali. Puoi anche utilizzare AD Connector per aggiungere istanze Amazon EC2 al tuo dominio esistente. Active Directory Usa Simple AD se hai bisogno di una directory a basso costo e a basso costo con Active Directory compatibilità di base che supporti le applicazioni compatibili con Samba 4, oppure hai bisogno della compatibilità LDAP per le applicazioni compatibili con LDAP.

Che cosa occorre fare?	AWS Directory Service Opzioni consigliate
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, vedi Come scegliere le soluzioni su. Active DirectoryAWS

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 un Microsoft Windows Server Active Directory sistema effettivo (AD), gestito 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 Chime QuickSight, 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 puoi connetterti alla tua infrastruttura AD esistente con un trust e utilizzare le credenziali di un Active Directory sistema operativo locale o su EC2 Windows. Se unisci istanze EC2 al tuo Managed AWS 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 Managed Microsoft AD supporta anche casi d'uso federati che utilizzano Active Directory credenziali. Da solo, AWS Managed Microsoft AD consente di accedere a AWS Management Console. 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 (precedentemente noto comeAzure Active Directory Connect) e facoltativamente Active Directory Federation Service (ADFS), puoi 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 si tratta di una directory LDAP, è possibile utilizzare anche l'autenticazione AWS Managed Microsoft AD per Linux Secure Shell (SSH) e per altre applicazioni compatibili con LDAP.

AWS fornisce monitoraggio, istantanee giornaliere e ripristino come parte del servizio: aggiungi utenti e gruppi a Managed AWS Microsoft AD e amministra i Criteri di gruppo utilizzando Active Directory strumenti familiari 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 Active Directory funzionalità effettive per supportare AWS applicazioni o Windows carichi di lavoro, tra cui Amazon Relational Database Service for. Microsoft SQL Server È anche la soluzione ideale se desideri una versione autonoma Active Directory 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 AWS Microsoft AD gestito.

AD Connector

AD Connector è un servizio proxy che offre un modo semplice per connettere AWS applicazioni compatibili WorkSpaces, ad esempio Amazon QuickSight, Amazon e Amazon EC2, alle Windows Server applicazioni locali esistenti. Microsoft Active Directory Con AD Connector, puoi semplicemente aggiungere un account di servizio al tuoActive 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 QuickSight, AD Connector legge Active Directory quello 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 Active Directory dominio locali per l'autenticazione. AD Connector funziona con molte AWS applicazioni e servizi tra cui Amazon WorkSpaces, Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect e Amazon. WorkMail Puoi anche unire le tue Windows istanze EC2 al tuo Active Directory dominio locale tramite AD Connector utilizzando l'aggiunta al dominio senza interruzioni. AD Connector consente inoltre agli utenti di accedere AWS Management Console e gestire AWS le risorse accedendo con le Active Directory credenziali 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 AD Connector, continui a gestire i tuoi Active Directory dati come fai ora. Ad esempio, aggiungi nuovi utenti e gruppi e aggiorni le password utilizzando strumenti di Active Directory amministrazione standard in localeActive Directory. 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 Active Directory directory compatibile basata su Samba 4. AWS Directory Service Simple AD supporta Active Directory funzionalità di base come account utente, appartenenza a gruppi, accesso a un dominio Linux o istanze EC2 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. È possibile utilizzare molte applicazioni e strumenti familiari Active Directory che richiedono funzionalità di base. Active Directory Simple AD è compatibile con le seguenti AWS applicazioni: Amazon WorkSpaces WorkDocs, Amazon QuickSight, Amazon e Amazon WorkMail. Puoi anche accedere agli account utente AWS Management Console 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 un server effettivo 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 Active Directory funzionalità di base, AWS applicazioni compatibili o per supportare carichi di lavoro Linux che richiedono il servizio LDAP. Per ulteriori informazioni, consulta Simple AD.

Amazon Cognito

Amazon Cognito è una directory utente che aggiunge la registrazione e l'accesso all'app per dispositivi mobili o all'applicazione Web tramite i pool di utenti.

Quando usare

Puoi utilizzare Amazon Cognito se devi creare campi di registrazione personalizzati e archiviare i metadati nella directory utente. Questo servizio completamente gestito è scalabile per supportare centinaia di milioni di utenti. Per ulteriori informazioni, consulta Pool di utenti di Amazon Cognito nella Guida per gli sviluppatori di Amazon Cognito.

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

Utilizzo di Amazon EC2

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

- Cos'è Amazon EC2? nella Guida per l'utente di Amazon EC2.
- Avvio delle istanze EC2 nella Guida per l'utente di Amazon EC2.
- Gruppi di sicurezza nella Guida per l'utente di Amazon EC2.
- Cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.
- Aggiunta di un gateway privato virtuale hardware al proprio VPC nella Guida per l'utente di Amazon VPC.

Guida introduttiva con AWS Directory Service

Se non l'hai ancora fatto, dovrai anche creare un AWS account e utilizzare il AWS Identity and Access Management servizio per controllare l'accesso.

Per utilizzare AWS Directory Service, è necessario soddisfare i prerequisiti per AWS Directory Service for Microsoft Active Directory, AD Connector o Simple AD. Per ulteriori informazioni, consulta AWS Prerequisiti Microsoft AD gestiti, Prerequisiti di AD Connector o Prerequisiti di Simple AD.

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

  Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente.AWS IAM Identity Center

Ulteriori informazioni

- Per ulteriori informazioni su come accedere come utente IAM Identity Center, consulta Accedere al portale di accesso IAM Identity Center. AWS Management Console
- Per ulteriori informazioni su come accedere AWS Management Console come utente IAM, consulta Accedere AWS Management Console come utente IAM.
- Per ulteriori informazioni sull'utilizzo delle policy IAM per controllare l'accesso alle AWS Directory Service risorse, consultaUtilizzo di politiche basate sull'identità (politiche IAM) per AWS Directory Service.

AWS Microsoft AD gestito

AWS Directory Service consente di eseguire Microsoft Active Directory (AD) come servizio gestito. AWS Directory Service per Microsoft Active Directory, noto anche come AWS Managed Microsoft AD, è basato su Windows Server 2019. Quando selezioni e avvii questo tipo di directory, viene creato come una coppia di controller di dominio ad alta disponibilità collegati al tuo cloud privato virtuale (Amazon VPC). I controller di dominio vengono eseguiti in diverse zone di disponibilità in una regione di tua scelta. Il monitoraggio e il ripristino degli host, la replica dei dati, le snapshot e gli aggiornamenti software vengono automaticamente configurati e gestiti al posto tuo.

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. Puoi anche configurare una relazione di trust tra AWS Managed Microsoft AD in the AWS Cloud e il tuo locale esistente MicrosoftActive Directory, fornendo a utenti e gruppi l'accesso alle risorse in entrambi i domini, utilizzando AWS IAM Identity Center.

AWS Directory Service semplifica la configurazione e l'esecuzione di directory nel AWS cloud o la connessione AWS delle risorse a un locale esistente. Microsoft Active Directory Una volta creata la directory, puoi utilizzarla per un'ampia gamma di attività:

- Gestione di utenti e gruppi
- Fornire Single Sign-On (SSO) ad applicazioni e a servizi
- Creare e applicare policy di gruppo
- Semplifica l'implementazione e la gestione di Linux e dei carichi di lavoro basati sul cloud Microsoft Windows
- È possibile utilizzare AWS Managed Microsoft AD per abilitare l'autenticazione a più fattori mediante l'integrazione con l'infrastruttura MFA esistente basata su RADIUS per fornire un ulteriore livello di sicurezza quando gli utenti accedono alle applicazioni. AWS
- Connessione sicura ad Amazon EC2 Linux e alle istanze Windows

> **Note**
>
> AWS gestisce le licenze delle istanze Windows Server per te; tutto ciò che devi fare è pagare per le istanze che usi. Inoltre, non è necessario acquistare licenze CAL (Windows Server Client Access License) aggiuntive, poiché l'accesso è incluso nel prezzo. Ogni istanza è dotata di due connessioni remote solo per scopi amministrativi. Se sono necessarie più di

due connessioni, o se tali connessioni sono necessarie per scopi diversi dall'amministrazione, potrebbe essere necessario aggiungere altre CAL di Servizi Desktop remoto da utilizzare su AWS.

Leggi gli argomenti di questa sezione per iniziare a creare una directory Microsoft AD AWS gestita, creare una relazione di trust tra AWS Managed Microsoft AD e le directory locali ed estendere lo schema Managed AWS Microsoft AD.

Argomenti

- Guida introduttiva a AWS Managed Microsoft AD
- Concetti fondamentali di Microsoft AD gestito da AWS
- Procedure consigliate per AWS Managed Microsoft AD
- Casi d'uso per AWS Managed Microsoft AD
- Come amministrare AWS Managed Microsoft AD
- AWS Quote Microsoft AD gestite
- Compatibilità delle applicazioni per AWS Managed Microsoft AD
- AWS Tutorial gestiti per laboratori di test Microsoft AD
- Risoluzione dei problemi relativi AWS a Managed Microsoft AD

Articoli correlati AWS del blog sulla sicurezza

- 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 AWS Directory ServiceAWS Managed Microsoft AD
- Come aumentare la ridondanza e le prestazioni di AWS Directory Service for Managed AWS Microsoft AD aggiungendo controller di dominio
- Come abilitare l'uso di desktop remoti distribuendo Microsoft Remote Desktop Licensing Manager su Managed AWS Microsoft AD
- Come accedere all' AWS Management Console 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

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, AWS 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 Distribuzione di controller di dominio aggiuntivi.

Argomenti

- AWS Prerequisiti Microsoft AD gestiti
- Crea il tuo AWS Managed Microsoft AD
- Cosa viene creato con AWS Managed Microsoft AD Active Directory
- Autorizzazioni per l'account Administrator

AWS Prerequisiti Microsoft AD gestiti

Per creare un AWS Managed Microsoft ADActive Directory, è necessario un Amazon VPC con quanto segue:

- Almeno due sottoreti. Ciascuna sottorete deve trovarsi in una diversa zona di disponibilità.
- 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 Active Directory dominio 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.

AWS Directory Service utilizza una struttura a due VPC. Le istanze EC2 che compongono la tua directory vengono eseguite all'esterno del tuo 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.

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 (DC) Microsoft AD AWS gestiti in. AWSÈ 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 controller di dominio AWS Microsoft AD gestiti. 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 controller di dominio Microsoft AD AWS gestiti utilizzati da. AWS

> **Note**
>
> Se il tuo server RADIUS supporta gli indirizzi DNS, è necessario creare solo una configurazione del client RADIUS. In caso contrario, è necessario creare una configurazione del client RADIUS per ogni DC di Microsoft AD gestito da AWS .

- 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 DC e il server RADIUS. I protocolli supportati sono PAP, CHAP MS-CHAPv1 e MS-CHAPv2. MS-CHAPv2 è consigliato perché, fra le tre opzioni, è quello che fornisce la massima protezione.
- 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 DNS AWS gestiti di Microsoft AD DC, vedere il passaggio 1) alla porta del server RADIUS.
3. Aggiungi una regola al gruppo di sicurezza Amazon EC2 nel tuo dominio AWS Microsoft AD 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 Aggiunta di regole a un gruppo di sicurezza nella Guida per l'utente di EC2.

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

Crea il tuo AWS Managed Microsoft AD

Per creare una nuova directory, completa queste fasi. Prima di iniziare la procedura, assicurati di soddisfare i prerequisiti illustrati in AWS Prerequisiti Microsoft AD gestiti.

Per creare una directory Microsoft AD AWS gestita

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.

   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.

   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.

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). La creazione di una directory richiede dai 20 ai 40 minuti. Una volta creato, il valore Status cambia in Active (Attivo).

Cosa viene creato con AWS Managed Microsoft AD Active Directory

Quando crei un Active Directory con AWS Managed Microsoft AD, AWS 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 questi ENI è essenziale per la connettività tra il VPC AWS Directory Service e i controller di dominio e non deve mai essere eliminato. È possibile identificare tutte le interfacce di rete riservate all'uso AWS 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 presso 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 Distribuzione di controller di dominio aggiuntivi.

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

- Crea un Gruppo di sicurezza AWS che stabilisce le regole di rete per il traffico in entrata e in uscita dai controller di dominio. La regola di uscita predefinita consente tutto il traffico ENI o le istanze collegate al gruppo di sicurezza creato. AWS Le regole in entrata predefinite consentono solo il traffico attraverso le porte richieste da Active Directory da qualsiasi origine (0.0.0.0/0). Le regole 0.0.0.0/0 non introducono vulnerabilità di sicurezza poiché il traffico verso i controller di dominio è limitato al traffico proveniente dal tuo VPC, da altri VPC peered o dalle reti che ti sei connesso utilizzando Transit Gateway o Virtual Private Network. AWS Direct Connect AWS Per una protezione aggiuntiva, gli ENI creati non dispongono di IP elastici collegati e non si dispone dell'autorizzazione per collegare un IP elastico a tali ENI. Pertanto, l'unico traffico in entrata che può comunicare con AWS Managed Microsoft AD è il VPC locale e il traffico VPC con routing VPC. 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, consulta Procedure consigliate per AWS Managed Microsoft AD. Le seguenti regole del gruppo AWS di sicurezza vengono create per impostazione predefinita:

  Regole in entrata

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
ICMP	N/D	0.0.0.0/0	Ping	LDAP Keep Alive, DFS
TCP e UDP	53	0.0.0.0/0	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	0.0.0.0/0	Kerberos	Autentica zione utente e computer, trust a livello di foresta
TCP e UDP	389	0.0.0.0/0	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	445	0.0.0.0/0	SMB/CIFS	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP e UDP	464	0.0.0.0/0	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	135	0.0.0.0/0	Replica	RPC, EPM

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP	636	0.0.0.0/0	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	1024 - 65535	0.0.0.0/0	RPC	Replica, autentica zione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	0.0.0.0/0	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
UDP	123	0.0.0.0/0	Ora di Windows	Ora di Windows, trust
UDP	138	0.0.0.0/0	DFSN e NetLogon	DFS, policy di gruppo
Tutti	Tutti	sg-###### ############	All Traffic	

Regole in uscita

Protocollo	Intervallo porte	Destinazione	Tipo di traffico	Utilizzo di Active Directory
Tutti	Tutti	sg-###### ############	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 documentazione Microsoft.
- Crea un account amministratore della directory con nome utente Admin e la password specificata. Questo account è disponibile nella UO Utenti (ad esempio, Corp > Utenti). Utilizzi questo account per gestire la tua rubrica nel AWS Cloud. Per ulteriori informazioni, consulta Autorizzazioni per l'account Administrator.

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

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

Nome UO	Descrizione
AWS Gruppi delegati	Memorizza tutti i gruppi che puoi utilizzare per delegare autorizzazioni AWS specifiche agli utenti.
AWS È riservato	Memorizza tutti gli account specifici di AWS 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

Nome UO	Descrizione

	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 predefini ta, a questa UO corrispondono due UO figlie: Computer e Utenti. Per esempio:
	• Corp
	  • Computer
	  • Utenti

- Crea i seguenti gruppi nell'unità organizzativa Gruppi AWS delegati:

Group name (Nome gruppo)	Descrizione
AWS Operatori di account delegati	I membri di questo gruppo di sicurezza hanno limitate funzionalità di gestione dell'account, come la reimpostazione delle password
AWS Amministratori delegati di attivazione basati su Active Directory	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.
AWS Aggiunta delegata di workstation agli utenti del dominio	I membri di questo gruppo di sicurezza possono aggiungere 10 computer a un dominio
AWS Amministratori delegati	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 nell'unità organizzativa AWS Delegated Groups.

Group name (Nome gruppo)	Descrizione
AWS Oggetti delegati autorizzati ad autentica re oggetti	Ai membri di questo gruppo di sicurezza viene fornita la possibilità di autenticarsi sulle risorse del computer nell'unità organizzativa AWS riservata (necessaria solo per oggetti locali con trust abilitati per l'autenticazione selettiva).
AWS Autenticazione delegata consentita ai controller di dominio	Ai membri di questo gruppo di protezione viene fornita la possibilità di autenticare le risorse del computer nell'unità organizzativa controller di dominio (necessaria solo per gli oggetti locali con autenticazione selettiva abilitata Trusts).
AWS Amministratori delegati a vita degli oggetti eliminati	I membri di questo gruppo di sicurezza possono modificare l'DeletedObjectLif etimeoggetto MSDS-, che definisce per quanto tempo un oggetto eliminato sarà disponibile per il ripristino dal Cestino di AD.
AWS Amministratori delegati del file system distribuito	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere i namespace FRS, DFS-R e DFS
AWS Amministratori delegati del Domain Name System	I membri di questo gruppo di sicurezza possono gestire il DNS integrato con Active Directory.
AWS Amministratori delegati del protocollo Dynamic Host Configuration	I membri di questo gruppo di sicurezza possono autorizzare i server Windows DHCP all'interno dell'azienda.
AWS Amministratori delegati dell'Enterprise Certificate Authority	I membri di questo gruppo di sicurezza possono distribuire e gestire l'infrastruttura dell'autorità di certificazione aziendale di Microsoft.

Group name (Nome gruppo)	Descrizione
AWS Amministratori dettagliati delegati delle politiche in materia di password	I membri di questo gruppo di sicurezza possono modificare le policy delle password fine-grained create in precedenza.
AWS Amministratori FSx delegati	Ai membri di questo gruppo di sicurezza viene fornita la possibilità di gestire le risorse Amazon FSx.
AWS Amministratori delegati delle politiche di gruppo	I membri di questo gruppo di sicurezza possono eseguire attività di gestione delle policy di gruppo (creare, modificare, eliminare , collegare).
AWS Amministratori delegati della delegazio ne Kerberos	I membri di questo gruppo di sicurezza possono abilitare la delega su oggetti di computer e account utenti.
AWS Amministratori delegati degli account di servizio gestito	I membri di questo gruppo di sicurezza possono creare e cancellare account Managed Service.
AWS Dispositivi delegati non conformi a MS-NPRC	Ai membri di questo gruppo di sicurezza verrà fornita l'esclusione dalla richiesta di comunicazioni sicure tra canali con i controlle r di dominio. Questo gruppo è destinato agli account computer.
AWS Amministratori delegati del servizio di accesso remoto	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere server RAS dal gruppo Server RAS e IAS
AWS Amministratori di Delegated Replicate Directory Changes	I membri di questo gruppo di sicurezza possono sincronizzare le informazioni del profilo in Active Directory con Server. SharePoint

Group name (Nome gruppo)	Descrizione
AWS Amministratori di server delegati	I membri di questo gruppo di sicurezza sono inclusi nel gruppo di amministratori locali in tutti i computer collegati al dominio
AWS Amministratori delegati di siti e servizi	I membri di questo gruppo di sicurezza possono rinominare l'oggetto Default-First-Site -Name nei siti e servizi Active Directory.
AWS Amministratori delegati di gestione del sistema	I membri di questo gruppo di sicurezza possono creare e gestire gli oggetti nel container System Management.
AWS Amministratori delegati delle licenze di Terminal Server	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere server Terminal Server License dal gruppo di server Terminal Server License
AWS Amministratori del suffisso del nome principale dell'utente delegato	I membri di questo gruppo di sicurezza possono aggiungere e rimuovere i suffissi nome principali degli utenti

- Crea e applica i seguenti oggetti policy di gruppo:

> **Note**
>
> Non disponi delle autorizzazioni per eliminare, modificare o scollegare questi GPO. Ciò è dovuto alla progettazione, in quanto sono riservati all'uso. AWS È possibile collegarli alle unità organizzative da te controllate, se necessario.

Nome policy di gruppo	Si applica a	Descrizione
Policy dominio predefinita	Domain	Include password di dominio e policy Kerberos.

Nome policy di gruppo	Si applica a	Descrizione
ServerAdmins	Tutti gli account computer controller non di dominio	Aggiunge «AWS Delegated Server Administrators» come membro del gruppo BUILTIN\ Administrators.
AWS Politica riservata: Utente	AWS Account utente riservati	Imposta le impostazioni di sicurezza consigliate su tutti gli account utente nell'unità organizzativa AWS riservata.
AWS Politica gestita di Active Directory	Tutti i controller di dominio	Definisce le impostazioni di sicurezza consigliate su tutti i controller di dominio.
TimePolicyNT5DS	Tutti i controller di dominio non PDCe	Imposta tutti i criteri temporali dei controller di dominio PDCe per l'utilizzo dell'ora di Windows (NT5DS).
TimePolicyPDC	Il controller di dominio PDCe	Imposta la policy ora del controller di dominio PDCe per utilizzare NTP (Network Time Protocol).
Policy controller di dominio predefinito	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.

Autorizzazioni per l'account Administrator

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 Active Directory. 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 Microsoft AD gestito da AWS.
- 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;
- creazione di UO aggiuntive e container;
- Delega dell'autorità di UO aggiuntive e container. Per ulteriori informazioni, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.
- creazione e collegamento policy di gruppo;
- ripristino degli oggetti eliminati dal cestino riciclaggio di Active Directory;
- Esegui i Windows 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.

> **Important**
>
> 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 sulla AWS gestione dei contenuti, incluse le informazioni sulle directory, archiviati sui AWS sistemi.

> **Note**
>
> 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.

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. AWS 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. AWS 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 sistema di richiesta/notifica 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 intraprese 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 Abilita inoltro dei log.

Gli ID evento di sicurezza 4624, 4672 e 4648 vengono tutti registrati quando qualcuno accede a un DC in modo interattivo. È possibile visualizzare il log degli eventi di sicurezza di Windows di ogni DC utilizzando il visualizzatore eventi Microsoft Management Console (MMC) da un computer Windows aggiunto al dominio. Puoi anche Abilita inoltro dei log 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 AWS 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 sui DC per la risoluzione dei problemi, viene creato un account utente temporaneo da utilizzare da parte di un AWS 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 AWS Directory Service gestione viene avvisato.

Concetti fondamentali di Microsoft AD gestito da AWS

Potrai ottimizzare l'utilizzo di Microsoft AD gestito da AWS acquisendo familiarità con i seguenti concetti fondamentali.

Argomenti

- Schema Active Directory
- Applicazione di patch e manutenzione per Microsoft AD gestito da AWS
- Account del servizio gestito del gruppo

- Delega vincolata Kerberos

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 utente 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 sono riportati alcuni dettagli sugli elementi dello schema da conoscere prima di iniziare il processo di estensione dello schema Microsoft AD gestito da AWS.

Attributi

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 sugli OID e su come ottenerli, consulta la pagina relativa agli identificatori di oggetto 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 Microsoft AD gestito da AWS
- Tutorial: estensione dello schema AWS Managed Microsoft AD

Applicazione di patch e manutenzione per Microsoft AD gestito da AWS

AWS Directory Service per Microsoft Active Directory, noto anche come AWS DS per Microsoft AD gestito da AWS, fa parte di Microsoft Active Directory Domain Services (AD DS), fornito come servizio gestito. Il sistema utilizza Microsoft Windows Server 2019 per i controller di dominio (DC) e AWS aggiunge il software ai DC per la gestione dei servizi. AWS aggiorna i DC (applica una patch) per aggiungere nuove funzionalità e mantenere il software di Microsoft Windows Server aggiornato. Durante il processo di applicazione di patch, la directory rimane disponibile per essere utilizzata.

Verifica della disponibilità

Per impostazione predefinita ciascuna directory è composta da due DC, ognuno dei quali installato su diverse zone di disponibilità. A tua scelta, puoi aggiungere DC per aumentare ulteriormente la disponibilità. Per ambienti critici che richiedono elevata disponibilità e tolleranza agli errori, consigliamo di implementare controller di dominio aggiuntivi. AWSapplica le patch ai controller di dominio in sequenza, durante il quale il controller di dominio che esegue attivamente le patch non è disponibile. AWS Nel caso in cui uno o più dei DC sia temporaneamente fuori servizio, AWS posticipa l'applicazione di patch finché la directory non avrà almeno due DC operativi. Ciò ti permette di utilizzare i DC operativi durante il processo di applicazione della patch, il quale solitamente richiede 30-45 minuti per DC, sebbene questa quantità di tempo possa variare. Per assicurarti che le

applicazioni possano raggiungere un DC operativo nel caso in cui uno o più DC non siano disponibili per varie ragioni, incluso il processo di applicazione della patch, tali applicazioni devono utilizzare il servizio di localizzazione DC di Windows e non indirizzi DC statici.

Comprendere la pianificazione dell'applicazione di patch

Per mantenere il software Microsoft Windows Server aggiornato sui tuoi DC, AWS utilizza gli aggiornamenti di Microsoft. Poiché Microsoft rende disponibile il rollup delle patch mensile per Windows server, AWS si sforza di verificare e applicare il rollup a tutti i DC personalizzati entro tre settimane di calendario. Inoltre, AWS esamina gli aggiornamenti rilasciati da Microsoft al di fuori del rollup mensile in base all'applicabilità ai DC e all'urgenza. Per le patch di sicurezza che Microsoft valuta come critiche o importanti che siano pertinenti ai DC, AWS si sforza di verificare e distribuire la patch entro cinque giorni.

Account del servizio gestito del gruppo

Con Windows Server 2012, Microsoft ha introdotto un nuovo metodo utilizzabile dagli amministratori per gestire gli account di servizio chiamati account del servizio gestito del gruppo. Tramite gli account del servizio gestito del gruppo, gli amministratori dei servizi non devono più 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 in Microsoft AD gestito da AWS siano in grado di creare un account del servizio gestito del gruppo, è necessario aggiungere i loro account come membri del gruppo di sicurezza Amministratori dell'account del servizio gestito delegati AWS. Per impostazione predefinita, l'account Admin è un membro di questo gruppo. Per ulteriori informazioni sulle GMSAS, vedere Panoramica degli account dei servizi gestiti di gruppo sul sito Web di Microsoft. TechNet

Articolo correlato del blog AWS sulla sicurezza

- In che modo AWS Managed Microsoft AD aiuta a semplificare la distribuzione e a migliorare la sicurezza delle applicazioni .NET integrate con 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 applicare limiti di attendibilità delle applicazioni

limitando l'ambito in cui è consentito agire per conto di un utente ai servizi delle applicazioni. 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 una applicazione per le risorse umane. 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 hr-app-service le autorizzazioni anziché le autorizzazioni configurate da jsmith. È necessario consentire all'applicazione del libro paga delle risorse umane di accedere al database di SQL Server tramite 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-service account 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 permettono agli utenti in Microsoft AD gestito da AWS di configurare la delega vincolata Kerberos, è necessario aggiungere i loro account come membri del gruppo di sicurezza Amministratori delegati AWS della delega Kerberos. 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.

Procedure consigliate per AWS Managed 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.

Configurazione: prerequisiti

Tieni presenti queste linee guida prima di creare la directory.

Verifica di avere il tipo di directory corretto

AWS 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 il tuo locale esistente Active Directory 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 e a basso costo con compatibilità di baseActive 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 AWS Directory Service opzioni, consulta. Quale scegliere

Verifica che i VPC e le istanze siano configurati correttamente

Per gestire, utilizzare e connetterti alle directory, è necessario configurare correttamente i VPC ai quali sono associate le directory. Consulta AWS Prerequisiti Microsoft AD gestiti, 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 Unisci un'istanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory.

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 di AWS sicurezza della tua directory

AWS crea 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. 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. AWS collega il gruppo di sicurezza alle interfacce dei controller di dominio accessibili dai tuoi VPC peerizzati o ridimensionati. 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 affinché accettino traffico da un elenco di indirizzi IP più restrittivo. Ad esempio, puoi modificare gli indirizzi accettati da 0.0.0.0/0 a un intervallo CIDR specifico di una sottorete o un computer singoli. 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 Gruppi di sicurezza Amazon EC2 per le istanze Linux nella Guida per l'utente di Amazon EC2. Modifiche improprie possono causare la perdita delle comunicazioni con i computer e le istanze previsti. AWS consiglia 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**
>
> Tecnicamente, hai la possibilità di associare i gruppi di sicurezza utilizzati dalla directory ad altre istanze EC2 da te create. 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 coinvolgono tutte le istanze alle quali hai associato il gruppo di sicurezza della directory. Inoltre, associare il gruppo di sicurezza della directory alle istanze EC2 crea un potenziale rischio per la sicurezza per le istanze EC2. Il gruppo di sicurezza della directory accetta traffico sulle porte Active

Directory necessarie proveniente da qualsiasi indirizzo IP. Se associ tale gruppo di sicurezza a un'istanza EC2 che dispone di un indirizzo IP pubblico collegato a Internet, qualsiasi computer su Internet può comunicare con l'istanza EC2 sulle porte aperte.

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. 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 AWS 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 Creare o modificare un set di opzioni DHCP.

Abilita l'impostazione condizionale del forwarder

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

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 Utilizzo del servizio di localizzazione DC di Windows.

Informazioni sulle limitazioni per il nome utente delle applicazioni AWS

AWS Directory Service fornisce 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, come WorkSpaces Amazon WorkMail, WorkDocs Amazon o Amazon. QuickSight Queste limitazioni richiedono che non vengano utilizzati i seguenti caratteri:

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

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

Utilizzo della directory

Di seguito sono elencati alcuni suggerimenti da tenere a mente quando utilizzi la directory.

Non modificare utenti, gruppi e unità organizzative predefiniti

Quando si utilizza AWS 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 da AWS. 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 Active Directory.

Unisci i domini automaticamente

Quando si avvia un'istanza di Windows che deve far parte di un AWS 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 Unisci senza problemi un'istanza Windows di Amazon EC2 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 completo (FQDN) sia i nomi NetBIOS devono essere univoci tra foreste e domini

Per ulteriori dettagli e istruzioni specifiche su come configurare una relazione di trust, consulta Creazione di una relazione di trust.

Gestione della directory

Considera questi suggerimenti per gestire la directory.

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 CloudWatch le metriche. Per ulteriori informazioni, consulta Monitorare i controller di dominio con parametri delle prestazioni.

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 Estensione dello schema.

Informazioni sui sistemi di bilanciamento del carico

Non utilizzare un sistema di bilanciamento del carico davanti agli endpoint Microsoft AD AWS gestiti. Microsoft Active Directory (AD) è stata progettata per essere utilizzata con un algoritmo di individuazione dei controller dei domini (DC) per individuare quelli più reattivi senza il bilanciamento del carico esterno. I Network Load Balancer esterni rilevano in modo inaccurato i DC attivi e possono essere la causa dell'invio della tua applicazione a un DC previsto ma non ancora pronto per l'utilizzo. 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 AWS 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 Snapshot o ripristino della directory.

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 messaggi AWS Directory 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 Configura le notifiche sullo stato delle directory con Amazon SNS.

Applica le impostazioni del servizio di directory

AWS Microsoft AD gestito consente di personalizzare la configurazione di sicurezza per soddisfare i requisiti di conformità e sicurezza. AWS Microsoft 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 Configurazione delle impostazioni di sicurezza della directory.

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, Amazon WorkDocs, Amazon o Amazon WorkMail Relational Database Service (Amazon RDS), devi prima rimuovere ogni applicazione. AWS Management Console Per ulteriori informazioni su come rimuovere queste applicazioni, consulta Elimina il tuo 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. AWS Microsoft AD gestito supporta solo la versione SMB 2.0 (SMBv2) e successive.

I protocolli SMBv2 e le versioni successive aggiungono una serie di caratteristiche che migliorano le prestazioni dei client e aumentano la sicurezza dei controller di dominio e dei client. Questa modifica segue le raccomandazioni di United States Computer Emergency Readiness Team (US-CERT) e di Microsoft per disabilitare il protocollo SMBv1.

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

I client SMBv1 funzioneranno con tutti i file server compatibili con SMBv1 di cui dispone l'utente. Tuttavia, si AWS consiglia di aggiornare tutti i server e client SMB a SMBv2 o versioni successive. Per ulteriori informazioni sulla disabilitazione di SMBv1 e sull'aggiornamento alle versioni SMB più recenti sui sistemi, consulta questi post su Microsoft and Documentation. TechNet Microsoft

Tracciamento delle connessioni remote SMBv1

È possibile esaminare il registro eventi di Microsoft-Windows-SMBServer/Audit Windows collegandosi in remoto 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:

Accesso SMB1

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

Linee guida:

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

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 (DC). 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 associ l'applicazione a un DC fisso e si deve applicare una patch o eseguire una procedura di ripristino, l'applicazione perde l'accesso al DC e non utilizza uno dei DC restanti. 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 è inoltre possibile che l'automazione delle AWS directory contrassegni la directory come compromessa 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. Qualora fosse necessaria una maggiore capacità, prova altri DC mentre distribuisci le richieste tra i vari DC. Per ulteriori informazioni, consulta Distribuzione di controller di dominio aggiuntivi.

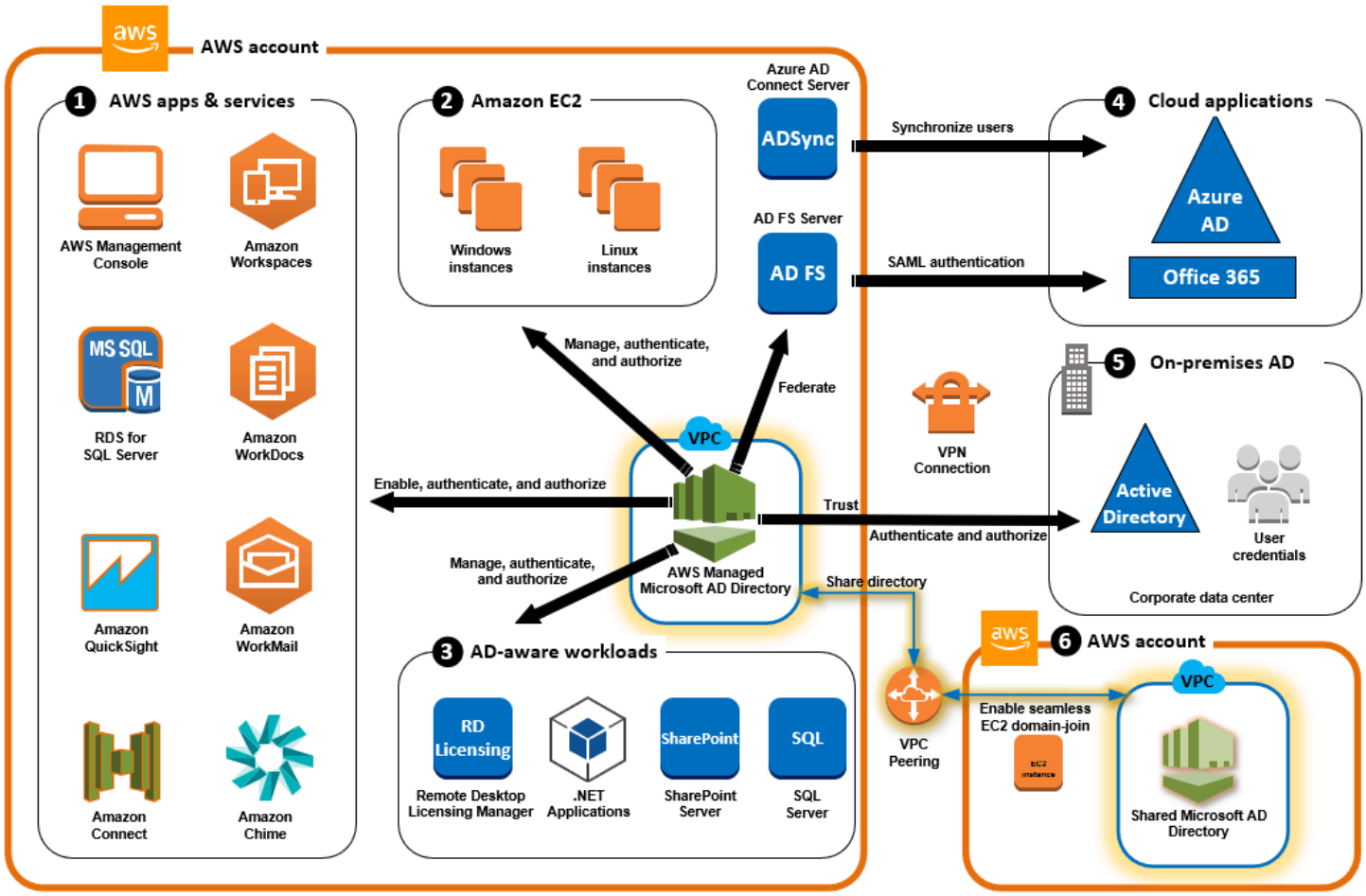
Utilizzo delle query LDAP

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 di Active Directory

Puoi abilitare più AWS applicazioni e servizi come Amazon Chime AWS Client VPNAWS Management ConsoleAWS IAM Identity Center, Amazon Connect, Amazon FSx, Amazon, QuickSightAmazon RDS for SQL Server, Amazon WorkSpaces, WorkDocs WorkMail Amazon e utilizzare la AWS tua directory Managed Microsoft AD. Quando abiliti un' AWS applicazione 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 AWS Management Console con le proprie credenziali di Active Directory. A tale scopo, abiliti l'applicazione AWS Management Console as a nella tua directory, quindi assegni gli utenti e i gruppi di Active Directory ai ruoli IAM. Quando i tuoi utenti accedono a AWS Management Console, assumono un ruolo IAM per gestire AWS le risorse. In questo modo è più semplice concedere agli utenti l'accesso alla AWS Management Console , senza dover configurare e gestire un'infrastruttura SAML separata.

Per migliorare ulteriormente l'esperienza dell'utente finale, puoi abilitare le funzionalità Single Sign-on per Amazon WorkDocs, che offrono agli utenti la possibilità di accedere ad Amazon 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 AWS Management Console o AWS CLI utilizzare le credenziali e le autorizzazioni esistenti per gestire le AWS risorse assegnando ruoli IAM direttamente agli account utente esistenti.

Integrazione di FSx for Windows File Server AWS con Managed Microsoft AD

L'integrazione di FSx for 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 lo storage di file condiviso) in. AWS Sebbene FSx per Windows File Server possa essere integrato con un Microsoft Active Directory autogestito, questo scenario non viene discusso in questa sede.

Casi d'uso e risorse comuni di Amazon FSx

Questa sezione fornisce un riferimento alle risorse sulle integrazioni comuni di FSx for Windows File Server con i casi d'uso di AWS Managed Microsoft AD. Ciascuno dei casi d'uso in questa sezione inizia con una configurazione di base di Microsoft AD gestito da AWS e FSx per Windows File Server. Per ulteriori informazioni su come creare queste configurazioni, consulta:

- Guida introduttiva a AWS Managed Microsoft AD
- Nozioni di base su Amazon FSx

FSx per Windows File Server come archiviazione persistente su container 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 di FSx per Windows File Server come archiviazione persistente nei container 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 con AppStream 2.0 fornisce un'unità di storage persistente personale che utilizza Amazon FSx e può essere configurato per fornire una cartella condivisa per accedere ai file comuni.

Voci correlate

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

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 del motore di database.

Voci correlate

- Installazione di SQL Server con archiviazione fileshare SMB
- Semplificazione delle implementazioni di Microsoft SQL Server ad alta disponibilità utilizzando FSx per Windows 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 cartelle home degli utenti di Active Directory e da I miei documenti in una posizione centrale. FSx per Windows File Server può essere utilizzato anche per archiviare dati dai profili utente in roaming.

Voci correlate

- Home directory di Windows semplificate con Amazon FSx
- Implementazione di profili utente in roaming
- Utilizzo di FSx for Windows File Server con WorkSpaces

Supporto per la condivisione di file in rete

Le condivisioni di file in rete su un FSx per Windows File Server forniscono una soluzione di condivisione di file gestita e dimensionabile. 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 di FSx for 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 le policy di gruppo.

Voci correlate

- Utilizzare 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 al file server FSx per Windows anziché al volume EBS collegato.

Voci correlate

- Esecuzione del ripristino dello stato del sistema del server

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

- Condividi la directory
- Utilizzo di Amazon FSx con Managed AWS 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, consultare:

- Condividi la directory
- 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 per SQL Server con un'applicazione .NET di base e gli account del servizio gestito del gruppo (gMSA). 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: Gestire le istanze di Amazon EC2

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

AWS Managed Microsoft AD è un vero e proprio Microsoft Active Directory che consente di eseguire carichi di lavoro tradizionali compatibili con Active Directory come Remote Desktop Licensing Manager e Microsoft SharePoint e Microsoft SQL Server Always On in the Cloud. AWS AWS Managed Microsoft AD consente inoltre di semplificare e migliorare la sicurezza delle applicazioni.NET integrate in Active Directory utilizzando gli account di servizio gestiti (GMSAS) di gruppo e la delega vincolata Kerberos (KCD).

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

Puoi utilizzare AWS Managed Microsoft AD AWS IAM Identity Center per fornire 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 AWS Management Console 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**
>
> AWS Single Sign-On è stato rinominato IAM Identity Center.

Caso d'uso 5: estendi la tua Active Directory locale al cloud AWS

Se disponi già di un'infrastruttura Active Directory e desideri utilizzarla per la migrazione di carichi di lavoro compatibili con Active Directory sul 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 AWS Management Console e ad 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, gli utenti Windows che hanno effettuato l'accesso possono accedere a tali applicazioni senza dover immettere 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 le istanze Amazon EC2 a un dominio tra più account AWS

La condivisione della directory tra più AWS account consente di gestire facilmente AWS servizi come Amazon EC2 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 rende più semplice e conveniente gestire carichi di lavoro sensibili alle directory con una singola directory in più account e VPC. Ad esempio, ora puoi gestire in modo semplice i carichi di lavoro Windows implementati in istanze EC2 su più account e VPC utilizzando una singola directory Microsoft AD gestito da AWS .

Quando condividi la tua directory AWS Managed Microsoft AD con un altro AWS account, puoi utilizzare la console Amazon EC2 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 sensibili alle directory su istanze EC2 eliminando la necessità di unire manualmente le istanze a un dominio o distribuire le directory in ciascun account e VPC. Per ulteriori informazioni, consulta Condividi la directory.

Come amministrare AWS Managed Microsoft AD

Questa sezione elenca tutte le procedure per il funzionamento e la manutenzione di un ambiente Microsoft AD AWS gestito.

Argomenti

Protezione di una directory Microsoft AD gestito da AWS

In questa sezione vengono riportate alcune considerazioni relative alla protezione dell'ambiente Microsoft AD gestito da AWS.

Argomenti

Gestione delle politiche relative alle password per AWS Managed 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 aActive 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

* Nota: la durata massima delle 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.

Di seguito sono riportate risorse per ulteriori informazioni sulle politiche Microsoft Active Directory granulari in materia di password e sulle politiche di sicurezza:

- Configurare le impostazioni delle politiche 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 Administrative Center. Active Directory Per iniziare a utilizzare gli strumenti relativi alle Microsoft politiche, consultaInstallare gli 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 Active Directory amministratore o un utente 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

Policy	Reimpostazione della password	Modifica della password
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.

Argomenti

- Impostazioni delle policy supportate
- Delegare di chi può gestire le tue policy sulle password
- Assegnazione delle policy sulle password ai tuoi utenti

Articolo correlato del blog AWS sulla sicurezza

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

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

Delegare di chi può gestire le tue policy sulle password

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 istanza EC2 gestita a cui hai aggiunto il tuo dominio AWS Microsoft AD 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 Active Directory.
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.

Assegnazione delle policy sulle password ai tuoi utenti

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 istanza EC2 gestita a cui hai aggiunto il tuo dominio AWS Microsoft AD 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 seguente PowerShell comando:

```
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.

Abilita l'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. 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 protocollo client/server 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 AWS 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 utilizzi Replica multi regione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.
- 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 AWS Support.

Abilita l'autenticazione a più fattori per AWS Managed Microsoft AD

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 o WorkSpaces Amazon QuickSight Chime. AWS Management Console Non fornisce MFA ai carichi di lavoro Windows in esecuzione su istanze EC2 o per l'accesso a un'istanza EC2. AWS 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, 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. AWS 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 .

Applicazioni Amazon Enterprise supportate

Tutte le applicazioni IT di Amazon Enterprise WorkSpaces, tra cui Amazon WorkDocs, Amazon WorkMail, Amazon QuickSight, e l'accesso AWS IAM Identity Center e AWS Management Console sono supportati quando si utilizza AWS Managed Microsoft AD e AD Connector con MFA.

Per informazioni su come configurare l'accesso utente di base alle applicazioni Amazon Enterprise, AWS Single Sign-On e l' AWS Management Console utilizzo AWS Directory Service, consulta Consentire l'accesso ad AWS applicazioni e servizi e. Abilitazione dell'accesso a AWS Management Console con le credenziali AD

Articolo correlato del blog AWS sulla sicurezza

- Come abilitare l'autenticazione a più fattori per AWS i servizi utilizzando AWS Managed Microsoft AD e credenziali locali

Abilita LDAP o LDAPS sicuri

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:

- Il protocollo LDAPS lato server crittografa le comunicazioni LDAP tra le applicazioni commerciali o sviluppate internamente (che agiscono come client LDAP) e Managed Microsoft AD (che funge

da server LDAP). AWS Per ulteriori informazioni, consulta Abilita LDAPS lato server utilizzando Managed Microsoft AD AWS.

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

Argomenti

Abilita LDAPS lato server utilizzando Managed Microsoft AD AWS

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

Abilita LDAPS lato server

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

È necessario eseguire gran parte della configurazione dall'istanza Amazon EC2 utilizzata per gestire i controller di dominio di Microsoft AD gestito da AWS . I seguenti passaggi ti guidano nell'attivazione di LDAPS per il tuo dominio nel cloud. AWS

Se desideri utilizzare l'automazione per configurare la tua infrastruttura PKI, puoi utilizzare Microsoft Public Key Infrastructure on AWS QuickStart Guide. In particolare, ti consigliamo di seguire le istruzioni contenute nella guida per caricare il modello per Implementa Microsoft PKI in un VPC esistente su 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 server Microsoft Enterprise CA 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 servizio LDAP sui controller di dominio di restare in attesa di connessioni SSL provenienti da client LDAP e accettarle automaticamente.

> **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 una CA Microsoft Enterprise subordinata — (Consigliata) Con questa opzione, puoi distribuire un server Microsoft Enterprise CA subordinato nel AWS cloud. Il server può utilizzare Amazon EC2 in modo che funzioni con la CA Microsoft root esistente. Per ulteriori informazioni su come configurare una CA aziendale Microsoft subordinata, vedere Passaggio 4: Aggiungere una CA Microsoft Enterprise alla directory AWS Microsoft AD in Come abilitare LDAPS lato server per la directory AWS Microsoft AD gestita.

- Crea una CA aziendale Microsoft root: con questa opzione, puoi creare una CA Microsoft enterprise root nel AWS cloud utilizzando Amazon EC2 e aggiungerla al tuo dominio AWS Microsoft AD 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 collegare l'Istanza EC2 al dominio, consulta Unisci un'istanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory.

Fase 3: creazione di un modello di certificato

Dopo aver configurato la CA aziendale, è possibile configurare il modello di certificato di autenticazione Kerberos.

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 impostando il sistema operativo 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 basato su Windows Server 2019.

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

6. Fai clic sulla scheda Generale e modifica 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

Nella fase finale, è necessario aprire la console Amazon EC2 e aggiungere regole del gruppo di sicurezza. Queste regole consentono ai controller di dominio di connettersi alla CA aziendale per richiedere un certificato. A tale scopo, aggiungi le regole in entrata in modo che la CA aziendale possa accettare il traffico in entrata dai controller di dominio. Aggiungi quindi regole in uscita per consentire il traffico proveniente dai controller di dominio verso la CA aziendale.

Dopo aver configurato entrambe le regole, i controller di dominio richiederanno automaticamente un certificato dalla CA aziendale e abiliteranno LDAPS per la directory. Il servizio LDAP sui controller di dominio è ora pronto per accettare le connessioni LDAPS.

Configurazione delle regole per i gruppi di sicurezza

1. Passa alla console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2 e registrati con le credenziali da 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 AWS di 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 di AWS sicurezza della directory (ad esempio, sg-123456789) nella casella accanto a Source.
- Selezionare 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).
- Digita il gruppo di AWS sicurezza della tua CA nella casella accanto a Destinazione.
- Selezionare Salva.

È possibile testare la connessione LDAPS alla directory AWS Managed Microsoft AD utilizzando lo strumento LDP. Lo strumento LDP viene fornito insieme agli strumenti di amministrazione di Active Directory. Per ulteriori informazioni, consulta Installare gli 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

Abilita 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 Amazon QuickSight e Amazon Chime. AWS IAM Identity Center Questa crittografia consente di proteggere meglio i dati di identità dell'organizzazione e soddisfare i requisiti di sicurezza.

Prerequisiti

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

Argomenti

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

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

Innanzitutto, è necessario stabilire una relazione di fiducia tra AWS Managed Microsoft AD e Self-managed Microsoft Active Directory per abilitare 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. AWS Management Console AWS CLI

> **Note**
>
> LDAPS lato client è una funzionalità regionale di Managed AWS Microsoft AD. Se utilizzi Replica multi regione, 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 AWS Directory Service
- Fase 2: controllare lo stato della registrazione

- Fase 3: abilitare LDAPS lato client
- Fase 4: controllare lo stato LDAPS

Fase 1: Registrare un certificato in AWS Directory Service

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

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

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 AWS 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 AWS Directory Service (AWS Management Console)

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 AWS 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. AWS Directory Service

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

Metodo 1: Per abilitare LDAPS lato client in () AWS Directory ServiceAWS Management Console

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 () AWS 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 LDAPS. AWS Directory Service

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

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 AWS 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 AWS Management Console 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 AWS Directory Service (AWS Management Console)

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 AWS 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 AWS Directory Service ()AWS Management Console

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 () AWS 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 () AWS Directory ServiceAWS Management Console

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 () AWS 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. AWS Support 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 Gestione delle politiche relative alle password per AWS Managed Microsoft AD.

Migliorare la configurazione della sicurezza di rete di Microsoft AD gestito da AWS

Il gruppo di sicurezza AWS di cui è stato eseguito il provisioning per la directory Microsoft AD gestito da AWS viene configurato con le porte di rete in ingresso minime necessarie per supportare tutti i casi d'uso noti per la directory AWS Microsoft AD gestito da. Per ulteriori informazioni sul gruppo di sicurezza AWS con provisioning, consulta Cosa viene creato con AWS Managed Microsoft AD Active Directory.

Per migliorare ulteriormente la sicurezza di rete della directory Microsoft AD gestito da AWS, è possibile modificare il gruppo di sicurezza AWS in base agli scenari comuni elencati di seguito.

Argomenti

- Solo supporto applicazioni AWS
- Solo applicazioni AWS con supporto trust
- Supporto per applicazioni AWS e carichi di lavoro nativi di Active Directory
- Supporto per applicazioni AWS e carichi di lavoro nativi di Active Directory con supporto trust

Solo supporto applicazioni AWS

Tutti gli account utente vengono sottoposti a provisioning solo in Microsoft AD gestito da AWS per essere utilizzati con le applicazioni AWS supportate, ad esempio le seguenti:

- Amazon Chime
- Amazon Connect

- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

È possibile utilizzare la seguente configurazione di gruppo di sicurezza AWS per bloccare tutto il traffico non essenziale ai controller di dominio Microsoft AD gestito da AWS.

> **Note**
>
> - I seguenti non sono compatibili con questa configurazione del gruppo di sicurezza AWS:
>   - Istanze Amazon EC2
>   - 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.

Solo applicazioni AWS con supporto trust

Tutti gli account utente vengono sottoposti a provisioning in Microsoft AD gestito da AWS o in Active Directory attendibile per essere utilizzati con le applicazioni AWS supportate, ad esempio le seguenti:

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

È possibile modificare la configurazione del gruppo di sicurezza AWS con provisioning per bloccare tutto il traffico non essenziale ai controller di dominio Microsoft AD gestito da AWS.

> **Note**
>
> - I seguenti non sono compatibili con questa configurazione del gruppo di sicurezza AWS:
>   - Istanze Amazon EC2
>   - 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 on-premise" 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	CIDR on-premise	DNS	Autenticazione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	CIDR on-premise	Kerberos	Autenticazione utente e computer, trust a livello di foresta
TCP e UDP	389	CIDR on-premise	LDAP	Policy di gruppo per l'autenticazione di directory, replica, utente e computer, trust
TCP e UDP	464	CIDR on-premise	Kerberos cambia/imposta la password	Autenticazione utente e computer, replica, trust
TCP	445	CIDR on-premise	SMB/CIFS	Replica, autenticazione utente e computer, trust di policy di gruppo
TCP	135	CIDR on-premise	Replica	RPC, EPM
TCP	636	CIDR on-premise	LDAP SSL	Policy di gruppo per l'autenti

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
				cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	CIDR on-premise	RPC	Replica, autenticazione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	CIDR on-premise	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenticazione di directory, replica, utente e computer, trust
UDP	123	CIDR on-premise	Ora di Windows	Ora di Windows, trust

Regole in uscita

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
Tutti	Tutti	CIDR on-premise	Tutto il traffico	

Supporto per applicazioni AWS e carichi di lavoro nativi di Active Directory

Gli account utente vengono sottoposti a provisioning solo in Microsoft AD gestito da AWS per essere utilizzati con le applicazioni AWS supportate, ad esempio le seguenti:

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

È possibile modificare la configurazione del gruppo di sicurezza AWS con provisioning per bloccare tutto il traffico non essenziale ai controller di dominio Microsoft AD gestito da AWS.

> **Note**
>
> - I trust di Active Directory non possono essere creati e gestiti tra la directory Microsoft AD gestito da AWS e il dominio on-premise.
> - Richiede che la rete "Client CIDR" sia sicura.
> - TCP 636 è richiesto solo quando LDAP su SSL è in uso.
> - Se si desidera utilizzare una CA Enterprise con questa configurazione è necessario 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	CIDR client	DNS	Autentica zione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	CIDR client	Kerberos	Autentica zione utente e computer, trust a livello di foresta
TCP e UDP	389	CIDR client	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	445	CIDR client	SMB/CIFS	Replica, autentica zione utente e computer, trust di policy di gruppo
TCP e UDP	464	CIDR client	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	135	CIDR client	Replica	RPC, EPM
TCP	636	CIDR client	LDAP SSL	Policy di gruppo per l'autenti cazione di

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

Regole in uscita

Nessuna.

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

Tutti gli account utente vengono sottoposti a provisioning in Microsoft AD gestito da AWS o in Active Directory attendibile per essere utilizzati con le applicazioni AWS supportate, ad esempio le seguenti:

- Amazon Chime

- Amazon Connect
- Istanze Amazon EC2
- Amazon FSx
- Amazon QuickSight
- Amazon RDS per MySQL
- Amazon RDS per Oracle
- Amazon RDS per PostgreSQL
- Amazon RDS per SQL Server
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

È possibile modificare la configurazione del gruppo di sicurezza AWS con provisioning per bloccare tutto il traffico non essenziale ai controller di dominio Microsoft AD gestito da AWS.

> **Note**
>
> - È necessario assicurarsi che le reti "CIDR on-premise" e "CIDR client" siano sicure.
> - TCP 445 con il "CIDR on-premise" viene utilizzato solo per la creazione di trust e può essere rimosso dopo che il trust è stato stabilito.
> - TCP 445 con il "CIDR client" deve essere lasciato aperto in quanto è necessario per l'elaborazione di policy di gruppo.
> - TCP 636 è richiesto solo quando LDAP su SSL è in uso.
> - Se si desidera utilizzare una CA Enterprise con questa configurazione è necessario 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	CIDR on-premise	DNS	Autenticazione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	CIDR on-premise	Kerberos	Autenticazione utente e computer, trust a livello di foresta
TCP e UDP	389	CIDR on-premise	LDAP	Policy di gruppo per l'autenticazione di directory, replica, utente e computer, trust
TCP e UDP	464	CIDR on-premise	Kerberos cambia/imposta la password	Autenticazione utente e computer, replica, trust
TCP	445	CIDR on-premise	SMB/CIFS	Replica, autenticazione utente e computer, trust di policy di gruppo
TCP	135	CIDR on-premise	Replica	RPC, EPM
TCP	636	CIDR on-premise	LDAP SSL	Policy di gruppo per l'autenti

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
				cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	CIDR on-premise	RPC	Replica, autenticazione utente e computer, policy di gruppo, trust
TCP	3268 - 3269	CIDR on-premise	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenticazione di directory, replica, utente e computer, trust
UDP	123	CIDR on-premise	Ora di Windows	Ora di Windows, trust
TCP e UDP	53	CIDR client	DNS	Autenticazione utente e computer, risoluzione dei nomi, trust
TCP e UDP	88	CIDR client	Kerberos	Autenticazione utente e computer, trust a livello di foresta

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
TCP e UDP	389	CIDR client	LDAP	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP e UDP	445	CIDR client	SMB/CIFS	Replica, autentica zione utente e computer, trust di policy di gruppo
TCP e UDP	464	CIDR client	Kerberos cambia/imposta la password	Autentica zione utente e computer, replica, trust
TCP	135	CIDR client	Replica	RPC, EPM
TCP	636	CIDR client	LDAP SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	49152 - 65535	CIDR client	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	CIDR client	LDAP GC e LDAP GC SSL	Policy di gruppo per l'autenti cazione di directory, replica, utente e computer, trust
TCP	9389	CIDR client	SOAP	Servizi Web DS AD
UDP	123	CIDR client	Ora di Windows	Ora di Windows, trust
UDP	138	CIDR client	DFSN e NetLogon	DFS, policy di gruppo

Regole in uscita

Protocollo	Intervallo porte	Origine	Tipo di traffico	Utilizzo di Active Directory
Tutti	Tutti	CIDR on-premis e	Tutto il traffico	

Configurazione delle impostazioni di sicurezza della directory

Puoi configurare impostazioni di directory granulari per Microsoft AD gestito da AWS 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, puoi disabilitare singole crittografie legacy, come RC4 o DES, e protocolli come SSL 2.0/3.0 e TLS 1.0/1.1. AWS Microsoft AD gestito implementa quindi la configurazione su tutti i controller di dominio nella directory, gestisce i loro riavvii e mantiene questa configurazione man mano che si impiega la scalabilità orizzontale o vengono implementate altre

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 gestione AWS e apri la console di AWS Directory Service all'indirizzo 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 hai completato le modifiche e vuoi implementare i nuovi valori, scegli Aggiorna impostazioni. Verrà eseguito il reindirizzamento alla pagina 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

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				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 Certificate Binding Enforcement. Per ulteriori informazioni, consulta KB5014754—Certificate-based authentication changes on Windows domain controllers nella documenta

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				zione 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 (impostazione predefinita): 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'autenti

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				cazione avrà esito negativo. • Applicazione avanzata: l'autenticazione 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, consulta KB5014754—Certificate-based

Tipo	Nome dell'impostazione	Nome API	Valori potenziali	Descrizione impostazione
				authentication changes on Windows domain controllers 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 l'algoritmo 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 l'algoritmo 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 l'algoritmo 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 l'algoritmo 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 l'algoritmo 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 l'algoritmo 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 l'algoritmo 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.

Configurare AWS Private CA Connector for AD

Puoi integrare AWS Managed Microsoft AD con AWS Private Certificate Authority (CA) per emettere e gestire certificati per utenti, gruppi e computer uniti al dominio Active Directory. AWS Private CA Connector for Active Directory consente di utilizzare un sostituto AWS Private CA drop-in completamente gestito per le CA aziendali autogestite senza la necessità di distribuire, applicare patch o aggiornare agenti locali o server proxy.

> **Note**
>
> La registrazione di certificati LDAPS lato server per i controller di dominio Microsoft AD AWS gestiti AWS Private CA con Connector for Active Directory non è supportata. Per abilitare LDAPS lato server per la tua directory, vedi Come abilitare LDAPS lato server per la tua AWS directory gestita di Microsoft AD.

Puoi configurare AWS Private CA l'integrazione con la tua directory tramite la console Directory Service, la console AWS Private CA Connector for Active Directory o chiamando l'`CreateTemplate`API. Per configurare l'integrazione di Private CA tramite la console AWS Private CA Connector for Active Directory, vedi Creazione di un modello di connettore. Di seguito sono riportati i passaggi su come configurare questa integrazione dalla AWS Directory Service console.

Per configurare AWS Private CA Connector for AD

1. Accedi a AWS Management Console e apri la AWS Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella scheda Rete e sicurezza, in AWS Private CA Connettore per AD, scegli Configura AWS Private CA connettore per AD. Active DirectoryViene visualizzata la pagina Crea certificato CA privato per. Segui i passaggi sulla console per creare la tua CA privata per il Active Directory connettore per la registrazione alla tua CA privata. Per ulteriori informazioni, consulta Creazione di un connettore.
4. Dopo aver creato il connettore, segui i passaggi seguenti per visualizzare i dettagli, tra cui lo stato del connettore e lo stato della CA privata associata.

Per visualizzare AWS Private CA Connector for AD

1. Accedi a AWS Management Console e apri la AWS Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. In Rete e sicurezza, in AWS Private CA Connector per AD, puoi visualizzare i connettori della CA privata e la CA privata associata. Per impostazione predefinita, vengono visualizzati i seguenti campi:

    a. AWS Private CA ID connettore: l'identificatore univoco di un AWS Private CA connettore. Facendo clic su di esso si accede alla pagina dei dettagli di quel AWS Private CA connettore.

    b. AWS Private CA oggetto: informazioni sul nome distinto della CA. Facendo clic su di esso, si accede alla pagina dei dettagli di quella AWS Private CA.

    c. Stato: basato su un controllo dello stato del AWS Private CA Connector e del AWS Private CA. Se entrambi i controlli vengono superati, viene visualizzato Attivo. Se uno dei controlli ha esito negativo, viene visualizzato il messaggio 1/2 dei controlli non riusciti. Se entrambi i controlli hanno esito negativo, viene visualizzato Non riuscito. Per ulteriori informazioni sullo stato non riuscito, passa il mouse sul collegamento ipertestuale per scoprire a quale controllo si riferisce. Segui le istruzioni indicate nella console per rimediare.

    d. Data di creazione: il giorno in cui è stato creato il AWS Private CA connettore.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli del connettore.

Monitora Microsoft AD gestito da AWS

Puoi monitorare la directory Microsoft AD gestito da AWS nei seguenti modi:

Argomenti

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 AWS 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 AWS Support.

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 la normale attività di manutenzione operativa, ad esempio applicazione di patch o la rotazione dell'istanza EC2, l'hot spotting temporaneo mediante un'applicazione su uno dei controller di dominio o modifiche apportate alla rete che interrompono inavvertitamente le comunicazioni di directory. 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 AWS Support.

> **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 Snapshot o ripristino 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 AWS Support.

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.

Configura le notifiche sullo stato delle directory 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. 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 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 AWS Directory Service come editore a un argomento di Amazon SNS. Quando AWS 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?.

> **Note**
>
> Le notifiche sullo stato delle directory sono una funzionalità regionale di AWS Managed Microsoft AD. Se utilizzi Replica multi regione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per abilitare la messaggistica SNS per la directory

1. Accedi a AWS Management Console e apri la AWS Directory Service console.
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 ulteriori privilegi per SNS.

8. Scegli Crea.

Se desideri designare abbonati SNS aggiuntivi, ad esempio un indirizzo e-mail aggiuntivo, code Amazon SQS oppure AWS Lambda, puoi farlo dalla console Amazon SNS.

Per rimuovere i messaggi di stato della directory da un argomento

1. Accedi e apri la console. AWS Management ConsoleAWS Directory Service
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. 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 messaggi AWS Directory Service, associa la directory a un argomento Amazon SNS diverso.

Analizzare i log della directory di Microsoft AD gestito da AWS

I log di sicurezza dalle istanze dei controller di dominio Microsoft AD gestito da AWS sono archiviati per un anno. Puoi anche configurare la directory Microsoft AD gestito da AWS per inoltrare i log del controller di dominio ai File di log Amazon CloudWatch quasi in tempo reale. Per ulteriori informazioni, consulta Abilita inoltro dei log.

AWS registra i seguenti eventi per motivi di 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
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	Success (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
	Audit della disconnessione	Success (Riuscito)
	Audit dell'accesso	Successo, fallimento

Categoria di monitoraggio	Impostazione di policy	Stato di audit
	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	Success (Riuscito)
	Audit altri eventi di modifica policy	Errore
Uso dei privilegi	Audit dell'uso di privilegi sensibili	Successo, fallimento
System (Sistema)	Audit del driver IPsec	Successo, fallimento
	Audit di altri eventi di sistema	Successo, fallimento
	Audit della modifica stato sicurezza	Successo, fallimento

Categoria di monitoraggio	Impostazione di policy	Stato di audit
	Audit dell'estensione del sistema di sicurezza	Successo, fallimento
	Audit dell'integrità del sistema	Successo, fallimento

Abilita inoltro dei log

Puoi utilizzare la console AWS Directory Service o le API per inoltrare i log degli eventi di sicurezza del controller di dominio ai File di log Amazon CloudWatch. 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 Logs può anche inoltrare questi eventi ad altri account AWS, servizi AWS 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 leggere i relativi dati, consulta Utilizzo di gruppi di log e flussi di log nella Guida per l'utente dei File di log Amazon CloudWatch.

> **Note**
>
> L'inoltro dei log è una funzionalità regionale di Microsoft AD gestito da AWS. Se utilizzi Replica multi regione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Per abilitare inoltro dei log

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Scegli l'ID directory della directory Microsoft AD gestito da AWS da 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 dialogo Enable log forwarding to CloudWatch (Abilita l'inoltro dei log in CloudWatch), scegliere una delle seguenti opzioni:

   a. Seleziona Crea un nuovo gruppo di log CloudWatch e, in Nome del gruppo di log CloudWatch, specifica un nome cui fare riferimento in CloudWatch Logs.
   b. Selezionare Choose an existing CloudWatch log group (Seleziona un gruppo di log CloudWatch esistente) e in Gruppi di log CloudWatch esistenti, selezionare un gruppo di log dal menu.

6. Esaminare le informazioni sui prezzi e il collegamento e quindi scegliere Enable (Abilita).

Per disabilitare l'inoltro dei log

1. Nel riquadro di navigazione AWS Directory Service console, scegliere Directories (Directory).
2. Scegli l'ID directory della directory Microsoft AD gestito da AWS da 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 Disable log forwarding (Disabilita inoltro dei log), scegliere Disable (Disabilita).

Utilizzo dell'interfaccia a riga di comando per abilitare l'inoltro dei log

Prima di poter usare il comando `ds create-log-subscription`, è necessario creare un gruppo di log Amazon CloudWatch e quindi creare una policy di risorse IAM che concederà le autorizzazioni

necessarie a quel gruppo. Per abilitare l'inoltro di log utilizzando l'interfaccia a riga di comando, completare tutte le fasi descritte di seguito.

Fase 1: creazione di un gruppo di log in CloudWatch Logs

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. Ad esempio:

ESEMPIO DI COMANDO CLI

```
aws logs create-log-group --log-group-name '/aws/directoryservice/
d-9876543210'
```

ESEMPIO DI COMANDO POWERSHELL

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

Per istruzioni su come creare un gruppo di log CloudWatch, consulta Creazione di un gruppo di log in CloudWatch Logs nella Guida per l'utente di File di log Amazon CloudWatch.

Fase 2: creazione di una policy di risorse CloudWatch Logs in IAM

Crea una policy di risorse CloudWatch Logs che conceda a AWS Directory Service i diritti per aggiungere log al nuovo gruppo di log creato nella Fase 1. È possibile specificare l'ARN esatto per il gruppo di log per limitare l'accesso di AWS Directory Service ad altri gruppi o utilizzare un carattere jolly per includere tutti i gruppi di log. La seguente policy di esempio usa il metodo con carattere jolly per specificare che saranno inclusi tutti i gruppi di log che iniziano con `/aws/directoryservice/` per l'account AWS in cui risiede la directory.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
```

```
            "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/*"
        }
    ]
}
```

È necessario salvare questa policy in un file di testo (ad esempio DSPolicy.json) sulla workstation locale poiché sarà necessario eseguirlo dall'interfaccia a riga di comando. Ad esempio:

ESEMPIO DI COMANDO CLI

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-
document file://DSPolicy.json
```

ESEMPIO DI COMANDO POWERSHELL

```
$PolicyDocument = Get-Content .\DSPolicy.json –Raw

Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument
$PolicyDocument
```

Fase 3: creazione di una sottoscrizione al log AWS Directory Service

In questa fase finale è possibile abilitare l'inoltro di log creando la sottoscrizione di log. Ad esempio:

ESEMPIO DI COMANDO CLI

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-
name '/aws/directoryservice/d-9876543210'
```

ESEMPIO DI COMANDO POWERSHELL

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/
directoryservice/d-9876543210'
```

Monitorare i controller di dominio con parametri delle prestazioni

AWS Directory Service si integra con Amazon CloudWatch per aiutarti a fornire importanti metriche prestazionali per ogni controller di dominio del tuo. 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 del tuo. Active Directory

Per ulteriori informazioni sul monitoraggio dei controller di dominio, consulta Determina quando aggiungere controller di dominio con metriche CloudWatch .

Sono previste commissioni associate ad Amazon CloudWatch. Per ulteriori informazioni, consulta CloudWatchfatturazione e costi.

> **Important**
>
> Le metriche delle prestazioni dei controller di dominio con CloudWatch non sono disponibili nella regione Canada occidentale (Calgary).

Trova le 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 AWS Management Console 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

Determina 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 del tuo. 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 il Active Directory periodo di utilizzo per identificare l'utilizzo medio e di picco. Active Directory Dopo aver determinato la linea di base, puoi monitorare queste metriche regolarmente per determinare quando aggiungere un controller di dominio al tuo. 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, vedere Pianificazione della capacità per i servizi di Active Directory dominio 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
	Sec/lettura del database I/O
	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

Categoria parametro	Nome parametro
NTDS	Ritardo di coda stimato ATQ
	Latenza delle richieste ATQ
	Letture della directory DS/sec
	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

Replica multi regione

La replica multiregione può essere utilizzata per replicare automaticamente i dati della directory AWS Microsoft AD gestita su più siti. Regioni AWSQuesta 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 multi regione automatica nella maggior parte delle Regioni in cui è disponibile Microsoft AD gestito da AWS .

Important

La replica in più regioni non è disponibile nelle seguenti 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
- 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

Per ulteriori informazioni sulle regioni che accettano l'iscrizione e su come abilitarle, consulta Specificare quali possono essere utilizzate dal Regioni AWS tuo account nella Guida.AWS Account Management

Vantaggi

Con la replica multiregione 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 SharePoint e AWS servizi come Amazon RDS for SQL Server e FSx for Windows File Server. 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 aggiungi una AWS regione alla tua directory utilizzando la replica multiregionale, AWS Directory Service migliora 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 AWS 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.

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.

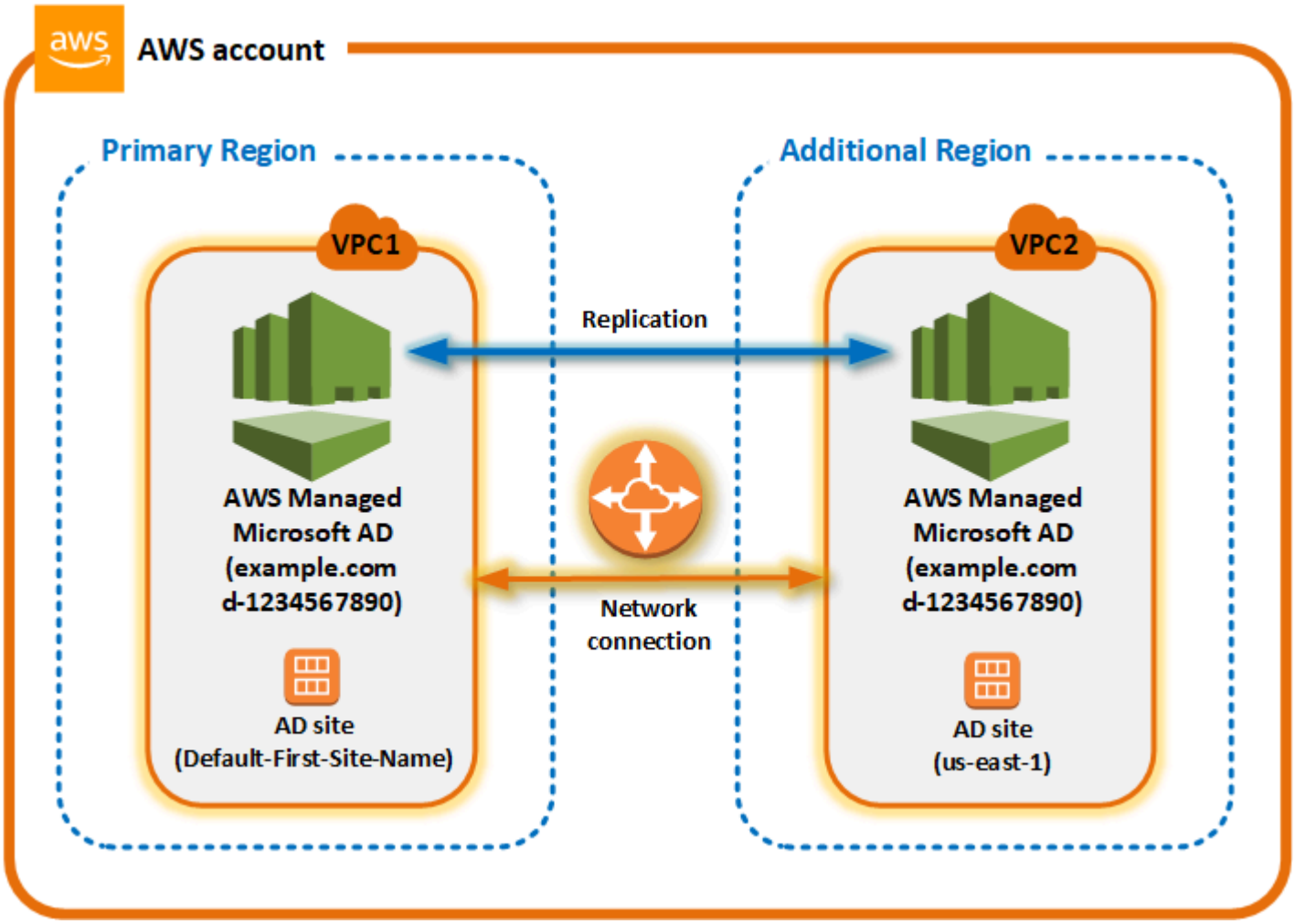
Come funziona la replica multi regione

Grazie alla 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, in più 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 Amazon FSx 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
- FSx per Windows File Server
- Amazon RDS 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.

Aggiungere una regione replicata

Quando aggiungi una regione utilizzando la Replica multi regione 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 AWS account in cui è già distribuita 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 all'infrastruttura Active Directory esistente.
- Se esiste una relazione di trust tra l'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.

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 Aggiunta o eliminazione di controller di dominio aggiuntivi.
- Condividi la tua directory con più AWS account per regione. Le configurazioni di condivisione delle directory non vengono replicate automaticamente dalla regione primaria. Per ulteriori informazioni, consulta Condividi la directory.
- 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 Abilita inoltro dei log.
- 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 Configura le notifiche sullo stato delle directory con Amazon SNS.

Eliminare una regione replicata

Utilizzare la procedura seguente per eliminare una regione per la 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 la directory

Microsoft AD gestito da AWS è strettamente integrato con AWS Organizations per consentire la condivisione di una directory ottimizzata su più account AWS. Puoi condividere una singola directory con altri account AWS affidabili all'interno della stessa organizzazione o condividere la directory con altri account AWS che si trovano all'esterno dell'organizzazione. Puoi anche condividere la directory quando il tuo account AWS non è attualmente un membro di un'organizzazione.

> **Note**
>
> AWS addebita un costo aggiuntivo per la condivisione directory. Per ulteriori informazioni, consulta la pagina Prezzi sul sito Web di AWS Directory Service.

La condivisione delle directory rende Microsoft AD gestito da AWS un metodo particolarmente conveniente per l'integrazione con Amazon EC2 in più account e VPC. Questa funzionalità è disponibile in tutte le regioni AWS in cui viene offerto Microsoft AD gestito da AWS.

> **Note**
>
> Nella regione AWS Cina (Ningxia), questa funzionalità è disponibile solo quando si utilizza AWS Systems Manager (SSM) per unire senza problemi le istanze Amazon EC2.

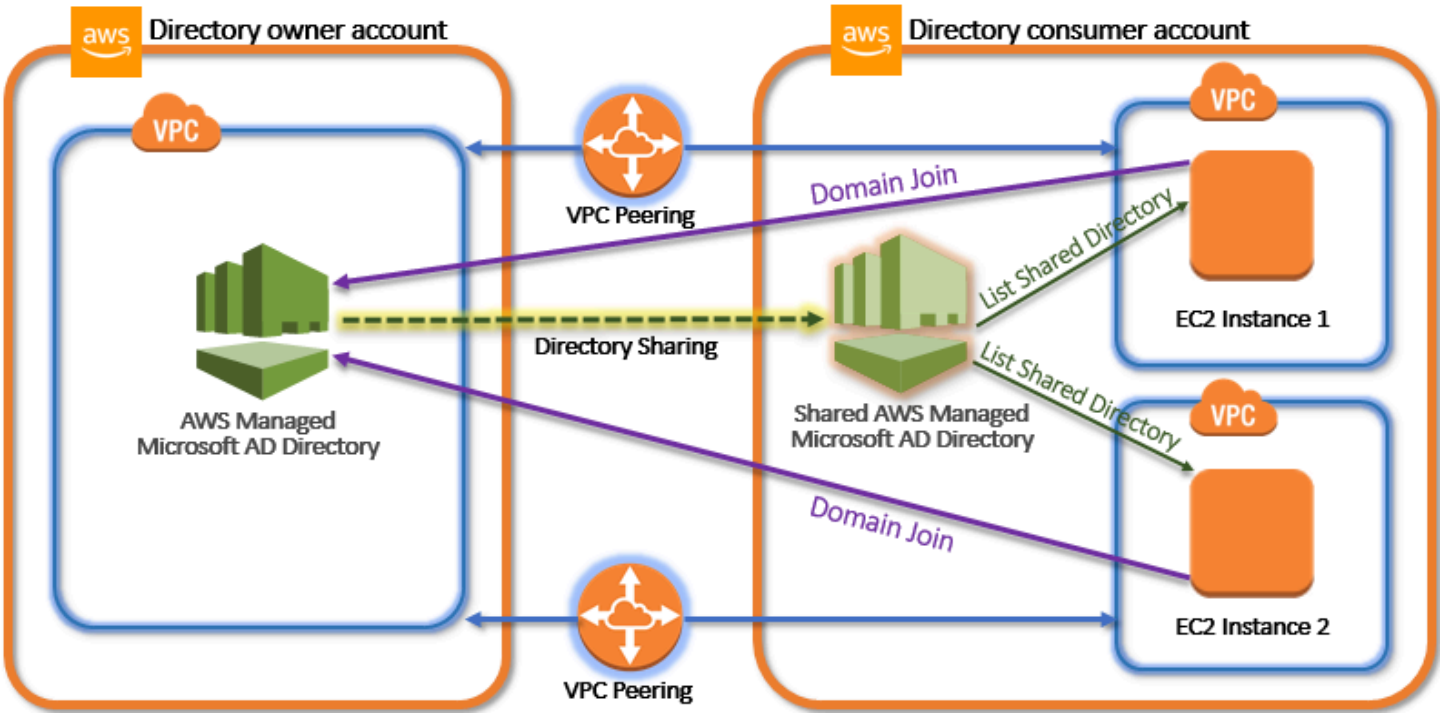
Per ulteriori informazioni sulla condivisione directory e su come estendere la copertura della directory Microsoft AD gestito da AWS sui limiti dell'account AWS, consulta i seguenti argomenti.

Argomenti

- Concetti chiave sulla condivisione di directory
- Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2
- Annullamento della condivisione della directory

Concetti chiave sulla condivisione di directory

Potrai ottimizzare l'utilizzo della caratteristica di condivisione directory acquisendo familiarità con i seguenti concetti fondamentali.



Account del proprietario della directory

Il proprietario di una directory è il titolare dell'Account AWS che possiede la directory di origine nella relazione directory condivisa. Un amministratore in questo account avvia il flusso di lavoro di condivisione delle directory specificando con quale Account AWS condividere la 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 AWS 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 di unire senza interruzioni l'istanza EC2 al dominio; ciò 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

Microsoft AD gestito da AWS fornisce i seguenti due metodi di condivisione della directory:

- 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 dell'utilizzatore della directory accettino la richiesta di condivisione della directory. Nella console, questo metodo è denominato Condividi questa directory con altri Account AWS nella tua organizzazione.
- 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 Account AWS. AWS supporta molte soluzioni per connettere i VPC, tra cui Peering VPC, Gateway di transito e VPN. Per iniziare, consulta Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2.

Tutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2

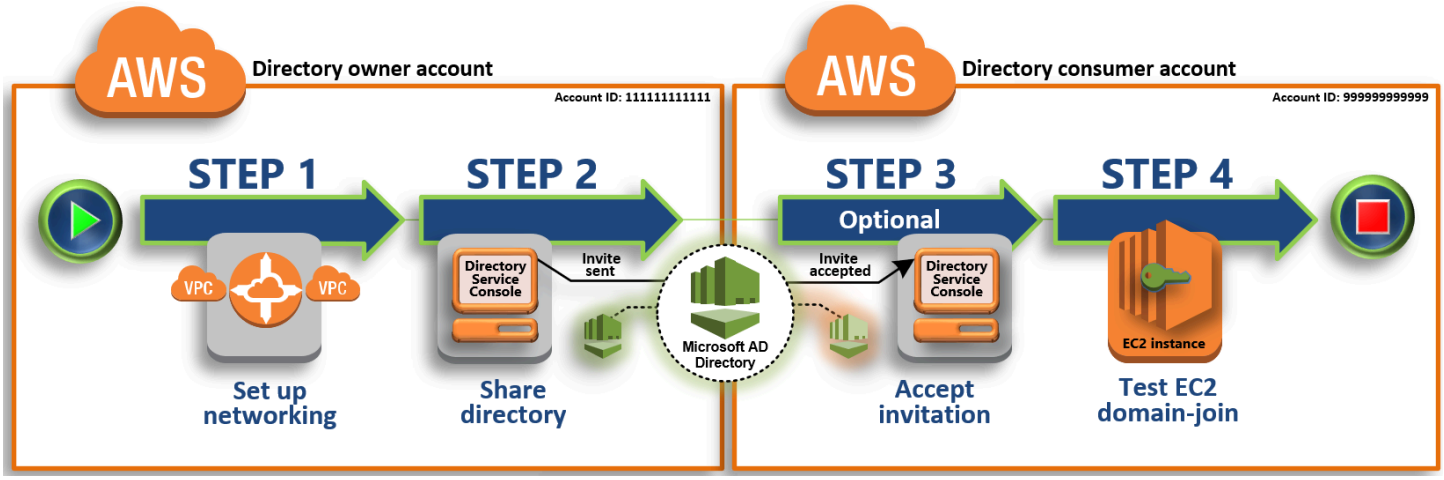
Questo tutorial mostra come condividere la directory AWS Managed Microsoft AD (l'account del proprietario della directory) con un'altra Account AWS (l'account utente della directory). Una volta

completati i prerequisiti di rete, condividerai una directory tra due Account AWS. Verrà quindi mostrato come unire senza interruzioni un'istanza EC2 a un dominio nell'account dell'utilizzatore della directory.

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 si condivida la directory 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 AWS 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 AWS Directory Service console e accetti l'invito alla condivisione della directory.

Fase 4: test dell'aggiunta ottimizzata di un'istanza EC2 per Windows Server a un dominio

Infine, in qualità di amministratore utilizzatore della directory, puoi tentare di unire un'istanza EC2 al dominio e verificare che funzioni.

Altre risorse

- Caso d'uso: condivisione della directory per aggiungere in modo ottimizzato le istanze Amazon EC2 a un dominio negli Account AWS
- AWS Articolo del blog sulla sicurezza: Come unire istanze Amazon EC2 da più account e VPC a un'unica directory Microsoft AD gestita AWS

Fase 1: configurazione dell'ambiente di rete

Prima di iniziare le fasi in questo tutorial, è necessario, innanzitutto, eseguire le operazioni seguenti:

- Creane due nuove a Account AWS scopo di test nella stessa regione. Quando ne crei uno Account 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 una connessione peering di VPC tra due VPC in ogni account utilizzando le procedure in questa fase.

> **Note**
>
> Sebbene ci siano molti modi per connettere i VPC del proprietario della directory e i VPC dell'account utente Directory, questa esercitazione 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 di VPC creata è tra i VPC dell'utilizzatore della directory e il proprietario della directory. Segui queste fasi per configurare una connessione peering di VPC per la connettività con l'account dell'utilizzatore della directory. Con questa connessione puoi instradare il traffico tra entrambi i VPC 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 alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/. Assicurarsi di eseguire l'accesso come un utente con credenziali di amministratore nell'account del proprietario della directory.
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.

Poiché entrambi i VPC si trovano nella stessa regione, l'amministratore dell'account del proprietario della directory che ha inviato la richiesta di peering di VPC può anche accettare la richiesta di peering per conto dell'account dell'utilizzatore della directory.

Per accettare la richiesta di peering per conto dell'account dell'utilizzatore della directory

1. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
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. Seleziona Salvataggio delle 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. Seleziona Salvataggio delle modifiche.

Accertati di configurare il gruppo di sicurezza del VPC dell'utilizzatore della directory per attivare il traffico in uscita aggiungendo i protocolli e le porte Active Directory alla tabella delle regole in uscita. 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 utilizzi Replica multi regione, 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 AWS Management Console con le credenziali di amministratore nell'account del proprietario della directory e apri la AWS Directory Service console all'indirizzo 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 AWS interno della tua 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 AWS 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 AWS Nella 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' AWS organizzazione. Puoi utilizzare questa opzione anche quando la tua rubrica non è membro di un' AWS organizzazione e desideri condividerla con un'altra Account AWS.

i. In ID Account AWS , inserisci tutti gli ID Account AWS con cui desideri 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 AWS interno dell'organizzazione, salta questo passaggio e procedi al Passaggio 4.

Per accettare l'invito directory condivisa

1. Accedi all'account consumer della directory AWS Management Console con le credenziali di amministratore e apri la AWS Directory Service console 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

Fase 4: test dell'aggiunta ottimizzata di un'istanza EC2 per Windows Server a un dominio

Fase 4: test dell'aggiunta ottimizzata di un'istanza EC2 per Windows Server a un dominio

Puoi utilizzare uno dei due metodi seguenti per testare l'aggiunta ottimizzata di un'istanza EC2 a un dominio.

Metodo 1: test dell'aggiunta di dominio utilizzando la console Amazon EC2

Utilizza questi passaggi nell'account dell'utilizzatore della directory.

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Windows EC2.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.

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.

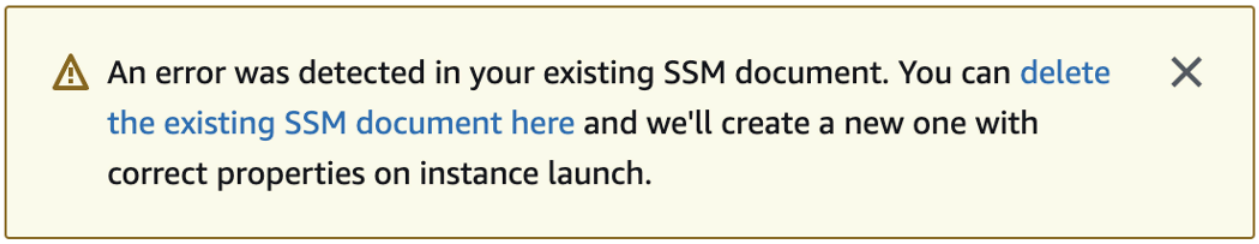
   > **Important**
   >
   > Questo è l'unico momento in cui salvare il file della chiave privata.

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 la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

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 DirectoryServiceAccess associate le policy AWS gestite AmazonSSM ManagedInstanceCore e AmazonSSM dall'elenco a discesa dei profili delle istanze 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. Per Use case (Caso d'uso), seleziona EC2.
    4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le politiche AmazonSSM e AmazonSSM. ManagedInstanceCore DirectoryServiceAccess Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Seleziona Successivo.

> **Note**
>
> AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un managed by. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 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. È necessario aggiungere questo nome del ruolo all'istanza EC2.
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: verifica l'accesso al dominio utilizzando AWS Systems Manager

Utilizza questi passaggi nell'account dell'utilizzatore della directory. Per completare questa procedura, avrai bisogno di alcune informazioni sull'account del proprietario della directory, come l'ID directory, il relativo nome e gli indirizzi IP DNS.

Prerequisiti

- Configurazione AWS Systems Manager.
  - Per ulteriori informazioni su Systems Manager, consulta la Configurazione generale per AWS Systems Manager.
- Le istanze che desideri aggiungere al dominio AWS Managed Microsoft Active Directory devono avere un ruolo IAM associato contenente le policy gestite di AmazonSSM ManagedInstanceCore e AmazonSSM. DirectoryServiceAccess

- 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 istanze EC2 a un dominio AWS Microsoft Active Directory gestito, vedi Come posso aggiungere un'istanza EC2 Windows in esecuzione al mio dominio AWS Directory Service? AWS Systems Manager .

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 Run command (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 AWS 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.

   - Per Directory ID, immettere il nome di AWS Managed Microsoft Active Directory.
   - 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, dovrebbe essere possibile aggiungere l'istanza EC2 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 directory

Per annullare la condivisione di una directory Microsoft AD gestito da AWS, utilizza la procedura seguente.

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 Microsoft AD gestito da AWS per la quale vuoi 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 directory per unire senza interruzioni le istanze Amazon EC2 a un dominio negli account AWS

- Articolo del blog sulla sicurezza AWS: come collegare istanze Amazon EC2 di più account e VPC a una singola directory Microsoft AD gestito da AWS
- Collegamento delle istanze DB Amazon RDS tra account in un singolo dominio condiviso

Unisci un'istanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory

Puoi aggiungere facilmente un'istanza Amazon EC2 al Active Directory tuo dominio quando l'istanza viene lanciata. Per ulteriori informazioni, consulta Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo AWS Managed Microsoft AD Active Directory. Puoi anche avviare un'istanza EC2 e aggiungerla a un Active Directory dominio direttamente dalla AWS Directory Service console con Automation.AWS Systems Manager

Se devi aggiungere manualmente un'istanza EC2 al tuo Active Directory dominio, 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

- Avvia l'istanza di amministrazione delle directory nel tuo AWS Managed Microsoft AD Active Directory
- Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo AWS Managed Microsoft AD Active Directory
- Unisci manualmente un'Windowsistanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory
- Unisci senza problemi un'istanza Amazon EC2 Linux alla tua directory AWS gestita di Microsoft AD Active Directory
- Unisci manualmente un'istanza Amazon EC2 Linux alla tua directory gestita di AWS Microsoft AD Active Directory
- Unisci manualmente un'istanza Amazon EC2 Linux alla tua directory gestita di AWS Microsoft AD Active Directory utilizzando Winbind
- Unisci manualmente un'istanza Mac di Amazon EC2 alla tua directory gestita di AWS Microsoft AD Active Directory

- Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS
- Creare o modificare un set di opzioni DHCP

Avvia l'istanza di amministrazione delle directory nel tuo AWS Managed Microsoft AD Active Directory

Questa procedura avvia un'istanza di Windows amministrazione delle directory di Amazon EC2 AWS Systems Manager utilizzando Automation per gestire le directory. AWS Management Console Puoi farlo anche eseguendo l'automazione AWS-CreateDS ManagementInstance direttamente nella console di automazione. AWS Systems Manager

Prerequisiti

Per avviare un'istanza EC2 di amministrazione delle directory dalla console, devi avere le seguenti autorizzazioni abilitate nel tuo account.

- `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

Per avviare un'istanza EC2 di amministrazione delle directory nel AWS Management Console

1. Accedi alla console AWS Directory Service.
2. In Active Directory, scegli Directory.
3. Scegli l'ID di directory della directory in cui desideri avviare un'istanza EC2 per l'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.

6. Nella pagina Avvia istanza EC2 di amministrazione della directory, 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 CLI il comando Visualizza per vedere un esempio che utilizzi AWS CLI per eseguire questa automazione.

7. Scegli 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.

Per visualizzare l'istanza EC2 di amministrazione delle directory

Se non hai avviato alcuna istanza EC2 per una directory, viene visualizzato un trattino (-) sotto l'istanza EC2 di amministrazione della directory.

1. In Active Directory, scegli Directory e seleziona la directory che desideri visualizzare.

2. In Dettagli della directory, sotto Istanza EC2 di amministrazione della directory, scegli una o tutte le istanze da visualizzare.

3. Quando scegli un'istanza, avviene un reindirizzamento alla pagina Connetti all'istanza EC2 per connettere un desktop remoto alla tua istanza.

Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo AWS Managed Microsoft AD Active Directory

Questa procedura unisce senza problemi un'istanza Amazon Windows EC2 al tuo AWS Managed Microsoft AD. Se devi eseguire un'unione di dominio senza interruzioni su più domini, consulta. Account AWSTutorial: Condivisione della directory AWS Managed Microsoft AD per aggiungere facilmente un dominio EC2 Per informazioni complete su Amazon EC2, consulta Che cos'è Amazon EC2?.

Per unirti senza problemi a un'istanza Amazon EC2 Windows

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.

3. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Windows EC2.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.
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.

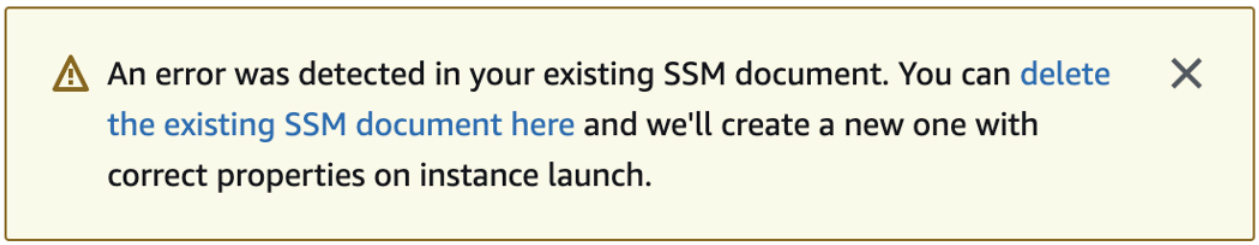
9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto 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 la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

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 DirectoryServiceAccess associate le policy AWS gestite AmazonSSM ManagedInstanceCore e AmazonSSM 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. Per Use case (Caso d'uso), seleziona EC2.
4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le politiche AmazonSSM e AmazonSSM. ManagedInstanceCore DirectoryServiceAccess Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Seleziona Successivo.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un managed by. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager .

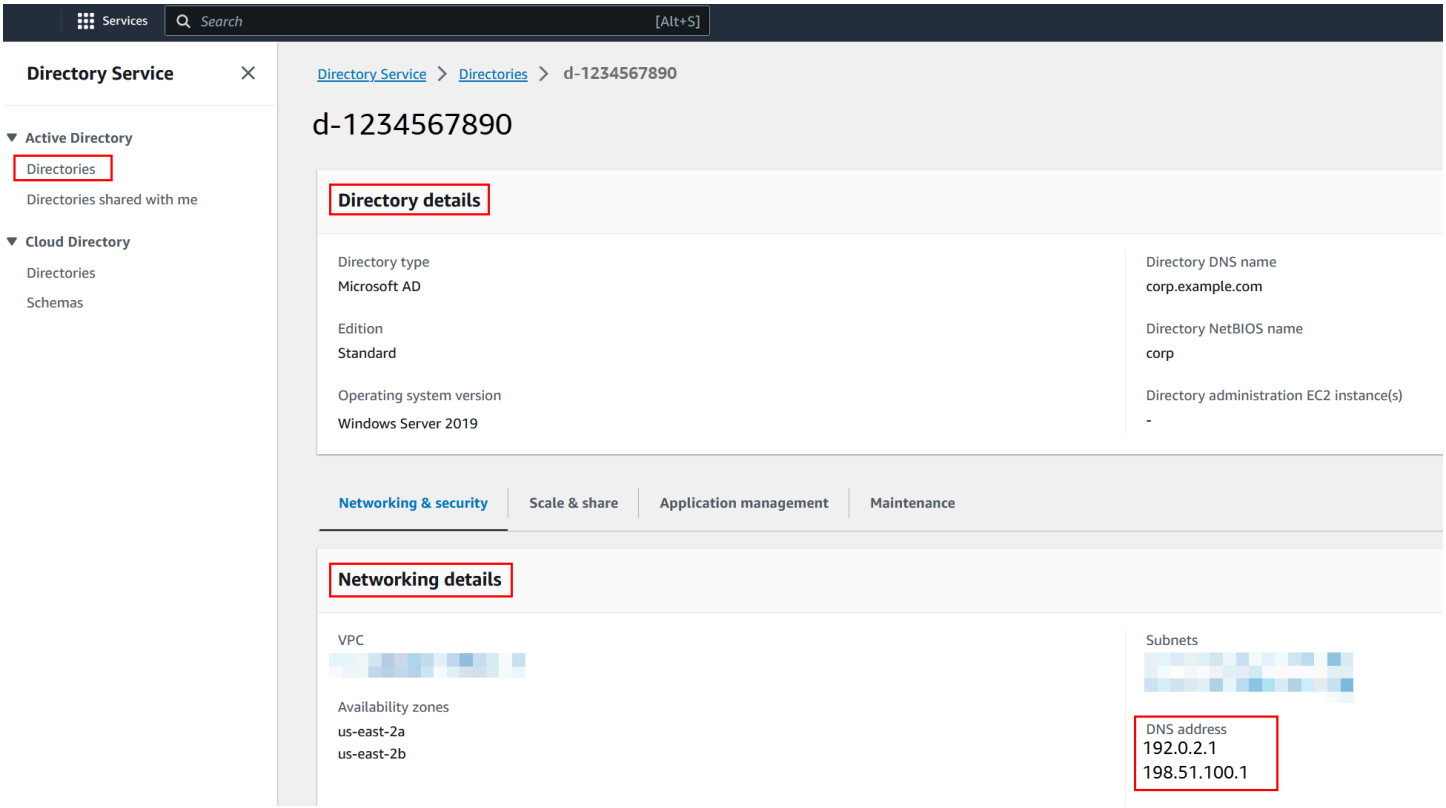
5. Nella pagina Denomina, rivedi e crea inserisci un Nome ruolo. È necessario aggiungere questo nome del ruolo all'istanza EC2.
6. (Facoltativo) Puoi fornire una descrizione del profilo dell'istanza IAM nel campo Descrizione.
7. Scegli Crea ruolo.
8. Torna alla pagina Avvia un'istanza e scegli l'icona 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).

Unisci manualmente un'Windowsistanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory

Per aggiungere manualmente un'Windowsistanza Amazon EC2 esistente a un Managed AWS Microsoft ADActive Directory, l'istanza deve essere avviata utilizzando i parametri specificati in. Unisci senza problemi un'istanza Windows di Amazon EC2 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 AWS Managed Microsoft AD Active Directory

1. Connettiti all'istanza utilizzando qualsiasi client Remote Desktop Protocol.
2. Apri la finestra di dialogo delle proprietà TCP/IPv4 sull'istanza.
   a. Apri Network Connections (Connessioni di rete).

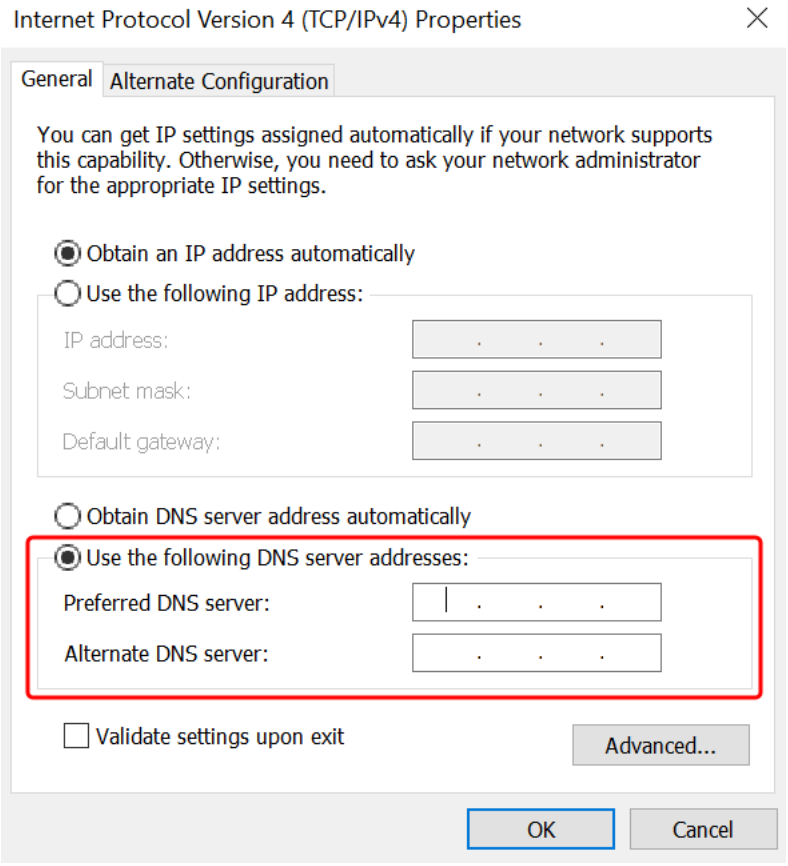
      Tip

      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 Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

> **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 Installare gli 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.

Unisci senza problemi un'istanza Amazon EC2 Linux alla tua directory AWS gestita di Microsoft AD Active Directory

Questa procedura unisce senza problemi un'istanza Amazon EC2 Linux alla tua directory AWS gestita di Microsoft AD Active Directory. Se devi eseguire un'unione di dominio senza interruzioni su più AWS account, puoi facoltativamente scegliere 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 non supportano la funzionalità di aggiunta ottimizzata del dominio.

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 .

Demo dell'aggiunta corretta del dominio AD di Amazon EC2 per Linux

Prerequisiti

Prima di poter configurare un'unione perfetta del dominio 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 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 Installare gli 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 AWS Secrets Manager per archiviare l'account del servizio di dominio.

Per creare segreti e archiviare le informazioni sull'account del servizio di dominio

1. Accedi AWS Management Console e apri la AWS Secrets Manager 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:

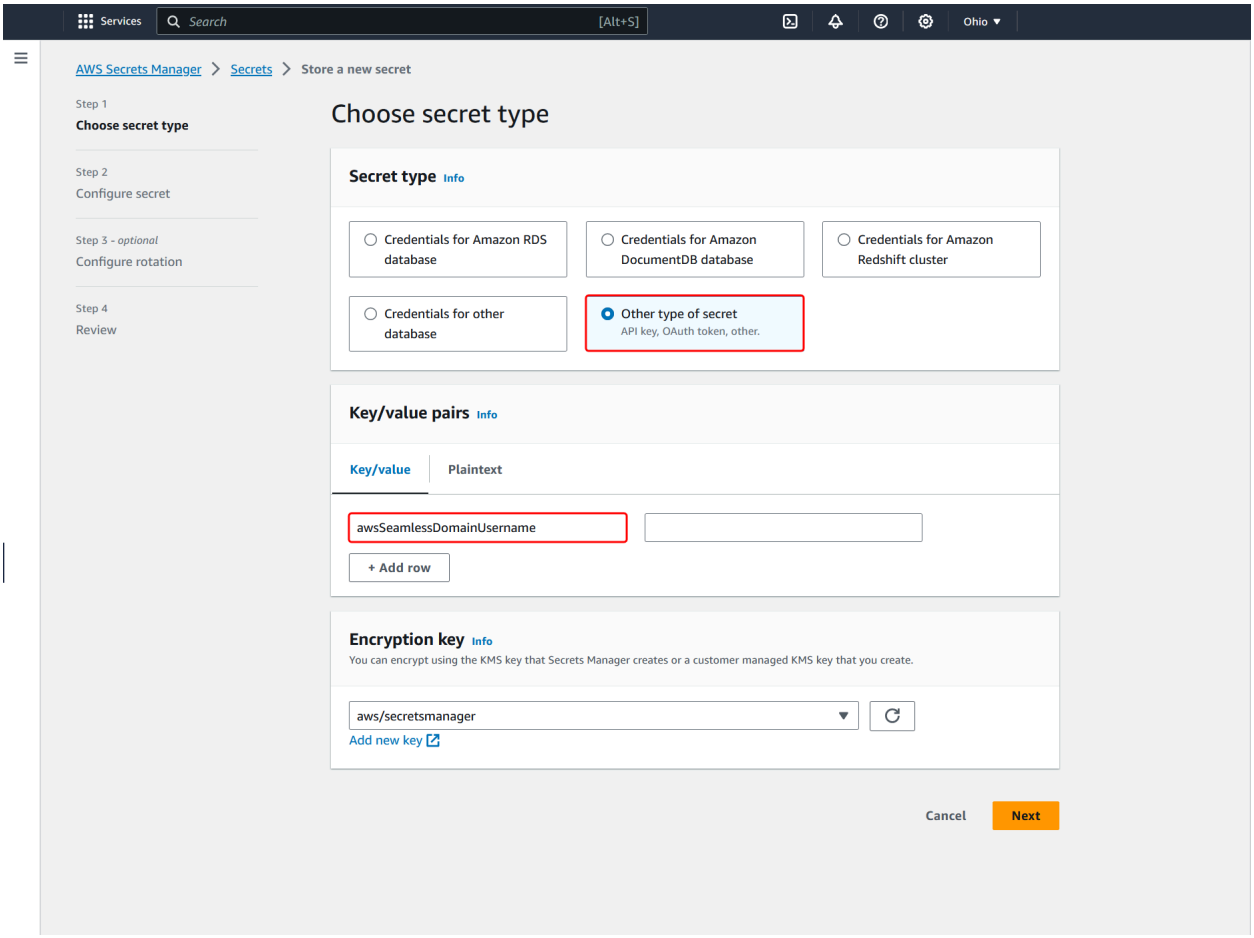
    a. In Tipo segreto, scegli Altro tipo di segreti.

    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`. AWS Secrets Manager crittografa sempre il segreto quando scegli questa opzione. Puoi anche scegliere una chiave creata da te.

> **Note**
>
> Sono previste delle commissioni AWS Secrets Manager, a seconda del segreto utilizzato. Per l'elenco completo dei prezzi aggiornati, consulta la pagina dei prezzi AWS Secrets Manager.
> Puoi utilizzare la chiave AWS `aws/secretsmanager` gestita creata 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 attuale. AWS KMS Per ulteriori informazioni, consulta la sezione Prezzi di AWS Key Management Service.

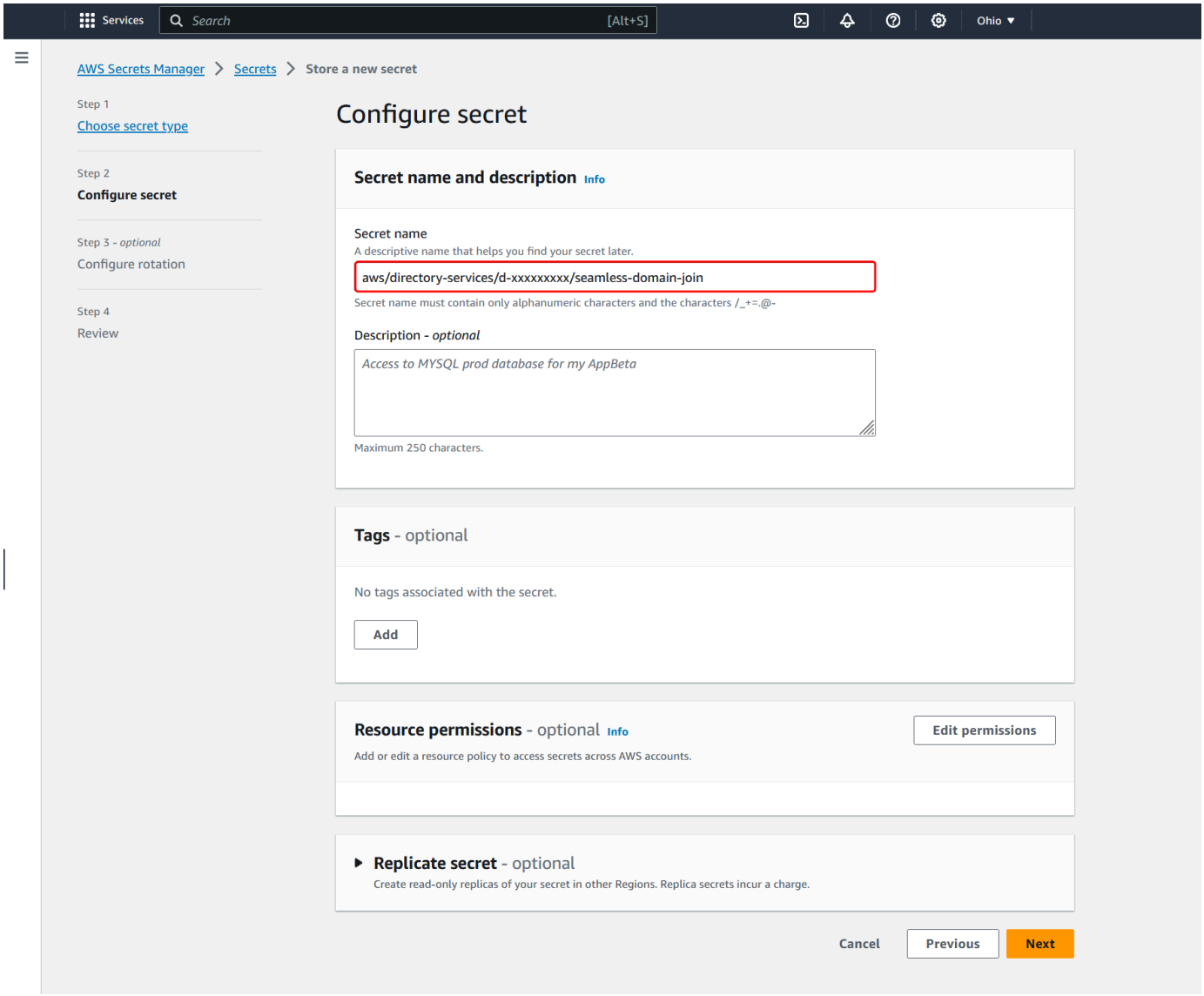
v. Seleziona Successivo.

4. In Nome segreto, inserisci un nome segreto che includa l'ID della tua directory utilizzando il seguente formato, sostituendo *`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 inserire **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** esattamente come è, e sostituire *`d-xxxxxxxxx`* con l'ID della 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 AWS Secrets Manager i segreti nella Guida per l'AWS Secrets Manager utente.

  Per il passaggio 5, utilizzare il modello di rotazione Microsoft Active Directory credenziali nella Guida per l'AWS Secrets Manager utente.

  Per assistenza, consulta Risoluzione dei problemi di AWS Secrets Manager rotazione nella Guida per l'AWS Secrets Manager utente.

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 IAM in LinuxEC2. 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 AWS Management Console come utente autorizzato a creare policy IAM. 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.

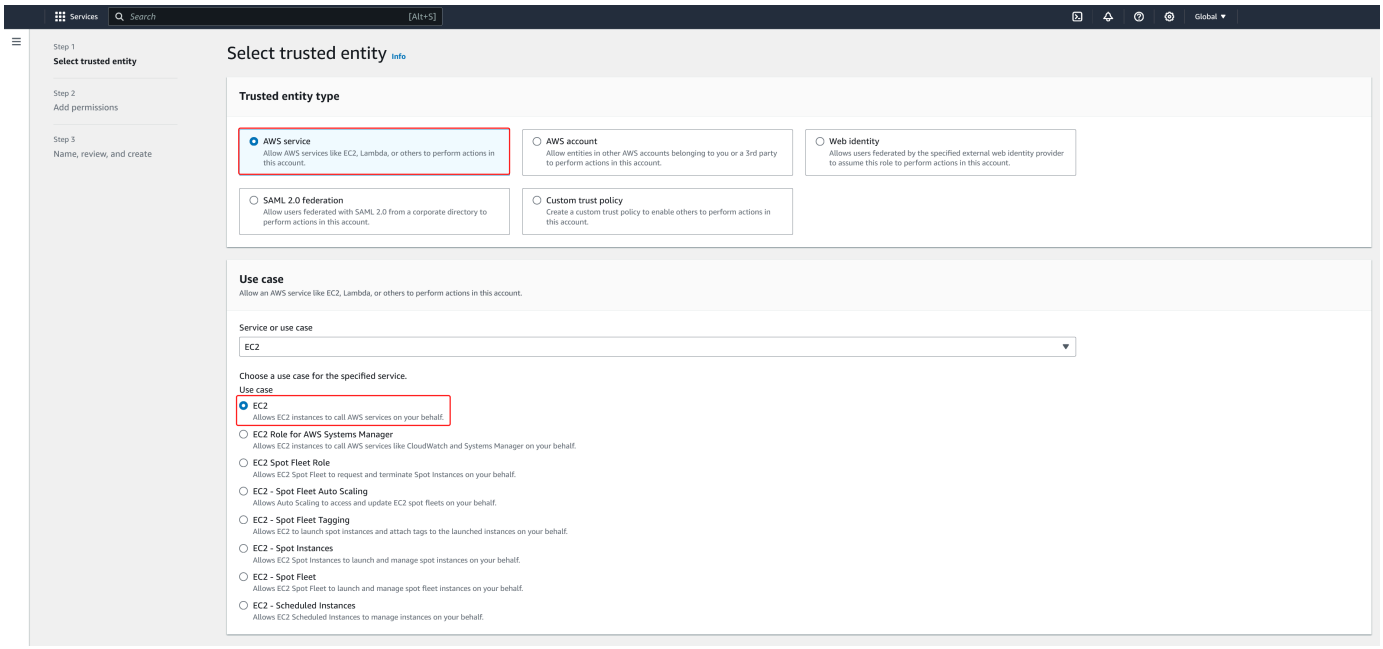
> **Note**
>
> Consigliamo di creare una policy per ogni segreto. In questo modo, ti assicuri che le istanze abbiano accesso solo al segreto in questione e riduci al minimo l'impatto se un'istanza viene compromessa.

Crea il ruolo LinuxEC2 DomainJoin

Utilizzi la console IAM per creare il ruolo che userai per aggiungere il dominio alla tua istanza EC2 Linux.

Per creare il ruolo LinuxEC2 DomainJoin

1. Accedi AWS Management Console come utente autorizzato a creare policy IAM. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro 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**
>
> AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un server gestito da. Active Directory AWS Directory Service AmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 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`** 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

Ora che hai configurato tutte le attività prerequisite, puoi utilizzare la seguente procedura per unire senza problemi la tua istanza EC2 Linux.

Per unirti senza problemi alla tua istanza Linux

1. Accedi AWS Management Console e apri la console Amazon EC2 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. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Linux EC2.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.

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, consulta Installazione e configurazione dell'Agente SSM su istanze EC2 per Linux.
> SSM utilizza il `aws:domainJoin` plug-in per aggiungere un'istanza Linux a un dominio. Active Directory *`Il plugin cambia il nome host per le istanze Linux nel formato EC2AMAZ-XXXXXXX.`* Per ulteriori informazioni in merito*`aws:domainJoin`*, consultate il riferimento al plugin AWS Systems Manager Command Document nella Guida per l'utente.AWS Systems Manager

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.

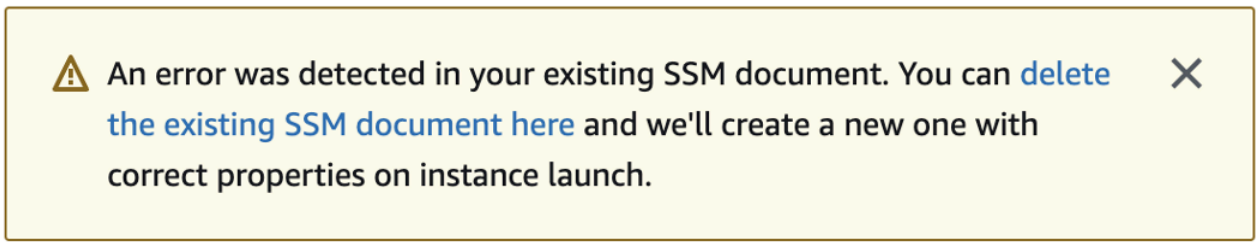
9. Nella pagina Avvia un'istanza, nella sezione Impostazioni di rete, scegli Modifica. Scegli il VPC in cui è stata creata la tua directory dall'elenco a discesa VPC - obbligatorio.
10. Scegli una delle sottoreti pubbliche nel tuo VPC dall'elenco a discesa Sottorete. La sottorete scelta deve avere tutto 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 la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

15. Per il profilo dell'istanza IAM, scegli il ruolo IAM creato in precedenza nella sezione dei prerequisiti Fase 2: Creazione del ruolo LinuxEC2. 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 alla tua directory gestita di AWS Microsoft AD Active Directory

Oltre alle istanze Windows di Amazon EC2, puoi anche aggiungere determinate istanze Amazon EC2 Linux alla tua AWS Managed 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 AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 informazioni su come determinare la versione di Amazon Linux in uso, consulta Identificazione delle immagini di Amazon Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.

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 dominio *example.com* che dispone di privilegi di aggiunta al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 "AWS Delegated 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. AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 dominio *example.com* che dispone di privilegi di aggiunta al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 "AWS Delegated 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. AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 SAM AccountName per un account nel dominio *example.com* che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 "AWS Delegated 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 AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 SAM AccountName nel dominio *example.com che dispone dei privilegi di accesso al dominio*. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 seguente riga 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 'AWS Delegated 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. AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 SAM AccountName per un account nel dominio *example.com* che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 "AWS Delegated 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. Per 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, OU è *Testou*.

dc

È il componente di dominio del tuo dominio. In questo esempio, *example* (esempio).

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.

Per 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, OU è *Testou*.

dc

È il componente di dominio del tuo dominio. In questo esempio, *example* (esempio).

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 Windows and Security Identifier (SID). Active Directory

1. Centralizzato
2. Distribuito

> **Note**
>
> La mappatura centralizzata dell'identità degli utenti Active Directory richiede l'interfaccia del sistema operativo portatile o POSIX.

Mappatura centralizzata delle identità degli utenti

Active Directoryo un altro servizio LDAP (Lightweight Directory Access Protocol) fornisce UID e GID agli utenti Linux. InActive Directory, questi identificatori sono memorizzati negli attributi degli utenti:

- 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 da cui utilizzare l'UID e il GIDActive Directory, impostatelo `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 dispone dell'estensione POSIX o se si sceglie 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.

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%
```

Unisci manualmente un'istanza Amazon EC2 Linux alla tua directory gestita di AWS Microsoft AD Active Directory utilizzando Winbind

Puoi utilizzare il servizio Winbind per aggiungere manualmente le tue istanze Amazon EC2 Linux a un dominio Microsoft AD Active AWS 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 AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 di 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 dominio *example.com* che dispone di privilegi di aggiunta al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 AWS 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 intendi configurarla manualmente,

consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 SAM AccountName nel dominio *`example.com`* che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

`esempio.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 AWS 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'istanza Amazon EC2 privata nel Knowledge Center per indicazioni sull'impostazione AWS del server DNS persistente per la tua particolare distribuzione e versione Linux.
3. Assicurati che l'istanza Linux sia aggiornata.

```
sudo yum -y update
```

```
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 dominio *example.com* che dispone di privilegi di aggiunta al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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%
```

Unisci manualmente un'istanza Mac di Amazon EC2 alla tua directory gestita di AWS Microsoft AD Active Directory

Questa procedura unisce manualmente un'istanza Amazon EC2 Mac alla tua directory AWS gestita di Microsoft AD Active Directory.

Prerequisiti

- Le istanze Mac di Amazon EC2 richiedono host dedicati Amazon EC2. È necessario allocare un host dedicato e avviare un'istanza sull'host. Per ulteriori informazioni, consulta Launch a Mac nella Guida per l'utente di Amazon EC2.

- 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 Creare o modificare un set di opzioni DHCP.

> **Note**
>
> I prezzi degli host dedicati variano in base all'opzione di pagamento selezionata. Per ulteriori informazioni, consulta la Guida per l'utente di Pricing and Billing in Amazon EC2.

Per partecipare manualmente a 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'account *utente ec2* utilizzando il seguente comando:

   ```
   sudo passwd ec2-user
   ```

3. *Quando richiesto dalla riga di comando, fornisci una password per l'account ec2-user.* Puoi aggiornare il sistema operativo e il software seguendo la procedura riportata nella Guida per l'utente di Amazon EC2 Update the operating system and software in Amazon EC2.
4. Usa il seguente comando *dsconfigad* per aggiungere l'istanza Mac al dominio gestito di AWS 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.

Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS

Per unire un computer alla directory, devi disporre di un account con privilegi per aggiungere computer alla directory.

Con AWS Directory Service for Microsoft Active Directory, i membri dei gruppi Admins e AWS Delegated 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.

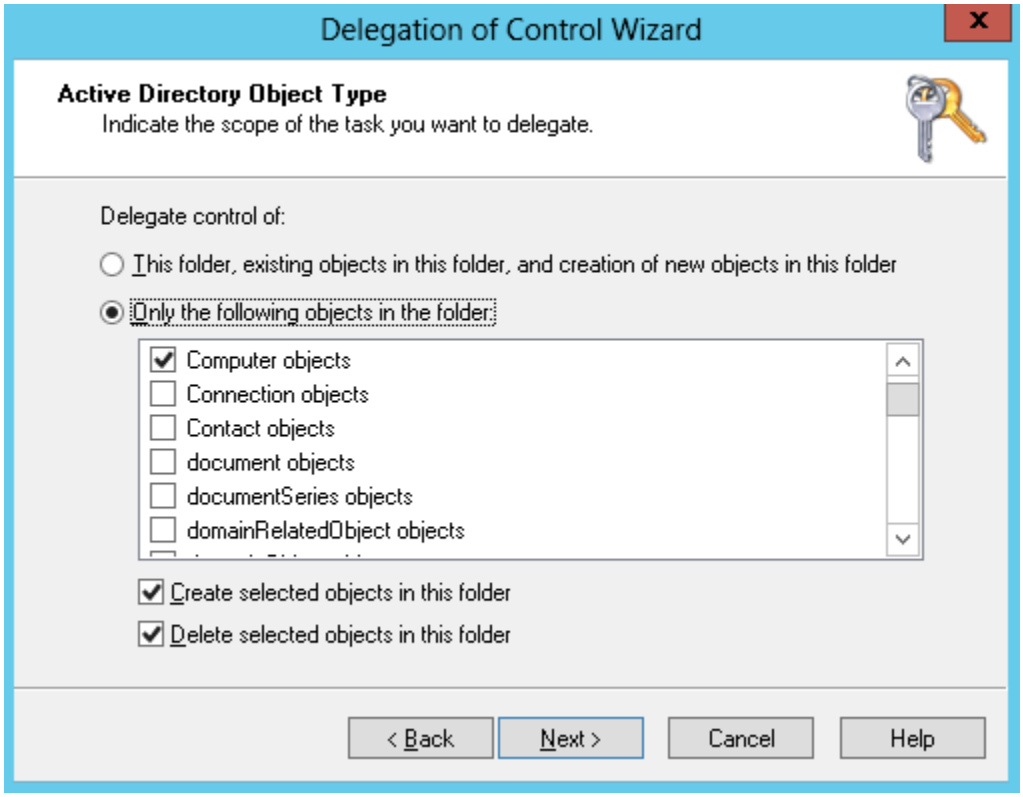
Per delegare i privilegi di iscrizione per Managed AWS Microsoft AD

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).

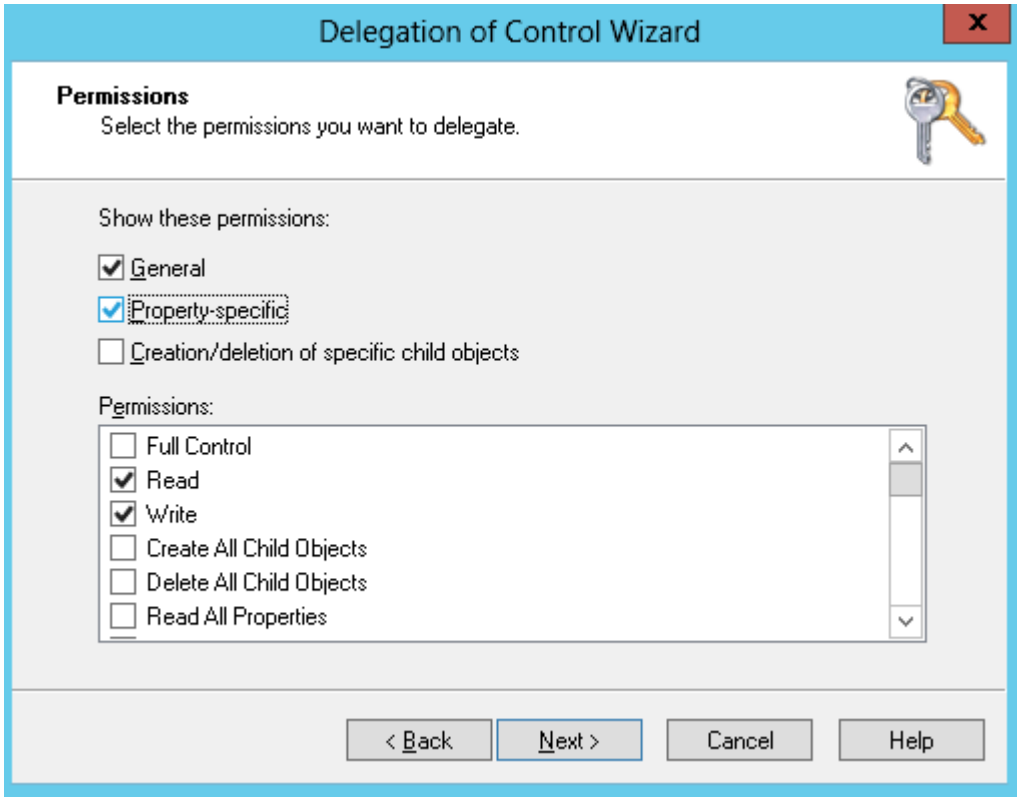
   > **Important**
   >
   > Quando si avvia un AWS Directory Service per Microsoft Active Directory, AWS crea un'unità organizzativa (OU) che contiene tutti gli oggetti della directory. Questa unità organizzativa, che ha lo stesso nome NetBIOS che hai digitato al momento della creazione della directory, si trova nella radice del dominio. La radice del dominio è di proprietà e gestita da AWS. 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. Seleziona 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.

Creare o modificare un set di opzioni DHCP

AWS consiglia di creare un set di opzioni DHCP per la AWS 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 alla 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. Annota l'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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
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 Microsoft AD gestito da AWS

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 AWS Directory Service, è necessario utilizzare un'istanza (on-premise o EC2) unita alla tua directory AWS Directory Service ed essere connessi come un utente che dispone di privilegi per creare utenti e gruppi. È inoltre necessario installare gli strumenti di Active Directory sull'istanza EC2 in modo da poter aggiungere gli utenti e i gruppi con lo snap-in di Utenti e computer di Active Directory.

Puoi implementare un'istanza EC2 preconfigurata con strumenti amministrativi di Active Directory preinstallati dalla console di gestione AWS Directory Service. Per ulteriori informazioni, consulta Avvia l'istanza di amministrazione delle directory nel tuo AWS Managed Microsoft AD Active Directory.

Se devi implementare un'istanza EC2 autogestita con strumenti amministrativi e installare gli strumenti necessari, consulta Fase 3: Implementa un'istanza Amazon EC2 per gestire la tua AWS Managed Microsoft AD Active Directory.

> **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, consulta la sezione preautenticazione su Microsoft TechNet.

Negli argomenti seguenti sono incluse istruzioni su come creare e gestire gli utenti e i gruppi.

Argomenti

Installare gli strumenti di amministrazione di Active Directory per AWS Managed Microsoft AD

Per gestire la tua Active Directory da un'istanza Amazon EC2 Windows Server, devi installarla Active Directory Domain Services and Active Directory Lightweight Directory Services Tools 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:

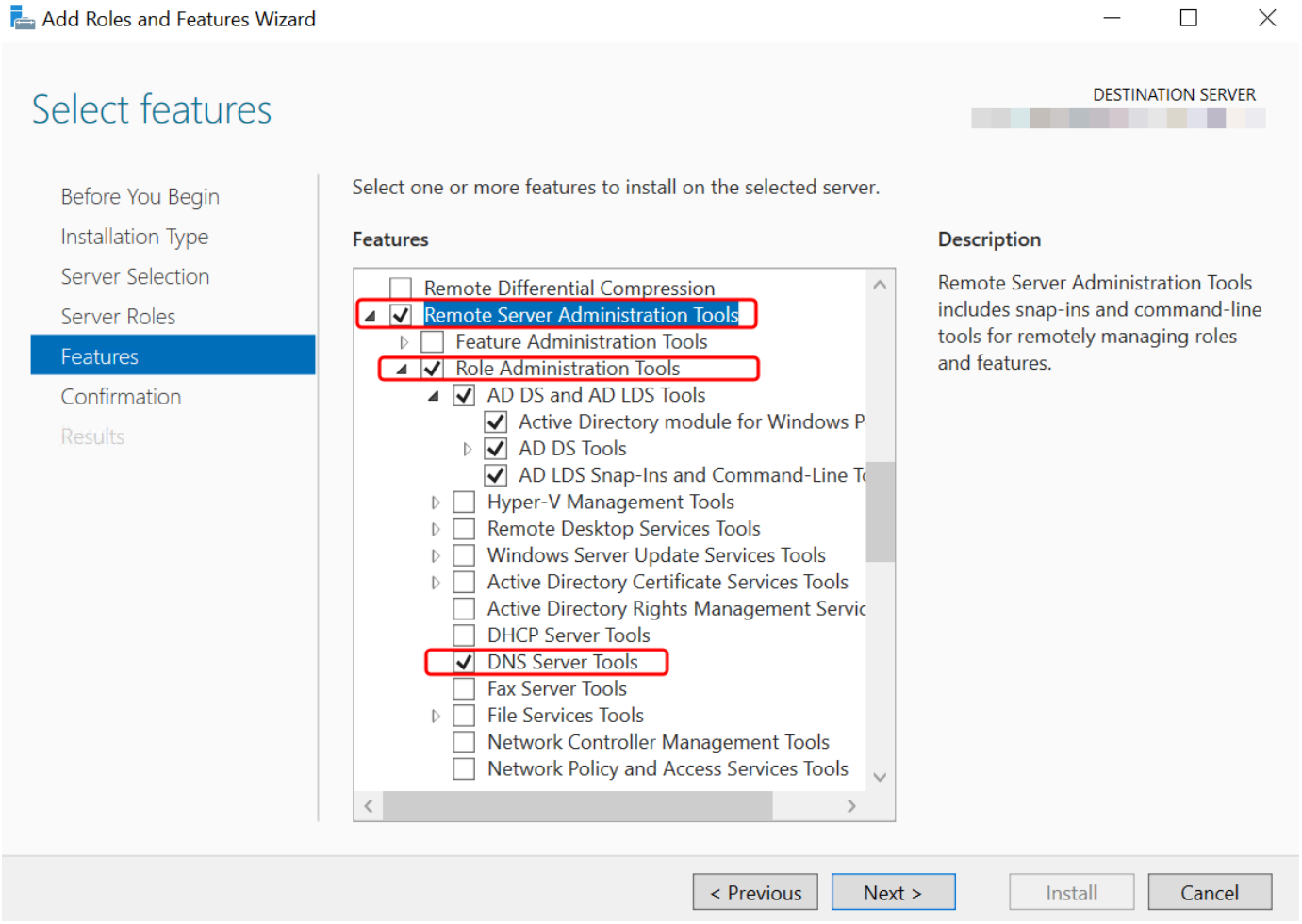
1. Crea un Microsoft AD AWS gestitoActive Directory. Per ulteriori informazioni, consulta Crea il tuo AWS Managed Microsoft AD.
2. Avvia e unisci un'istanza EC2 Windows Server alla tua AWS Managed Microsoft AD Active Directory. L'istanza EC2 necessita delle seguenti policy per creare utenti e gruppi: **`AWSSSMManagedInstanceCore`** e. **`AmazonSSMDirectoryServiceAccess`** Per ulteriori informazioni, consulta Avvia l'istanza di amministrazione delle directory nel tuo AWS Managed Microsoft AD Active Directory e Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo AWS Managed Microsoft AD Active Directory.

3. Avrai bisogno delle credenziali dell'amministratore del tuo Active Directory dominio. Queste credenziali sono state create al momento della creazione di AWS Managed Microsoft AD. Se hai seguito la procedura riportata inCrea il tuo AWS Managed Microsoft AD, il nome utente dell'amministratore include il nome NetBIOS,. **`corp\admin`**

Installa gli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

Per installare gli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella console Amazon EC2, scegli Istanze, seleziona l'istanza appena creata, quindi scegli Collega.
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 inCrea il 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 Active Directorymodulo per Windows PowerShell, AD DS Tools, gli snap-in e gli strumenti della 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.

Metodi alternativi all'installazione degli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

- Ecco alcuni altri metodi per installare gli strumenti di amministrazione di Active Directory:
  - Facoltativamente, puoi scegliere di installare gli strumenti di amministrazione di Active Directory utilizzandoWindows PowerShell. 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.

- Puoi anche avviare un'istanza EC2 per l'amministrazione delle directory in AWS Management Console cui sono già installati gli strumenti Active Directory Domain Services e Active Directory Lightweight Directory Services Tools seguendo le procedure riportate inAvvia l'istanza di amministrazione delle directory nel tuo AWS Managed Microsoft AD Active Directory.

Creazione di un utente

Utilizza la procedura seguente per creare un utente con un'istanza EC2 aggiunta alla directory Microsoft AD gestito da AWS . Prima di poter creare utenti, devi completare le procedure descritte in Installazione degli strumenti di amministrazione di Active Directory.

È possibile utilizzare uno dei seguenti metodi per creare un utente:

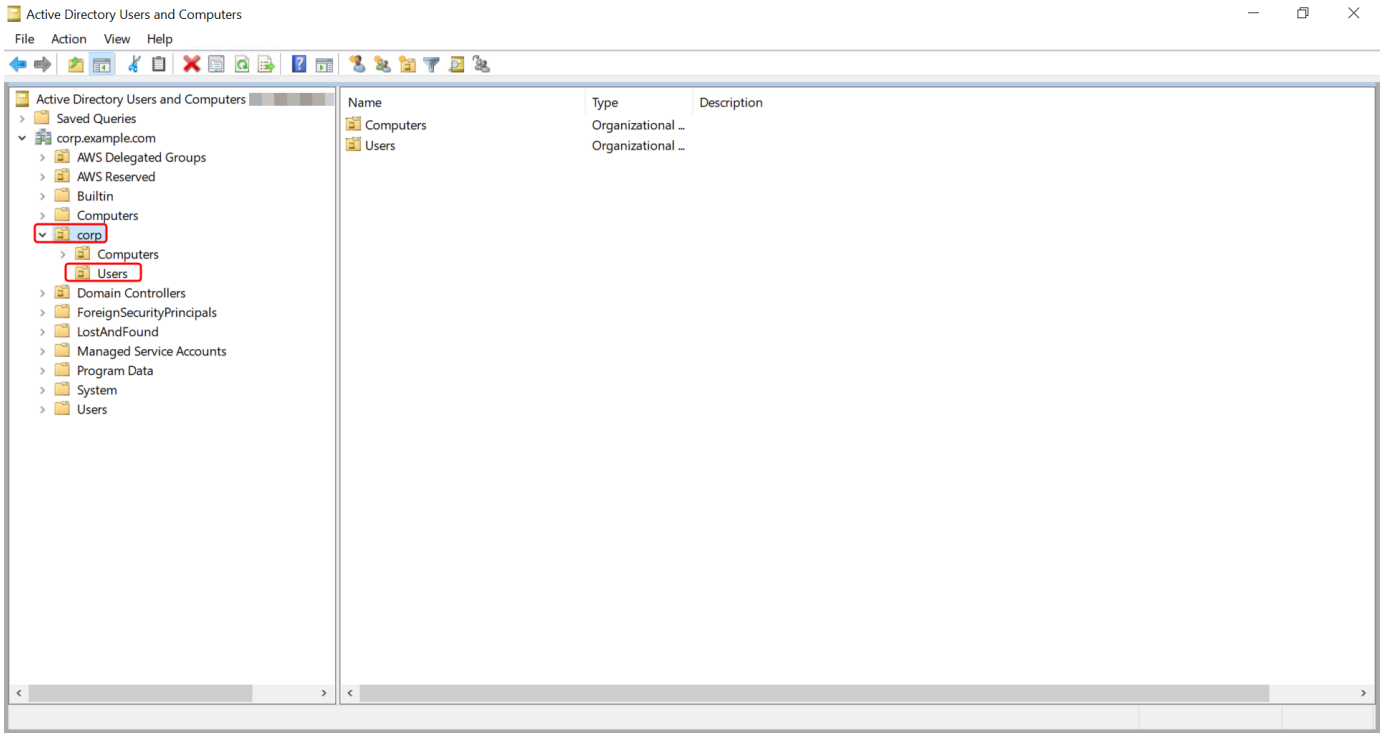
- Active DirectoryStrumenti di amministrazione
- Windows PowerShell

Crea un utente con gli strumenti di Active Directory amministrazione

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 Active Directory



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. Seleziona 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).

Crea un utente in Windows PowerShell

1. Connect all'istanza aggiunta al tuo Active Directory dominio come Active Directory amministratore.
2. Aprire Windows 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 Windows PowerShell fornire una password per il nuovo utente. Per ulteriori informazioni sui requisiti di complessità delle Active Directory password, consulta Microsoftla documentazione. Per ulteriori informazioni sul comando New-ADUser, consultate la documentazione. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Eliminazione di un utente

Utilizzare la procedura seguente per eliminare un utente aggiunto a AWS Managed Microsoft ADActive Directory.

È possibile utilizzare uno dei seguenti metodi per eliminare un utente:

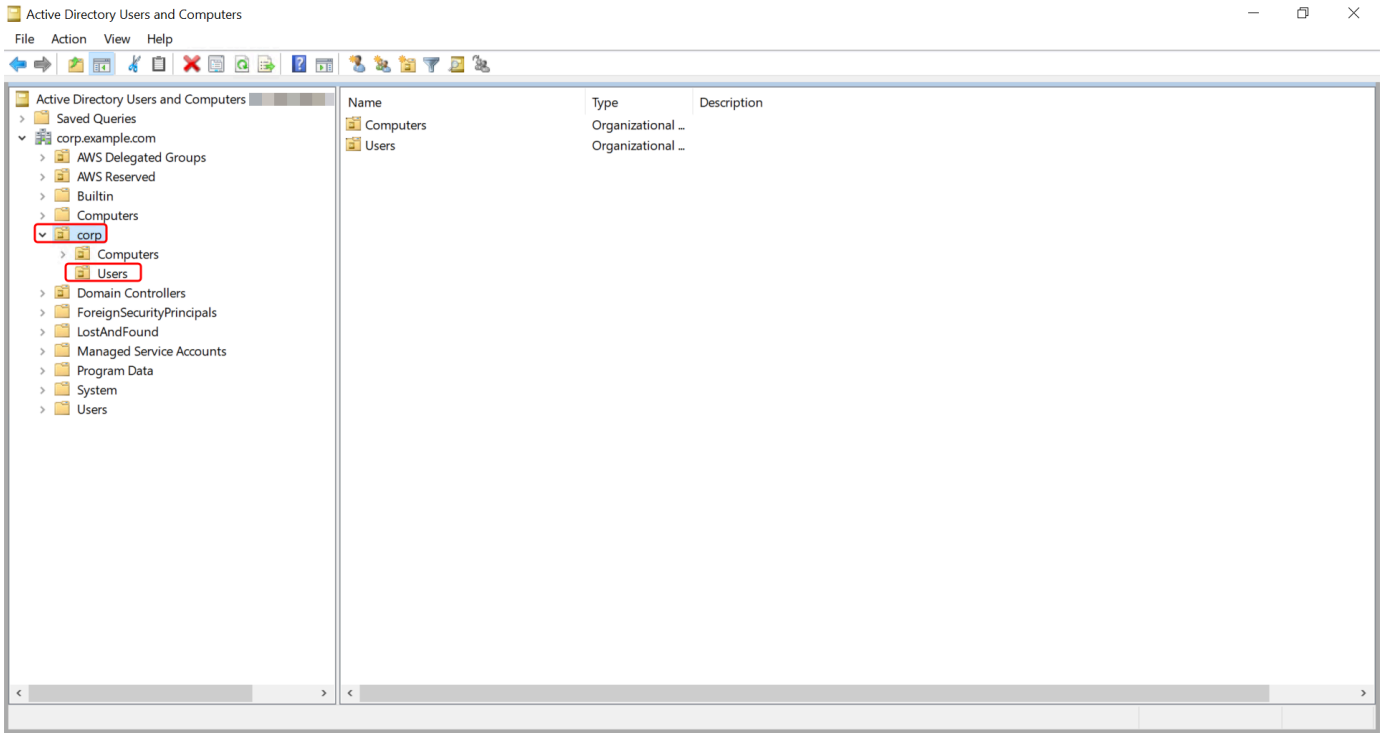
- Active DirectoryStrumenti di amministrazione
- Windows PowerShell

Eliminare un utente con gli strumenti di Active Directory amministrazione

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.

Eliminare un utente in Windows PowerShell

1. Connect all'istanza aggiunta al tuo Active Directory dominio come Active Directory amministratore.
2. Aprire Windows PowerShell.
3. Digita il seguente comando sostituendo il nome utente **`jane.doe`** con il nome utente dell'utente che desideri eliminare. Per ulteriori informazioni sul comando Remove-ADUser, consultate la documentazione. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Considerazioni sul cestino di riciclaggio AD

Gli utenti eliminati vengono archiviati temporaneamente nel Cestino di AD. Per ulteriori informazioni su AD Recycle Bin, consulta The AD Recycle Bin: Understanding, Implementation, Best Practices, and Troubleshooting nel Microsoft blog Ask the Directory Services Team.

Reimpostazione della password utente

Gli utenti devono rispettare le politiche relative alle password definite in. Active Directory A volte in questo modo gli utenti, incluso l'Active Directoryamministratore, possono avere la meglio e dimenticarsi la password. Quando ciò accade, puoi reimpostare rapidamente la password dell'utente utilizzando AWS 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 AWS Directory Service.

Puoi reimpostare la password per qualsiasi utente del tuo account 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 al momento della creazione del. Active Directory Ad esempio, se seguissi la procedura indicata nel Crea il 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 al momento della creazione del. Active Directory Ad esempio, non è possibile reimpostare la password di un utente in AWS Reserved OU. Per ulteriori informazioni sulla struttura dell'unità organizzativa per AWS Managed Microsoft AD, vedereCosa viene creato con AWS Managed Microsoft AD Active Directory.

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 metodi per reimpostare una password utente:

- AWS Management Console

- AWS CLI
- Windows PowerShell

Reimpostare una password utente in AWS Management Console

1. Nel riquadro di navigazione della AWS Directory Service console Active Directory, sotto, scegli Directory, quindi seleziona la Active Directory cartella dall'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.

Reimposta la password di un utente in AWS CLI

1. Per installare AWS CLI, vedi Installare o aggiornare la versione più recente di AWS CLI.
2. Apri il AWS CLI.
3. Digita il comando seguente e sostituisci l'ID di directory, il nome utente **`jane.doe`** e la password **`P@ssw0rd`** con il tuo ID di Active Directory directory e le credenziali desiderate. Per ulteriori informazioni reset-user-password, consulta la sezione AWS CLI Command Reference.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Reimposta una password utente in Windows PowerShell

1. Connect all'istanza aggiunta al tuo Active Directory dominio come Active Directory amministratore.
2. Aprire Windows PowerShell.
3. Digita il comando seguente sostituendo il nome utente**`jane.doe`**, l'ID di directory e la password **`P@ssw0rd`** con il tuo ID di Active Directory directory e le credenziali desiderate. Per ulteriori informazioni, vedere il UserPassword cmdlet Reset-DS.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Creazione di un gruppo

Utilizza la seguente procedura per creare un gruppo di sicurezza con un'istanza EC2 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.

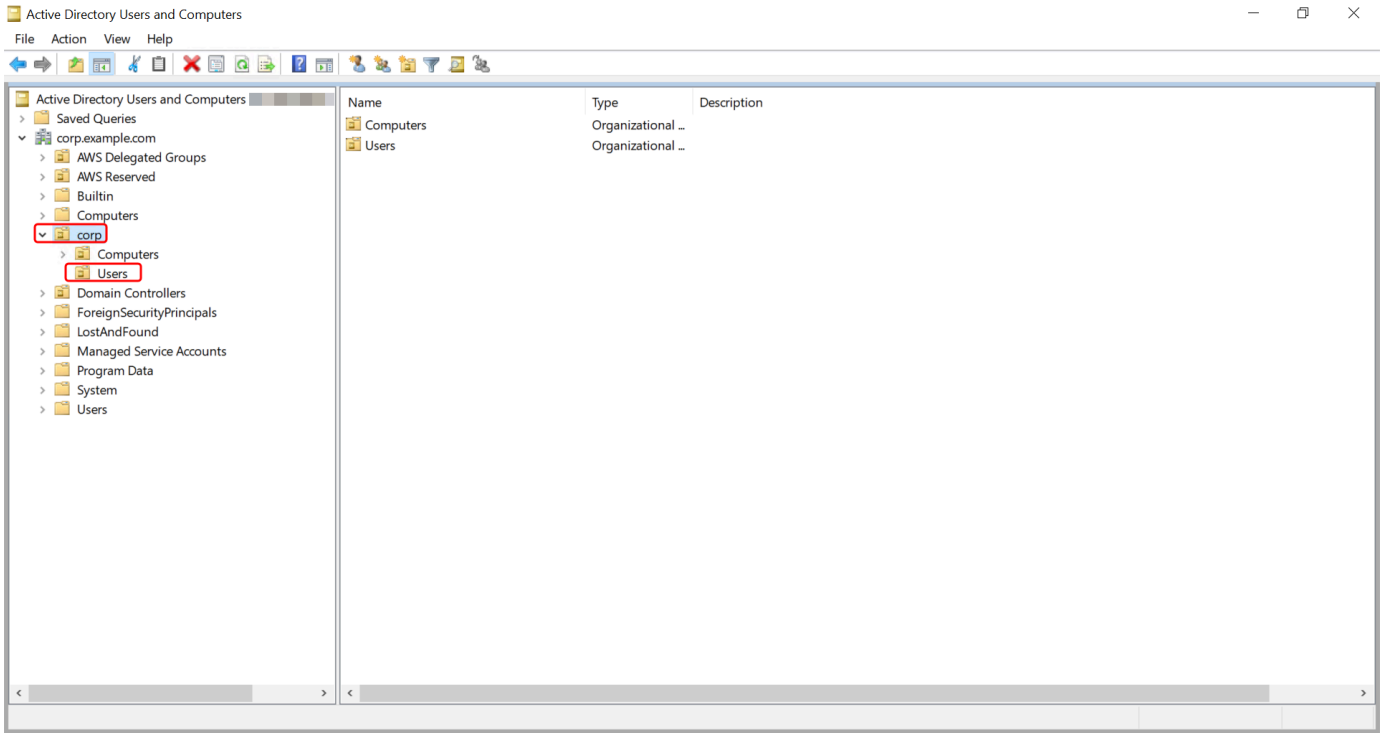
Puoi anche usare Windows PowerShell i comandi per creare gruppi. Per ulteriori informazioni, consulta New-ADGroup nella documentazione di Windows Server 2022. PowerShell

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, vedere. AWSCosa viene creato con AWS Managed Microsoft AD Active Directory



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.

Aggiunta di un utente a un gruppo

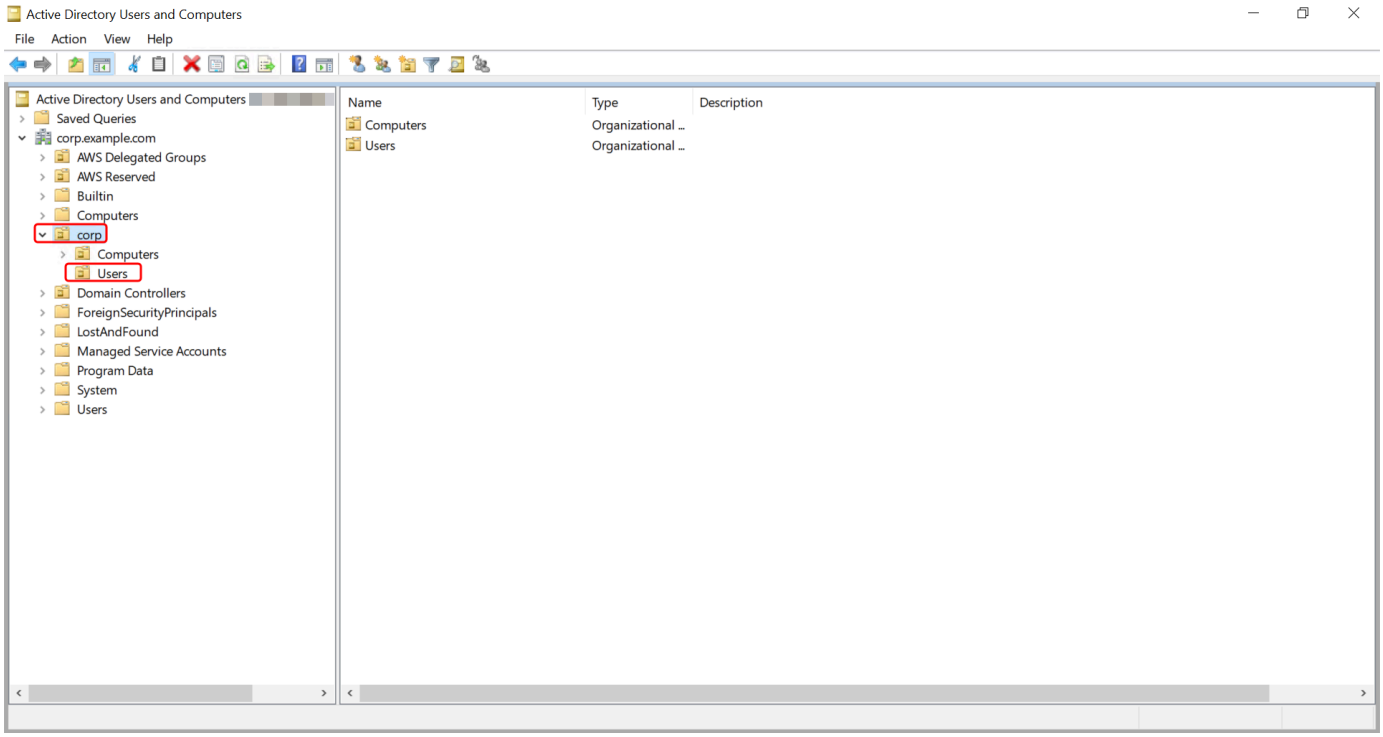
Utilizza la procedura seguente per aggiungere un utente a un gruppo di sicurezza con un'istanza EC2 aggiunta alla directory Microsoft AD gestito da AWS.

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.

Connect 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.

Argomenti

- Creazione di una relazione di trust
- Aggiunta di route IP durante l'utilizzo di indirizzi IP pubblici
- 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 trust

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 AWS Microsoft 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 AWS Directory Service s. Per ulteriori informazioni sulle proprie responsabilità, consultare il nostro modello sulla responsabilità condivisa.

AWS Microsoft 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 le app AWS aziendali come Amazon Chime, Amazon Connect AWS IAM Identity Center, QuickSight Amazon WorkDocs, Amazon WorkMail, WorkSpaces Amazon e. AWS Management Console AWS Microsoft AD gestito deve essere in grado di interrogare gli utenti e i gruppi gestiti automaticamenteActive Directory.

Amazon EC2, Amazon RDS e Amazon FSx funzionano 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**
>
> AWS Microsoft 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 AD AWS . 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 QuickSight, è necessario 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 Service console, nella pagina Dettagli della directory, annota l'ID della directory Microsoft AD AWS gestita.

2. Apri alla 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 di AWS 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 AWS Management Console 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 Replica multi regione, 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. Scegli 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 disponi di un trust unidirezionale esistente in "direzione in entrata" e desideri configurare un'altra relazione di trust nella

"direzione in uscita", sarà necessario eliminare la relazione di trust esistente e crearne una nuova "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. AWS non 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).

Aggiunta di route IP durante l'utilizzo di indirizzi IP pubblici

Puoi utilizzare AWS Directory Service per Microsoft Active Directory per sfruttare molte potenti funzionalità di Active Directory, tra cui stabilire attendibilità 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 trust.

Analogamente, è necessario inserire anche le informazioni dell'indirizzo IP quando instradi il traffico da Microsoft AD gestito da AWS su AWS a un VPC AWS in peering, se il VPC utilizza intervalli di IP pubblici.

Quando aggiungi gli indirizzi IP come descritto in Creazione di una relazione di trust, 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 di AWS 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 ti guiderà attraverso tutte le fasi necessarie per configurare una relazione di trust tra il Servizio di directory AWS per Microsoft Active Directory e Microsoft Active Directory autogestito (on-premise). 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 trust

Prerequisiti

Questo tutorial presuppone che tu abbia già:

> **Note**
>
> Microsoft AD gestito da AWS non supporta il trust con Single Label Domain.

- Una directory Microsoft AD gestito da AWS creata su AWS. Se hai bisogno di aiuto per eseguire questa operazione, consulta Guida introduttiva a AWS Managed Microsoft AD.
- Un'istanza EC2 in esecuzione di Windows aggiunta a tale Microsoft AD gestito da AWS. Se hai bisogno di aiuto per eseguire questa operazione, consulta Unisci manualmente un'Windowsistanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory.

  > **Important**
  >
  > L'account amministratore per il tuo Microsoft AD gestito da AWS deve disporre dell'accesso amministrativo a questa istanza.

- I seguenti strumenti di Windows Server installati su tale istanza:
  - Strumenti AD DS e AD LDS
  - DNS

  Se hai bisogno di aiuto per eseguire questa operazione, consulta Installare gli 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 di Windows Server sopra elencati devono essere disponibili per questa directory.
- Una connessione attiva tra la rete autogestita e il VPC contenente Microsoft AD gestito da AWS. 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 trust.

Configurazione del tutorial

Per questo tutorial, abbiamo già creato un Microsoft AD gestito da AWS e un dominio autogestito. La rete autogestita è connessa al VPC di Microsoft AD gestito da AWS. Di seguito sono riportate le proprietà delle due directory:

Microsoft AD gestito da AWS in esecuzione su AWS

- Nome del dominio (FQDN): MyManagedAD.example.com
- Nome NetBIOS: MyManagedAD
- Indirizzi DNS: 10.0.10.246, 10.0.20.121
- CIDR VPC: 10.0.0.0/16

Il Microsoft AD gestito da AWS risiede nell'ID VPC: vpc-12345678.

Dominio di Microsoft AD gestito da AWS 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 ai CIDR per tutte 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 Amazon.) WorkDocs QuickSight

> **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.

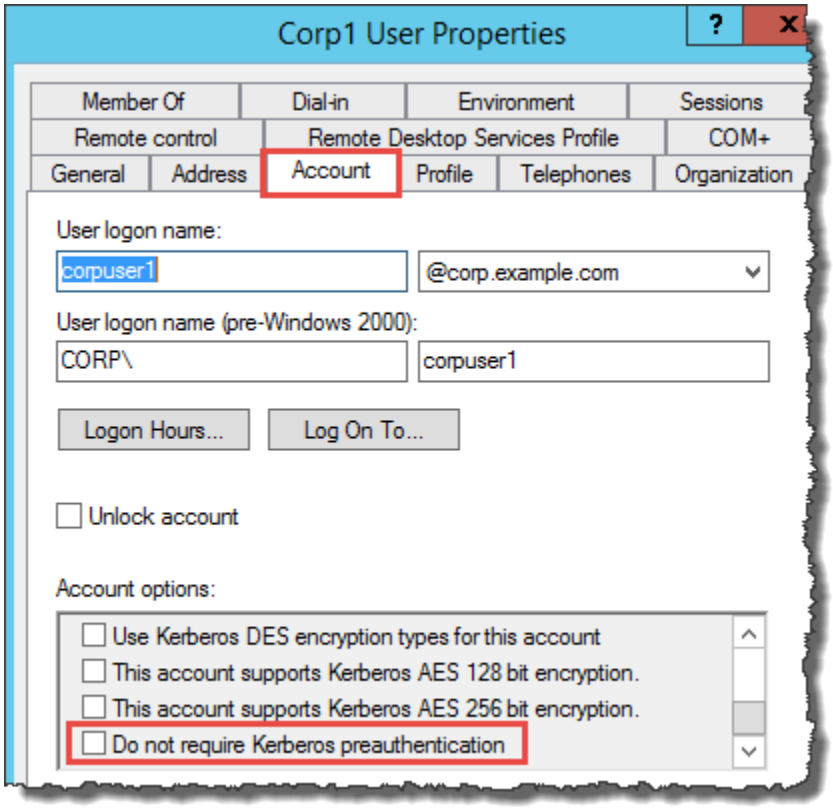
Assicurarsi che la preautenticazione di Kerberos sia abilitata

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

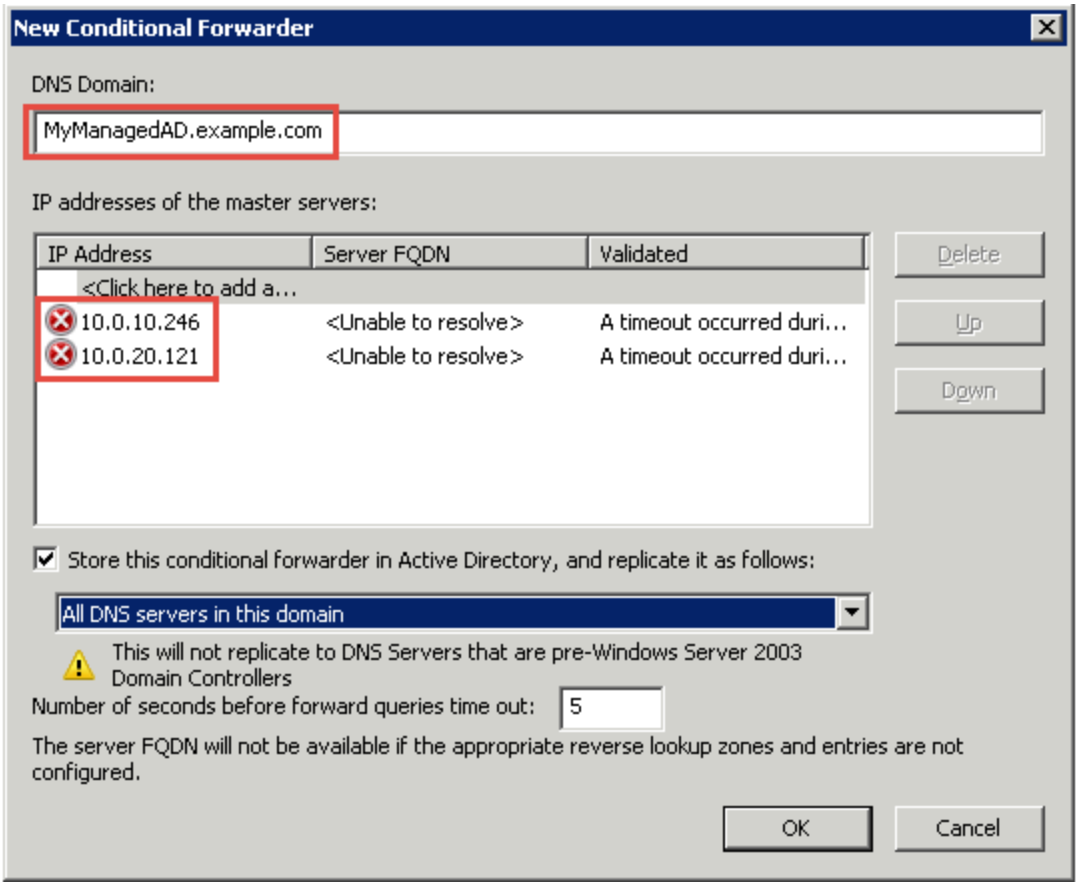
È necessario configurare i server d'inoltro condizionale DNS su ciascun dominio. Prima di eseguire questa operazione sul tuo dominio autogestito, otterrai alcune informazioni sul tuo AWS Managed Microsoft AD.

Configurazione dei server d'inoltro condizionale sul dominio autogestito

1. Accedi a AWS Management Console 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-5V70CN7VJ0.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 gli ACL associati 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.

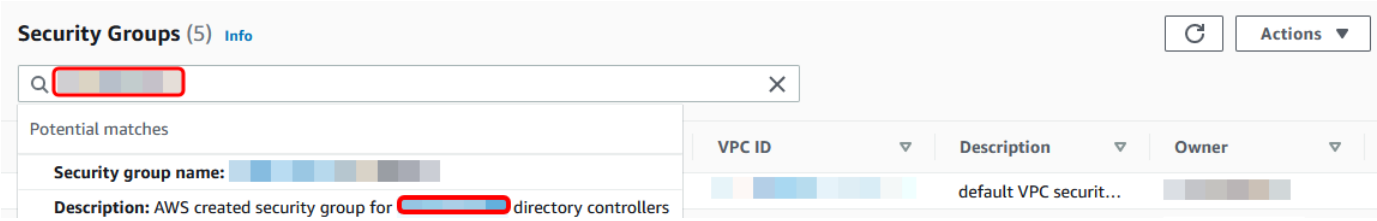
In uscita

- 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

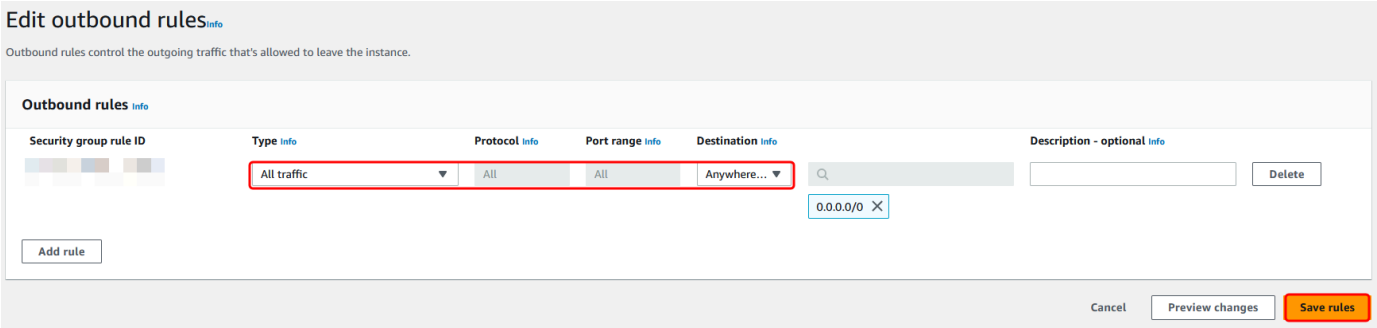
1. Tornare alla console AWS Directory Service. Nell'elenco delle directory, prendi nota dell'ID della directory AWS Managed Microsoft AD.
2. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
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 di AWS sicurezza della tua directory.

6. Seleziona Salva regola.

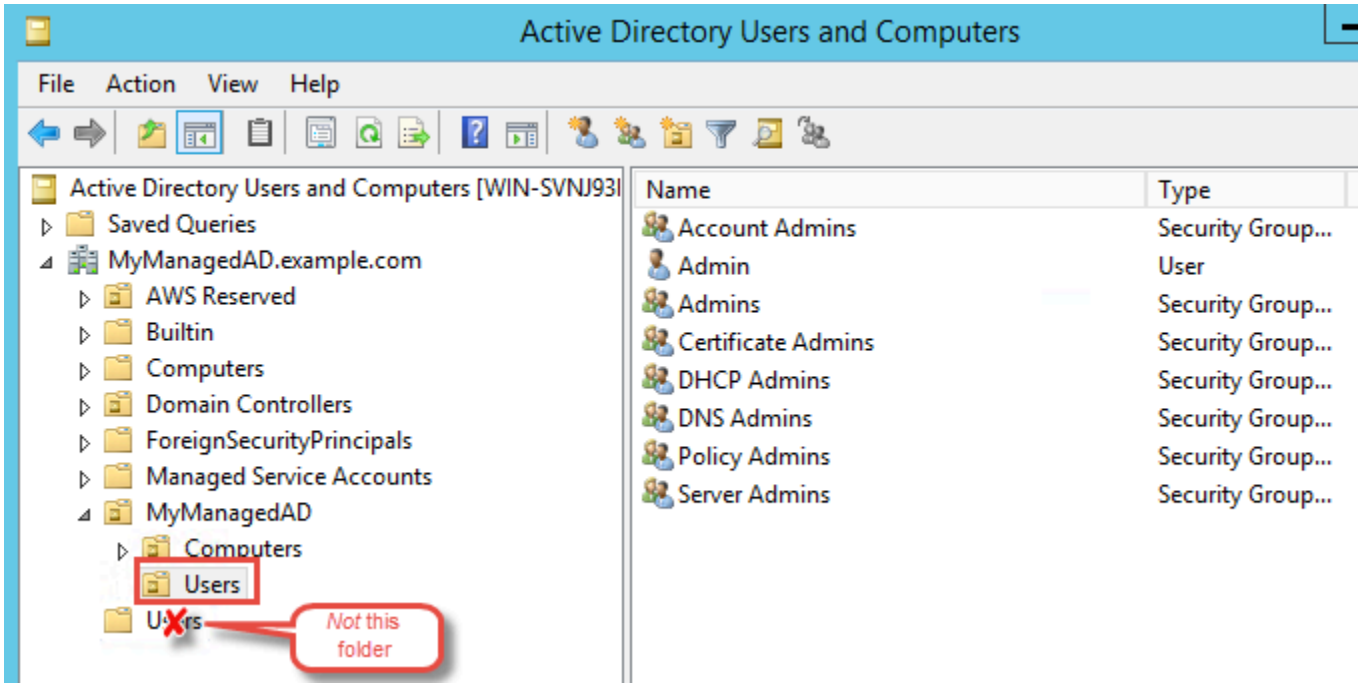


Assicurarsi che la preautenticazione di Kerberos sia abilitata

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 Autorizzazioni per l'account Administrator 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 Installare gli 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. In primo luogo crea il trust sul dominio autogestito, quindi su Microsoft AD gestito da AWS. 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 dominio autogestito, devi creare un trust unidirezionale in ingresso su Microsoft AD gestito da AWS.

> **Note**
>
> Microsoft AD gestito da AWS supporta anche trust esterni. Tuttavia, ai fini di questo tutorial, verrà creato un trust tra foreste bidirezionale.

Per configurare la fiducia nel tuo 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 Microsoft AD gestito da AWS e scegli Successivo.
4. Scegliere Forest Trust (Trust tra foreste). Seleziona Successivo.
5. Scegliere Two-way (Bidirezionale). Seleziona Successivo.
6. Scegliere This domain only (Solo questo dominio). Seleziona Successivo.
7. Scegliere Forest-wide authentication (Autenticazione a livello di foresta). Seleziona Successivo.
8. Digitare una Trust password (Password di trust). Assicurati di ricordare questa password perché sarà necessaria durante la configurazione del trust per il Microsoft AD gestito da AWS.
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). Seleziona Successivo.
11. Scegliere No, do not confirm the incoming trust (No, non confermare il trust in ingresso). Seleziona Successivo.

Configurazione del trust nella directory Microsoft AD gestito da AWS

Infine, configura la relazione di trust tra foreste con la directory Microsoft AD gestito da AWS. Poiché hai creato un trust tra foreste bidirezionale sul dominio autogestito, crea anche un trust bidirezionale utilizzando la directory Microsoft AD gestito da AWS.

> **Note**
>
> Le relazioni di trust sono una funzionalità globale di Microsoft AD gestito da AWS. Se utilizzi Replica multi regione, 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 il trust nella directory Microsoft AD gestito da AWS

1. Tornare alla console AWS Directory Service.
2. Nella pagina Directory, scegli il tuo ID Microsoft AD gestito da AWS.
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. Scegliere 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 trust.

Tutorial: creazione di una relazione di trust tra due domini Microsoft AD gestito da AWS

Questo tutorial ti guiderà attraverso tutte le fasi necessarie per configurare una relazione di trust tra due domini del Servizio di directory AWS per Microsoft Active Directory.

Argomenti

- Fase 1: preparazione di Microsoft AD gestito da AWS
- Fase 2: creazione della relazione di trust con un altro dominio di Microsoft AD gestito da AWS

Vedi anche

Creazione di una relazione di trust

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 gli ACL associati 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

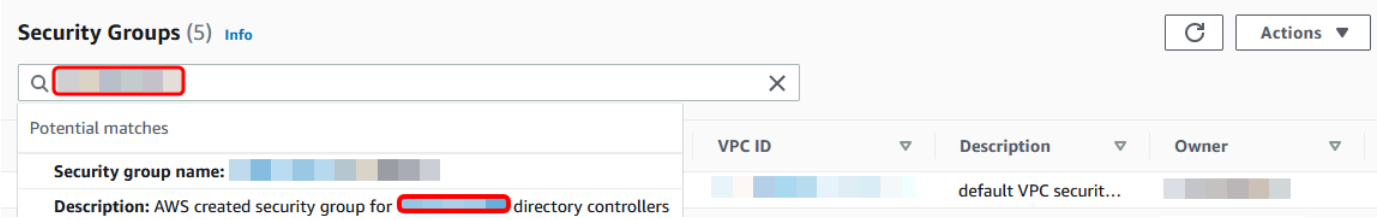
- ALL

> **Note**
>
> Queste sono le porte minime necessarie per connettere i VPC di entrambi i Microsoft AD gestiti da AWS . 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.

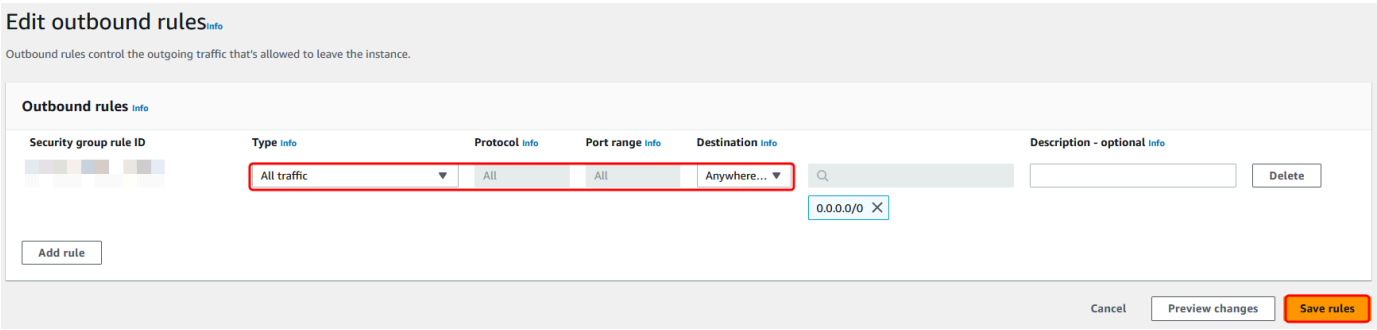
Per configurare le regole in uscita del controller di dominio Microsoft AD AWS gestito

> **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. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro 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 di AWS sicurezza della tua directory.
6. Seleziona Salva.

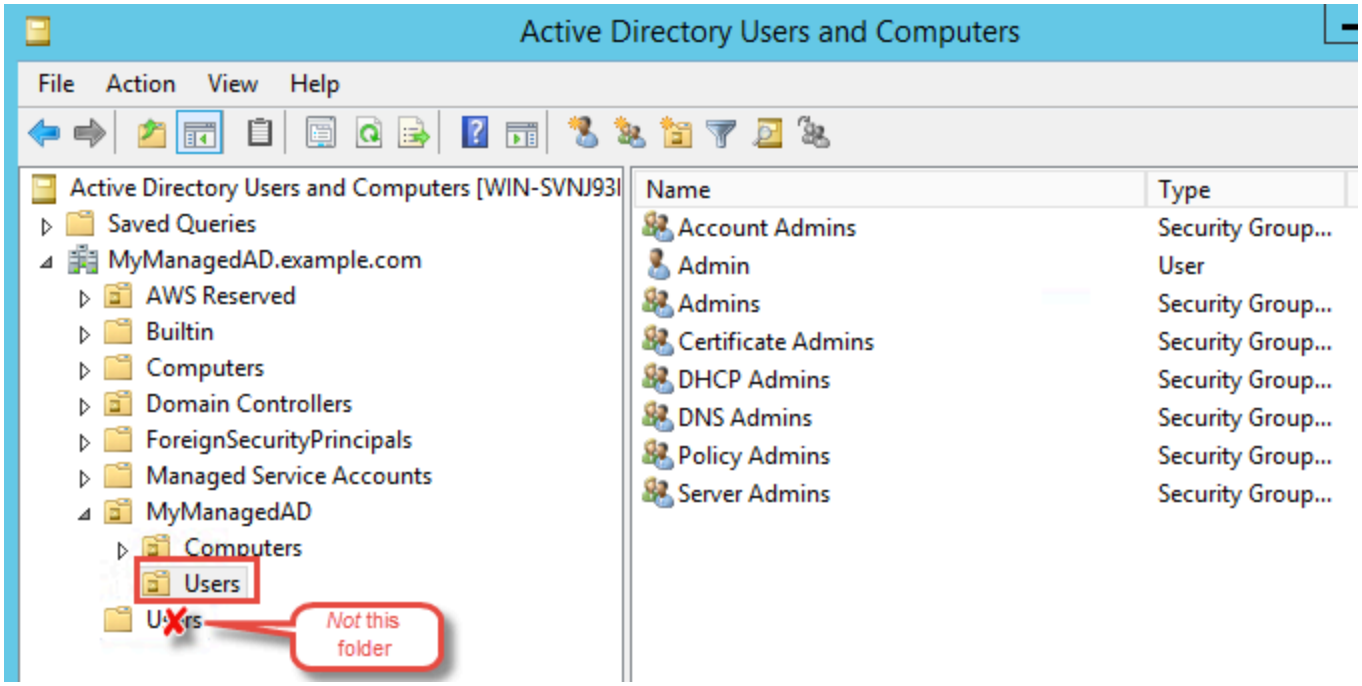


Assicurarsi che la preautenticazione di Kerberos sia abilitata

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 Autorizzazioni per l'account Administrator 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 Installare gli 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: creazione della relazione di trust con un altro dominio di Microsoft AD gestito da AWS

Fase 2: creazione della relazione di trust con un altro dominio di Microsoft AD gestito da AWS

Ora che il lavoro di preparazione è completato, le fasi finali servono a creare i trust tra i due domini di Microsoft AD gestito da AWS. In caso di problemi durante il processo di creazione del trust, consultare Motivo stato di creazione trust per ricevere assistenza.

Configurazione del trust nel primo dominio Microsoft AD gestito da AWS

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 sul primo dominio, è necessario creare un trust unidirezionale in ingresso sul secondo dominio di Microsoft AD gestito da AWS.

> **Note**
>
> Microsoft AD gestito da AWS supporta anche trust esterni. Tuttavia, ai fini di questo tutorial, verrà creato un trust tra foreste bidirezionale.

Per configurare l'attendibilità nel primo dominio Microsoft AD gestito da AWS

1. Aprire la console AWS Directory Service.
2. Nella pagina Directory, scegli il tuo primo ID Microsoft AD gestito da AWS.
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 di Microsoft AD gestito da AWS. Assicurati di ricordare questa password perché sarà necessaria durante la configurazione del trust per il secondo Microsoft AD gestito da AWS. Specificare la direzione. In questo caso scegli Bidirezionale.
6. Nel campo Server d'inoltro condizionale, inserisci l'indirizzo IP del secondo server DNS di Microsoft AD gestito da AWS.
7. (Facoltativo) Scegli Aggiungi un altro indirizzo IP e inserisci l'indirizzo IP del secondo server DNS di Microsoft AD gestito da AWS. È possibile specificare fino a un totale di quattro server DNS.
8. Scegliere Add (Aggiungi). A questo punto, il trust ha esito negativo, come previsto, finché non viene creato l'altro lato del trust.

Configurazione del trust nel secondo dominio di Microsoft AD gestito da AWS

Adesso, configura la relazione di trust tra foreste con la seconda directory Microsoft AD gestito da AWS. Poiché hai creato un trust tra foreste bidirezionale nel primo dominio di Microsoft AD gestito da AWS, crei anche un trust bidirezionale utilizzando questo dominio Microsoft AD gestito da AWS.

Per configurare il trust nel secondo dominio Microsoft AD gestito da AWS

1. Tornare alla console AWS Directory Service.
2. Nella pagina Directory, scegli il tuo secondo ID Microsoft AD gestito da AWS.
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 primo dominio di Microsoft AD gestito da AWS. 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 l'indirizzo IP del primo server DNS di Microsoft AD gestito da AWS. È possibile specificare fino a un totale di quattro server DNS.
8. Scegliere Add (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 disponi di una relazione di trust tra i tuoi due domini di Microsoft AD gestito da AWS. 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.

Connect 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 Windows 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 “Crea il tuo AWS Managed Microsoft AD”.
- Un'istanza del Windows server Amazon EC2 aggiunta al tuo Managed AWS Microsoft AD. Per ulteriori informazioni, consulta Unisciti senza problemi a un'istanza Windows.
- Un Windows server EC2 Active Directory Administration Tools installato per gestire il tuo AWS Managed Microsoft AD. Per ulteriori informazioni, consulta the section called “Installa gli strumenti di amministrazione di AD per AWS Managed Microsoft AD”.

Fase 1: Creare un utente di Active Directory dominio

Questo tutorial presuppone che tu abbia già installato un AWS Managed Microsoft AD e un'istanza Windows del server EC2. Active Directory Administration Tools Per ulteriori informazioni, consulta the section called “Installa gli strumenti di amministrazione di AD per AWS Managed Microsoft AD”.

1. Connect all'istanza in cui Active Directory Administration Tools sono stati installati.
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”.

Fase 2: Scarica Entra Connect Sync

- Scarica Entra Connect Sync dal Microsoftsito Web sull'istanza EC2 che è l'amministratore di Microsoft AD AWS gestito.

> **Warning**
>
> Non aprirlo o eseguirlo Entra Connect Sync a questo punto. I passaggi successivi forniranno le autorizzazioni necessarie per l'utente di dominio creato nel passaggio 1.

Passaggio 3: Esegui Windows PowerShell lo script

- Apri PowerShell come amministratore ed esegui lo script seguente. Durante l'esecuzione dello script, ti verrà chiesto di inserire il SAM AccountName per l'utente di dominio appena creato dal passaggio 1.

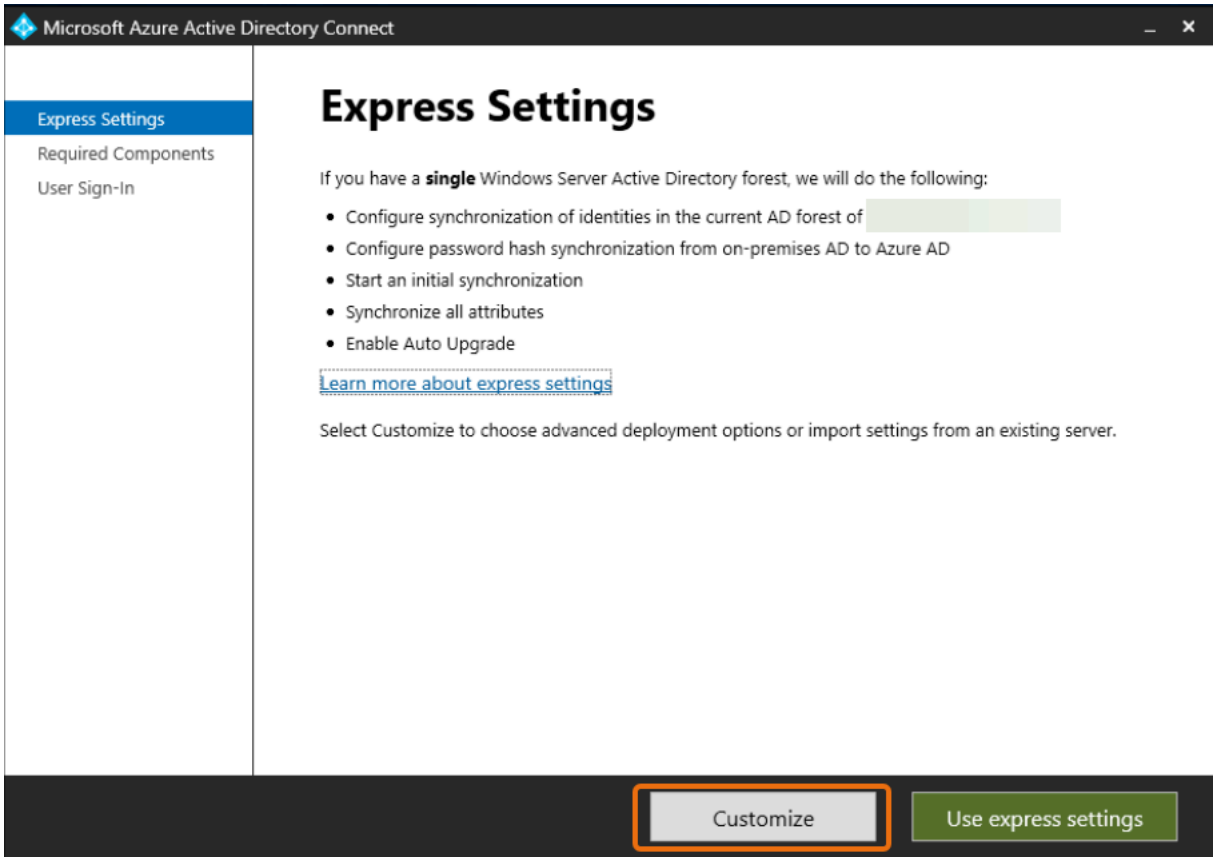
```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

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 : $_"
    }
    }
}
```

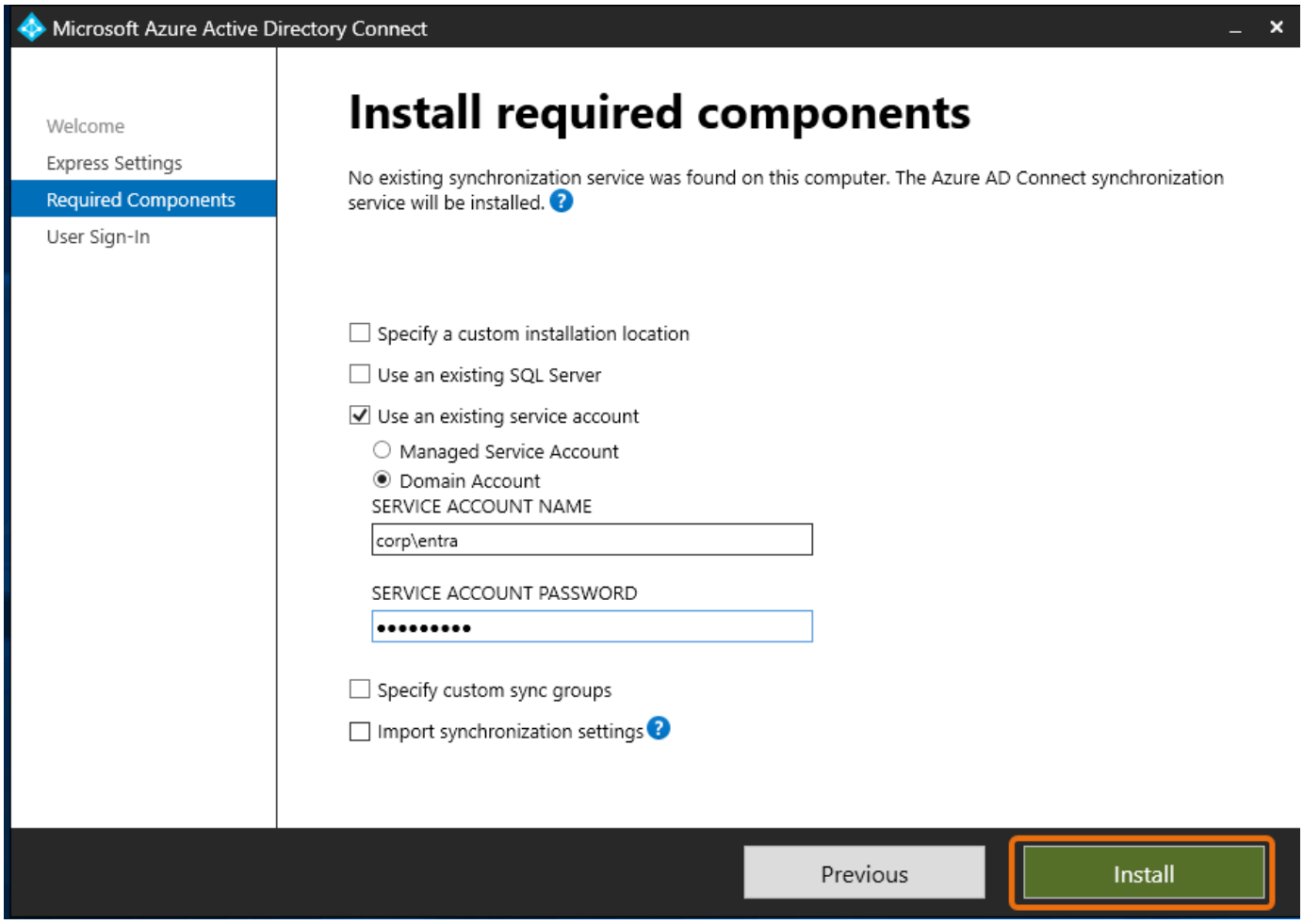
Fase 4: Installazione Entra Connect Sync

1. Una volta completato lo script, puoi eseguire il file di configurazione scaricato Microsoft Entra Connect (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 ti consente di accedere al tuo Active Directory con nome utente e password.

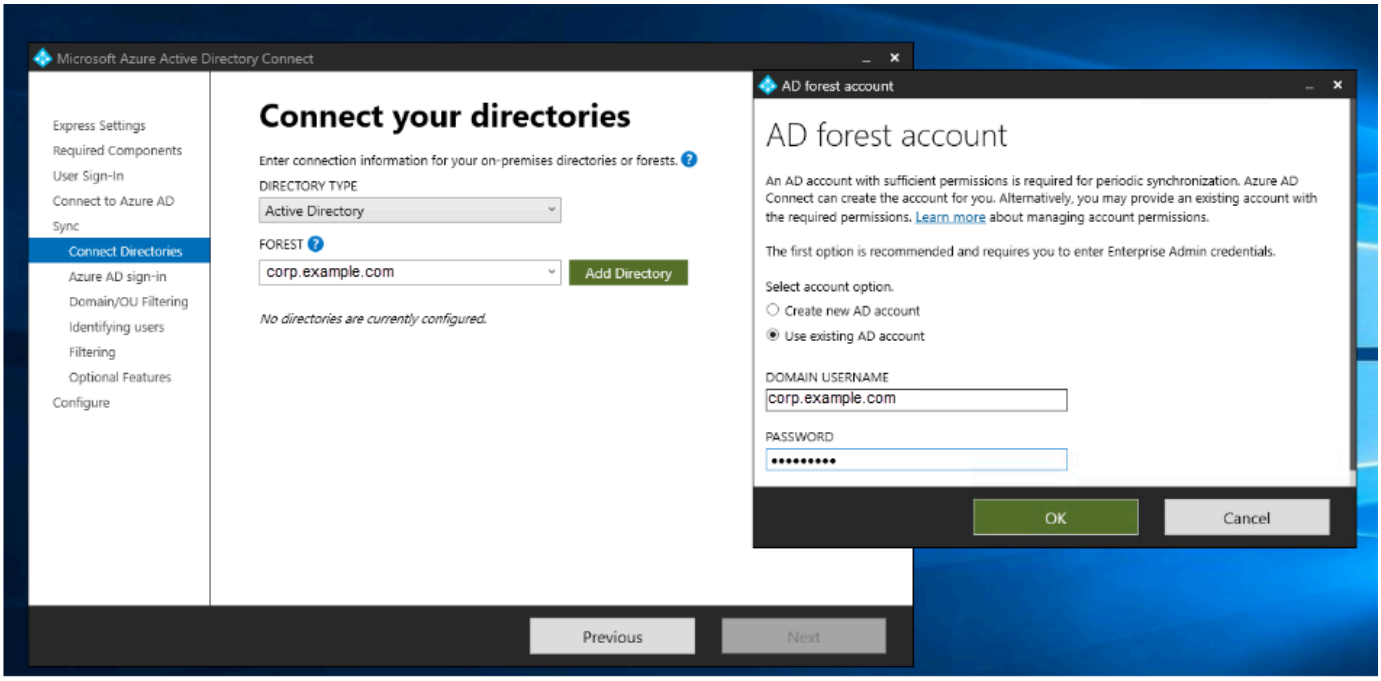
   b. Non configurare: consente di utilizzare l'accesso federato con Microsoft Entra (precedentemente noto come Azure Active Directory (AzureAD)) o. Office 365

   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 DirectoryDIRECTORY 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

Estensione dello schema

Microsoft AD gestito da AWS utilizza gli schemi per organizzare e applicare il modo in cui i dati della directory vengono archiviati. Il processo di aggiunta di definizioni allo schema viene definito "estensione dello schema". Le estensioni dello schema consentono di modificare lo schema della directory Microsoft AD gestito da AWS 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.

Argomenti

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

Quando estendere lo schema Microsoft AD gestito da AWS

Puoi estendere lo schema Microsoft AD gestito da AWS aggiungendo nuovi attributi e classi di oggetto. 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 tu debba trasferire applicazioni aziendali che dipendono da Microsoft AD gestito da AWS nel cloud AWS.

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 ID vengono definiti Identificatori oggetto AD (OID) e sono archiviati in Microsoft AD gestito da AWS.

Per iniziare, consulta Tutorial: estensione dello schema AWS Managed Microsoft AD.

Argomenti correlati

- Estensione dello schema
- Elementi dello schema

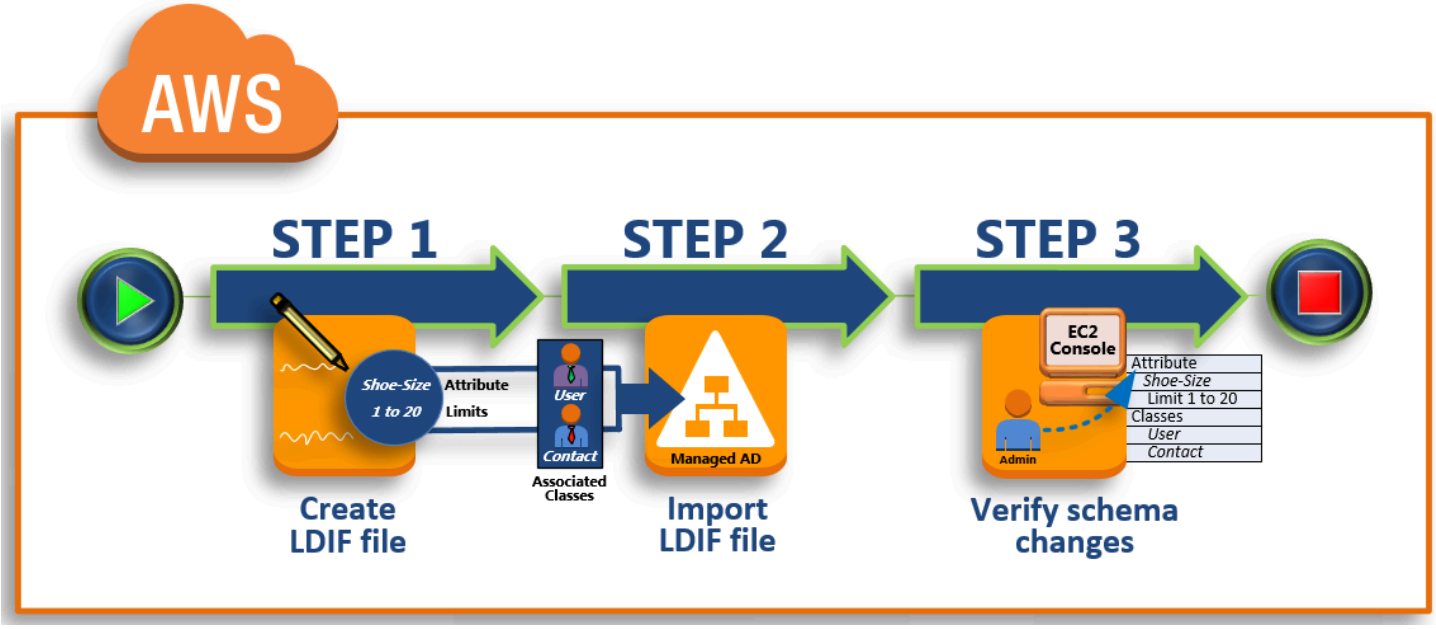
Tutorial: estensione dello schema AWS Managed Microsoft AD

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. AWS Le 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 Microsoft AD gestito da AWS.

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, come amministratore, utilizzi un'istanza EC2 per verificare che le nuove estensioni vengano visualizzate nello snap-in Active Directory Schema (Schema 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 Service Importa il file LDIF con le modifiche dello schema eseguendo l'`ldifde.exe`applicazione nella directory Managed AWS Microsoft AD. Pertanto, potrai trovarlo utile per comprendere la sintassi degli 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 ulteriori informazioni sugli elementi dello schema, ad esempio attributi, classi, ID oggetto 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 contenere anche il nome comune (CN) dell'oggetto Active Directory. La prima voce CN è l'attributo o il nome della classe. Successivamente, devi utilizzare `CN=Schema,CN=Configuration`. Questo CN assicura che tu possa estendere lo schema Active Directory. Come accennato in precedenza, non puoi aggiungere o modificare il contenuto degli oggetti Active Directory. Il formato generale per un DN è indicato di seguito.

  ```
  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 commetti un errore e non desideri eseguire il ripristino dal backup, puoi 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 le API dell'estensione dello schema, consulta la Documentazione di riferimento dell'API AWS Directory Service . 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, dopo aver creato una nuova classe o un nuovo attributo, Active Directory non ne consente la rimozione. 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 Replica multi regione, 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 applicare alcun aggiornamento dello schema nell'ambiente di produzione senza prima verificarlo con l'applicazione in un ambiente di test o sviluppo.

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. AWS Microsoft AD gestito isola uno dei controller di dominio e applica gli aggiornamenti nel file LDIF al controller di dominio isolato. Seleziona quindi uno dei controller di dominio come schema principale, rimuove il controller di dominio dalla replica delle directory e applica il file LDIF utilizzando. `Ldifde.exe`

4. La replica viene eseguita su tutti i DC. AWS Microsoft 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 e/o 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 (consulta Come avviare una nuova istanza EC2 tramite l'aggiunta ottimizzata del dominio).

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. Per 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 Windows PowerShell comando e imposta il nuovo attributo con il comando seguente. In questo esempio, aggiungeremo un nuovo valore EC2InstanceID all'attributo per un computer specifico.

   ```
   PS C:\> set-adcomputer -Identity computer name -add @{example-
   EC2InstanceID = 'EC2 instance ID'}
   ```
2. Puoi verificare se il valore EC2InstanceID è stato aggiunto all'oggetto computer, eseguendo il seguente comando:

   ```
   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

Gestisci la tua directory AWS Managed Microsoft AD

Questa sezione descrive come gestire le attività amministrative comuni per l'ambiente Microsoft AD AWS gestito.

Argomenti

Aggiunta di suffissi UPN alternativi

È possibile semplificare la gestione dei nomi di accesso di Active Directory (AD) e migliorare l'esperienza di accesso degli utenti aggiungendo suffissi di nomi utente principali (UPN) alternativi alla directory Microsoft AD gestito da AWS. 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 Active Directory.

Aggiunta di suffissi UPN alternativi

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Individua un'istanza Amazon EC2 aggiunta alla tua directory Microsoft AD gestito da AWS. 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.

Elimina il tuo AWS Managed Microsoft AD

Quando un AWS Managed Microsoft AD viene eliminato, 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.

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 Active Directory è installato il tuo. 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 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 AWS app e servizi, puoi vedere quali AWS applicazioni sono abilitate per la tua directory.

      - Disabilita AWS Management Console l'accesso. Per ulteriori informazioni, consulta Disabilita l'accesso alla AWS Management Console..
      - Per disabilitare Amazon WorkSpaces, devi annullare la registrazione del servizio dalla directory nella WorkSpaces console. Per ulteriori informazioni, consulta Annullamento della registrazione da una directory nella Amazon WorkSpaces Administration Guide.
      - Per disabilitare Amazon WorkDocs, devi eliminare il WorkDocs sito Amazon nella WorkDocs console Amazon. 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 per Windows File Server, devi rimuovere il file system Amazon FSx dal dominio. Per ulteriori informazioni, consulta Lavorare con Active Directory FSx for Windows File Server nella Guida per l'utente di Amazon FSx for Windows File Server.

- 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 Active DirectoryAuthentication nella AWS Client VPN Administrator Guide.
- Per disabilitare Amazon Connect, è necessario eliminare l'istanza di Amazon Connect. Per ulteriori informazioni, consulta Eliminazione di un'istanza Amazon Connect nella Guida all'amministrazione di Amazon Connect.
- Per disattivare Amazon QuickSight, devi annullare l'iscrizione ad Amazon QuickSight. Per ulteriori informazioni, consulta la sezione Chiusura Amazon QuickSight dell'account nella Amazon QuickSight User Guide.

> **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.

Rinomina il sito della directory

Puoi modificare il nome del sito predefinito della directory Microsoft AD gestito da AWS in modo che corrisponda ai nomi dei siti esistenti di Microsoft Active Directory (AD). In questo modo, Microsoft AD gestito da AWS trova e autentica più velocemente gli utenti AD esistenti nella directory on-premise. Il risultato è un'esperienza migliore quando gli utenti si collegano a risorse AWS quali le istanze Amazon EC2 e Amazon RDS per SQL Server che sono state collegate alla directory Microsoft AD gestito da AWS.

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 Active Directory.

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 sito Microsoft AD gestito da AWS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Individua un'istanza Amazon EC2 aggiunta alla tua directory Microsoft AD gestito da AWS. 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).

Snapshot o ripristino della directory

AWS Directory Service offre 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. Sono disponibili al massimo cinque istantanee manuali per ogni AWS Managed Microsoft AD Active Directory. Se hai già raggiunto questo limite, devi eliminare uno degli snapshot manuali esistenti prima di crearne un altro. Non è possibile acquisire snapshot del connettore AD.

> **Note**
>
> Snapshot è una funzionalità globale di AWS Managed Microsoft AD. Se utilizzi Replica multi regione, 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 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 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).

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 AWS Support 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 che tu capisca che tutti i DC e i server DNS associati con la directory saranno offline fino a quando l'operazione di ripristino non sia stata completata.

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 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).

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

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 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).

Aggiorna il tuo AWS Managed Microsoft AD

Puoi aggiornare la tua edizione Standard AWS Managed Microsoft AD Active Directory all'edizione Enterprise contattando AWS Support. Per ulteriori informazioni, consulta Creazione di casi di supporto e gestione dei casi nella Guida AWS Support per l'utente.

> **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)
> - Africa (Città del Capo)
> - Asia Pacific (Hong Kong)
> - Asia Pacifico (Mumbai)
> - Asia Pacific (Hyderabad)
> - Asia Pacifico (Osaka-Locale)
> - Asia Pacific (Seul)
> - Asia Pacifico (Singapore)
> - Asia Pacifico (Sydney)
> - Asia Pacifico (Giacarta)
> - Asia Pacifico (Melbourne)
> - Asia Pacifico (Tokyo)
> - Canada (Centrale)
> - Canada occidentale (Calgary)
> - Cina (Pechino)
> - China (Ningxia)
> - Europa (Francoforte)
> - Europa (Zurigo)
> - Europa (Irlanda)

- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europa (Milano)
- Europa (Spagna)
- Israele (Tel Aviv)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- 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 AWS Directory Service.
- Una volta aggiornato, Active Directory non può essere ripristinato alla versione precedente.
- Le istantanee precedenti non possono essere utilizzate per ripristinare una copia Active Directory dopo l'aggiornamento.
- Gli upgrade avvengono alla data e all'ora pianificate concordate con. AWS Support 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.
- Se le applicazioni utilizzano i nomi host o gli indirizzi IP dei controller di dominio anziché il nome di dominio di Active Directory, tali applicazioni dovranno essere aggiornate.
- Se si utilizza LDAPS (Lightweight Directory Access Protocol over SSL), i controller di dominio avranno bisogno di nuovi certificati.

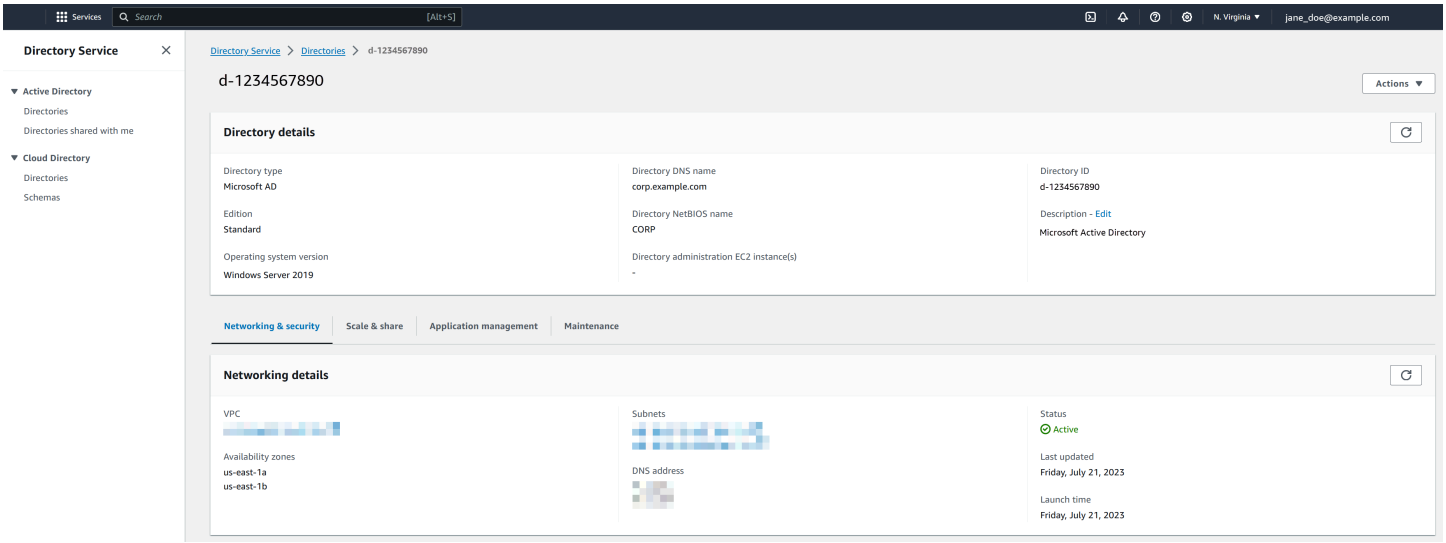
Visualizzazione delle informazioni sulla directory

Puoi visualizzare informazioni dettagliate su una directory.

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione della AWS Directory Service console, sotto Active Directory, seleziona Directory.
2. Fai clic sul link dell'ID directory della 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.



Concessione dell'accesso alle risorse AWS a utenti e gruppi

AWS Directory Service offre la possibilità di fornire agli utenti e ai gruppi della directory l'accesso a AWS servizi e risorse, come l'accesso alla console Amazon EC2. Analogamente alla concessione agli utenti IAM dell'accesso alla gestione delle directory come descritto inPolicy basate su identità (policy IAM), affinché gli utenti della directory abbiano accesso ad altre AWS risorse, come Amazon EC2, è necessario 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, consulta. AWS Management ConsoleAbilitazione dell'accesso a AWS Management Console con le credenziali AD

Argomenti

- Creazione di un nuovo ruolo
- Modifica della relazione di attendibilità per un ruolo esistente
- Assegnazione di utenti o gruppi a un ruolo esistente
- Visualizzazione di utenti e gruppi assegnati a un ruolo
- Rimozione di un utente o di un gruppo da un ruolo
- Utilizzo delle policy gestite di AWS con AWS Directory Service

Creazione di un nuovo ruolo

Se devi creare un nuovo ruolo IAM da utilizzare con AWS Directory 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 AWS Directory Service console. Per ulteriori informazioni, consulta Modifica della relazione di attendibilità per un ruolo 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 (AWS Management Console) 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, AmazonEC2 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 AWS Management Console

L'elenco di controllo seguente fornisce un esempio di attività da completare per creare un nuovo ruolo che garantirà a specifici utenti della directory l'accesso alla console Amazon EC2.

1. Creare un ruolo con la console IAM utilizzando la procedura descritta sopra. Quando viene richiesta una politica, scegli AmazonEC2. FullAccess
2. Utilizzare le istruzioni riportate nelle fasi Modifica della relazione di attendibilità per un ruolo 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 AWS Management Console nel passaggio successivo.
3. Segui le istruzioni fornite nelle fasi Abilitazione dell'accesso a AWS Management Console con le credenziali AD per configurare l'accesso generale alla AWS Management Console.
4. Segui le istruzioni fornite nelle fasi Assegnazione di utenti o gruppi a un ruolo esistente per aggiungere al nuovo ruolo gli utenti che necessitano di accesso completo alle risorse EC2.

Modifica della relazione di attendibilità per un ruolo esistente

Puoi assegnare i ruoli IAM esistenti ai tuoi AWS Directory Service utenti e gruppi. Per fare ciò, tuttavia, il ruolo deve avere un rapporto di fiducia con AWS Directory Service. Quando si utilizza AWS Directory Service per creare un ruolo utilizzando la procedura inCreazione di un nuovo ruolo, questa relazione di fiducia viene impostata automaticamente. È necessario solo stabilire questa relazione di attendibilità per i ruoli IAM che non sono stati creati da AWS Directory Service.

Stabilire una relazione di fiducia per un ruolo esistente AWS 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.

```
{
  "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 esistente

Puoi assegnare un ruolo IAM esistente a un AWS Directory Service utente o a un gruppo. Per fare ciò, assicurati di aver completato quanto segue.

Prerequisiti

- Crea un Microsoft AD AWS gestito.
- Crea un utente o crea un gruppo.
- Crea un ruolo con cui instaurare un rapporto di fiducia AWS Directory Service. È possibile modificare la relazione di fiducia per un ruolo esistente.

> **Note**
>
> L'accesso per gli utenti nei gruppi nidificati all'interno della directory non è supportato. I membri del gruppo padre hanno accesso alla console, diversamente dai membri dei gruppi figli.

Assegnazione di utenti o gruppi 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:
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
   - 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 AWS Management Consolesezione, 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 AWS Management Console. 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 assegnati a un ruolo, esegui la procedura seguente.

Prerequisiti

- Assegna i tuoi utenti o gruppi a un ruolo esistente.

Visualizzazione di utenti e gruppi assegnati a un ruolo

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:
   - 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.
   - Se non hai alcuna regione visualizzata in Replica multi regione, scegli la scheda Gestione dell'applicazione.
4. Nella sezione Delega dell'accesso alla console, scegli il ruolo IAM da visualizzare.
5. Nella pagina Ruolo selezionato, in Gestione di utenti e gruppi per questo ruolo, sono presenti gli utenti e i gruppi assegnati al ruolo.

Rimozione di un utente o di un gruppo da un ruolo

Per rimuovere un utente o un gruppo da un ruolo, esegui la procedura seguente.

Rimozione di un utente o di un gruppo da un ruolo

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 rimuovere le assegnazioni, 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 AWS Management Console, scegli il ruolo da visualizzare.
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.

Utilizzo delle policy gestite di AWS con AWS Directory Service

AWS Directory Service fornisce le seguenti policy gestite in AWS per offrire ai tuoi utenti e ai tuoi gruppi l'accesso ai servizi e alle risorse di AWS, come la console Amazon EC2. È necessario accedere alla AWS Management Console prima di poter visualizzare queste policy.

- Accesso in sola lettura
- Accesso utenti avanzati
- Accesso completo a AWS Directory Service
- Accesso in sola lettura a AWS Directory Service
- Accesso completo alla directory del cloud Amazon
- Accesso in sola lettura alla directory del cloud Amazon
- Accesso completo ad Amazon EC2
- Accesso in sola lettura ad Amazon EC2
- 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
- Accesso completo a AWS CloudTrail
- Accesso in sola lettura a AWS CloudTrail
- Accesso completo ad Amazon CloudWatch
- Accesso in sola lettura ad Amazon CloudWatch
- Accesso completo ai File di log Amazon CloudWatch
- Accesso in sola lettura ai File di log Amazon CloudWatch

Per ulteriori informazioni su come creare le policy, consulta Esempi di policy per amministrare le risorse AWS nella Guida per l'utente di IAM.

Consentire l'accesso ad AWS applicazioni e servizi

Gli utenti possono autorizzare AWS Managed Microsoft AD a fornire ad AWS applicazioni e servizi, come Amazon WorkSpaces, l'accesso al tuoActive 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, consulta la Guida all'amministrazione di Amazon Chime.
Amazon Connect	Per ulteriori informazioni, consulta la Guida all'amministrazione di Amazon Connect.
Amazon FSx per Windows File Server	Per ulteriori informazioni, consulta Using Amazon FSx with AWS Directory Service per Microsoft Active Directory.
Amazon QuickSight	Per ulteriori informazioni, consulta la Amazon QuickSight User Guide.
Amazon Relational Database Service	Per ulteriori informazioni, consultare la Guida per l'utente di Amazon RDS.
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.

AWS applicazione/servizio	Ulteriori informazioni…
AWS Client VPN	Per ulteriori informazioni, consulta la AWS Client VPN Guida per l'utente.
AWS IAM Identity Center	Per ulteriori informazioni, consulta la AWS IAM Identity Center Guida per l'utente.
AWS License Manager	Per ulteriori informazioni, consultare la Guida per l'utente di License Manager.
AWS Management Console	Per ulteriori informazioni, consulta Abilitazione dell'accesso a AWS Management Console con le credenziali AD.
AWS Private Certificate Authority	Per ulteriori informazioni, consulta AWS Private CA Connector for Active Directory.
AWS Transfer Family	Per ulteriori informazioni, consulta la AWS Transfer Family Guida per l'utente.

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 collegamenti AWS alle applicazioni e ai servizi sopra descritti nella AWS 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 AWS Directory Service di AWS applicazioni e servizi, vedere. Autorizzazione per l'utilizzo di AWS applicazioni e servizi AWS Directory Service

Argomenti

Creazione di un URL di accesso

Un URL di accesso viene utilizzato con applicazioni e servizi AWS, come Amazon WorkDocs per raggiungere una pagina di accesso che è associata con la 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.

> **Note**
>
> L'URL di accesso può essere configurato solo dalla regione primaria quando si utilizzano directory multi regione.

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 Amazon WorkDocs.

Autenticazione unica

AWS Directory Service offre la possibilità di consentire agli utenti di accedere ad Amazon WorkDocs da un computer collegato 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 AWS 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 Amazon 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 Amazon. 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.

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 desideri disabilitare il Single Sign-On con Amazon WorkDocs, scegli Disabilita, quindi nella finestra di dialogo Disabilita il Single Sign-On per questa directory, scegli 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 l'accesso 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:

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      Path

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      \ZoneMap\Domains\awsapps.com\<alias>
      ```

Il valore di *<alias>* deriva dall'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:

Action

```
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 permettere al browser Firefox di Mozilla di supportare l'accesso single sign-on, aggiungi l'URL di accesso (ad esempio, https://*<alias>*.awsapps.com) all'elenco dei siti approvati per l'accesso 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, vai a https://support.mozilla.org/en-US/questions/939037.

Abilitazione dell'accesso a AWS Management Console con le credenziali AD

AWS Directory Service consente di concedere l'accesso alla AWS Management Console ai membri della directory. Per impostazione predefinita, i membri della directory non hanno accesso a nessuna risorsa AWS. Puoi assegnare ruoli IAM ai membri della directory per consentirgli l'accesso ai vari servizi e risorse AWS. 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. Per ulteriori informazioni su come creare un URL di accesso, consulta Creazione di un URL di accesso.

Per ulteriori informazioni su come creare e assegnare ruoli IAM ai membri della directory, consulta Concessione dell'accesso alle risorse AWS a utenti e gruppi.

Argomenti

- Abilitazione dell'accesso alla AWS Management Console
- Disabilita l'accesso alla AWS Management Console.
- Impostazione della durata della sessione di accesso

Articolo correlato del Blog sulla sicurezza AWS

- Come accedere alla AWS Management Console tramite Microsoft AD gestito da AWS e le credenziali on-premise

> **Note**
>
> L'accesso alla AWS Management Console è una funzionalità regionale di Microsoft AD gestito da AWS. Se utilizzi Replica multi regione, le seguenti procedure devono essere applicate separatamente in ciascuna regione. Per ulteriori informazioni, consulta Funzionalità globali e regionali.

Abilitazione dell'accesso alla AWS Management Console

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 multi regione sono visualizzate più Regioni, seleziona quella in cui vuoi abilitare l'accesso alla AWS Management Console, 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 AWS Management Console, scegli Abilita. Ora l'accesso alla console è abilitato per la tua directory.

   Prima che gli utenti possano accedere alla console con il tuo URL di accesso, devi aggiungere gli utenti al ruolo. Per ulteriori informazioni sull'assegnazione di ruoli IAM agli utenti, consulta Assegnazione di utenti o gruppi a un ruolo 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 della directory è example-corp.awsapps.com, l'URL per accedere alla console sarà https://example-corp.awsapps.com/console/.

Disabilita l'accesso alla AWS Management Console.

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 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'accesso alla AWS Management Console, 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 AWS Management Console, 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 eseguito il logout. 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 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 risorse AWS, seleziona 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).

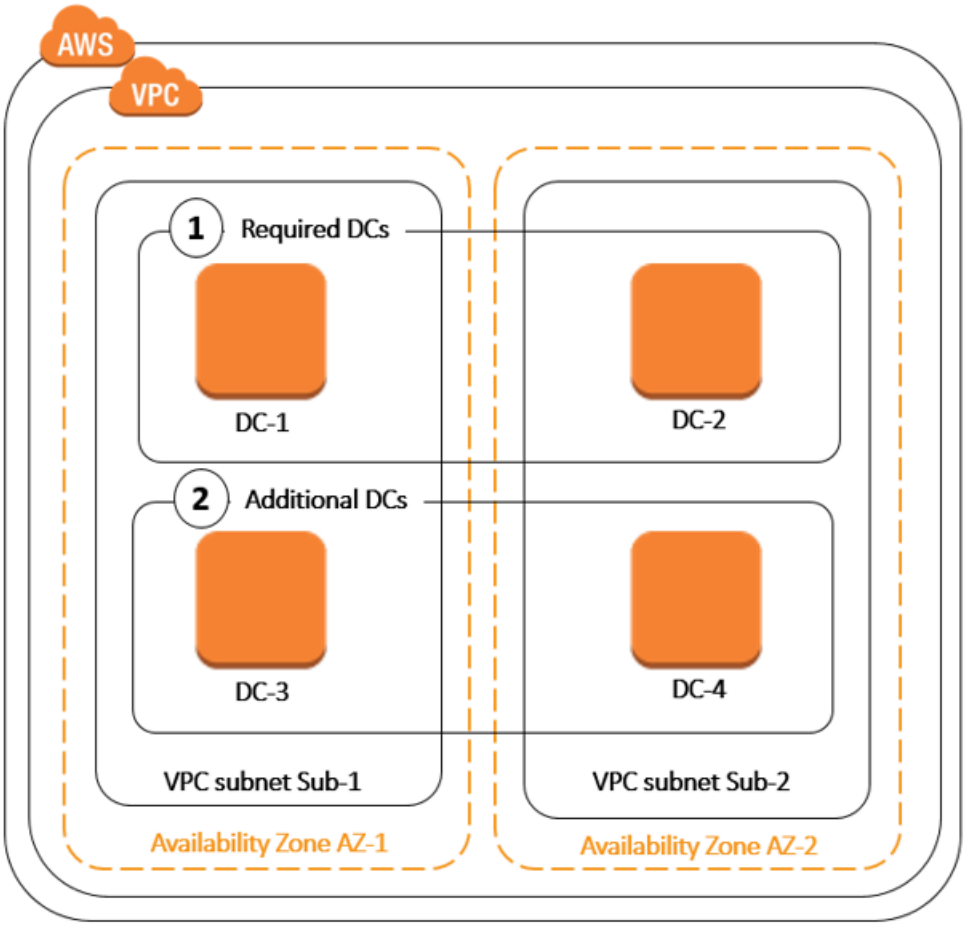
Distribuzione di controller di dominio aggiuntivi

La distribuzione di controller di dominio aggiuntivi aumenta la ridondanza, che comporta maggiori resilienza e disponibilità. 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 AWS Directory Service console semplicemente specificando il numero totale di controller di dominio desiderati. AWS Microsoft 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 AWS Directory Service console fa riferimento a questi controller di dominio predefiniti come obbligatori. AWS Microsoft 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. È più semplice migrare ed eseguire carichi di lavoro mission critical integrati con Active Directory nel Cloud AWS senza dover implementare e mantenere la tua infrastruttura Active Directory. Puoi anche distribuire o rimuovere controller di dominio aggiuntivi per Managed AWS Microsoft AD utilizzando l'UpdateNumberOfDomainControllersAPI.

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

Aggiunta o eliminazione di controller di dominio aggiuntivi

Prima di aggiungere o rimuovere controller di dominio aggiuntivi, 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 LDAP o LDAPS sicuri.

Utilizza la procedura seguente per implementare o rimuovere controller di dominio aggiuntivi nella tua directory Microsoft AD gestito da AWS .

Aggiunta o eliminazione di controller di dominio aggiuntivi

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.

Articolo correlato del blog sulla sicurezza AWS

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

Migrazione degli utenti da Active Directory a Microsoft AD gestito da AWS

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 e le password crittografate di Active Directory per gli utenti.

Per istruzioni dettagliate, consulta Come eseguire la migrazione del dominio on-premise in Microsoft AD gestito da AWS utilizzando ADMT nel Blog sulla sicurezza AWS.

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	20
Snapshot manuali *	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 ***	5
Domini condivisi per Microsoft AD Enterprise ***	125
Numero massimo di certificati emessi da una CA registrati per directory	5

Risorsa	Quota predefinita
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 Programmazione delle applicazioni.

Per le quote di archiviazione e degli oggetti, consulta la Tabella di confronto nella pagina Prezzi del Servizio di directory AWS.

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: per istruzioni dettagliate, consulta Connessione ad Active Directory.
- Amazon Connect: per ulteriori informazioni, consulta Come funziona Amazon Connect.
- Amazon EC2: per ulteriori informazioni, consulta Amazon Unisci un'istanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory.
- Amazon QuickSight : per ulteriori informazioni, consulta Gestione degli account utente in Amazon QuickSight Enterprise Edition.
- Amazon RDS per MySQL: per ulteriori informazioni, consulta Utilizzo dell'autenticazione Kerberos per MySQL.
- Amazon RDS per Oracle: per ulteriori informazioni, consulta Utilizzo dell'autenticazione Kerberos con Amazon RDS per Oracle.
- Amazon RDS per PostgreSQL: per ulteriori informazioni, consulta Utilizzo dell'autenticazione Kerberos con Amazon RDS per PostgreSQL.
- Amazon RDS per SQL Server: per ulteriori informazioni, consulta Utilizzo dell'autenticazione di Windows con un'istanza DB di Amazon RDS per SQL Server.
- Amazon WorkDocs - Per istruzioni dettagliate, consulta Connessione alla directory locale con AWS Managed Microsoft AD.
- Amazon WorkMail : per istruzioni dettagliate, consulta Integrare Amazon WorkMail con una directory esistente (configurazione standard).
- AWS Client VPN - Per istruzioni dettagliate, consulta Autenticazione e autorizzazione del client.
- AWS IAM Identity Center - Per istruzioni dettagliate, consulta Connect IAM Identity Center a un Active Directory locale.
- AWS License Manager - Per ulteriori informazioni, consulta Abbonamenti basati sugli utenti in. AWS License Manager
- AWS Management Console — Per ulteriori informazioni, vedere. Abilitazione dell'accesso a AWS Management Console con le credenziali AD
- FSx per Windows File Server: per ulteriori informazioni, consulta Cos'è FSx per Windows File Server?
- WorkSpaces - Per istruzioni dettagliate, consulta Avvio di un programma WorkSpace con 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 Active Directory

- Accesso ai Active Directory contenitori 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 sulla gestione dell'unità organizzativa, consulta Come amministrare AWS Managed Microsoft AD.
- Modifiche allo schema durante il flusso di lavoro di installazione: alcune Active Directory applicazioni richiedono modifiche allo schema predefinito di Active Directory e potrebbero tentare di installare tali modifiche come parte del 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 AWS 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. AWS 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

AWS Tutorial gestiti per laboratori di test Microsoft AD

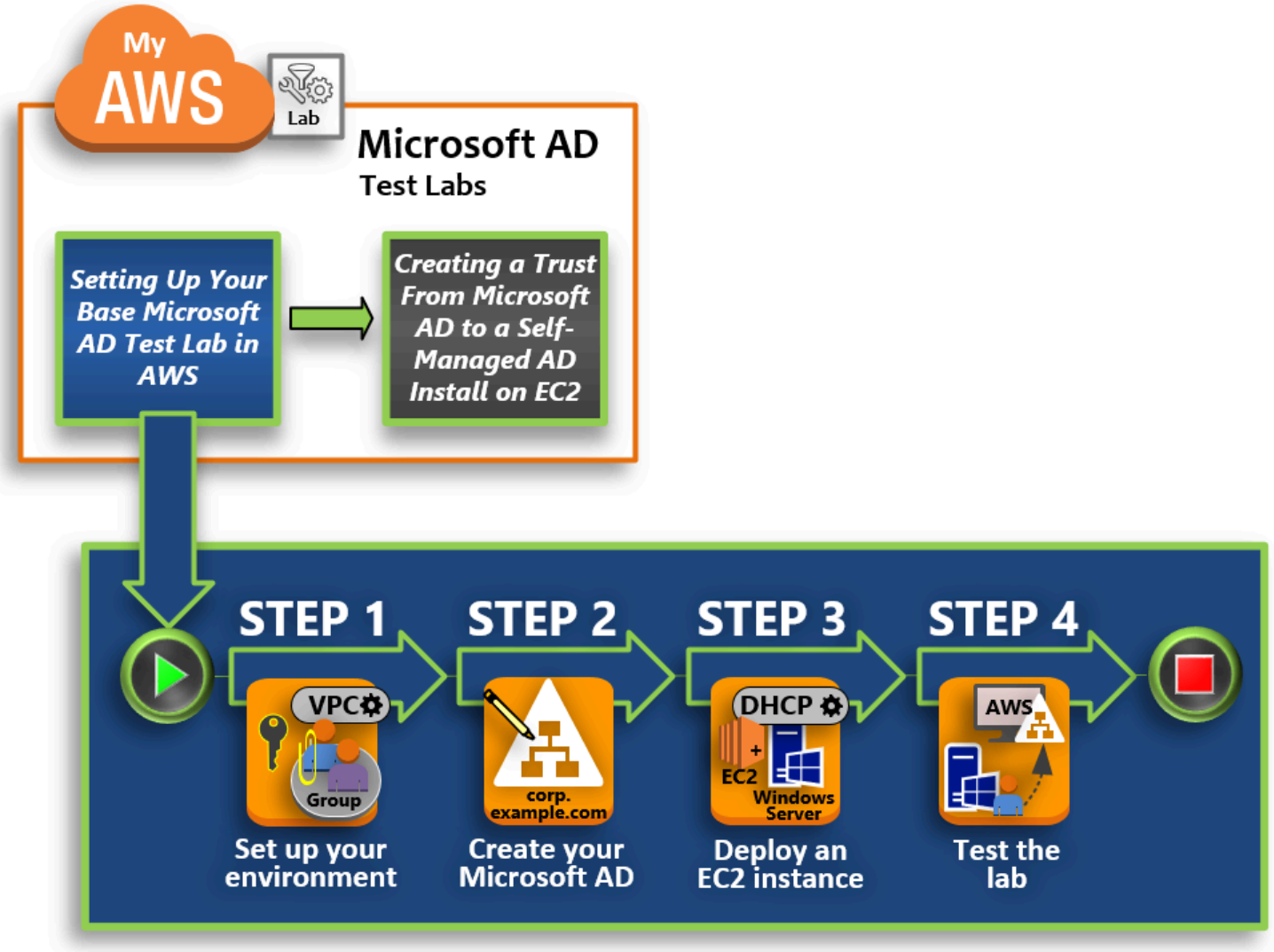
Questa sezione fornisce una serie di tutorial guidati per aiutarti a creare un ambiente di test lab in AWS cui sperimentare con Managed AWS Microsoft AD.

Argomenti

Tutorial: configurazione del laboratorio di test Microsoft AD AWS gestito di base in AWS

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 istanza Amazon EC2 con Windows Server 2019. Ti insegna quindi a utilizzare gli strumenti di amministrazione tipici di Active Directory per gestire l'ambiente Microsoft AD AWS gestito dalla tua istanza 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 tua istanza EC2.

[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'istanza Amazon EC2 per gestire la tua AWS Managed Microsoft AD Active Directory]

Di seguito, ti guiderà attraverso le varie attività successive alla distribuzione necessarie per i computer dei client per connetterti al tuo nuovo dominio e configurare un nuovo sistema di Windows Server in EC2.

[Fase 4: verifica che il laboratorio di sviluppo di base sia operativo]

Infine, in qualità di amministratore, è necessario verificare se è possibile accedere e collegarsi a Microsoft AD gestito da AWS dal tuo sistema di Windows Server in 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 (AWS Management Console)].
- AWS Command Line Interface (opzionale): [scaricalo e installalo AWS CLI su Windows]. Una volta installato, apri il prompt dei comandi o la Windows 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:
  - AWS ID della chiave di accesso [Nessuno]: `AKIAIOSFODNN7EXAMPLE`
  - AWS chiave 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 (facoltativo): scarica e installa la versione più recente degli AWS Tools for Windows PowerShell da 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 coppia di chiavi Amazon EC2 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 chiavi Amazon EC2, consulta Creare coppie di chiavi.

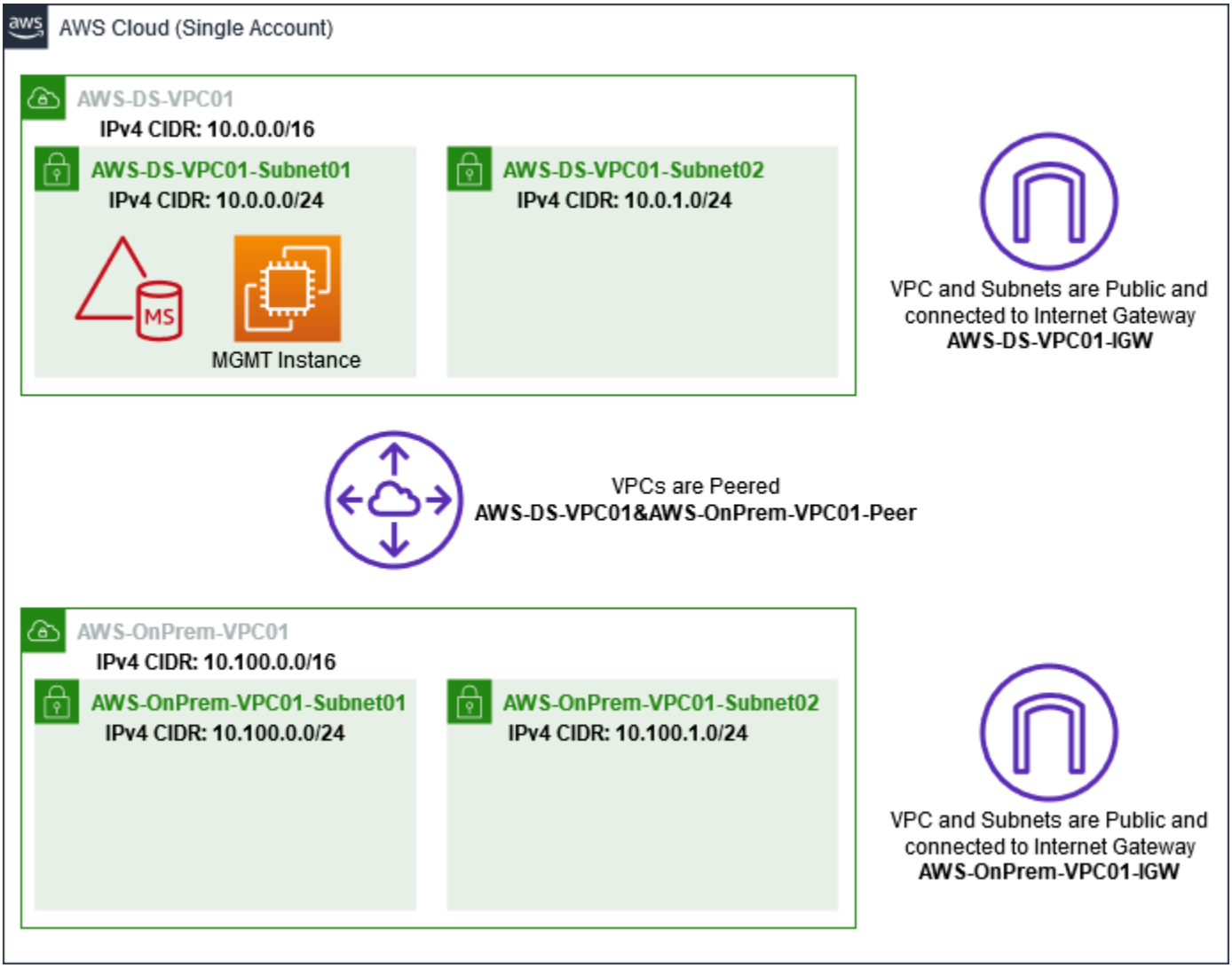
Per creare una coppia di chiavi

1. Accedi AWS Management Console e apri la console Amazon EC2 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 VPC

Come illustrato nella figura seguente, al termine di questo processo in più passaggi verranno creati e configurati due VPC pubblici, due subnet pubbliche per VPC, un gateway Internet per VPC e una connessione peering VPC tra i VPC. Abbiamo scelto di utilizzare VPC pubblici per semplicità e costi. Per i carichi di lavoro di produzione, si consiglia di utilizzare VPC privati. 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: Creare due VPC

In questo passaggio, è necessario creare due VPC nello stesso account utilizzando i parametri specificati nella tabella seguente. AWS Microsoft AD gestito supporta l'uso di account separati con Condividi la directory 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 Blocco CIDR IPv4: 10.0.0.0/16 IPv6 CIDR block (Blocco CIDR IPv6): No IPv6 CIDR Block (Nessun blocco CIDR IPv6) Tenancy: predefinito	Targhetta con nome: - -VPC01 AWS OnPrem Blocco CIDR IPv4: 10.100.0.0/16 IPv6 CIDR block (Blocco CIDR IPv6): No IPv6 CIDR Block (Nessun blocco CIDR IPv6) Tenancy: predefinito

Per istruzioni dettagliate, consulta Creazione di un VPC.

Passaggio 2: Creare due sottoreti per VPC

Dopo aver creato i VPC, sarà 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 AWS Prerequisiti Microsoft AD gestiti.

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 Blocco CIDR IPv4: 10.0.0.0/24	Nomenclatura: - -VPC01-subnet01 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem Zona di disponibilità predefinita: us-west-2a Blocco CIDR IPv4: 10.100.0.0/24
Nome tag: -DS-VPC01-subnet02 AWS VPC: vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS Zona di disponibilità: us-west-2b Blocco CIDR IPv4: 10.0.1.0/24	Nomenclatura: - -VPC01-subnet02 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx - AWS-VPC01 OnPrem Zona di disponibilità: us-west-2b

Informazioni sulla sottorete AWS-DS-VPC01:	AWS- Informazioni sulla sottorete OnPrem - VPC01
	Blocco CIDR IPv4: 10.100.1.0/24

Per istruzioni dettagliate, consulta Creazione di una sottorete nel VPC.

Passaggio 3: Creare e collegare un Internet Gateway ai VPC

Dal momento che stiamo utilizzando VPC pubblici sarà necessario creare e collegare un gateway Internet ai VPC utilizzando i parametri specificati nella tabella seguente. Ciò consentirà di connettersi e gestire le istanze EC2.

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 sono già stati creati due VPC in precedenza, sarà necessario collegarli in rete utilizzando il peering VPC utilizzando i parametri specificati nella tabella seguente. Sebbene esistano molti modi per connettere i tuoi VPC, questo tutorial utilizzerà il peering VPC. AWS Managed Microsoft AD supporta molte soluzioni per connettere i tuoi VPC, alcune di queste includono peering VPC, Transit Gateway e VPN.

Denominazione della connessione peering: -DS-VPC01& - -VPC01-Peer AWSAWS 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: Aggiungere due route alla tabella di route principale di ciascun VPC

Affinché i gateway Internet e la connessione peering VPC creati nei passaggi precedenti siano funzionali, è necessario aggiornare la tabella di route principale di entrambi i VPC 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 istanze Amazon EC2

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, sarà necessario creare 2 gruppi di

sicurezza (uno per ogni VPC) che verranno utilizzati per gestire il traffico all'interno del VPC per le istanze EC2, 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 di sicurezza Amazon EC2 per le 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

Type	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

Type	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

Type	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

Type	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

Type	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 AWS Management Console 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 (AWS Management Console)

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 **`AWS DS 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 (Windows PowerShell) (opzionale)

1. Aprire Windows PowerShell.
2. Digita il seguente comando. Assicuratevi di utilizzare i valori forniti nel passaggio 4 della AWS Management Console procedura precedente.

```
New-DSMicrosoftAD -Name corp.example.com –ShortName corp –Password P@ssw0rd
 –Description “AWS DS 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. Apri il AWS CLI.
2. Digita il seguente comando. Accertarsi di utilizzare i valori forniti nel passaggio 4 della AWS Management Console procedura precedente.

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

Fase 3: Implementa un'istanza Amazon EC2 per gestire la tua AWS Managed Microsoft AD Active Directory

Per questo laboratorio, utilizziamo istanze Amazon EC2 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 AWS Direct Connect o un collegamento. Non è necessario che l'istanza abbia un indirizzo IP pubblico.

In questa sezione, procedi gradualmente nelle varie attività successive alla distribuzione, necessarie per i computer client per connettere il tuo dominio usando il Windows Server sulla tua 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 le istanze EC2 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 alla 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 **`AWS DS 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 AWS Directory Service Directory, quindi scegli l'ID di directory applicabile. Nella pagina Dettagli, identifica e utilizza gli IP visualizzati in Indirizzo DNS.
     > In alternativa, per trovare questi indirizzi, vai alla pagina Directory del AWS Directory Service e scegli l'ID directory applicabile. Quindi, scegli Dimensiona e condividi. In Controller di dominio, identifica e utilizza gli IP visualizzati in 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. Annota l'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 pannello di navigazione, scegli Your VPCs (I tuoi VPC).
7. Nell'elenco di VPC, seleziona AWS DS VPC, scegli Operazioni e 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 Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo AWS Managed Microsoft AD Active Directory.

Configurazione di EC2 per aggiungere le 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. Sotto l'opzione Choose the service that will use this role (Scegli il servizio che utilizzerà questo ruolo) scegli EC2, quindi Next: Permissions (Successivo: Autorizzazioni).
5. Nella pagina Attached permissions policy (Policy autorizzazioni collegate), eseguire quanto segue:

   - Seleziona la casella accanto alla politica gestita di AmazonSSM ManagedInstanceCore. Questa policy fornisce le autorizzazioni minime necessarie per utilizzare il servizio Systems Manager.
   - Seleziona la casella accanto alla politica gestita da AmazonSSM DirectoryServiceAccess. La policy fornisce le autorizzazioni per collegare le istanze a una Active Directory gestita da AWS 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 esempio EC2. DomainJoin

9. (Facoltativo) Per Role Description (Descrizione ruolo), immetti una descrizione.
10. Scegliere Create role (Crea ruolo). Il sistema visualizza di nuovo la pagina Roles (Ruoli).

Crea un'istanza Amazon EC2 e accedi automaticamente alla directory

In questa procedura configuri un sistema Windows Server in un'istanza EC2 che può essere utilizzato in seguito per amministrare utenti, gruppi e politiche in Active Directory.

Creazione di un'istanza EC2 e aggiunta automatica della directory

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Scegliere Launch Instance (Avvia istanza).
3. Nella pagina Fase 1, accanto a Microsoft Windows Server 2019 Base - ami-***xxxxxxxx*** scegliere 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-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01).
   - In Sottorete scegli Sottorete pubblica 1, che dovrebbe essere preconfigurata per la zona di disponibilità che preferisci (ad esempio, subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***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 Domain join directory (Directory aggiunta dominio), scegli corp.example.com (d-***xxxxxxxxxx***).
   - Per il ruolo IAM scegli il nome a cui hai assegnato il ruolo dell'istanzaCrea un ruolo per aggiungere istanze Windows al tuo dominio Microsoft AD AWS gestito, ad esempio EC2. DomainJoin
   - 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 console Amazon EC2 e visualizzare lo stato dell'implementazione.

Installazione degli strumenti di Active Directory sull'istanza EC2

È possibile scegliere tra due metodi per installare gli strumenti di gestione del dominio di Active Directory sulla tua istanza EC2. Puoi utilizzare l'interfaccia utente di Server Manager (consigliata per questo tutorial) oppureWindows PowerShell.

Installazione degli strumenti di Active Directory sull'istanza EC2 (Server Manager)

1. Nella console Amazon EC2, scegli Istanze, seleziona l'istanza appena creata, quindi scegli Connetti.
2. Nella casella di dialogo Connect To Your Instance (Connetti all’istanza), scegliere Get Password (Ottieni password) per recuperare la password se non è stato già fatto e scegliere Download Remote Desktop File (Scarica file 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).
    - Seleziona 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 Windows 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 sulla tua istanza EC2 (Windows PowerShell) (opzionale)

1. Avvia Windows 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. Disconnettiti dall'istanza EC2 in cui hai effettuato l'accesso come amministratore locale.
2. Torna nella console Amazon EC2, nel riquadro di navigazione scegli Istanze. 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 e UO di default 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.

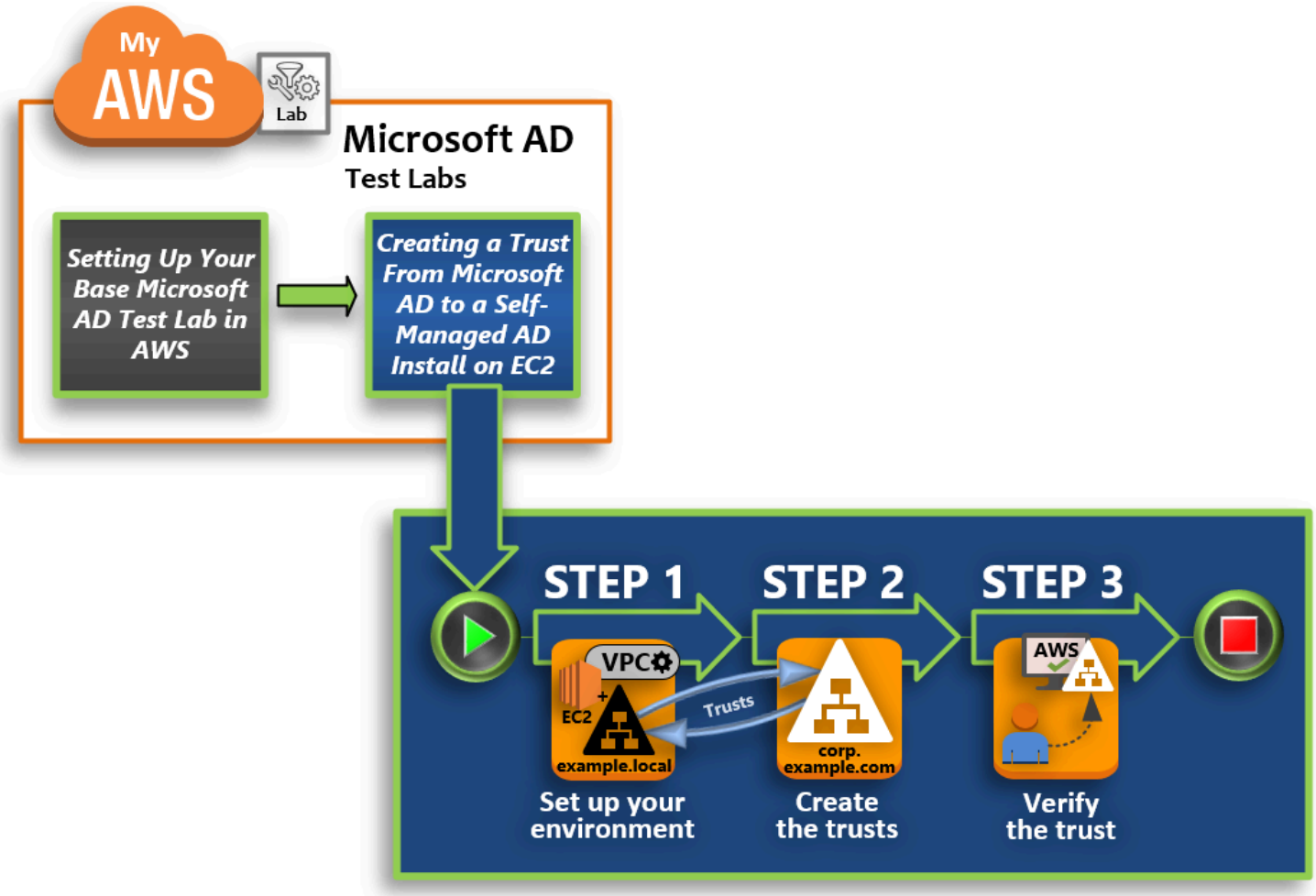
Complimenti! L'ambiente di test di base AWS Managed Microsoft AD è stato ora configurato. Sei pronto per iniziare ad aggiungere il prossimo lab di sicurezza nelle serie.

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 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

Prima di stabilire trust tra una nuova foresta di Active Directory e quella di Microsoft AD gestito da AWS creata nel tutorial di base, devi l'ambiente Amazon EC2. A tale scopo, crea un server di Windows Server 2019, promuovilo a controller di dominio, quindi configura il VPC di conseguenza.

Fase 2: creazione dei trust

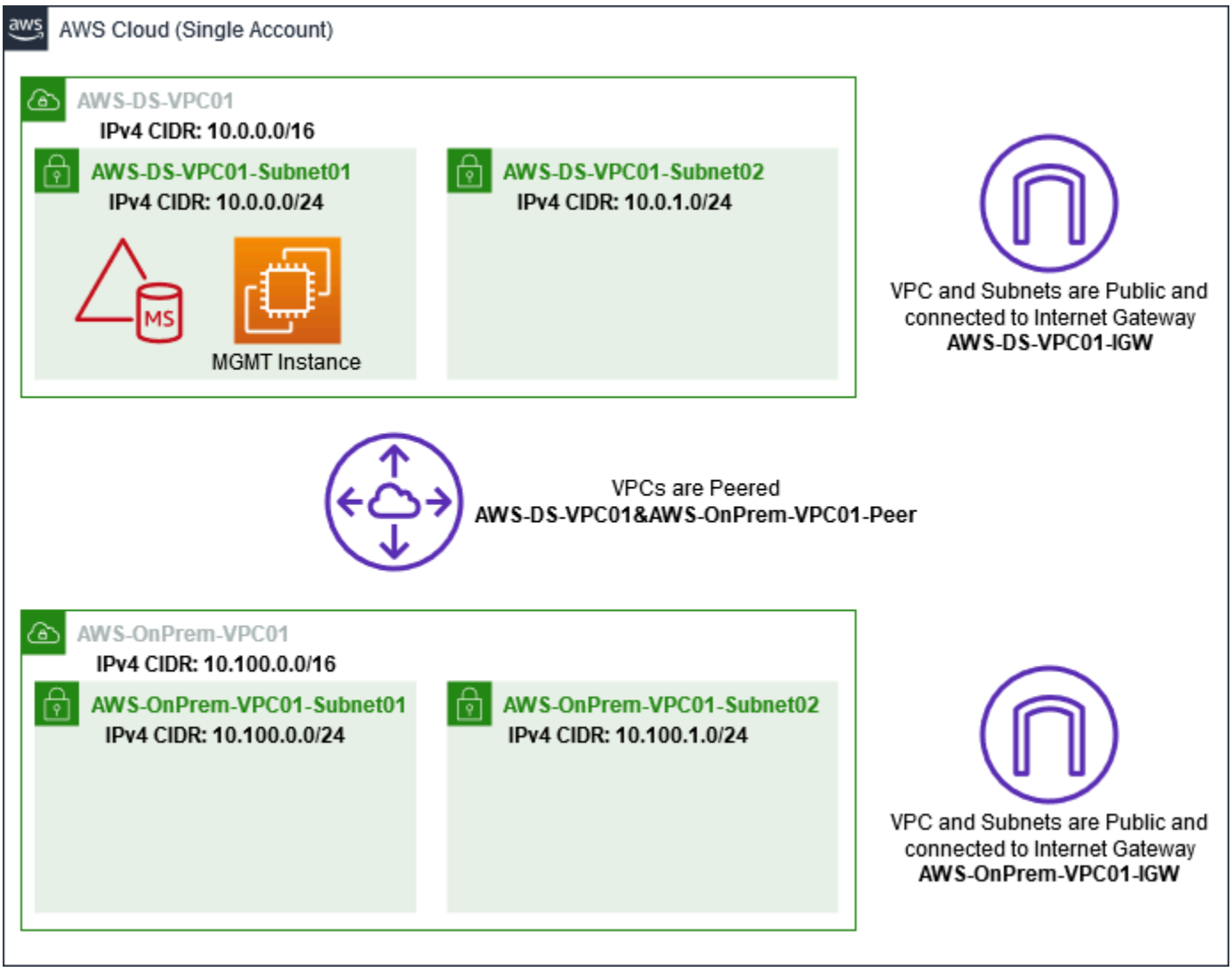
In questo passaggio, crei una relazione di trust bidirezionale tra la foresta di Active Directory appena creata ospitata in Amazon EC2 e la foresta AWS gestita di Microsoft AD in. AWS

Fase 3: verifica del trust

Infine, in qualità di amministratore, utilizzi la AWS Directory Service console per verificare che i nuovi trust siano operativi.

Fase 1: configurazione dell'ambiente per i trust

In questa sezione, configurerai il tuo ambiente Amazon EC2, distribuirai la tua nuova foresta e preparerai il tuo VPC per i trust. AWS



Creazione di un'istanza EC2 di Windows Server 2019

Utilizza la procedura seguente per creare un server membro di Windows Server 2019 in Amazon EC2.

Creazione di un'istanza EC2 di Windows Server 2019

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella console Amazon EC2 scegli Avvia istanza.
3. Nella pagina Fase 1, individua Microsoft Windows Server 2019 Base - ami-***xxxxxxxx*** 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, seleziona vpc- ***xxxxxxxxxxxxxxxxx*** AWS - -VPC01 (che hai precedentemente configurato nel tutorial di Base). OnPrem
   - ***Per Subnet, selezionate subnet- xxxxxxxxxxxxxxxxx \| - -VPC01-Subnet01 \| - -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 console Amazon EC2 e visualizzare lo stato dell'implementazione.

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 che si replichi con la tua rete locale, devi prima aggiungere manualmente l'istanza EC2 al tuo dominio AWS locale. Dopo potrai promuovere il server a un controller di dominio.

Promuovere il server a un controller di dominio

1. Nella console Amazon EC2, scegli Istanze, seleziona l'istanza appena creata, quindi scegli Connetti.
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 di amministratore locale, ritorna alla console Amazon EC2, fai clic con il pulsante destro del mouse sull'istanza e scegli Ottieni 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 il 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. Accedi alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.
3. Fai clic su Security Groups (Gruppi di sicurezza) nel riquadro di navigazione.
4. Cerca il tuo ID di directory AWS Managed Microsoft AD. Nei risultati di ricerca, seleziona la voce con la descrizione AWS ha creato un gruppo di sicurezza per i controller della directory d-***xxxxxx***.

   > **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 sulla tua istanza EC2 e l'altro dal tuo AWS Managed Microsoft AD in AWS.

Per creare la fiducia dal tuo dominio EC2 al tuo AWS Managed Microsoft AD

1. Accedi a example.local.
2. Apri Server Manager e nella struttura della console scegli DNS. Annota l'indirizzo IPv4 elencato nel 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 Replica multi regione, 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 dominio EC2

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 fiducia che scegli qui corrisponda allo stesso tipo di fiducia configurato nella procedura precedente (per creare la fiducia dal tuo dominio EC2 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.

Risoluzione dei problemi relativi AWS a Managed Microsoft AD

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potrebbero verificarsi durante la creazione o l'utilizzo della tua directory.

Problemi con AWS Managed Microsoft AD

Alcune attività di risoluzione dei problemi possono essere completate solo da AWS Support. Ecco alcune delle attività:

- Riavvio dei controller di dominio AWS Directory Service forniti.
- Aggiorna il tuo AWS Managed 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 del CVE-2020-1472, Microsoft ha rilasciato una patch che modifica il modo in cui le comunicazioni tra i canali sicuri 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 gli ID evento 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, vedereAbilita inoltro dei log.

Per ulteriori informazioni sulla mitigazione del CVE-2020-1472, consulta Come gestire le modifiche alle connessioni ai canali sicuri Netlogon associate a CVE-2020-1472 sul sito Web di Microsoft.

Problemi con la reimpostazione della password utente

Quando si tenta di reimpostare la password di un utente, viene visualizzato 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 la 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 Simple AD o AWS Managed Microsoft AD, puoi reimpostare la password utilizzando il AWS Management Console, Windows PowerShell o il AWS CLI.

Per ulteriori informazioni, consulta Reimpostazione della password utente.

Altre risorse

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

- AWS Knowledge Center: trova domande frequenti e collegamenti ad altre risorse per aiutarti a risolvere i problemi.
- AWS Centro assistenza: ottieni supporto tecnico.
- AWS Premium Support Center: ottieni supporto tecnico premium.

Le seguenti risorse possono aiutarti a risolvere i problemi più comuni. Active Directory

- Documentazione Active Directory
- AD DSRisoluzione dei problemi

Argomenti

Monitoraggio del server DNS con Microsoft Event Viewer

Puoi controllare gli eventi DNS di Microsoft AD gestito da AWS in modo da semplificare l'individuazione e la risoluzione dei problemi di 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 Active Directory.

Per accedere a Event Viewer per il tuo DNS Microsoft AD gestito da AWS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione a sinistra, scegliere Instances (Istanze).
3. Individua un'istanza Amazon EC2 aggiunta alla tua directory Microsoft AD gestito da AWS. Seleziona l'istanza quindi scegli Connect (Connetti).

4. Una volta connesso all'istanza Amazon EC2, apri il menu Avvia 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 server DNS Microsoft AD gestito da AWS e quindi scegli OK.
7. Nel riquadro di sinistra, passa a Applications and Services Logs>Microsoft>Windows>DNS-Server, quindi seleziona Audit.

Errori di aggiunta al dominio Linux

Le informazioni seguenti possono aiutarti a risolvere i problemi relativi ai messaggi di errore che potrebbero verificarsi durante l'aggiunta di un'istanza EC2 Linux alla directory Microsoft AD gestito da AWS.

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

no such identity: /Users/username/.ssh/id_ed25519: No such file or directory

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 for admin@EXAMPLE.COM: ubuntu@ip-192-0-2-0:~$ klist Ticket cache: FILE:/tmp/krb5cc_1000 Default principal: admin@EXAMPLE.COM

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 EC2AMAZ-LSMWqT sshd [23832]: password errata per user@corp.example.com dalla porta xxx.xxx.xxx.xxx 18309 ssh2

31 luglio 00:05:00 EC2AMAZ-LSMWqT sshd [23832]: pam_winbind (sshd:auth): acquisizione della password (0x00000390)

31 luglio 00:05:00 EC2AMAZ-LSMWqT sshd [23832]: pam_winbind (sshd:auth): pam_get_item ha restituito una password

31 luglio 00:05:00 EC2AMAZ-LSMWQt 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 EC2AMAZ-LSMWqT sshd [23832]: pam_winbind (sshd:auth): errore interno del modulo (retval = PAM_SYSTEM_ERR (4), user = '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
```

Spazio di archiviazione disponibile insufficiente in Active Directory

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 AWS 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 possono essere EXE, MSI o qualsiasi altro file non essenziale per l'elaborazione di policy di gruppo. Gli oggetti essenziali per l'elaborazione di policy di gruppo sono gli oggetti Policy di gruppo, gli script di accesso/disattivazione e i Central Store for Group Policy objects. 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 i file non necessari è possibile accedere alla condivisione SYSVOL tramite il suo percorso UNC (Universal naming Convention). Ad esempio, se il nome di dominio completo (FQDN) del dominio è example.com, il percorso UNC per SYSVOL è "\\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 AWS 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 Microsoft AD gestito da AWS.

```
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 AWS 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 AWS 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 Snapshot o ripristino della directory. 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 vuoi renderlo più lungo o più corto sostituisci "30" con il numero che si preferisce. 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

Le informazioni seguenti possono aiutarti a risolvere i problemi relativi ai messaggi di errore che potrebbero verificarsi durante l'estensione degli schemi della directory di Microsoft AD gestito da AWS.

Riferimento

Errore

> Aggiungi errore alla voce a partire dalla riga 1: Riferimento Errore lato server: 0x202b Il server ha restituito un riferimento. Errore server esteso: 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. Errore server esteso: 00002083: AtrErr: DSID-03151830, #1:\t0: 00002083: DSID-03151830, problema 1006 (ATT_OR_VALUE_EXISTS), dati 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. Errore server esteso: 00002085: AtrErr: DSID-03152367, #1:\t0: 00002085: DSID-03152367, problema 1001 (NO_ATTRIBUTE_OR_VAL), dati 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. Errore server esteso: "00000057: LdapErr: DSID-0C090D8A, commento: errore nell'operazione di conversione dell'attributo, 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. Errore server esteso: 0000208D: NameErr: DSID-03100238, problema 2001 (NO_OBJECT), dati 0, migliore corrispondenza di: "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 di un trust non va a buon fine, il messaggio sullo stato contiene informazioni aggiuntive. Di seguito ti aiutiamo a capire cosa significano questi messaggi.

L'accesso viene negato

L'accesso è stato negato nel tentativo di creazione di un trust. È possibile che la password di trust sia errata o che le impostazioni di sicurezza del dominio remoto non consentano la configurazione di un trust. Per risolvere questo problema, prova le seguenti soluzioni:

- Microsoft AD AWS gestito Active Directory e quello autogestito con Active Directory cui desideri creare una relazione di fiducia devono avere lo stesso nome del primo sito. Il nome del primo sito è impostato su. `Default-First-Site-Name` Si verifica un errore di accesso negato se questi nomi variano tra i domini.
- 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

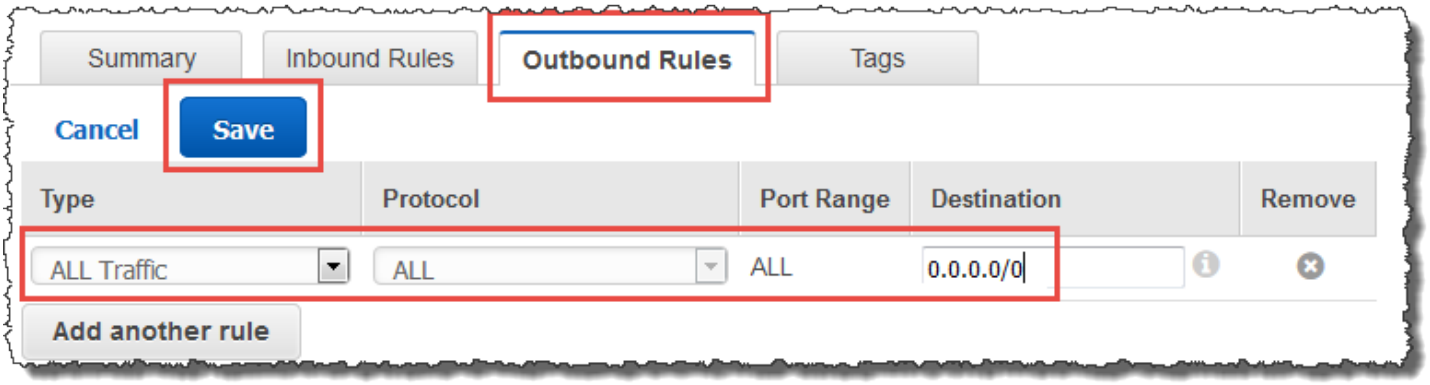
  - lsarpc
- Verificate che le pipe sopra menzionate esistano come valori sulla chiave di NullSessionPipesregistro che si trova nel percorso di registro HKLM\ SYSTEM\\ services \CurrentControlSet\ Parameters. LanmanServer Questi valori devono essere inseriti su righe separate.

  > **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

Il nome di dominio specificato non esiste o non può essere contattato

Per risolvere questo problema, assicurati che le impostazioni del gruppo di sicurezza del dominio e della lista di controllo degli accessi (ACL) del VPC siano corrette; assicurati inoltre di aver inserito accuratamente le informazioni di inoltro condizionale. AWS configura il gruppo di sicurezza per aprire solo le porte necessarie per le comunicazioni di 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.

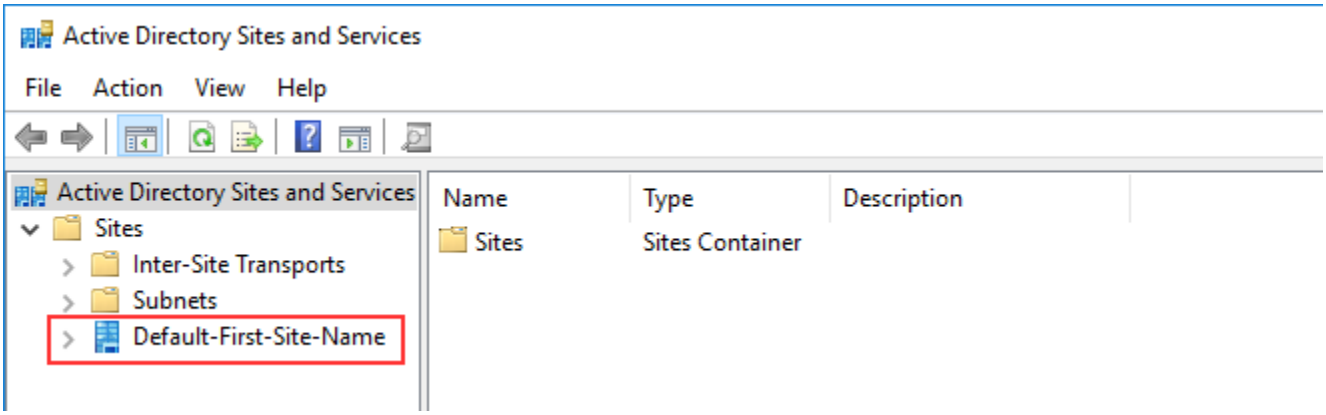
L'Internet Assigned Numbers Authority (IANA) ha riservato i seguenti tre blocchi dello spazio degli indirizzi IP per reti private:

- 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 Single Label.
- 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 Nome di dominio) 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. AWS Directory ServiceLo strumento AWSSupport-TroubleshootDirectoryTrust runbook consente di diagnosticare i problemi più comuni di creazione di trust tra AWS Managed Microsoft AD e un locale. Microsoft Active Directory

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 la directory. 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 Amazon o Amazon WorkDocs. WorkMail
- Puoi gestire AWS risorse come istanze Amazon EC2 o bucket Amazon S3 tramite l'accesso basato sui ruoli IAM a. AWS Management Console
- 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 AWS Directory Service alla tua azienda esistenteActive Directory. Una volta connesso alla directory esistente, tutti i dati della directory rimangono nei controller di dominio. AWS Directory Service non replica nessuno dei dati 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 diversa zona di disponibilità.
- Il VPC deve essere connesso alla rete esistente tramite una connessione VPN (rete privata virtuale) o AWS Direct Connect.
- Il VPC deve disporre di una tenancy hardware predefinita.

AWS Directory Service utilizza una struttura a due VPC. Le istanze EC2 che compongono la tua directory vengono eseguite all'esterno del tuo 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
- 169.254,0/16
- 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 su AWS Direct Connect, consulta la Guida per l'utente.AWS Direct Connect

Esistente Active Directory

Dovrai connetterti a una rete esistente con un Active Directory dominio.

> **Note**
>
> AD Connector non supporta i domini con etichetta singola.

Il livello di funzionalità di questo Active Directory dominio deve essere pari `Windows Server 2003` o superiore. AD Connector supporta anche la connessione a un dominio ospitato su un'istanza Amazon EC2.

> **Note**
>
> AD Connector non supporta i controller del dominio di sola lettura (RODC) se utilizzato in combinazione con la funzionalità di aggiunta del dominio di Amazon 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 Active Directory dominio esistenti, il firewall della rete esistente deve avere le seguenti porte aperte ai CIDR 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 DisableVLVSupportLDAP 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 DisableVLVSupportLDAP è abilitato. Ciò impedisce il funzionamento di AD Connector con Amazon WorkSpaces.

> **Note**
>
> Se i server DNS o i server Domain Controller del Active Directory dominio esistente si trovano all'interno del VPC, i gruppi di sicurezza associati a tali server devono avere le porte sopra indicate aperte ai CIDR per entrambe 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 AWS 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. AWS 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 AWS Directory Service a questo gruppo.

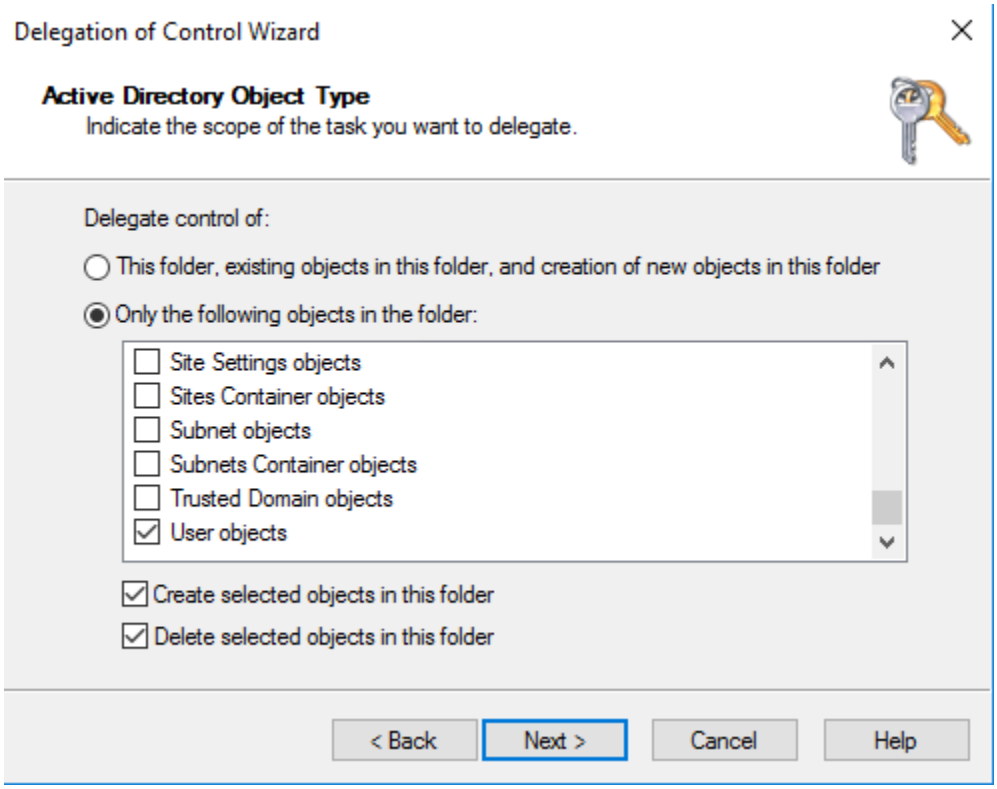
Questa procedura deve essere eseguita su un computer che sia collegato alla directory e che abbia installato lo snap-in di MMC Utenti e computer di Active Directory. Inoltre, è necessario aver eseguito l'accesso come amministratore del dominio.

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.

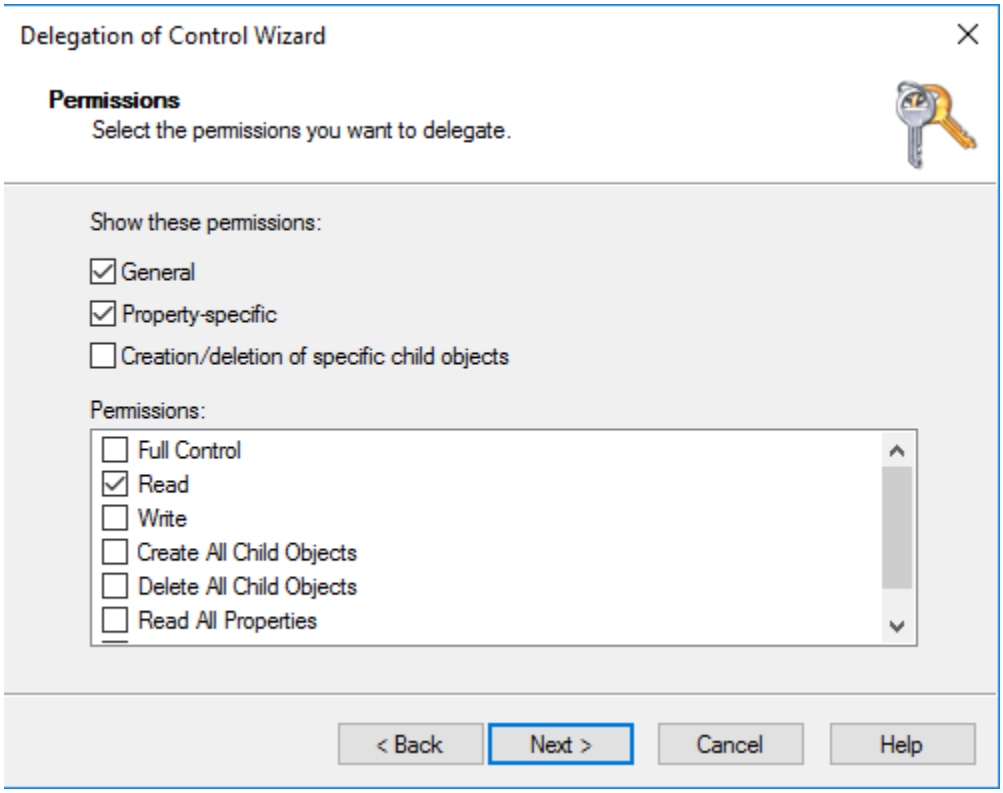
Campo	Valore/Selezione
Group name (Nome gruppo)	`Connectors`
Ambito del gruppo	Globale
Tipo gruppo	Sicurezza

4. Nell'albero di spostamento Utenti e computer di Active Directory, selezionare la radice del dominio. Nel menu, selezionare Azione e quindi Delega controllo. Se il tuo AD Connector è connesso a AWS Managed Microsoft AD, non avrai accesso al controllo dei delegati 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 AWS Directory Service alla directory.

Test di un AD Connector

Per consentire a AD Connector di connettersi alla directory esistente, il firewall della rete esistente deve avere alcune porte specifiche aperte per i CIDR di entrambe le sottoreti presenti nel 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 DirectoryServicePortTestprova. 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).

Cosa viene creato con il tuo AD Connector

Quando crei un AD Connector, crea e associa AWS Directory Service automaticamente un'interfaccia di rete elastica (ENI) a ciascuna delle tue istanze di AD Connector. Ciascuno di questi ENI è essenziale per la connettività tra VPC e AD AWS Directory Service Connector e non deve mai essere eliminato. È possibile identificare tutte le interfacce di rete riservate all'uso AWS Directory Service mediante la descrizione: "interfaccia di rete AWS creata per directory directory-id». Per informazioni, consulta Interfacce di rete elastiche nella Guida per l'utente di Amazon EC2.

> **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.

Come amministrare AD Connector

In questa sezione sono elencate tutte le procedure per gestire e mantenere un ambiente AD Connector.

Argomenti

Protezione della directory AD Connector

In questa sezione vengono riportate alcune considerazioni relative alla protezione dell'ambiente AD Connector.

Argomenti

Aggiornare le credenziali dell'account del servizio AD Connector in AWS Directory Service

Le credenziali AD Connector fornite in AWS Directory Service rappresentano l'account del servizio utilizzato per accedere alla directory on-premise esistente. Puoi modificare le credenziali dell'account del servizio in AWS Directory Service eseguendo la procedura di seguito riportata.

> **Note**
>
> Se AWS IAM Identity Center è abilitato per la directory, AWS Directory Service deve trasferire il nome del principale del servizio (SPN) dall'account del servizio corrente al nuovo account del 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 AWS 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.

Abilitazione dell'autenticazione a più fattori per AD Connector

È possibile abilitare l'autenticazione a più fattori per AD Connector quando disponi di Active Directory in esecuzione on-premise o in istanze di EC2. Per ulteriori informazioni sull'uso dell'autenticazione a più fattori con AWS Directory Service, consulta Prerequisiti di AD Connector.

> **Note**
>
> L'autenticazione a più fattori non è disponibile per Simple AD. Tuttavia, può essere abilitata per la directory Microsoft AD gestito da AWS. Per ulteriori informazioni, consulta Abilita l'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 o WorkSpaces Amazon QuickSight Chime. AWS Management Console Non fornisce MFA per carichi di lavoro Windows in esecuzione su istanze EC2 o per l'accesso a un'istanza EC2. AWS Directory Service non supporta l'autenticazione Challenge/Response RADIUS.
   > 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 tramite la porta predefinita del server RADIUS (UDP:1812) da parte dei server di AWS 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 .

Abilita LDAPS lato client utilizzando 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, Amazon QuickSight e Amazon Chime. Questa crittografia consente di proteggere meglio i dati di identità dell'organizzazione e soddisfare i requisiti di sicurezza.

Argomenti

Prerequisiti

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

Argomenti

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

L'applicazione AWS del traffico LDAP verrà eseguita esclusivamente sulla porta TCP 636, senza alcun fallback alla 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 di sicurezza AWS e i firewall di rete per consentire le comunicazioni TCP sulla porta 636 in AD Connector (in uscita) e Active Directory autogestita (in ingresso).

Abilita 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. 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. Puoi utilizzare il metodo AWS Management Console o il metodo AWS CLI.

Argomenti

Passaggio 1: registrare il certificato in AWS Directory Service

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

Metodo 1: registrare il certificato in AWS Directory Service (AWS Management Console)

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 AWS 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: verificare lo stato di registrazione del certificato in AWS Directory Service (AWS Management Console)

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: verificare lo stato di registrazione del certificato in AWS 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

Utilizza uno dei seguenti metodi per abilitare LDAPS lato client in AWS Directory Service.

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

Metodo 1: abilitare LDAPS lato client in AWS Directory Service (AWS Management Console)

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: abilitare LDAPS lato client in AWS Directory Service (AWS CLI)

- Esegui il comando seguente.

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

Fase 4: controllare lo stato LDAPS

Utilizza uno dei seguenti metodi per verificare lo stato LDAPS in AWS Directory Service.

Metodo 1: verificare lo stato LDAPS in AWS Directory Service (AWS Management Console)

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: verificare lo stato LDAPS in AWS 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. Puoi utilizzare il metodo AWS Management Console o il metodo AWS CLI.

Visualizzare i dettagli del certificato

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

Metodo 1: visualizzare i dettagli del certificato in AWS Directory Service (AWS Management Console)

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: visualizzare i dettagli del certificato in AWS 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 AWS Directory Service (AWS Management Console)

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 AWS 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 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 AWS Directory Service (AWS Management Console)

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 AWS Directory Service (AWS CLI)

- Esegui il comando seguente.

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

Abilita l'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)
> - US West (Oregon)
> - Asia Pacifico (Sydney)
> - Asia Pacifico (Tokyo)
> - Europa (Irlanda)
> - AWS GovCloud (Stati Uniti occidentali)

Argomenti

- Gestisci le impostazioni di autenticazione con 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 la tua gestione automatica. Active Directory Per ulteriori informazioni su come configurare l'autenticazione con smart card con Amazon WorkSpaces Active Directory, consulta la Amazon WorkSpaces Administration Guide.

Prima di abilitare l'autenticazione con smart card per WorkSpaces, consulta le seguenti considerazioni:

- Requisiti del certificato CA
- Requisiti in termini di certificato utente
- Processo di verifica della revoca del certificato
- Altre 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.

Altre 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.

Abilitazione 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.

Argomenti

- Passaggio 1: abilitare la delega vincolata Kerberos per l'account del servizio AD Connector
- Fase 2: registrare il certificato CA in AD Connector

- Fase 3: abilitare l'autenticazione con smart card per le applicazioni e i servizi AWS supportati

Passaggio 1: abilitare la 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 permette agli amministratori dei servizi di specificare e applicare limiti di attendibilità delle applicazioni limitando l'ambito in cui è consentito agire per conto di un utente ai servizi delle applicazioni. 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 SAM dello stesso AccountName utente. Il saM AccountName è limitato a 20 caratteri. sAM AccountName 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

Fase 2: registrare il 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 (AWS Management Console)

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)

- Esegui il 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.

Fase 3: abilitare l'autenticazione con smart card per le applicazioni e i servizi AWS 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 (AWS Management Console)

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)

- Esegui il 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.

Gestisci le impostazioni di autenticazione con smart card

Sono disponibili due metodi diversi per gestire le impostazioni delle smart card. È possibile utilizzare il AWS Management Console metodo o il AWS CLI metodo.

Argomenti

- Visualizzare i dettagli del certificato
- Annullare la registrazione di un certificato
- Disattivare l'autenticazione con smart card

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 AWS Directory Service (AWS Management Console)

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 AWS 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 l'autenticazione con smart card prima di poter annullare la registrazione.

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

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 () AWS 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
```

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 AWS Directory Service ()AWS Management Console

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 AWS Directory Service (AWS CLI)

- Esegui il comando seguente.

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

Configurare AWS Private CA Connector for AD

Puoi integrare il tuo Active Directory (AD) autogestito con AWS Private Certificate Authority (CA) con AD Connector per emettere e gestire certificati per utenti, gruppi e macchine uniti al tuo dominio AD. AWS Private CA Connector for AD consente di utilizzare un sostituto AWS Private CA drop-in completamente gestito per le CA aziendali autogestite 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 console Directory Service, la console AWS Private CA Connector for AD o chiamando l'`CreateTemplate`API. Per configurare l'integrazione di Private CA tramite la console AWS Private CA Connector for Active Directory, vedi AWS Private CA Connettore per Active Directory. Di seguito sono riportati i passaggi su come configurare questa integrazione dalla AWS Directory Service console.

Prerequisiti

Quando utilizzi AD Connector, devi delegare autorizzazioni aggiuntive all'account del servizio. Imposta la lista di controllo degli accessi (ACL) sul tuo account di servizio per poter eseguire le seguenti operazioni.

- Aggiungere e rimuovere un nome del principale del servizio (SPN).
- Creare e aggiornare le autorità di certificazione nei seguenti container:

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- Crea e aggiorna un oggetto NT AuthCertificates Certification Authority come nell'esempio seguente. Se l'oggetto NT AuthCertificates Certification Authority esiste, è necessario delegare le relative autorizzazioni. Se l'oggetto non esiste, è necessario delegare la possibilità di creare un oggetto figlio nel container Public Key Services.

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> Se utilizzi AWS Managed Microsoft AD, le autorizzazioni aggiuntive verranno delegate automaticamente quando autorizzi il servizio AWS Private CA Connector for AD con la tua directory.

È possibile utilizzare PowerShell lo script seguente per delegare le autorizzazioni aggiuntive e creare l'oggetto dell'autorità di certificazione NT. AuthCertifiates Sostituisci "myconnectoraccount" con il nome dell'account del servizio.

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE

# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGuid, 'None'
$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"
```

```
# Add ACLs allowing AD Connector service account the ability to create certification
 authorities
[System.GUID]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'certificationAuthority' }
 -Properties 'schemaIDGUID').schemaIDGUID
$CAAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
 $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
 @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
 -Path "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.GUID]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
```

```
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

Per configurare AWS Private CA Connector for AD

1. Accedi a AWS Management Console e apri la AWS Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. Nella scheda Rete e sicurezza, in AWS Private CA Connettore per AD, scegli Configura AWS Private CA connettore per AD. Active DirectoryViene visualizzata la pagina Crea certificato CA privato per. Segui i passaggi sulla console per creare la tua CA privata per il Active Directory connettore per la registrazione alla tua CA privata. Per ulteriori informazioni, consulta Creazione di un connettore.
4. Dopo aver creato il connettore, segui i passaggi seguenti per visualizzare i dettagli, tra cui lo stato del connettore e lo stato della CA privata associata.

Per visualizzare AWS Private CA Connector for AD

1. Accedi a AWS Management Console e apri la AWS Directory Service console all'indirizzohttps://console.aws.amazon.com/directoryservicev2/.
2. Nella pagina Directories (Directory), scegli l'ID della directory.
3. In Rete e sicurezza, in AWS Private CA Connector per AD, puoi visualizzare i connettori della CA privata e la CA privata associata. Per impostazione predefinita, vengono visualizzati i seguenti campi:

    a. AWS Private CA ID connettore: l'identificatore univoco di un AWS Private CA connettore. Facendo clic su di esso si accede alla pagina dei dettagli di quel AWS Private CA connettore.

    b. AWS Private CA oggetto: informazioni sul nome distinto della CA. Facendo clic su di esso, si accede alla pagina dei dettagli di quella AWS Private CA.

    c. Stato: basato su un controllo dello stato del AWS Private CA Connector e del AWS Private CA. Se entrambi i controlli vengono superati, viene visualizzato Attivo. Se uno dei controlli ha esito negativo, viene visualizzato il messaggio 1/2 dei controlli non riusciti. Se entrambi i controlli hanno esito negativo, viene visualizzato Non riuscito. Per ulteriori informazioni sullo stato non riuscito, passa il mouse sul collegamento ipertestuale per scoprire a quale controllo si riferisce. Segui le istruzioni indicate nella console per rimediare.

d. Data di creazione: il giorno in cui è stato creato il AWS Private CA connettore.

Per ulteriori informazioni, consulta Visualizzazione dei dettagli del connettore.

Monitoraggio della directory AD Connector

Puoi monitorare la directory AD Connector nei seguenti modi:

Argomenti

- Comprendere lo stato della directory
- Configura le notifiche sullo stato delle directory 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 AWS 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 AWS Support.

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 la normale attività di manutenzione operativa, ad esempio applicazione di patch o la rotazione dell'istanza EC2, l'hot spotting temporaneo mediante un'applicazione su uno dei controller di dominio o modifiche apportate alla rete che interrompono inavvertitamente le comunicazioni di directory. 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 AWS Support.

> **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 Snapshot o ripristino della directory.

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.

Configura le notifiche sullo stato delle directory 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 la

procedura riportata di seguito puoi aggiungere AWS Directory Service un editore a un argomento di Amazon SNS. Quando AWS 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 AWS Management Console e apri la console.AWS 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 Crea.

Se desideri designare abbonati SNS aggiuntivi, ad esempio un indirizzo e-mail aggiuntivo, code Amazon SQS oppure AWS Lambda, puoi farlo dalla console Amazon SNS.

Per rimuovere i messaggi di stato della directory da un argomento

1. Accedi a e apri la console. AWS Management ConsoleAWS Directory 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 messaggi AWS Directory Service, associa la directory a un argomento Amazon SNS diverso.

Aggiungi un'istanza Amazon EC2 al tuo Active Directory

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. Ecco ulteriori informazioni su come collegare un Amazon EC2 a un dominio Active Directory:

- Puoi aggiungere facilmente un'istanza Amazon EC2 al Active Directory tuo dominio quando l'istanza viene lanciata. Per ulteriori informazioni, consulta Unisci senza problemi un'istanza Amazon Windows EC2 al tuo AWS Managed Microsoft AD con AD Connector.
- Se devi aggiungere manualmente un'istanza EC2 al tuo Active Directory dominio, devi avviare l'istanza nel gruppo o nella sottorete appropriata Regione AWS e sicura, 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 gestita autonomamente Active Directory (in locale), l'istanza comunica direttamente con te Active Directory e aggira AD Connector.

Argomenti

Unisci senza problemi un'istanza Amazon Windows EC2 al tuo AWS Managed Microsoft AD con AD Connector

Questa procedura unisce senza problemi un'istanza Amazon Windows EC2 al tuo AWS Managed Microsoft AD. Active Directory

Per unirsi senza problemi a un'istanza EC2 Windows

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Windows EC2.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.
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.

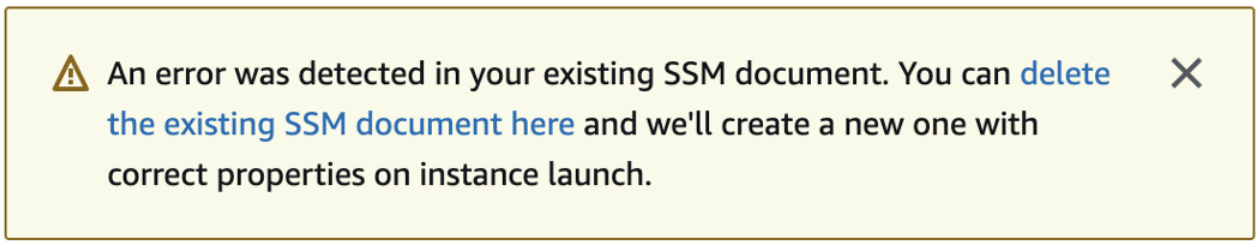
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

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 DirectoryServiceAccess associate le policy

AWS gestite AmazonSSM ManagedInstanceCore e AmazonSSM dall'elenco a discesa dei profili delle istanze 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. Per Use case (Caso d'uso), seleziona EC2.
4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le politiche AmazonSSM e AmazonSSM. ManagedInstanceCore DirectoryServiceAccess Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Seleziona Successivo.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un managed by. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 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. È necessario aggiungere questo nome del ruolo all'istanza EC2.
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).

Unisci senza problemi un'istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD con AD Connector

Questa procedura unisce senza problemi un'istanza Amazon EC2 Linux alla directory AWS Managed 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 non supportano la funzionalità di aggiunta ottimizzata del dominio.

Prerequisiti

Prima di poter configurare un join di dominio senza interruzioni su un'istanza Linux EC2, devi completare le procedure descritte in questa sezione.

Selezione dell'account del servizio di aggiunta ottimizzata del dominio

Puoi aggiungere facilmente computer Linux al tuo Active Directory dominio locale tramite AD Connector. A tale scopo, devi creare un account utente con le autorizzazioni di creazione di account di computer per aggiungere i computer al dominio. Se preferisci, puoi utilizzare il tuo account del servizio AD Connector. In alternativa, puoi utilizzare qualsiasi altro account che disponga di privilegi sufficienti per aggiungere 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 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 computer al dominio, puoi eseguire i seguenti comandi. PowerShell È necessario eseguire questi comandi da un computer aggiunto al dominio su cui è installato il fileWindows. Installare gli 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. Se preferisci utilizzare un'interfaccia utente grafica (GUI), puoi utilizzare il processo manuale descritto in Delegare privilegi all'account del servizio.

```
$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 AWS Secrets Manager per archiviare l'account del servizio di dominio.

Per creare segreti e archiviare le informazioni sull'account del servizio di dominio

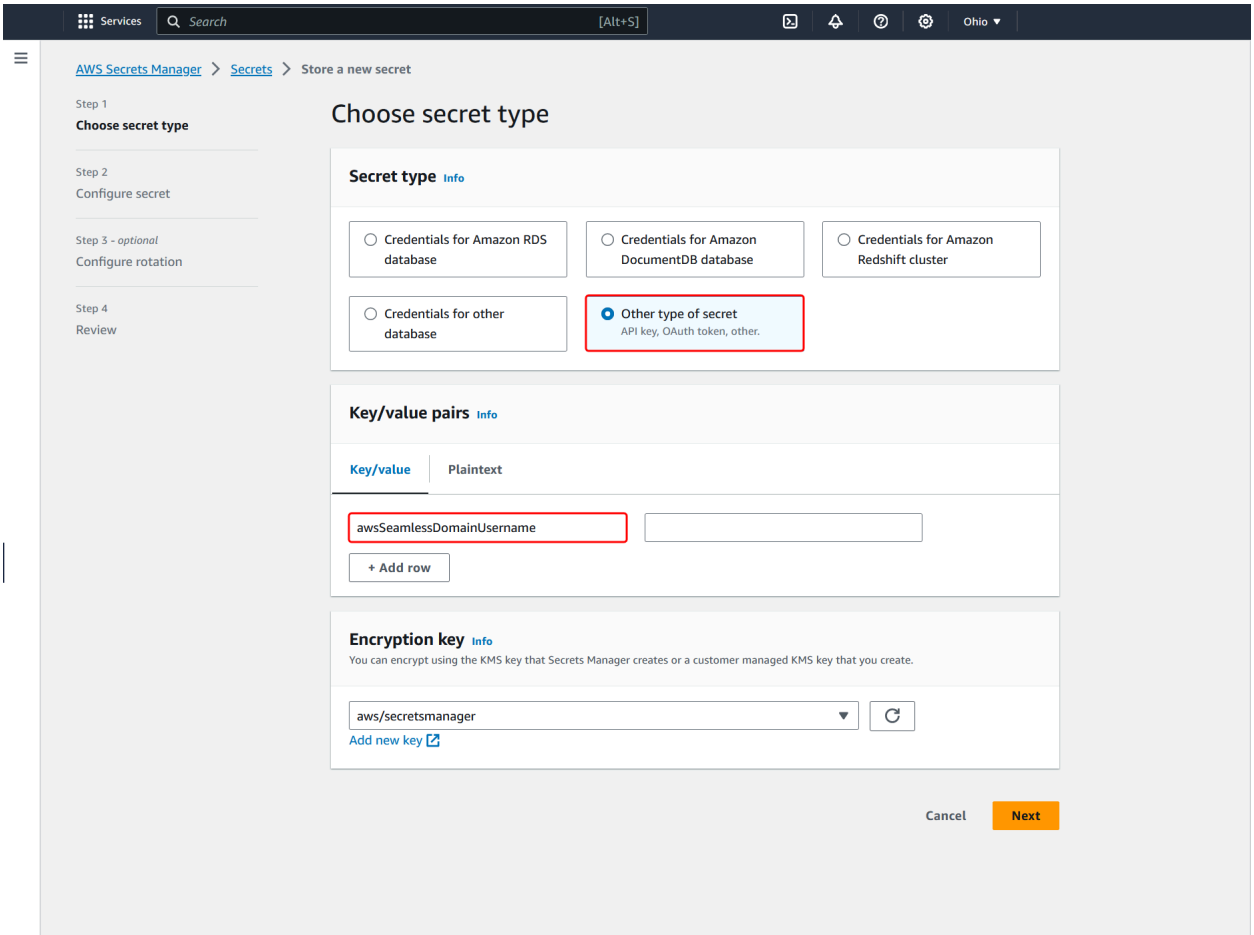
1. Accedi AWS Management Console e apri la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Archivia un nuovo segreto, procedere nel seguente modo:

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`. AWS Secrets Manager crittografa sempre il segreto quando scegli questa opzione. Puoi anche scegliere una chiave creata da te.

> **Note**
>
> Sono previste delle commissioni AWS Secrets Manager, a seconda del segreto utilizzato. Per l'elenco completo dei prezzi aggiornati, consulta la pagina dei prezzi AWS Secrets Manager.
> Puoi utilizzare la chiave AWS `aws/secretsmanager` gestita creata 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 attuale. AWS KMS Per ulteriori informazioni, consulta la sezione Prezzi di AWS Key Management Service.

v. Seleziona Successivo.

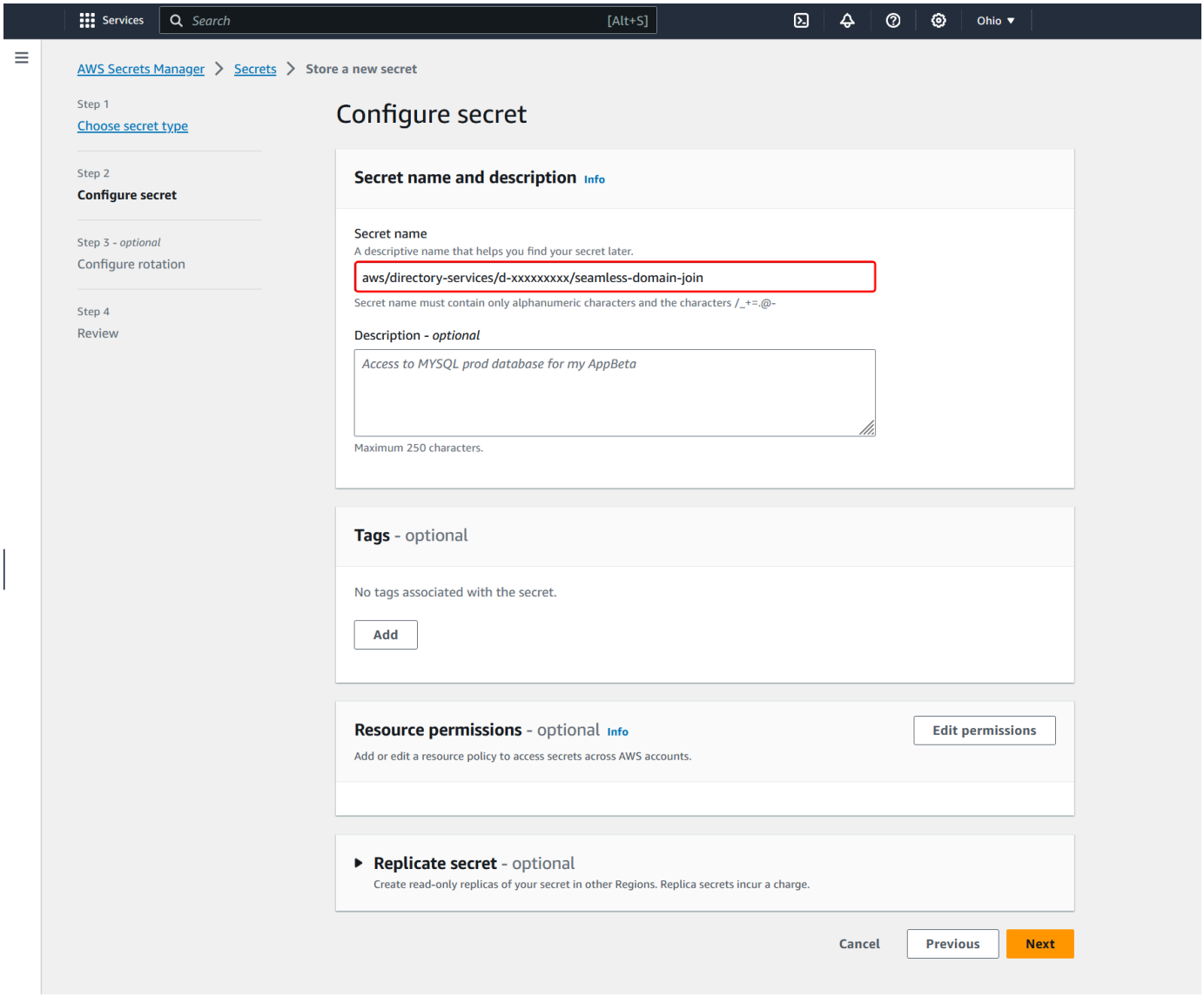
4. In Nome segreto, inserisci un nome segreto che includa l'ID della tua directory utilizzando il seguente formato, sostituendo *`d-xxxxxxxxx`* con il tuo ID di directory:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Questo nome viene utilizzato per recuperare i segreti nell'applicazione.

> **Note**
>
> Devi inserire **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** esattamente come è, e sostituire *`d-xxxxxxxxx`* con l'ID della 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 AWS Secrets Manager i segreti nella Guida per l'AWS Secrets Manager utente.

  Per il passaggio 5, utilizzare il modello di rotazione Microsoft Active Directory credenziali nella Guida per l'AWS Secrets Manager utente.

  Per assistenza, consulta Risoluzione dei problemi di AWS Secrets Manager rotazione nella Guida per l'AWS Secrets Manager utente.

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 IAM in LinuxEC2. 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 AWS Management Console come utente autorizzato a creare policy IAM. 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.

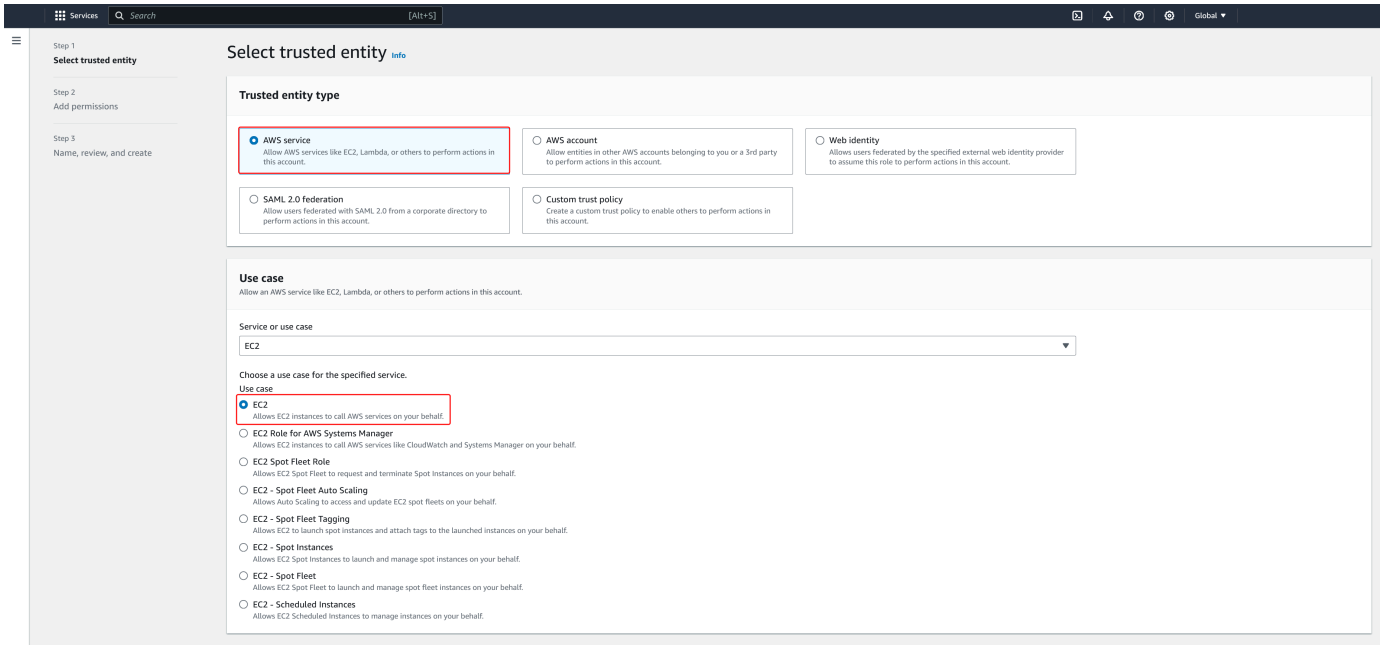
> **Note**
>
> Consigliamo di creare una policy per ogni segreto. In questo modo, ti assicuri che le istanze abbiano accesso solo al segreto in questione e riduci al minimo l'impatto se un'istanza viene compromessa.

Crea il ruolo LinuxEC2 DomainJoin

Utilizzi la console IAM per creare il ruolo che userai per aggiungere il dominio alla tua istanza EC2 Linux.

Per creare il ruolo LinuxEC2 DomainJoin

1. Accedi AWS Management Console come utente autorizzato a creare policy IAM. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro 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**
>
> AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un server gestito da. Active Directory AWS Directory Service AmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 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`** 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 la tua istanza Amazon EC2 Linux al tuo AWS Managed Microsoft AD Active Directory

Ora che hai configurato tutte le attività prerequisite, puoi utilizzare la seguente procedura per unire senza problemi la tua istanza EC2 Linux.

Per unirti senza problemi alla tua istanza Linux

1. Accedi AWS Management Console e apri la console Amazon EC2 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. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Linux EC2.

5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.
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, consulta Installazione e configurazione dell'Agente SSM su istanze EC2 per Linux.
> SSM utilizza il `aws:domainJoin` plug-in per aggiungere un'istanza Linux a un dominio. Active Directory *`Il plugin cambia il nome host per le istanze Linux nel formato EC2AMAZ-XXXXXXX.`* Per ulteriori informazioni in merito*`aws:domainJoin`*, consultate il riferimento al plugin AWS Systems Manager Command Document nella Guida per l'utente.AWS Systems Manager

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.

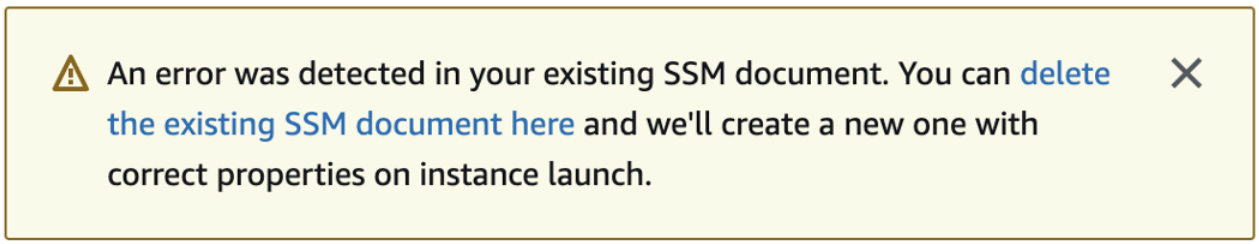
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

15. Per il profilo dell'istanza IAM, scegli il ruolo IAM creato in precedenza nella sezione dei prerequisiti Fase 2: Creazione del ruolo LinuxEC2. 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.

Gestione della directory AD Connector

In questa sezione viene descritto come gestire le attività di amministrazione più comuni per l'ambiente AD Connector.

Argomenti

- Eliminare AD Connector
- Visualizzazione delle informazioni sulla directory

Eliminare 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. AWS Le 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 AWS app e servizi, puoi vedere quali AWS applicazioni sono abilitate per il tuo AD Connector.

- Disabilita AWS Management Console l'accesso. Per ulteriori informazioni, consulta Disabilita l'accesso alla AWS Management Console..
- Per disabilitare Amazon WorkSpaces, devi annullare la registrazione del servizio dalla directory nella WorkSpaces console. Per ulteriori informazioni, consulta Annullamento della registrazione da una directory nella Amazon WorkSpaces Administration Guide.
- Per disabilitare Amazon WorkDocs, devi eliminare il WorkDocs sito Amazon nella WorkDocs console Amazon. 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 per Windows File Server, devi rimuovere il file system Amazon FSx dal dominio. Per ulteriori informazioni, consulta Lavorare con Active Directory FSx for Windows File Server nella Guida per l'utente di Amazon FSx for Windows File Server.
- 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 Active DirectoryAuthentication nella AWS Client VPN Administrator Guide.
- Per disabilitare Amazon Connect, è necessario eliminare l'istanza di Amazon Connect. Per ulteriori informazioni, consulta Eliminazione di un'istanza Amazon Connect nella Guida all'amministrazione di Amazon Connect.
- Per disattivare Amazon QuickSight, devi annullare l'iscrizione ad Amazon QuickSight. Per ulteriori informazioni, consulta la sezione Chiusura Amazon QuickSight dell'account nella Amazon QuickSight User Guide.

> **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.

Visualizzazione delle informazioni sulla directory

Puoi visualizzare informazioni dettagliate su una directory.

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione della AWS Directory Service console, sotto Active Directory, seleziona Directory.
2. Fai clic sul link dell'ID directory della 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.

Consentire l'accesso ad AWS applicazioni e servizi

Gli utenti possono autorizzare AD Connector a fornire ad AWS applicazioni e servizi, come Amazon WorkSpaces, l'accesso al tuoActive 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, consulta la Guida all'amministrazione di Amazon Chime.
Amazon Connect	Per ulteriori informazioni, consulta la Guida all'amministrazione di Amazon Connect.
Amazon WorkDocs	Per ulteriori informazioni, consulta la Amazon WorkDocs Administration Guide.

AWS applicazione/servizio	Ulteriori informazioni…
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.
AWS Client VPN	Per ulteriori informazioni, consulta la AWS Client VPN Guida per l'utente.
AWS IAM Identity Center	Per ulteriori informazioni, consulta la AWS IAM Identity Center Guida per l'utente.
AWS Management Console	Per ulteriori informazioni, consulta Abilitazione dell'accesso a AWS Management Console con le credenziali AD.
AWS Transfer Family	Per ulteriori informazioni, consulta la AWS Transfer Family Guida per l'utente.

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 AWS 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 serviziAWS .

Per ulteriori informazioni su come autorizzare o rimuovere l'autorizzazione all'utilizzo AWS Directory Servicedi AWS applicazioni e servizi, vedere. Autorizzazione per l'utilizzo di AWS applicazioni e servizi AWS Directory Service

Aggiornamento dell'indirizzo DNS per 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 utilizzi WorkSpaces con AD Connector, assicurati che anche gli indirizzi DNS di WorkSpace siano aggiornati. Per maggiori informazioni, consulta Aggiornamento dei 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.

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

AWS 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 il tuo locale esistente Active Directory 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 e a basso costo con compatibilità di baseActive 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 AWS Directory Service opzioni, consulta. Quale scegliere

Verifica che i VPC e le istanze siano configurati correttamente

Per gestire, utilizzare e connetterti alle directory, è necessario configurare correttamente i VPC ai quali sono associate le directory. Consulta AWS Prerequisiti Microsoft AD gestiti, 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 Unisci un'istanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory.

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 di AWS sicurezza della tua directory

AWS crea un gruppo di sicurezza e lo collega alle interfacce di rete elastiche della tua directory, accessibili dall'interno dei tuoi VPC peerizzati o ridimensionati. 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

Se desideri modificare la sicurezza dei gruppi di sicurezza delle directory, puoi farlo. Apporta tali modifiche solo se hai compreso a pieno come funziona il filtraggio del gruppo di sicurezza. Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon EC2 per le istanze Linux nella Guida per l'utente di Amazon EC2. Modifiche improprie possono causare la perdita delle comunicazioni verso 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**
>
> Tecnicamente, hai la possibilità di associare il gruppo di sicurezza della directory ad altre istanze EC2 da te create. 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, associare il gruppo di sicurezza della directory alle istanze EC2 può creare un potenziale rischio per la sicurezza per le istanze EC2.

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 AWS 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, come WorkSpaces Amazon WorkMail, WorkDocs Amazon o Amazon. QuickSight 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 Aggiornare le credenziali dell'account del servizio AD Connector in AWS Directory Service.

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 AWS Directory Service s. Per ulteriori informazioni sulle proprie responsabilità, consultare il nostro modello sulla responsabilità condivisa.

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

Policy di compatibilità delle applicazioni per AD connector

In alternativa a AWS Directory Service for Microsoft Active Directory (AWS Microsoft 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 applicazioni e servizi AWS 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 funzionalità di aggiunta al dominio Active Directory senza interruzioni 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 Aggiungi un'istanza Amazon EC2 al tuo Active Directory.
- AWS Management Console: puoi utilizzare AD Connector per autenticare gli utenti di AWS Management Console con le credenziali Active Directory senza configurare l'infrastruttura SAML. Per ulteriori informazioni, consulta Abilitazione dell'accesso a AWS Management Console con le credenziali AD.
- Amazon QuickSight : per ulteriori informazioni, consulta Gestione degli account utente in Amazon QuickSight Enterprise Edition.
- AWS IAM Identity Center: per istruzioni dettagliate, consulta Connessione di IAM Identity Center a un Active Directory on-premise.
- AWS Transfer Family: per istruzioni dettagliate, vedi Lavorare con AWS Directory Service per Microsoft Active Directory.
- Client VPN AWS: per istruzioni dettagliate, consulta Autenticazione e autorizzazione client.
- Amazon 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 Microsoft AD gestito da AWS e non è compatibile con AD Connector. Per ulteriori informazioni, consulta la sezione AWS Managed Microsoft AD nella pagina AWS Directory ServiceDomande frequenti.

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

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

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 AWS Directory Service le directory. Se ricevi un errore come questo durante la creazione di unaActive 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.

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

Ricevi un messaggio di errore simile al seguente quando ti connetti alla tua directory in locale:

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
 Kerberos/authentication unavailable (TCP port 88) for IP: <IP address> Please ensure
 that the listed ports are available and retry the operation.
```

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 TCP/UDP aggiuntive a seconda delle esigenze. Vedi l'elenco seguente per alcune di queste porte. Per ulteriori informazioni sulle porte utilizzate daActive Directory, vedi Come configurare un firewall per Active Directory domini e trust 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 cerco 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 il messaggio di errore «Impossibile autenticarsi» 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 cerco di accedere Amazon WorkSpaces con una smart card

Quando tenti di accedere al tuo account WorkSpaces con una smart card, ricevi un messaggio di errore simile al seguente:

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

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:

1. Nell'editor del registro, accedi alla seguente chiave hive

   HKEY_LOCAL_MACHINE\ SYSTEM\\ Services\ Kdc\ CurrentControlSet UseSubjectAltName
2. Seleziona UseSubjectAltName. Assicurati che il valore sia impostato su 0.

> **Note**
>
> Se la chiave di registro è impostata sui controller di dominio locali, AD Connector non sarà in grado di localizzare gli utenti 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 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'archivio Active Directory NTAuth:

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

Per ulteriori informazioni sulla pubblicazione dei certificati nello store NTAuth, consulta Importazione del certificato CA emittente nell'archivio Enterprise NTAuth 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 il messaggio di errore «Impossibile autenticarsi» quando utilizzo AWS le applicazioni per cercare utenti o gruppi

Potresti riscontrare errori durante la ricerca di utenti durante l'utilizzo di AWS applicazioni, come Amazon WorkSpaces o Amazon QuickSight, anche quando lo stato di AD Connector era attivo. Le credenziali scadute possono impedire a AD Connector di completare le query su oggetti in Active Directory. Aggiorna la password per l'account del servizio utilizzando i passaggi ordinati forniti inL'aggiunta fluida al dominio per le istanze Amazon EC2 ha smesso di funzionare.

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:

```
Message:An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials.
```

```
An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials
following Update your AD Connector Service Account Credentials
```

```
Message:
An Error Has Occurred
```

```
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

Potrebbe esserci un problema con la sincronizzazione dell'ora e Kerberos. AD Connector invia le richieste di autenticazione Kerberos a. 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 istanze Amazon EC2 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 AWS Support.

L'aggiunta fluida al dominio per le istanze Amazon EC2 ha smesso di funzionare

Se l'aggiunta del dominio uniforme per istanze EC2 funzionava e poi si è arrestata mentre AD Connector era attivo, le credenziali per l'account del servizio di AD Connector potrebbero essere scadute. Le credenziali scadute possono impedire ad AD Connector di creare oggetti informatici nel tuo. 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 nel tuo. Active Directory
2. Aggiorna la password per l'account di servizio nel tuo AD Connector in AWS Directory Service. Per ulteriori informazioni, consulta Aggiornare le credenziali dell'account del servizio AD Connector in AWS Directory Service.

> **Important**
>
> L'aggiornamento della password solo in AWS Directory Service non trasferisce la modifica della password all'ambiente locale esistente, Active Directory 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, consultaEliminare AD Connector. Se ancora non riesci a eliminare il tuo AD Connector, puoi richiedere assistenza tramite AWS Support.

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, inclusa la possibilità di gestire gli account utente e le appartenenze ai gruppi, creare e applicare policy di gruppo, connettersi in modo sicuro alle istanze Amazon EC2 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 delle istanze Amazon EC2 che eseguono Linux e Windows e la distribuzione di applicazioni Windows nel cloud. AWS
- 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 WorkSpaces ad AWS applicazioni come Amazon WorkDocs o Amazon WorkMail.
- Puoi gestire AWS le risorse tramite l'accesso basato sui ruoli IAM a. AWS Management Console
- Le istantanee automatizzate giornaliere consentono il ripristino. point-in-time

Simple AD non supporta:

- Amazon AppStream 2.0
- Amazon Chime
- 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, AWS 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

Prerequisiti di Simple AD

Per creare un Simple ADActive Directory, è necessario un Amazon VPC con quanto segue:

- Il VPC deve disporre di una tenancy hardware predefinita.
- Il VPC non deve essere configurato con i seguenti endpoint VPC:
  - Endpoint VPC Route53 che includono sostituzioni condizionali DNS per *.amazonaws.com che si risolvono in indirizzi IP non pubblici AWS
  - CloudWatch Endpoint VPC
  - Endpoint VPC di Systems Manager
  - Endpoint VPC del Servizio di token di sicurezza
- Almeno due sottoreti in due diverse zone di disponibilità. 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, AWS 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 i tuoi VPC e 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

AWS Directory Service utilizza una struttura a due VPC. Le istanze EC2 che compongono la tua directory vengono eseguite all'esterno del tuo 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
- 169.254,0/16
- 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.

Crea il tuo Simple AD Active Directory

Per creare un nuovo Simple ADActive Directory, procedi nel seguente modo. Prima di iniziare la procedura, assicurati di soddisfare i prerequisiti illustrati in Prerequisiti di Simple AD.

Per creare un Simple AD Active Directory

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. Con 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.

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).

Cosa viene creato con il tuo Simple AD Active Directory

Quando crei un file Active Directory con Simple AD, AWS 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. AWS Directory Service non memorizza questa password e non può essere recuperata. Tuttavia, è possibile reimpostare una password dalla AWS 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 AWS 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 AWS Directory Service.

- crea e associa automaticamente una interfaccia di rete elastica (ENI) a ciascuno dei controller di dominio. Ciascuno di questi ENI è essenziale per la connettività tra il VPC AWS Directory Service e i controller di dominio e non deve mai essere eliminato. È possibile identificare tutte le interfacce di rete riservate all'uso AWS 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 presso 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. 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.

Configurazione del 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 si utilizzano server DNS personalizzati che sono al di fuori del VPC e si desidera utilizzare un DNS privato, sarà necessario riconfigurarli per l'utilizzo di server DNS personalizzati su istanze EC2 all'interno del 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.

> **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.

Come amministrare Simple AD

In questa sezione sono elencate tutte le procedure per gestire e mantenere un ambiente Simple AD.

Argomenti

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 AWS Directory Service, è necessario utilizzare un'istanza (on-premise o EC2) unita alla tua directory AWS Directory Service ed essere connessi come un utente che dispone di privilegi per creare utenti e gruppi. È inoltre necessario installare gli strumenti di Active Directory sull'istanza EC2 in modo che tu possa aggiungere gli utenti e i gruppi con lo snap-in di Utenti e computer di Active Directory. Per ulteriori informazioni su come configurare un'Istanza EC2

e installare gli strumenti necessari, consulta Unisci un'istanza Amazon EC2 al tuo Simple AD Active Directory.

> **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

- Installare gli strumenti di amministrazione di Active Directory per Simple AD
- Crea un utente Simple AD
- Eliminare un utente Simple AD
- Reimpostazione di una password utente Simple AD
- Crea un gruppo Simple AD
- Aggiungere un utente Simple AD a un gruppo

Installare gli strumenti di amministrazione di Active Directory per Simple AD

Per gestire Active Directory da un'istanza 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:

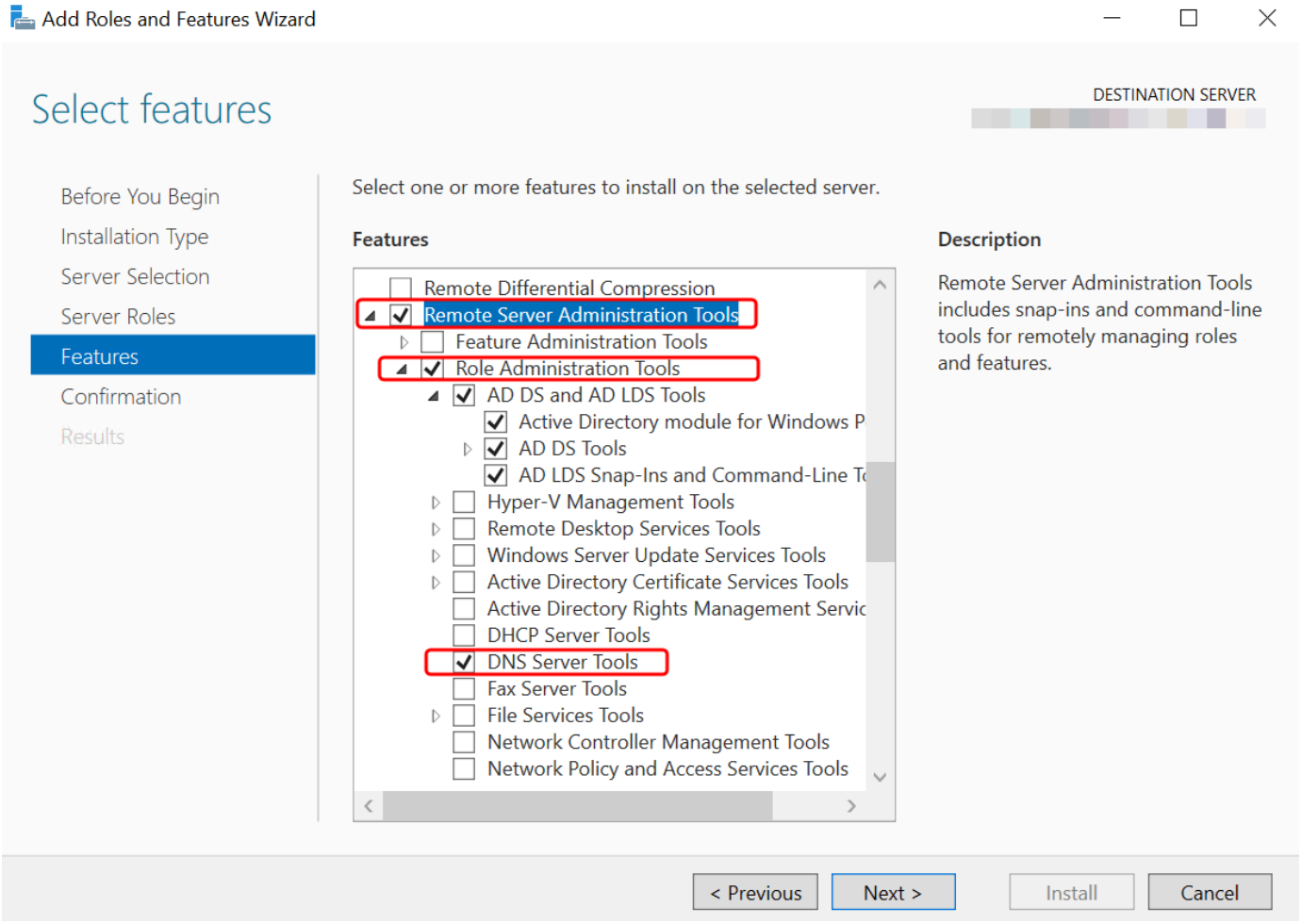
1. Crea un Simple AD Active Directory. Per ulteriori informazioni, consulta Crea il tuo Simple AD Active Directory.
2. Avvia e unisci un'istanza EC2 Windows Server al tuo Simple AD Active Directory. L'istanza EC2 necessita delle seguenti policy per creare utenti e gruppi: **`AWSSSMManagedInstanceCore`** e. **`AmazonSSMDirectoryServiceAccess`** Per ulteriori informazioni, consulta Unisci senza problemi un'istanza Windows di Amazon EC2 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 Active Directory, il nome utente dell'amministratore include il nome NetBIOS,. **corp\administrator**

Installa gli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

Per installare gli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella console Amazon EC2, scegli Istanze, seleziona l'istanza appena creata, quindi scegli Collega.
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 Active Directory.
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 Active Directorymodulo per Windows PowerShell, AD DS Tools, gli snap-in e gli strumenti della 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.

Metodo alternativo all'installazione degli strumenti di amministrazione di Active Directory sull'istanza EC2 di Windows Server

- Ecco un altro metodo per installare gli strumenti di amministrazione di Active Directory:
  - Facoltativamente, puoi scegliere di installare gli strumenti di amministrazione di Active Directory utilizzandoWindows PowerShell. 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.

Crea un utente Simple AD

Utilizza la seguente procedura per creare un utente con un'istanza Amazon EC2 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.

Puoi utilizzare uno dei seguenti metodi per creare un utente:

- Active DirectoryStrumenti di amministrazione
- Windows PowerShell

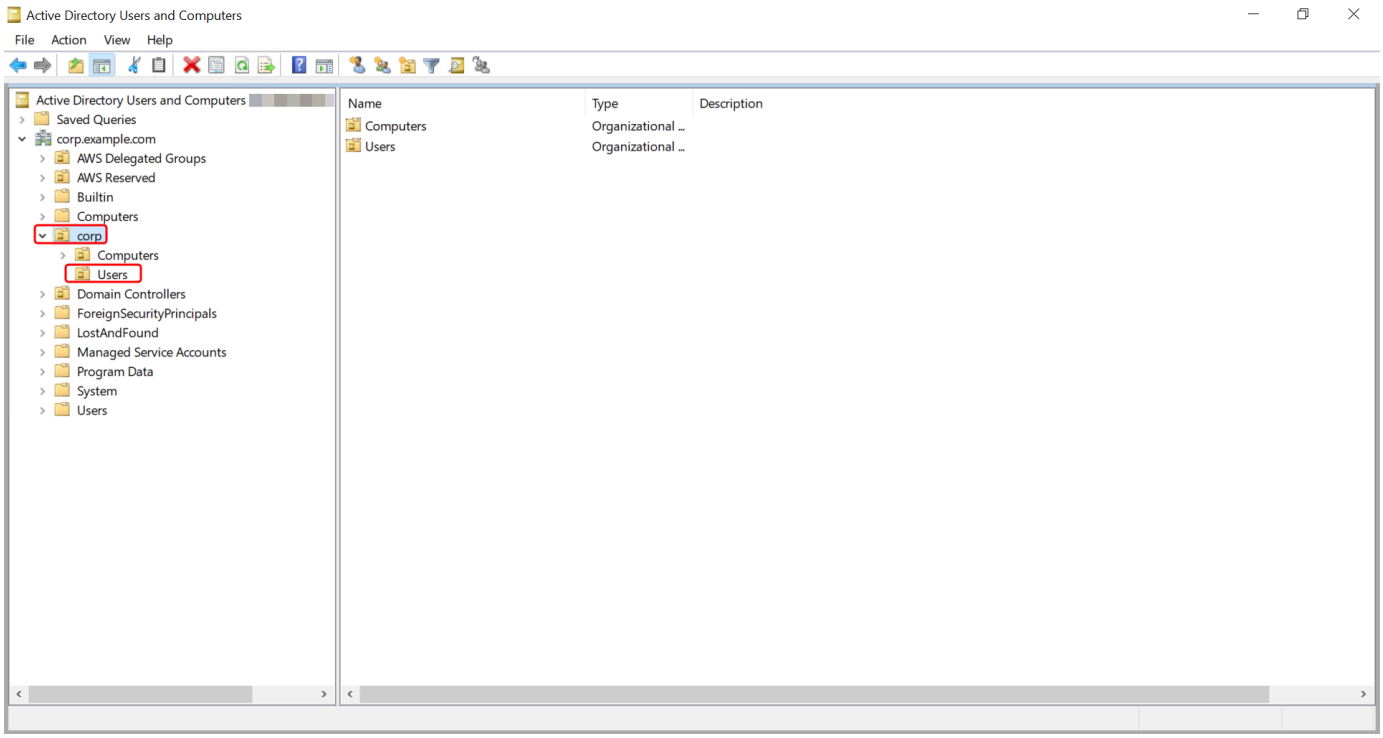
Crea un utente con gli strumenti di Active Directory amministrazione

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 Active Directory



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. Seleziona 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).

Crea un utente in Windows PowerShell

1. Connect all'istanza aggiunta al tuo Active Directory dominio come Active Directory amministratore.
2. Aprire Windows 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 Windows PowerShell fornire una password per il nuovo utente. Per ulteriori informazioni sui requisiti di complessità delle Active Directory password, consulta Microsoftla documentazione. Per ulteriori informazioni sul comando New-ADUser, consultate la documentazione. Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

Eliminare un utente Simple AD

Utilizza la seguente procedura per eliminare un utente con un'istanza Amazon EC2 Windows aggiunta alla tua directory Simple AD.

Puoi utilizzare uno dei seguenti metodi per eliminare un utente:

- Active DirectoryStrumenti di amministrazione
- Windows PowerShell

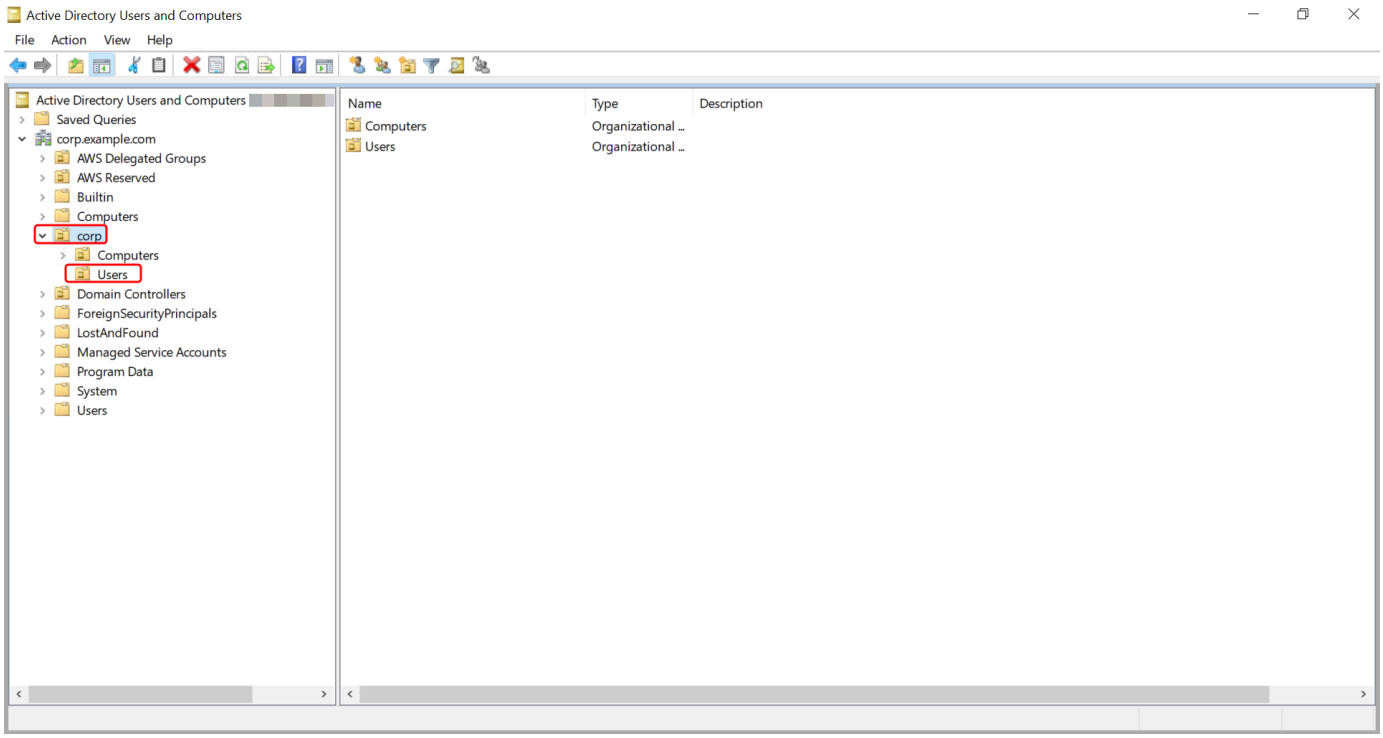
Eliminare un utente con gli strumenti di Active Directory amministrazione

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.

Eliminare un utente in Windows PowerShell

1. Connect all'istanza aggiunta al tuo Active Directory dominio come Active Directory amministratore.
2. Aprire Windows PowerShell.
3. Digita il seguente comando sostituendo il nome utente **`jane.doe`** con il nome utente dell'utente che desideri eliminare. Per ulteriori informazioni sul comando Remove-ADUser, consultate la documentazione. Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

Reimpostazione di una password utente Simple AD

Gli utenti devono rispettare le politiche in materia di password definite in. Active Directory A volte in questo modo gli utenti, incluso l'Active Directoryamministratore, possono avere la meglio e dimenticarsi la password. Quando ciò accade, puoi reimpostare rapidamente la password dell'utente utilizzando AWS 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 AWS Directory Service.

Puoi reimpostare la password per qualsiasi utente del tuo account 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 al momento della creazione del. Active Directory Ad esempio, se si segue la procedura descritta inCrea il tuo Simple AD Active Directory, 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 al momento della creazione del. Active Directory Per ulteriori informazioni sulla struttura delle unità organizzative per Simple AD, vedereCosa viene creato con il tuo Simple AD Active Directory.
- 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:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Reimpostare la password di un utente in AWS Management Console

1. Nel riquadro di navigazione della AWS Directory Service console Active Directory, sotto, scegli Directory, quindi seleziona la Active Directory cartella dall'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.

Reimposta la password di un utente in AWS CLI

1. Per installare AWS CLI, vedi Installare o aggiornare la versione più recente di AWS CLI.
2. Aprire il AWS CLI.
3. Digita il comando seguente e sostituisci l'ID di directory, il nome utente **`jane.doe`** e la password **`P@ssw0rd`** con il tuo ID di Active Directory directory e le credenziali desiderate. Per ulteriori informazioni reset-user-password, consulta la sezione AWS CLI Command Reference.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

Reimposta la password di un utente in Windows PowerShell

1. Connect all'istanza aggiunta al tuo Active Directory dominio come Active Directory amministratore.
2. Aprire Windows PowerShell.
3. Digita il comando seguente sostituendo il nome utente**`jane.doe`**, l'ID di directory e la password **`P@ssw0rd`** con il tuo ID di Active Directory directory e le credenziali desiderate. Per ulteriori informazioni, vedere il UserPassword cmdlet Reset-DS.

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

Crea un gruppo Simple AD

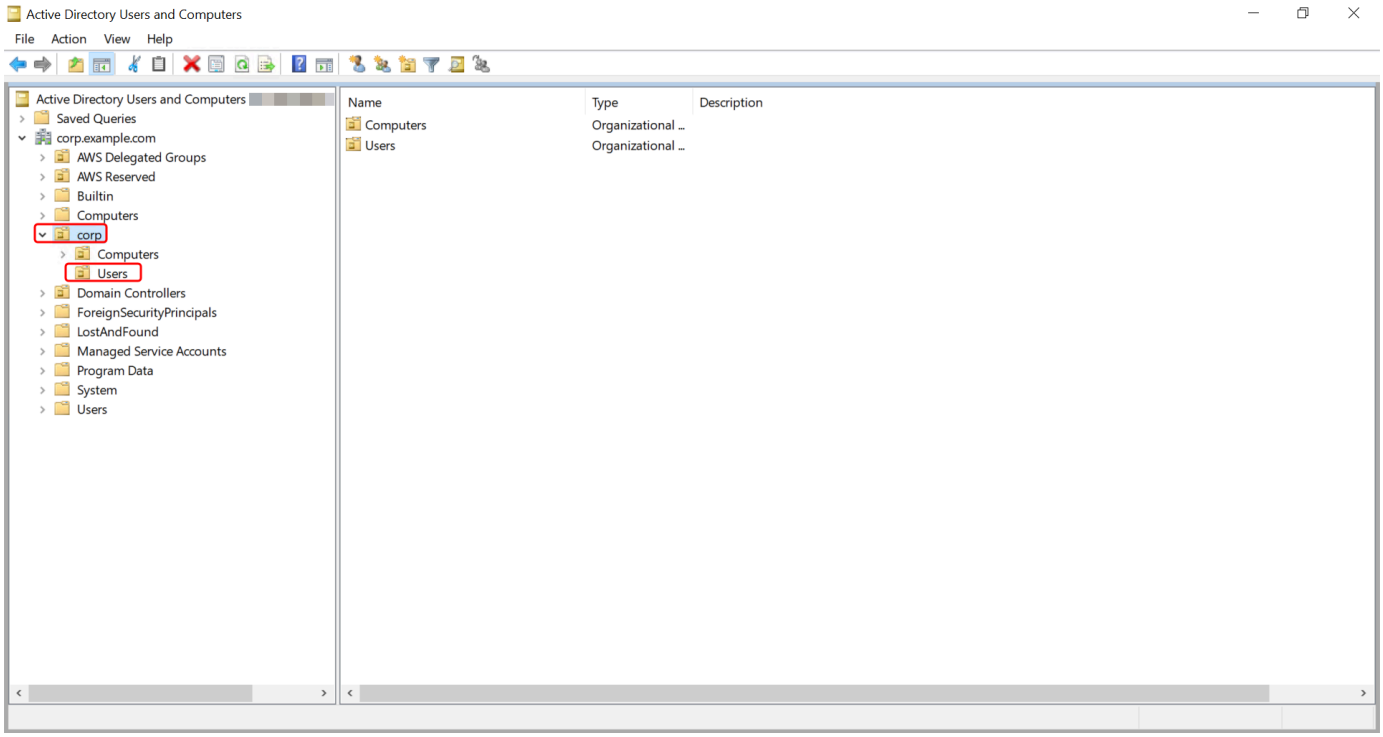
Utilizza la seguente procedura per creare un gruppo di sicurezza con un'istanza Amazon EC2 aggiunta alla tua directory Simple AD. Prima di poter creare gruppi di sicurezza, è necessario completare le procedure descritte in Installazione degli strumenti di amministrazione di Active Directory.

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, consulta. Cosa viene creato con AWS Managed Microsoft AD Active Directory



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

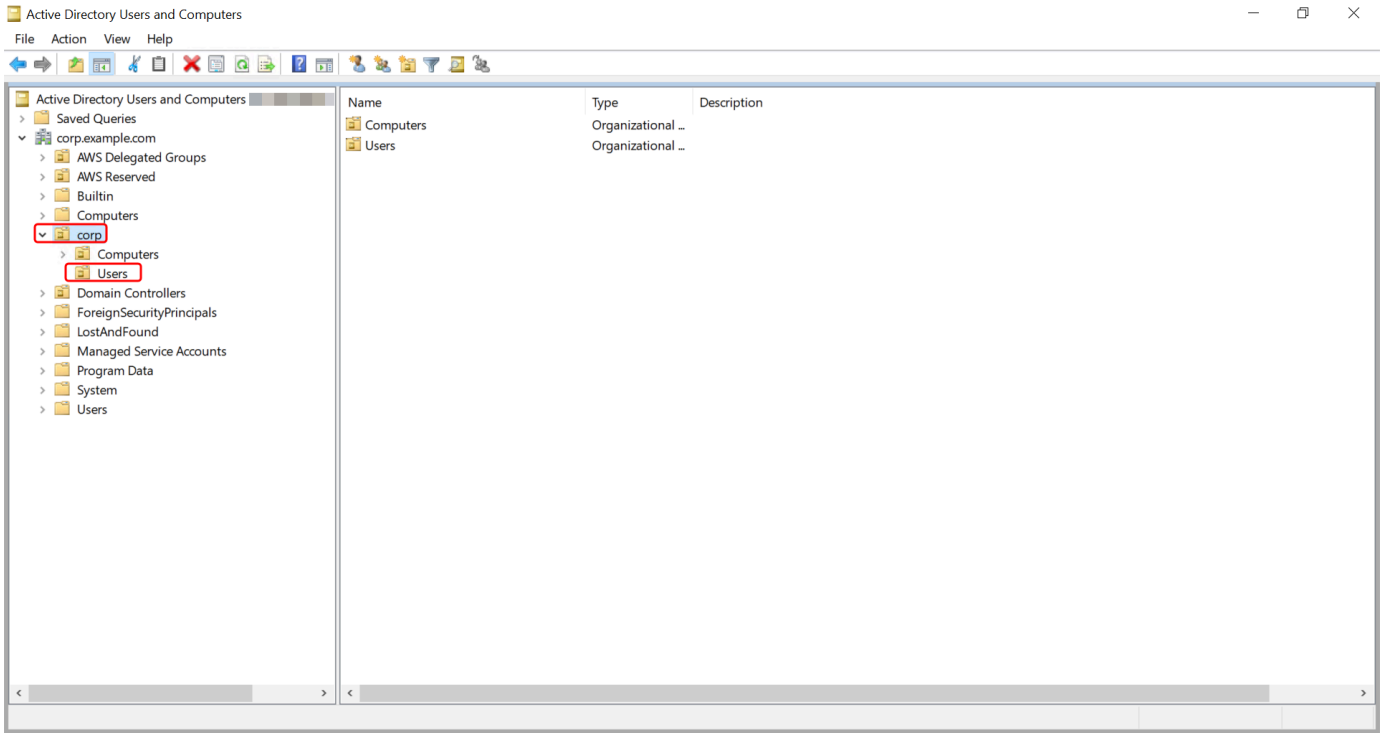
Utilizza la procedura seguente per aggiungere un utente a un gruppo di sicurezza con un'istanza EC2 aggiunta alla directory Simple AD.

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.

Monitoraggio della directory Simple AD

Puoi monitorare la directory Simple AD nei seguenti modi:

Argomenti

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 AWS 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 AWS Support.

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 la normale attività di manutenzione operativa, ad esempio applicazione di patch o la rotazione dell'istanza EC2, l'hot spotting temporaneo mediante un'applicazione su uno dei controller di dominio o modifiche apportate alla rete che interrompono inavvertitamente le comunicazioni di directory. 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 AWS Support.

> **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 Snapshot o ripristino della directory.

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 AWS Support.

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 Motivi dello stato della directory Simple AD.

Configura le notifiche sullo stato delle directory 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 AWS Directory Service come editore a un argomento di Amazon SNS. Quando AWS 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 AWS Management Console e apri la console.AWS 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 Crea.

Se desideri designare abbonati SNS aggiuntivi, ad esempio un indirizzo e-mail aggiuntivo, code Amazon SQS oppure AWS Lambda, puoi farlo dalla console Amazon SNS.

Per rimuovere i messaggi di stato della directory da un argomento

1. Accedi e apri la console. AWS Management ConsoleAWS Directory 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 messaggi AWS Directory Service, associa la directory a un argomento Amazon SNS diverso.

Unisci un'istanza Amazon EC2 al tuo Simple AD Active Directory

Puoi aggiungere facilmente un'istanza Amazon EC2 al Active Directory tuo dominio quando l'istanza viene lanciata. Per ulteriori informazioni, consulta Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo AWS Managed Microsoft AD Active Directory. Puoi anche avviare un'istanza EC2 e aggiungerla a un Active Directory dominio direttamente dalla AWS Directory Service console con Automation.AWS Systems Manager

Se devi aggiungere manualmente un'istanza EC2 al tuo Active Directory dominio, 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

- Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo Simple AD Active Directory
- Unisci manualmente un'istanza Windows di Amazon EC2 al tuo Simple AD Active Directory
- 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
- Delegazione dei privilegi di aggiunta della directory per Simple AD
- Creazione di un set di opzioni DHCP

Unisci senza problemi un'istanza Windows di Amazon EC2 al tuo Simple AD Active Directory

Questa procedura unisce senza problemi un'istanza Amazon EC2 Windows al tuo Simple AD Active Directory.

Per unirsi senza problemi a un'istanza EC2 per Windows

1. Accedi AWS Management Console e apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nella barra di navigazione, scegli la Regione AWS stessa cartella esistente.
3. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Windows EC2.
5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.
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.

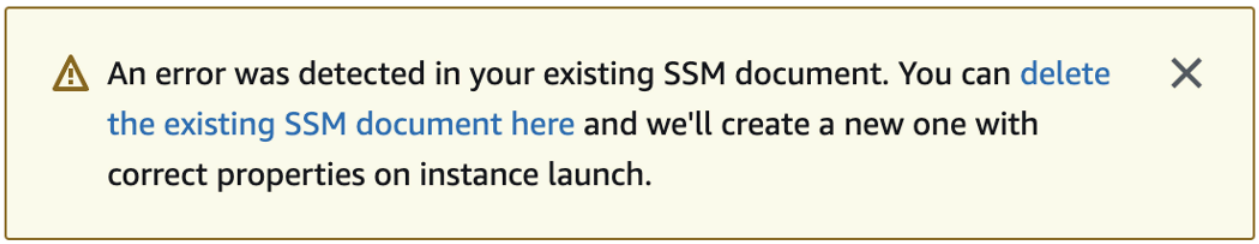
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

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 DirectoryServiceAccess associate le policy

AWS gestite AmazonSSM ManagedInstanceCore e AmazonSSM dall'elenco a discesa dei profili delle istanze 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. Per Use case (Caso d'uso), seleziona EC2.
4. In Aggiungi autorizzazioni, nell'elenco delle politiche, seleziona le politiche AmazonSSM e AmazonSSM. ManagedInstanceCore DirectoryServiceAccess Nella casella di ricerca, digita **`SSM`** per filtrare l'elenco. Seleziona Successivo.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un managed by. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 Creazione di un profilo dell'istanza IAM per Systems Manager nella Guida per l'utente di AWS Systems Manager .

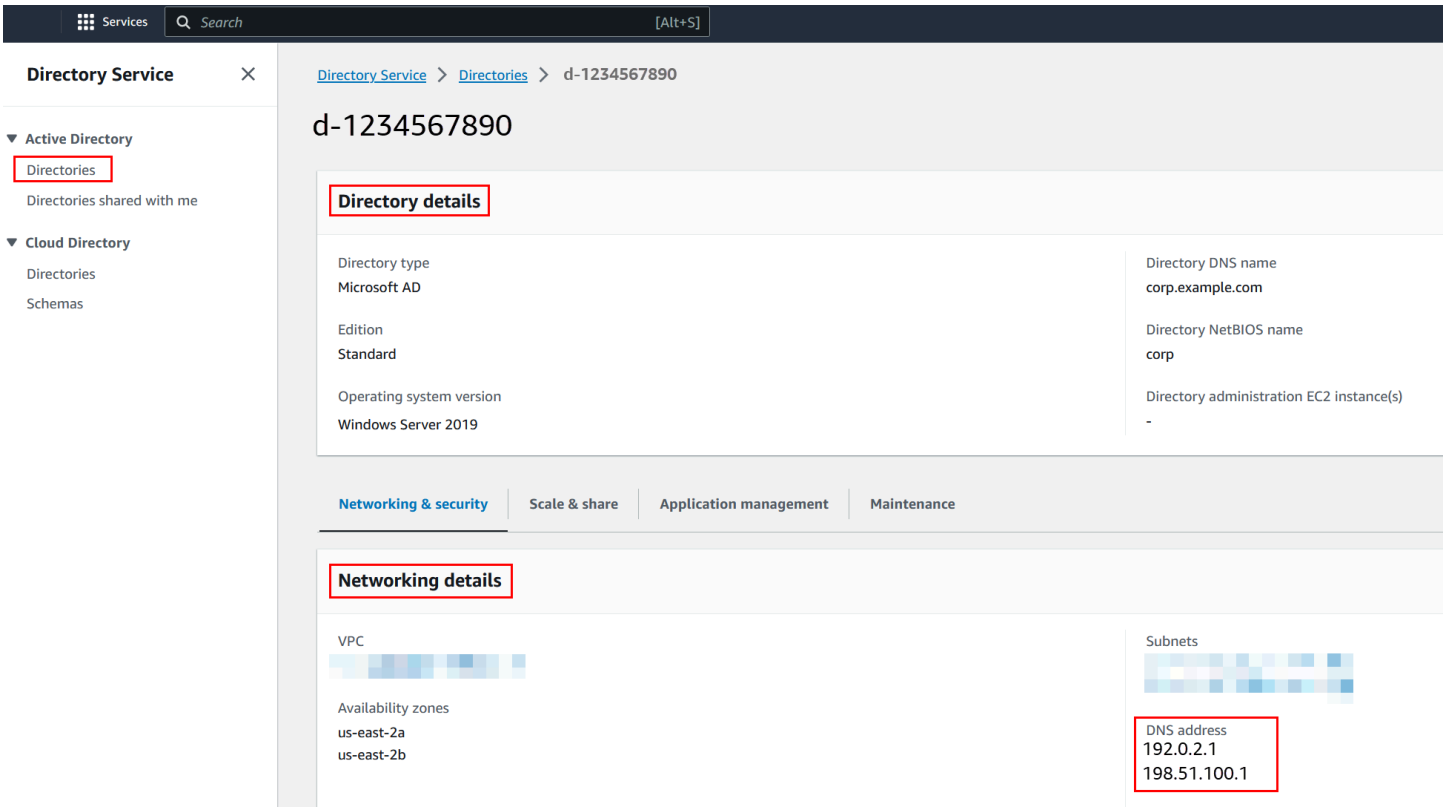
5. Nella pagina Denomina, rivedi e crea inserisci un Nome ruolo. È necessario aggiungere questo nome del ruolo all'istanza EC2.
6. (Facoltativo) Puoi fornire una descrizione del profilo dell'istanza IAM nel campo Descrizione.
7. Scegli Crea ruolo.
8. Torna alla pagina Avvia un'istanza e scegli l'icona 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).

Unisci manualmente un'istanza Windows di Amazon EC2 al tuo Simple AD Active Directory

Per unire manualmente un'istanza Amazon EC2 Windows esistente a un Simple AD Active Directory, l'istanza deve essere avviata utilizzando i parametri specificati in. Unisci senza problemi un'istanza Windows di Amazon EC2 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

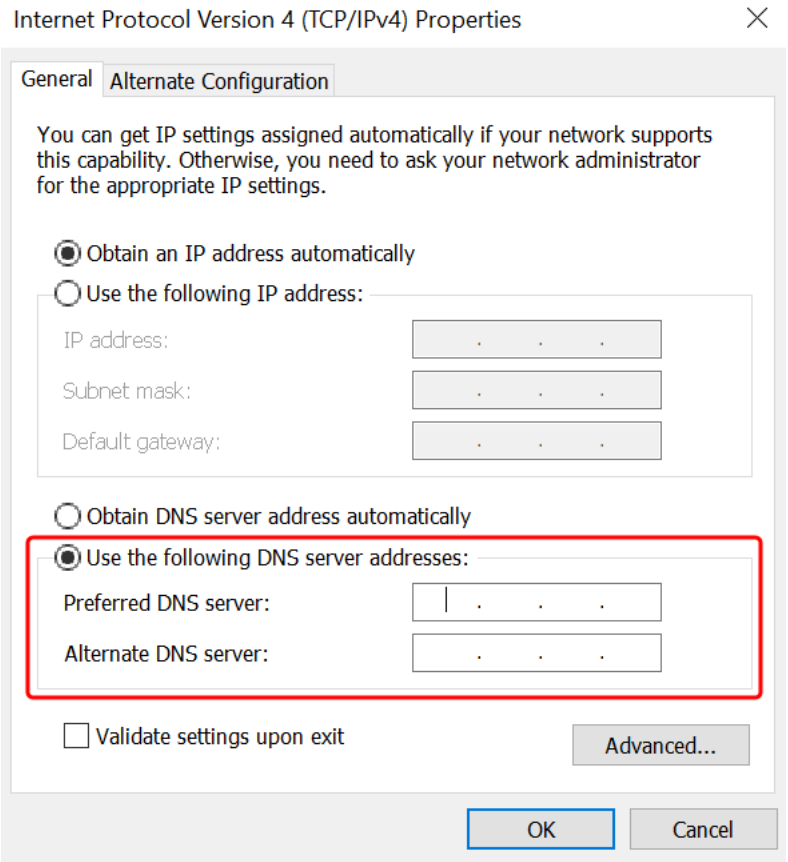
1. Connettiti all'istanza utilizzando qualsiasi client Remote Desktop Protocol.
2. Apri la finestra di dialogo delle proprietà TCP/IPv4 sull'istanza.
    a. Apri Network Connections (Connessioni di rete).

> **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 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 Delegazione dei privilegi di aggiunta della 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 Installare gli strumenti di amministrazione di Active Directory per Simple AD.

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 non supportano la funzionalità di aggiunta ottimizzata del dominio.

Prerequisiti

Prima di poter configurare un join di dominio senza interruzioni su un'istanza Linux, devi 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 AWS Secrets Manager per archiviare l'account del servizio di dominio.

Per creare segreti e archiviare le informazioni sull'account del servizio di dominio

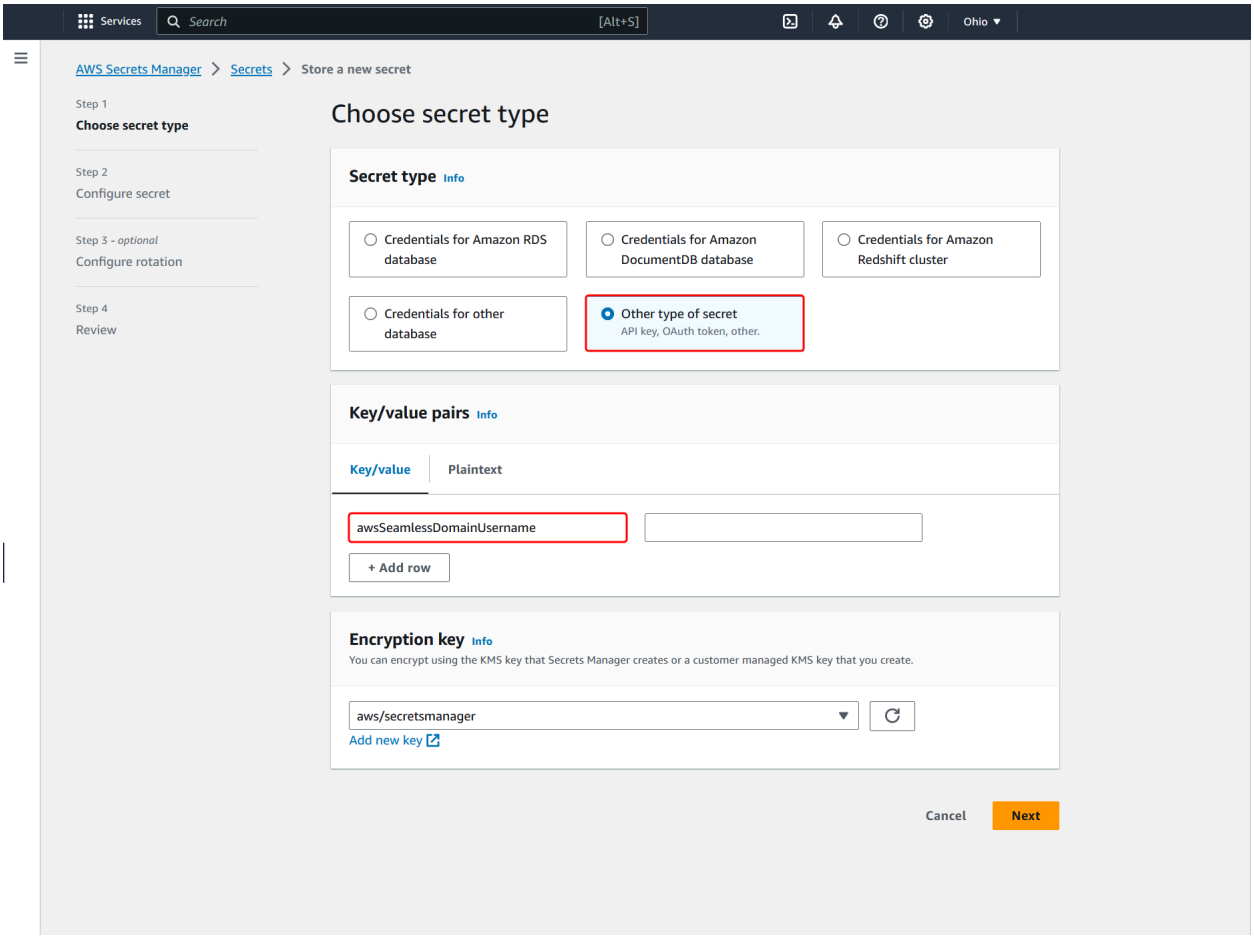
1. Accedi AWS Management Console e apri la AWS Secrets Manager console all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Archivia un nuovo segreto, procedere nel seguente modo:

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`. AWS Secrets Manager crittografa sempre il segreto quando scegli questa opzione. Puoi anche scegliere una chiave creata da te.

> **Note**
>
> Sono previste delle commissioni AWS Secrets Manager, a seconda del segreto utilizzato. Per l'elenco completo dei prezzi aggiornati, consulta la pagina dei prezzi AWS Secrets Manager.
> Puoi utilizzare la chiave AWS `aws/secretsmanager` gestita creata 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 attuale. AWS KMS Per ulteriori informazioni, consulta la sezione Prezzi di AWS Key Management Service.

v. Seleziona Successivo.

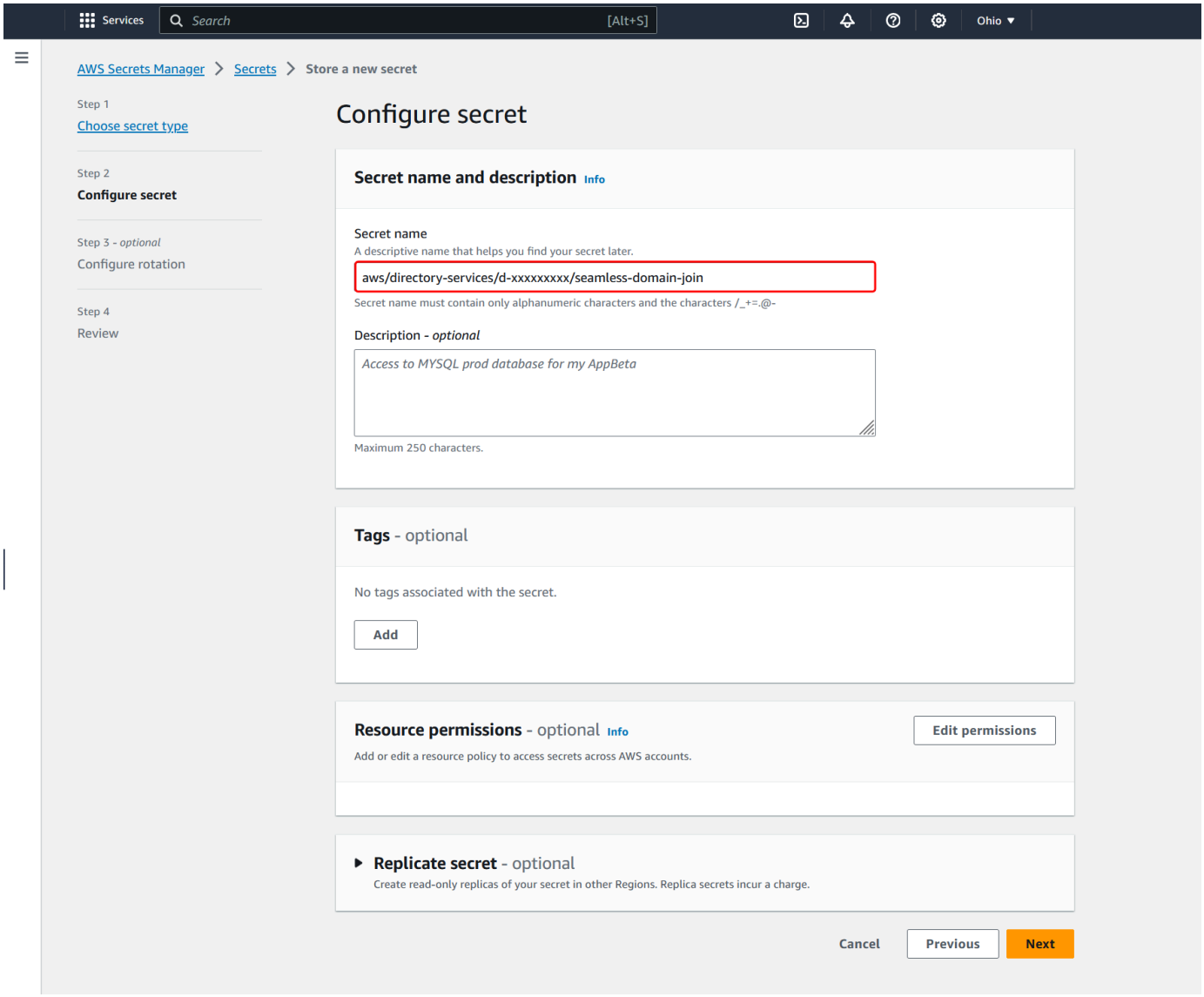
4. In Nome segreto, inserisci un nome segreto che includa l'ID della tua directory utilizzando il seguente formato, sostituendo *`d-xxxxxxxxx`* con il tuo ID di directory:

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

Questo nome viene utilizzato per recuperare i segreti nell'applicazione.

> **Note**
>
> Devi inserire **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** esattamente come è, e sostituire *`d-xxxxxxxxxx`* con l'ID della 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 AWS Secrets Manager i segreti nella Guida per l'AWS Secrets Manager utente.

  Per il passaggio 5, utilizzare il modello di rotazione Microsoft Active Directory credenziali nella Guida per l'AWS Secrets Manager utente.

  Per assistenza, consulta Risoluzione dei problemi di AWS Secrets Manager rotazione nella Guida per l'AWS Secrets Manager utente.

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 IAM in LinuxEC2. 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 AWS Management Console come utente autorizzato a creare policy IAM. 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.

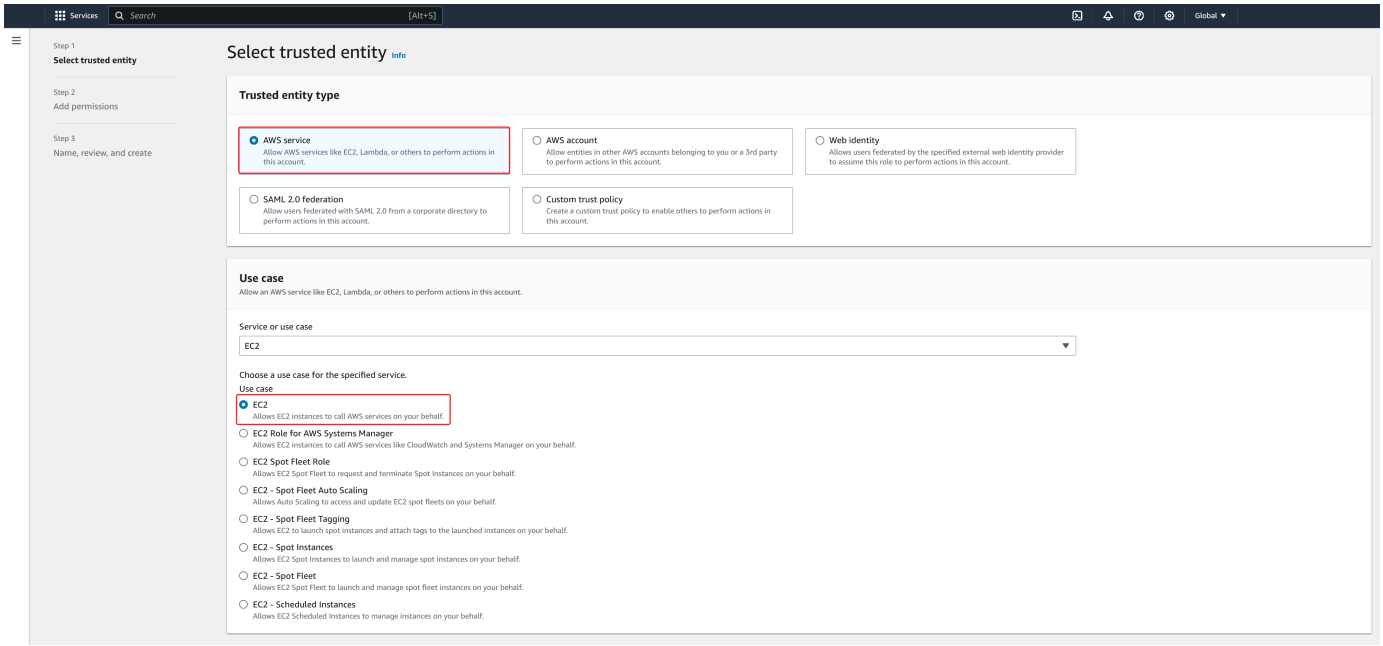
> **Note**
>
> Consigliamo di creare una policy per ogni segreto. In questo modo, ti assicuri che le istanze abbiano accesso solo al segreto in questione e riduci al minimo l'impatto se un'istanza viene compromessa.

Crea il ruolo LinuxEC2 DomainJoin

Utilizzi la console IAM per creare il ruolo che userai per aggiungere il dominio alla tua istanza EC2 Linux.

Per creare il ruolo LinuxEC2 DomainJoin

1. Accedi AWS Management Console come utente autorizzato a creare policy IAM. Apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel riquadro 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**
>
> AmazonSSM DirectoryServiceAccess fornisce le autorizzazioni per unire le istanze a un server gestito da. Active Directory AWS Directory Service AmazonSSM ManagedInstanceCore fornisce le autorizzazioni minime necessarie per utilizzare il servizio. 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 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`** 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

Ora che hai configurato tutte le attività prerequisite, puoi utilizzare la seguente procedura per unire senza problemi la tua istanza EC2 Linux.

Per unirti senza problemi alla tua istanza Linux

1. Accedi AWS Management Console e apri la console Amazon EC2 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. Nel Pannello di controllo EC2, nella sezione Avvia istanza, scegli Avvia istanza.
4. Nella pagina Avvia un'istanza, nella sezione Nome e tag, inserisci il nome che desideri utilizzare per la tua istanza Linux EC2.

5. (Facoltativo) Scegli Aggiungi tag aggiuntivo, per aggiungere una o più coppie tag chiave-valore per organizzare, monitorare o controllare l'accesso per questa istanza EC2.
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, consulta Installazione e configurazione dell'Agente SSM su istanze EC2 per Linux.
> SSM utilizza il `aws:domainJoin` plug-in per aggiungere un'istanza Linux a un dominio. Active Directory *`Il plugin cambia il nome host per le istanze Linux nel formato EC2AMAZ-XXXXXXX.`* Per ulteriori informazioni in merito*`aws:domainJoin`*, consultate il riferimento al plugin AWS Systems Manager Command Document nella Guida per l'utente.AWS Systems Manager

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.

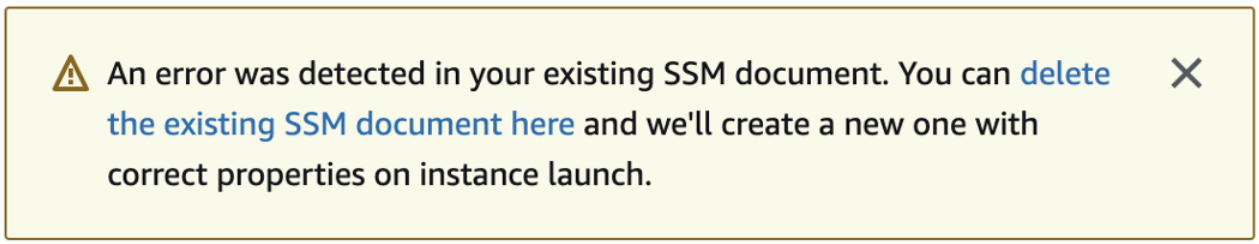
11. In Assegna automaticamente IP pubblico, scegli Abilita.

    Per ulteriori informazioni sull'indirizzamento IP pubblico e privato, consulta la sezione Indirizzamento IP delle istanze Amazon EC2 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 avvio di EC2 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'istanza EC2 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'istanza EC2.

15. Per il profilo dell'istanza IAM, scegli il ruolo IAM creato in precedenza nella sezione dei prerequisiti Fase 2: Creazione del ruolo LinuxEC2. 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 Windows di Amazon EC2, puoi aggiungere alcune istanze Amazon EC2 Linux alla tua 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 AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 informazioni su come determinare la versione di Amazon Linux in uso, consulta Identificazione delle immagini di Amazon Linux nella Guida per l'utente di Amazon EC2 per le istanze Linux.

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 dominio *example.com* che dispone di privilegi di aggiunta al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 dominio *example.com* che dispone di privilegi di aggiunta al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 dei server DNS dei server DNS forniti. AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 SAM AccountName per un account nel dominio *example.com* che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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 forniti. AWS 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 intendi configurarla manualmente, consulta Come assegnare un server DNS statico a un'istanza Amazon EC2 privata in AWS Knowledge Center per istruzioni sull'impostazione del server DNS persistente per la tua distribuzione e versione specifica di 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 SAM AccountName per un account nel dominio *example.com* che dispone dei privilegi di accesso al dominio. Inserisci la password dell'account quando richiesta. Per ulteriori informazioni sulla delega di questi privilegi, consulta Delegare i privilegi di aggiunta della directory per Microsoft AD gestito da AWS.

esempio.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. Impostare krb5_use_kdcinfo su False (Falso) nel file /etc/sssd/sssd.conf. Per 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. Per 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, OU è *Testou*.

dc

È il componente di dominio del tuo dominio. In questo esempio, *example* (esempio).

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 Windows e Security Identifier (SID). Active Directory

1. Centralizzato
2. Distribuito

> **Note**
>
> La mappatura centralizzata dell'identità degli utenti Active Directory richiede l'interfaccia del sistema operativo portatile o POSIX.

Mappatura centralizzata delle identità degli utenti

Active Directoryo un altro servizio LDAP (Lightweight Directory Access Protocol) fornisce UID e GID agli utenti Linux. InActive Directory, questi identificatori sono memorizzati negli attributi degli utenti:

- 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 da cui utilizzare l'UID e il GIDActive Directory, impostatelo `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 dispone dell'estensione POSIX o se si sceglie 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.

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%
```

Delegazione dei privilegi di aggiunta della 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.

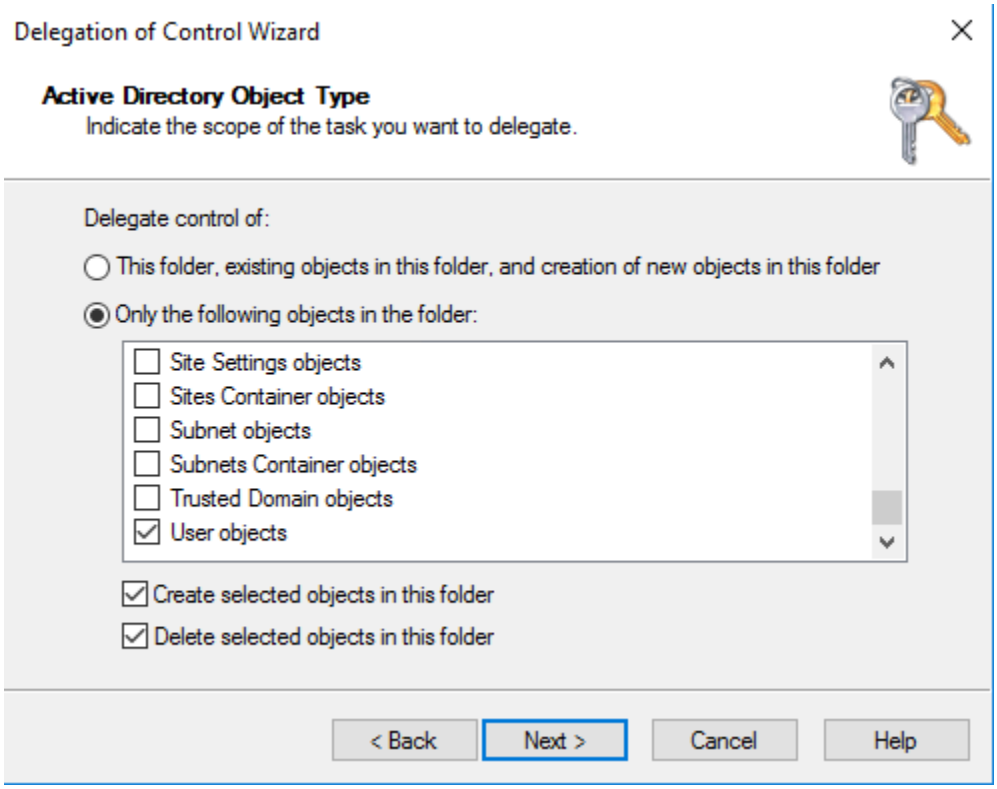
Tuttavia, come best practice, dovresti utilizzare un account che disponga solo dei privilegi minimi necessari. La seguente procedura mostra come creare un nuovo gruppo denominato `Joiners` e delegare i privilegi necessari a questo gruppo per aggiungere i computer alla directory.

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.

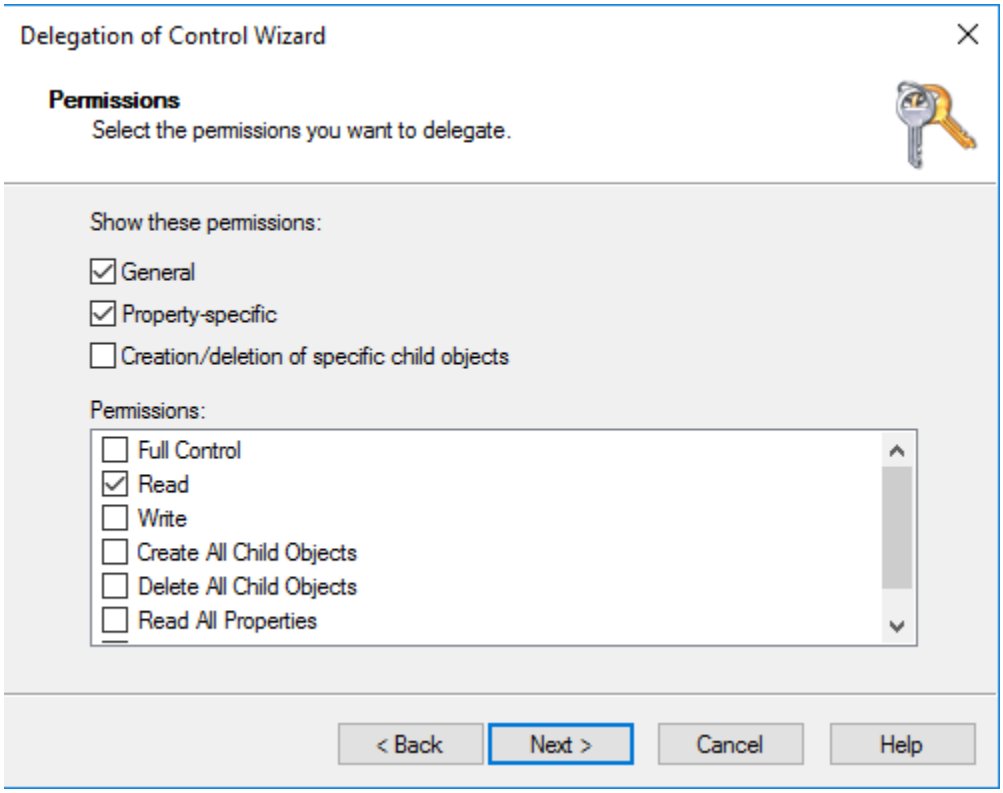
Per delegare i privilegi di aggiunta per Simple AD

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. Seleziona 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. AWS Directory Service

Creazione di un set di opzioni DHCP

AWS consiglia di creare un set di opzioni DHCP per la AWS 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 alla 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. Annota l'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. Accedere alla console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.

2. Nel pannello di navigazione scegliere Your VPCs (I tuoi VPC).
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 della directory Simple AD

In questa sezione viene descritto come gestire le attività amministrative più comuni per l'ambiente Simple AD.

Argomenti

Eliminazione del 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.

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 Active Directory è installato il tuo. 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 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 AWS app e servizi, puoi vedere quali AWS applicazioni sono abilitate per la tua directory.

- Disabilita AWS Management Console l'accesso. Per ulteriori informazioni, consulta Disabilita l'accesso alla AWS Management Console..
- Per disabilitare Amazon WorkSpaces, devi annullare la registrazione del servizio dalla directory nella WorkSpaces console. Per ulteriori informazioni, consulta Annullamento della registrazione da una directory nella Amazon WorkSpaces Administration Guide.
- Per disabilitare Amazon WorkDocs, devi eliminare il WorkDocs sito Amazon nella WorkDocs console Amazon. 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 per Windows File Server, devi rimuovere il file system Amazon FSx dal dominio. Per ulteriori informazioni, consulta Lavorare con Active Directory FSx for Windows File Server nella Guida per l'utente di Amazon FSx for Windows File Server.
- 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 Active DirectoryAuthentication nella AWS Client VPN Administrator Guide.
- Per disabilitare Amazon Connect, è necessario eliminare l'istanza di Amazon Connect. Per ulteriori informazioni, consulta Eliminazione di un'istanza Amazon Connect nella Guida all'amministrazione di Amazon Connect.
- Per disattivare Amazon QuickSight, devi annullare l'iscrizione ad Amazon QuickSight. Per ulteriori informazioni, consulta la sezione Chiusura Amazon QuickSight dell'account nella Amazon QuickSight User Guide.

> **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.

Snapshot o ripristino della directory

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
- 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 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 AWS Support 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 che tu capisca che tutti i DC e i server DNS associati con la directory saranno offline fino a quando l'operazione di ripristino non sia stata completata.

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).

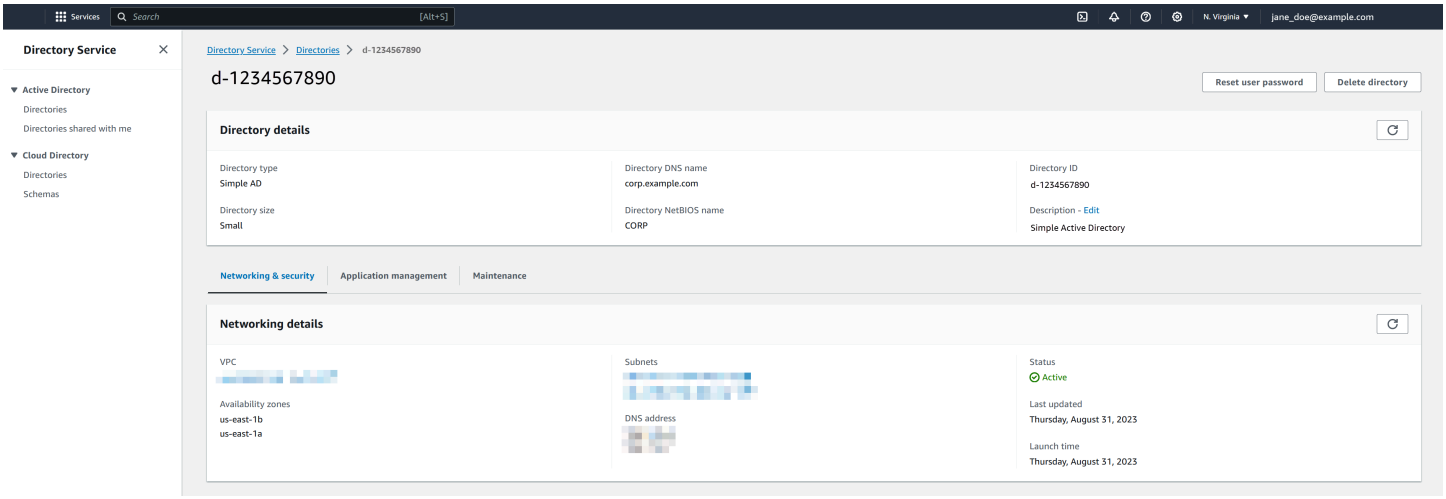
Visualizzazione delle informazioni sulla directory

Puoi visualizzare informazioni dettagliate su una directory.

Per visualizzare informazioni dettagliate sulla directory

1. Nel riquadro di navigazione della AWS Directory Service console, sotto Active Directory, seleziona Directory.
2. Fai clic sul link dell'ID directory della 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.



Consentire l'accesso ad AWS applicazioni e servizi

Gli utenti possono autorizzare Simple AD a fornire ad AWS applicazioni e servizi, come Amazon WorkSpaces, l'accesso al tuoActive Directory. Le seguenti AWS applicazioni e servizi possono essere abilitati o disabilitati per funzionare con Simple AD.

AWS applicazione/servizio	Ulteriori informazioni…
Amazon Chime	Per ulteriori informazioni, consulta la Guida all'amministrazione di Amazon Chime.
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.

AWS applicazione/servizio	Ulteriori informazioni…
AWS Management Console	Per ulteriori informazioni, consulta Abilitazione dell'accesso a AWS Management Console con le credenziali AD.

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 AWS 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 serviziAWS .

Per ulteriori informazioni su come autorizzare o rimuovere l'autorizzazione all'utilizzo AWS Directory Servicedi AWS applicazioni e servizi, vedere. Autorizzazione per l'utilizzo di AWS applicazioni e servizi AWS Directory Service

Argomenti

- Creazione di un URL di accesso
- Autenticazione unica

Creazione di un URL di accesso

Un URL di accesso viene utilizzato con applicazioni e servizi AWS, come Amazon WorkDocs per raggiungere una pagina di accesso che è associata con la 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.

Creazione di 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.

Autenticazione unica

AWS Directory Service offre la possibilità di consentire agli utenti di accedere ad Amazon WorkDocs da un computer collegato 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 AWS 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 Amazon 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 Amazon. 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.
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 desideri disabilitare il Single Sign-On con Amazon WorkDocs, scegli Disabilita, quindi nella finestra di dialogo Disabilita il Single Sign-On per questa directory, scegli 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://*<aliases>*.awsapps.com) all'elenco dei siti approvati per l'accesso 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. 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:

Action

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Path

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

Il valore di *<alias>* deriva dall'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:

Action

```
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 permettere al browser Firefox di Mozilla di supportare l'accesso single sign-on, aggiungi l'URL di accesso (ad esempio, https://*<alias>*.awsapps.com) all'elenco dei siti approvati per l'accesso 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, vai a https://support.mozilla.org/en-US/questions/939037.

Abilitazione dell'accesso alla AWS Management Console con le credenziali AD

AWS Directory Service consente di concedere l'accesso alla AWS Management Console ai membri della directory. Per impostazione predefinita, i membri della directory non hanno accesso a nessuna risorsa AWS. Puoi assegnare ruoli IAM ai membri della directory per consentirgli l'accesso ai vari servizi e risorse AWS. 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. Per ulteriori informazioni su come creare un URL di accesso, consulta Creazione di un URL di accesso.

Per ulteriori informazioni su come creare e assegnare ruoli IAM ai membri della directory, consulta Concessione dell'accesso alle risorse AWS a utenti e gruppi.

Argomenti

- Abilitazione dell'accesso alla AWS Management Console
- Disabilita l'accesso alla AWS Management Console
- Impostazione della durata della sessione di accesso

Articolo correlato del Blog di AWS sulla sicurezza

- Come accedere alla AWS Management Console tramite Microsoft AD gestito da AWS e le credenziali on-premise

Abilitazione dell'accesso alla AWS Management Console

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 AWS Management Console, scegli Abilita. Ora l'accesso alla console è abilitato per la tua directory.

   Prima che gli utenti possano accedere alla console con il tuo URL di accesso, devi aggiungere gli utenti al ruolo. Per ulteriori informazioni sull'assegnazione di ruoli IAM agli utenti, consulta Assegnazione di utenti o gruppi a un ruolo 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 della directory è example-corp.awsapps.com, l'URL per accedere alla console sarà https://example-corp.awsapps.com/console/.

Disabilita l'accesso alla AWS Management Console

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 AWS Management Console, 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 risorse AWS, seleziona 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).

Tutorial: Creare un Simple AD Active Directory

Il seguente tutorial illustra tutti i passaggi necessari per configurare un Simple AD Active Directory. È stato progettato per consentirti di iniziare a usare Simple AD Active Directory in modo rapido e semplice, ma non è destinato all'uso in un ambiente di produzione su larga scala.

Prerequisiti dei tutorial

Questo tutorial presuppone quanto segue:

- Hai un attivo Account AWS.
- Il tuo account non ha raggiunto il limite di Amazon VPC 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`

Per ulteriori informazioni, consulta Prerequisiti di Simple AD.

Fase 1: Crea e configura Amazon VPC for Simple AD Active Directory

Crea e configura un Amazon VPC da utilizzare con Simple AD. Prima di iniziare la procedura, assicurati di soddisfare i Prerequisiti dei tutorial.

Crea un VPC per il tuo Simple AD Active Directory

Crea un VPC con due sottoreti pubbliche. AWS Directory Service richiede due sottoreti nel VPC e ogni sottorete deve trovarsi in una zona di disponibilità diversa.

1. Apri alla 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 CIDR IPv4 dovrebbe essere `10.0.0.0/16`.
    - Mantieni selezionata l'opzione Nessun blocco CIDR IPv6.

- La Tenancy deve rimanere Predefinita.
- Seleziona 2 in Numero di zone di disponibilità (AZ).
- 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.

Passaggio 2: crea il tuo Simple AD Active Directory

Per creare un nuovo Simple AD Active Directory, effettuate le seguenti operazioni. Prima di iniziare questa procedura, assicurati di aver completato i prerequisiti identificati nella Prerequisiti dei tutorial Fase 1: Crea e configura Amazon VPC for Simple AD. Active Directory

Per creare un Simple AD Active Directory

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 si crea la 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. Il processo di creazione della directory crea un account amministratore con il 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.

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).

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

AWS 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 il tuo locale esistente Active Directory 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 e a basso costo con compatibilità di baseActive 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 AWS Directory Service opzioni, consulta. Quale scegliere

Verifica che i VPC e le istanze siano configurati correttamente

Per gestire, utilizzare e connetterti alle directory, è necessario configurare correttamente i VPC ai quali sono associate le directory. Consulta AWS Prerequisiti Microsoft AD gestiti, 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 Unisci un'istanza Amazon EC2 al tuo Managed AWS Microsoft AD Active Directory.

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 di AWS 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

Se desideri modificare la sicurezza dei gruppi di sicurezza delle directory, puoi farlo. Apporta tali modifiche solo se hai compreso a pieno come funziona il filtraggio del gruppo di sicurezza. Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon EC2 per le istanze Linux nella Guida per l'utente di Amazon EC2. Modifiche improprie possono causare la perdita delle comunicazioni verso 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**
>
> Tecnicamente, hai la possibilità di associare il gruppo di sicurezza della directory ad altre istanze EC2 da te create. 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, associare il gruppo di sicurezza della directory alle istanze EC2 può creare un potenziale rischio per la sicurezza per le istanze EC2.

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 AWS 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

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, come WorkSpaces Amazon WorkMail, WorkDocs Amazon o Amazon. QuickSight 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 (DC). 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 associ l'applicazione a un DC fisso e si deve applicare una patch o eseguire una procedura di ripristino, l'applicazione perde l'accesso al DC e non utilizza uno dei DC restanti. 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 è inoltre possibile che l'automazione delle AWS directory contrassegni la directory come compromessa 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 AWS Directory Service Microsoft Active Directory, che consente di aggiungere controller di dominio per prestazioni elevate. Per ulteriori informazioni, consulta Distribuzione di controller di dominio aggiuntivi.

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.

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 dimensionamento più flessibili e caratteristiche Active Directory aggiuntive, puoi utilizzare il Servizio di directory AWS 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 all'interfaccia di rete elastica AWS (ENI).

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 del gran numero di applicazioni personalizzate e commerciali predefinite che utilizzano Active Directory, AWS non esegue e non può eseguire la verifica formale o generale della compatibilità delle applicazioni di terze parti con Simple AD. Sebbene AWS collabori con i clienti nel tentativo di superare i potenziali problemi di installazione delle applicazioni, non siamo in grado di garantire la compatibilità corrente o futura di una determinata applicazione 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 Foundation 2010
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

I clienti possono scegliere di utilizzare il Servizio di directory AWS per Microsoft Active Directory (AWS Microsoft AD gestito) per un livello più elevato di compatibilità basato su Active Directory.

Risoluzione dei problemi di Simple AD

Quanto segue può aiutarti a risolvere alcuni problemi comuni che potrebbero verificarsi durante la creazione o l'utilizzo della tua directory.

Argomenti

Recupero della password

Se un utente dimentica una password o ha problemi di accesso alla directory Simple AD o AWS Managed Microsoft AD, puoi reimpostare la password utilizzando il AWS Management Console, Windows PowerShell o il AWS CLI.

Per ulteriori informazioni, consulta Reimpostazione di una password utente Simple AD.

Ricevo un messaggio di errore "KDC non è in grado di soddisfare l'opzione richiesta" durante l'aggiunta di un utente a Simple AD

Questo si può verificare quando il client Samba CLI non invia correttamente i comandi "net" a tutti i controller di dominio. Se viene visualizzato questo messaggio di errore quando si usa il comando "net ads" per aggiungere un utente alla directory Simple AD, utilizzare l'argomento -S 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 Installare gli 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 posso accedere a SQL Server utilizzando un account SQL Server

Potresti ricevere un messaggio di 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 EC2 Windows 2012 R2. Il problema si verifica quando SSMS viene eseguito come utente del dominio e può causare l'errore "Accesso non riuscito per l'utente", anche quando vengono fornite credenziali valide. Si tratta di un problema noto e AWS si sta lavorando attivamente per risolverlo.

Per ovviare al problema, accedere a SQL Server con l'autenticazione di Windows anziché quella SQL. In alternativa, puoi avviare SSMS come utente locale anziché come utente di dominio Simple AD.

La mia directory è bloccata nello stato "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 il centro AWS Support.

Visualizzo un messaggio di errore "AZ vincolata" quando creo una directory

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 AWS Directory Service le directory. 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 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 dovrebbe essere modificata. Per ulteriori informazioni su questa impostazione, vai a Preautenticazione su Microsoft TechNet.

Risorse aggiuntive

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

- AWS Knowledge Center: trova domande frequenti e collegamenti ad altre risorse per aiutarti a risolvere i problemi.
- AWS Centro assistenza: ottieni supporto tecnico.
- AWS Premium Support Center: ottieni supporto tecnico premium.

Argomenti

Motivi dello stato della directory Simple AD

Quando una directory è danneggiata o inutilizzabile, il messaggio di stato della directory contiene ulteriori informazioni. Il messaggio di stato viene visualizzato nella console AWS Directory Service o restituito nel membro `DirectoryDescription.StageReason` tramite l'API `DescribeDirectories`. Per ulteriori informazioni sugli stati della directory, consulta Comprendere lo stato della directory.

Di seguito sono riportati i messaggi di stato di una directory Simple AD:

Argomenti

- L'utente riservato del AWS Directory Service principale deve appartenere al gruppo di amministratori di dominio
- L'utente riservato del AWS Directory Service principale è disabilitato
- Il controller di dominio principale non dispone di tutti i ruoli FSMO
- Errori di replica del controller di dominio

L'interfaccia di rete elastica del servizio di directory non è collegata

Descrizione

L'interfaccia di rete elastica (ENI) principale 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. Le applicazioni AWS 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 AWS Support. 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 il AWS Support per ricevere assistenza.

L'utente riservato del AWS Directory Service principale non è presente nella directory

Descrizione

Quando viene creato un Simple AD, il AWS Directory Service crea un account di servizio nella directory con il nome `AWSAdmin`*`D-xxxxxxxxxx`*. Questo errore viene restituito quando è

impossibile individuare l'account del servizio. Senza questo account, AWS 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 riservato del AWS Directory Service principale deve appartenere al gruppo di amministratori di dominio

Descrizione

Quando viene creato un Simple AD, il AWS 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 fornire a AWS Directory Service i privilegi necessari per eseguire le operazioni di manutenzione e di ripristino, come il trasferimento di ruoli FSMO, l'aggiunta al dominio di nuovi controller della directory e il ripristino da snapshot.

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 del AWS Directory Service principale è disabilitato

Descrizione

Quando viene creato un Simple AD, il AWS 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 che AWS Directory Service sia in grado di eseguire le operazioni di manutenzione e di 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 AWS 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, consulta https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. Se il problema persiste, contatta AWS Support per 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.
- Le liste di controllo degli accessi di rete sono troppo restrittive.
- 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 AWS Prerequisiti Microsoft AD gestiti, 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 AWS Support 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. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per ulteriori informazioni sui programmi di conformità applicabili AWS Directory Service, consulta AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS Directory Service. Negli argomenti seguenti viene illustrato come eseguire la configurazione AWS Directory Service per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS 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 AWS 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

- Autorizzazioni per l'account Administrator
- Account del servizio gestito del gruppo
- Creazione di una relazione di trust
- Delega vincolata Kerberos
- Concessione dell'accesso alle risorse AWS a utenti e gruppi
- Autorizzazione per l'utilizzo di AWS applicazioni e servizi AWS Directory Service

Protezione della directory

- Protezione di una directory Microsoft AD gestito da AWS
- Protezione della directory AD Connector

Registrazione e monitoraggio

- Monitora Microsoft AD gestito da AWS
- Monitoraggio della directory AD Connector

Resilienza

- Applicazione di patch e manutenzione per Microsoft AD gestito da AWS

Gestione delle identità e degli accessi per AWS Directory Service

L'accesso a AWS 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. AWS Directory Service Le seguenti sezioni forniscono dettagli su come utilizzare AWS Identity and Access Management (IAM) e su come AWS 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. AWS Directory Service Ad esempio, è necessario disporre delle autorizzazioni per creare una AWS Directory Service directory o per creare uno snapshot della directory.

Le seguenti sezioni descrivono come gestire le autorizzazioni per. AWS Directory Service Consigliamo di leggere prima la panoramica.

- Panoramica della gestione delle autorizzazioni di accesso alle risorse AWS Directory Service
- Utilizzo di politiche basate sull'identità (politiche IAM) per AWS Directory Service
- AWS Directory Service Autorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Panoramica della gestione delle autorizzazioni di accesso alle risorse AWS Directory Service

Ogni AWS risorsa è di proprietà di un AWS account e le autorizzazioni per creare o accedere alle risorse sono regolate da politiche di autorizzazione. Un amministratore di account può allegare politiche di autorizzazione alle identità IAM (ovvero utenti, gruppi e ruoli) e alcuni servizi (come AWS Lambda) supportano anche l'associazione di politiche di autorizzazione alle risorse.

> **Note**
>
> Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consultare la sezione best practice IAM nella Guida per l'utente IAM.

Argomenti

- AWS Directory Service risorse 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

AWS Directory Service risorse e operazioni

In AWS Directory Service, la risorsa principale è una directory. AWS Directory Service supporta anche le risorse relative agli snapshot delle directory. Tuttavia, puoi creare snapshot solo nel contesto di una directory esistente. Pertanto, una snapshot è nota come subresource.

Alle risorse sono associati nomi Amazon Resource Name (ARN) univoci, come illustrato nella tabella seguente.

Tipo di risorsa	Formato ARN
Directory	`arn:aws:ds:` *`region`*`:`*`account-id`* `:directory/` *`external-directory-id`*
Snapshot	`arn:aws:ds:` *`region`*`:`*`account-id`* `:snapshot/` *`external-snapshot-id`*

AWS Directory Service 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.

Informazioni sulla proprietà delle risorse

Il proprietario della risorsa è l' AWS account che ha creato una risorsa. Cioè, il proprietario della risorsa è l' AWS account 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 AWS Directory Service risorsa, ad esempio una directory, l' AWS account è il proprietario di quella risorsa.
- Se crei un utente IAM nel tuo AWS account e concedi le autorizzazioni per creare AWS Directory Service risorse a quell'utente, anche l'utente può creare AWS 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 AWS Directory Service risorse, chiunque possa assumere il ruolo può creare AWS Directory Service risorse. Il tuo AWS account, a cui appartiene il ruolo, possiede le AWS 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 di AWS Directory 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. AWS Directory Service supporta solo politiche basate sull'identità (politiche IAM).

Argomenti

- Policy basate su identità (policy IAM)
- Policy basate su risorse

Policy basate su identità (policy IAM)

Puoi 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 AWS 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 AWS 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 AWS Directory Service risorse di proprietà dell'account.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni sull'utilizzo di politiche basate sull'identità con, vedere. AWS Directory ServiceUtilizzo di politiche basate sull'identità (politiche IAM) per AWS 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 su 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. AWS Directory Service non supporta politiche basate sulle risorse.

Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità

Per ogni AWS Directory Service risorsa, il servizio definisce una serie di operazioni API. Per ulteriori informazioni, consulta AWS Directory Service risorse 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, AWS 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 AWS Directory Service le risorse, usi sempre il carattere jolly (*) nelle policy IAM. Per ulteriori informazioni, consulta AWS Directory Service risorse 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 AWS 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). AWS Directory Service non 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 AWS Directory Service API e le risorse a cui si applicano, consulta. AWS Directory Service Autorizzazioni 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 AWS 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.

Utilizzo di politiche basate sull'identità (politiche IAM) per AWS 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.

> **Important**
>
> Ti consigliamo di esaminare innanzitutto gli argomenti introduttivi che spiegano i concetti e le opzioni di base disponibili per gestire l'accesso alle tue risorse. AWS Directory Service Per ulteriori informazioni, consulta la pagina Panoramica della gestione delle autorizzazioni di accesso alle risorse AWS Directory Service.

In questa sezione vengono trattati gli argomenti seguenti:

- Autorizzazioni necessarie per utilizzare la console AWS Directory Service
- AWS politiche gestite (predefinite) per AWS Directory Service
- Esempi di policy gestite dal cliente
- Utilizzo dei tag con policy IAM

Di seguito viene illustrato un esempio di policy di autorizzazione.

```
{
   "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": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

La policy include quanto segue.

- La prima istruzione concede il permesso di creare una directory. AWS Directory Service AWS Directory Service non supporta le autorizzazioni per questa particolare azione a livello di risorsa. e di conseguenza la policy specifica una carattere jolly (*) come valore di `Resource`.

- La seconda istruzione concede autorizzazioni a determinate operazioni IAM. L'accesso alle azioni IAM è necessario per AWS Directory Service poter 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 set specifico di risorse Amazon EC2 necessarie per AWS Directory Service consentire la creazione, la configurazione e la distruzione delle relative directory. Il carattere jolly (*) alla fine del valore `Resource` indica che l'istruzione concede l'autorizzazione alle operazioni EC2 su qualsiasi risorsa EC2 o sottorisorsa. Per limitare questa autorizzazione a un ruolo specifico, sostituisci il carattere jolly (*) nell'ARN della risorsa con la risorsa o sottorisorsa specifica. Per ulteriori informazioni, consulta Operazioni di Amazon EC2

La policy non specifica l'elemento `Principal` poiché in una policy basata su identità l'entità che ottiene l'autorizzazione non viene specificata. Quando si collega una policy a un utente, quest'ultimo è l'entità implicita. 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 AWS Directory Service API e le risorse a cui si applicano, consulta. AWS Directory Service Autorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Autorizzazioni necessarie per utilizzare la console AWS Directory Service

Affinché un utente possa utilizzare la AWS 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. AWS politiche gestite (predefinite) per AWS 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.

AWS politiche gestite (predefinite) per AWS Directory Service

AWS affronta molti casi d'uso comuni fornendo policy IAM autonome create e amministrate da. AWS Le policy gestite concedono le autorizzazioni necessarie per i casi di utilizzo comune in modo da non dover cercare quali sono le autorizzazioni richieste. Per ulteriori informazioni, consultare Policy gestite da AWS nella Guida per l'utente di IAM.

Le seguenti politiche AWS gestite, che puoi allegare agli utenti del tuo account, sono specifiche per AWS Directory Service:

- AWSDirectoryServiceReadOnlyAccess— Concede a un utente o a un gruppo l'accesso in sola lettura a tutte le AWS Directory Service risorse, le sottoreti EC2, le interfacce di rete EC2 e gli argomenti e gli abbonamenti di Amazon Simple Notification Service (Amazon SNS) per l'account root. AWS Per ulteriori informazioni, consulta Utilizzo delle policy gestite di AWS con AWS Directory Service.
- AWSDirectoryServiceFullAccess: concede a un utente o a un gruppo quanto segue:
  - Accesso completo a AWS Directory Service
  - Accesso ai principali servizi Amazon EC2 necessario per l'uso AWS Directory Service
  - Possibilità di elencare argomenti di Amazon SNS
  - Possibilità di creare, gestire ed eliminare argomenti di Amazon SNS con un nome che inizia con «» DirectoryMonitoring

  Per ulteriori informazioni, consulta Utilizzo delle policy gestite di AWS con AWS Directory Service.

Inoltre, esistono altre policy AWS gestite adatte all'uso con altri ruoli IAM. Queste politiche vengono assegnate ai ruoli associati agli utenti nella AWS Directory Service directory. Queste policy sono necessarie per consentire a tali utenti di accedere ad altre AWS risorse, come Amazon EC2. Per ulteriori informazioni, consulta Concessione dell'accesso alle risorse AWS a utenti e gruppi.

Puoi anche creare policy IAM personalizzate che consentono agli utenti di accedere alle operazioni e risorse API richieste. Puoi collegare queste policy personalizzate agli utenti o ai gruppi IAM che richiedono le autorizzazioni.

Esempi di policy gestite dal cliente

In questa sezione, puoi trovare esempi di politiche utente che concedono autorizzazioni per varie AWS Directory Service azioni.

> **Note**
>
> Tutti gli esempi utilizzano la regione Stati Uniti occidentali (Oregon) (`us-west-2`) e contengono ID account fittizi.

Esempi

- Esempio 1: consentire a un utente di eseguire qualsiasi azione Descrivi su qualsiasi risorsa AWS 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 AWS Directory Service

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 AWS 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 AWS Directory Service risorse di proprietà dell'account.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

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. Per farlo, sono necessarie anche le autorizzazioni per determinati servizi Amazon EC2.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
```

```
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
          "Resource":"*"
          ]
       }
   ]
}
```

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. AWS 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 AWS 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.

Il seguente esempio di policy di tag consente tutte le chiamate `ds` purché contengano il tag coppia chiave-valore "`fooKey`"."`fooValue`".

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Il seguente esempio di policy della risorsa consente tutte le chiamate `ds` purché la risorsa contenga l'ID directory "`d-1234567890`".

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
```

```
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Per ulteriori informazioni sugli ARN, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

Il seguente elenco di operazioni AWS 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

AWS Directory Service Autorizzazioni 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 AWS Directory Service Autorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni come riferimento. Ogni voce API nella include quanto segue:

- Nome dell'operazione AWS Directory Service API
- Le operazioni corrispondenti per le quali è possibile concedere le autorizzazioni per eseguire l'operazione
- La AWS risorsa per la quale 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 AWS Directory Service API non pubbliche come`ds:AuthorizeApplication`,,`ds:CheckAlias`, `ds:CreateIdentityPoolDirectory` `ds:GetAuthorizedApplicationDetails``ds:UpdateAuthorizedApplication`, e `ds:UnauthorizeApplication` nelle relative politiche.

Alcune AWS Directory Service API possono essere richiamate solo tramite. AWS Management Console Non sono API pubbliche, nel senso che non possono essere chiamate a livello di codice e non sono fornite 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 AWS Directory Service politiche per esprimere condizioni. Per un elenco completo delle AWS chiavi, consulta Available Global Condition Keys nella IAM User Guide.

Argomenti correlati

- Controllo accessi

Autorizzazione per l'utilizzo di AWS applicazioni e servizi AWS Directory Service

Autorizzazione di un' AWS applicazione su Active Directory

AWS Directory Service concede autorizzazioni specifiche per consentire alle applicazioni selezionate di integrarsi perfettamente con Active Directory quando si autorizza un'applicazione. AWS AWS alle applicazioni viene concesso solo l'accesso necessario per il loro caso d'uso. L'insieme di autorizzazioni interne concesse alle applicazioni e agli amministratori delle applicazioni dopo l'autorizzazione è fornito di seguito:

> **Note**
>
> L'`ds:AuthorizationApplication`autorizzazione è necessaria per autorizzare una nuova AWS applicazione in 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 FSx si 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 AWS Directory Service API, vedere. AWS Directory Service Autorizzazioni API: riferimento alle azioni, alle risorse e alle condizioni

Per ulteriori informazioni sull'abilitazione di AWS applicazioni e servizi per AWS Managed Microsoft AD, vedereConsentire l'accesso ad AWS applicazioni e servizi. Per ulteriori informazioni sull'abilitazione di AWS applicazioni e servizi per AD Connector, consultaConsentire l'accesso ad AWS applicazioni e servizi. Per ulteriori informazioni sull'attivazione di AWS applicazioni e servizi per Simple AD, vedereConsentire l'accesso ad AWS applicazioni e servizi.

Annullare l'autorizzazione di un' AWS applicazione su Active Directory

Per rimuovere le autorizzazioni per consentire a un' AWS applicazione di accedere ad Active Directory, è `ds:UnauthorizedApplication` necessaria l'autorizzazione. Segui i passaggi forniti dall'applicazione per disabilitarla.

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 Service attualmente supporta i due AWS servizi seguenti in modo da poter monitorare l'organizzazione e le attività che si svolgono al suo interno.

- Amazon CloudWatch : puoi utilizzare CloudWatch Events con il tipo di directory AWS Managed Microsoft AD. Per ulteriori informazioni, consulta Abilita inoltro dei log. Inoltre, puoi utilizzare CloudWatch Metrics per monitorare le prestazioni dei controller di dominio. Per ulteriori informazioni, consulta Determina quando aggiungere controller di dominio con metriche CloudWatch .
- AWS CloudTrail - È possibile utilizzarlo CloudTrail con tutti i tipi di AWS Directory Service directory. Per ulteriori informazioni, consulta Registrazione delle chiamate AWS Directory Service API con CloudTrail.

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 AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty

può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.

- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Resilienza in AWS Directory Service

L'infrastruttura AWS globale è costruita attorno a AWS regioni e zone di disponibilità. AWS Le regioni offrono 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, AWS 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 Snapshot o ripristino della directory.

Sicurezza dell'infrastruttura in AWS Directory Service

In quanto servizio gestito, AWS Directory Service è protetto dalle procedure di sicurezza della rete AWS globale descritte nel white paper Amazon Web Services: panoramica dei processi di sicurezza.

Utilizzi chiamate API AWS pubblicate per accedere AWS Directory Service attraverso la rete. I client devono supportare Transport Layer Security (TLS). È consigliabile TLS 1.2 o versioni successive. I client devono, inoltre, supportare le suite di cifratura con PFS (Perfect Forward Secrecy), 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.

Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Inoltre, le richieste devono essere firmate utilizzando un chiave di accesso ID e una chiave di accesso segreta associata a un account principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Prevenzione del problema "confused deputy" tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel frattempo AWS, 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 del tuo 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 AWS Directory Service per Microsoft Active Directory fornisce a 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. Utilizza `aws:SourceAccount` se desideri 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.

```
{
  "Version": "2012-10-17",
  "Statement": {
```

```
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
    "Resource": [
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

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 eDirectoryMonitoring" _d-966739499f» è il nome dell'argomento Amazon SNS che hai creato.

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.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "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:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

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 AWS 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.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
```

```
    },
    "Action": [
                "sts:AssumeRole"
            ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

AWS Directory Service API e interfaccia che utilizzano gli endpoint Amazon VPC AWS PrivateLink

Puoi stabilire una connessione privata tra i tuoi endpoint Amazon VPC e AWS Directory Service API creando un endpoint VPC di interfaccia. Endpoint di interfaccia con tecnologia AWS PrivateLink.

AWS PrivateLink ti consente di accedere in modo privato alle operazioni AWS Directory Service API senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Il traffico tra il tuo VPC e AWS Directory Service non esce dalla AWS rete.

Ogni endpoint di interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Per ulteriori informazioni sull'interfaccia di rete elastica, consulta Elastic network interface nella Amazon EC2 User Guide.

Per ulteriori informazioni sugli endpoint VPC, consulta Accedere e Servizio AWS utilizzare un endpoint VPC con interfaccia nella Amazon VPC User Guide. Per ulteriori informazioni sulle operazioni delle API, consulta AWS Directory Service API Reference.AWS Directory Service

Considerazioni sugli endpoint VPC

Prima di configurare un endpoint VPC di interfaccia per endpoint AWS Directory Service API, assicurati di aver letto Access an using Servizio AWS an interface VPC endpoint nella Guida.AWS PrivateLink

Tutte le operazioni AWS Directory Service API relative alla gestione AWS Directory Service delle risorse sono disponibili tramite il tuo VPC utilizzando. AWS PrivateLink

Le policy degli endpoint VPC sono supportate per gli endpoint dell'API Directory Service. Per impostazione predefinita, l'accesso completo alle operazioni dell'API Directory Service è consentito tramite l'endpoint. Per ulteriori informazioni, consulta Controlla l'accesso agli endpoint VPC utilizzando le policy degli endpoint nella Amazon VPC User Guide.

Disponibilità

AWS Directory Service supporta gli endpoint VPC nei seguenti casi: Regioni AWS

Regione AWS disponibilità

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- Stati Uniti occidentali (California settentrionale)
- Stati Uniti occidentali (Oregon)
- Africa (Città del Capo)
- Asia Pacifico (Hong Kong)
- Asia Pacific (Hyderabad)
- Asia Pacifico (Giacarta)
- Asia Pacifico (Melbourne)
- Asia Pacifico (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Canada (Centrale)
- Canada occidentale (Calgary)
- Cina (Pechino e Ningxia)
- Asia Pacifico (Hong Kong)
- Europa (Francoforte)

- Europa (Irlanda)
- Europa (Londra)
- Europa (Milano)
- Europa (Parigi)
- Europa (Spagna)
- Europa (Stoccolma)
- Europa (Zurigo)
- Israele (Tel Aviv)
- Medio Oriente (Bahrein)
- Medio Oriente (Emirati Arabi Uniti)
- Sud America (San Paolo)
- AWS GovCloud (Stati Uniti orientali)
- AWS GovCloud (Stati Uniti occidentali)

Creazione di un endpoint di interfaccia per l'API AWS Directory Service

Puoi creare un endpoint di interfaccia VPC per l' AWS Directory Service API utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint VPC nella Guida di AWS PrivateLink .

Crea un endpoint di interfaccia per l' AWS Directory Service API utilizzando il seguente nome di servizio: `com.amazonaws.region.ds`

Ad eccezione Regioni AWS della Cina, se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API all' AWS Directory Service endpoint VPC utilizzando il suo nome DNS predefinito per, ad esempio. Regione AWS`ds.us-east-1.amazonaws.com` Per la Cina (Pechino e Ningxia) Regioni AWS, puoi effettuare richieste API con l'endpoint VPC utilizzando e, rispettivamente. `ds-api.cn-north-1.amazonaws.com.cn` `ds-api.cn-northwest-1.amazonaws.com.cn`

Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS con interfaccia nella Amazon VPC User Guide.

Creazione di una policy di endpoint VPC per l’API AWS Directory Service

Puoi allegare una policy di endpoint all'endpoint VPC che controlla l'accesso all’API AWS Directory Service . La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire azioni.

Per ulteriori informazioni, consulta Controlla l'accesso agli endpoint VPC utilizzando le policy degli endpoint nella Amazon VPC User Guide.

Esempio: policy degli endpoint VPC per le azioni API AWS Directory Service

Di seguito è riportato un esempio di policy sugli endpoint per l'API. AWS Directory Service Quando alleghi questa policy all'endpoint dell'interfaccia, concede l'accesso alle azioni AWS Directory Service API elencate per tutti i principali su tutte le risorse.

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeCertificate",
         ],
         "Resource":"*"
      }
   ]
}
```

Esempio: policy degli endpoint VPC che nega tutti gli accessi provenienti da una determinata area Account AWS

La seguente policy sugli endpoint VPC nega a Account AWS *123456789012* tutti gli accessi alle risorse che utilizzano l'endpoint. La policy consente tutte le operazioni da altri account.

```
{
   "Statement": [
      {
         "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal:" "*"
```

```
      },
      {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "*",
        "Principal": {
            "AWS": [
               "123456789012"
            ]
         }
      ]
}
```

Contratto sul livello di servizio per AWS Directory Service

Il AWS Directory Service è un servizio altamente disponibile ed è sviluppato su un'infrastruttura gestita da AWS. È supportato da un contratto sul livello di servizio che definisce la nostra policy di disponibilità dei servizi.

Per ulteriori informazioni, consulta il Contratto sul livello di servizio per AWS Directory Service.

Disponibilità regionale per AWS 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	AWS Microsoft AD gestito	AD Connector	Simple AD
US East (N. Virginia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 Sì	 Sì	 Sì
Stati Uniti orientali (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 Sì	 Sì	 No
US West (N. California)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 Sì	 Sì	 No
US West (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 Sì	 Sì	 Sì
Africa (Cape Town)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 Sì	 Sì	 No
Asia Pacifico	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 Sì	 Sì	 No

Nome Regione	Regione	Endpoint	Protocollo	AWS Microsoft AD gestito	AD Connector	Simple AD
(Hong Kong)						
Asia Pacific (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 S	 S	 No
Asia Pacifico (Giacarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 S	 S	 No
Asia Pacifico (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 S	 S	 No
Asia Pacific (Mumbai)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 S	 S	 No
Asia Pacifico (Osaka-Locale)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 S	 S	 No
Asia Pacifico (Seul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 S	 S	 No

Nome Regione	Regione	Endpoint	Protocollo	AWS Microsoft AD gestito	AD Connector	Simple AD
Asia Pacific (Singapore)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 S	 S	 Sì
Asia Pacific (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 S	 S	 Sì
Asia Pacifico (Tokyo)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 S	 S	 Sì
Canada (Central)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 S	 S	 No
Canada occidentale (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 S	 S	 No
China (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 S	 S	 No
Cina (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	 S	 S	 No
Europe (Frankfurt)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 S	 S	 No

Nome Regione	Regione	Endpoint	Protocollo	AWS Microsoft AD gestito	AD Connector	Simple AD
Europa (Irlanda)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	Sì	Sì	Sì
Europe (London)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	Sì	Sì	No
Europa (Milano)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	Sì	Sì	No
Europe (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	Sì	Sì	No
Europa (Spagna)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	Sì	Sì	No
Europa (Stoccolma)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	Sì	Sì	No
Europa (Zurigo)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	Sì	Sì	No
Israele (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	Sì	Sì	No
Medio Oriente (Bahrein)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	Sì	Sì	No

Nome Regione	Regione	Endpoint	Protocollo	AWS Microsoft AD gestito	AD Connect	Simple AD
Medio Oriente (Emirati Arabi Uniti)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 S	 S	 No
Sud America (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 S	 S	 No
AWS GovClou (Stati Uniti occidentali)	us-gov-west-1	annunci. us-gov-west-1. amazonaws .com	HTTPS	 S	 S	 No
AWS GovClou (Stati Uniti orientali)	us-gov-east-1	annunci. us-gov-east-1. amazonaws .com	HTTPS	 S	 S	 No

Per informazioni sull'utilizzo AWS Directory Service nella regione AWS GovCloud (Stati Uniti occidentali) e nella regione (Stati Uniti orientali), AWS GovCloud consulta Service endpoints.

Per informazioni sull'utilizzo AWS Directory Service nelle regioni di Pechino e Ningxia, consulta Endpoints and ARNs for Amazon Web Services in Cina.

Compatibilità browser

AWS applicazioni e servizi come Amazon WorkSpaces, Amazon Connect WorkMail, Amazon Chime, Amazon 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

Dopo aver verificato che stai utilizzando una versione supportata del tuo browser, ti consigliamo di rivedere anche la sezione seguente per verificare che il tuo browser sia stato configurato per utilizzare l'impostazione TLS (Transport Layer Security) richiesta da AWS.

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

AWS le 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 varie opzioni per TLS in Proprietà Internet, la scheda Avanzate e quindi nella sezione Sicurezza. Controlla il sito Web della Guida 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
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 AWS Management Console, Windows 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
AWS gruppi 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 AWS Managed Microsoft AD.	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	È stato aggiunto contenuto sulle estensioni dello schema con AWS Directory Service per Microsoft Active Directory.	14 novembre 2016
Riorganizzazione importante della AWS 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 con AWS Directory Service.	25 febbraio 2016
AWS Microsoft 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 AWS 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.