Administratorhandbuch

AWS Directory Service

Version 1.0

AWS Directory Service: Administratorhandbuch

Table of Contents

Was ist AWS Directory Service?

AWS Directory Service bietet mehrere Möglichkeiten, Microsoft Active Directory (AD) mit anderen AWS Diensten zu verwenden. Verzeichnisse speichern Informationen über Benutzer, Gruppen und Geräte, und Administratoren verwenden sie, um den Zugriff auf Informationen und Ressourcen zu verwalten. AWS Directory Service bietet Kunden, die bestehende Microsoft AD- oder LDAP-fähige Anwendungen (Lightweight Directory Access Protocol) in der Cloud verwenden möchten, mehrere Verzeichnisoptionen. Dieselben Optionen bietet es Entwicklern, die ein Verzeichnis zum Verwalten von Benutzern, Gruppen, Geräten und Zugriff benötigen.

Welche sollte man auswählen

Sie können Verzeichnisdienste mit der Kapazität und der Skalierbarkeit wählen, die Ihren Anforderungen am besten entsprechen. Anhand der folgenden Tabelle können Sie ermitteln, welche AWS Directory Service Verzeichnisoption für Ihr Unternehmen am besten geeignet ist.

Was müssen Sie als Nächstes tun?	Empfohlene AWS Directory Service Optionen
Ich benötige Active Directory oder LDAP für meine Anwendungen in der Cloud.	Verwenden Sie AWS Directory Service für Microsoft Active Directory (Standard Edition oder Enterprise Edition), wenn Sie eine Lösung Microsoft Active Directory in der AWS Cloud benötigen, die Workloads oder AWS Anwendung en und Dienste wie Amazon WorkSpaces und Amazon unterstützt Active Directory QuickSight, oder wenn Sie LDAP-Unterstützung für Linux-Anwendungen benötigen. Verwenden Sie AD Connector, wenn Sie Ihren lokalen Benutzern nur erlauben müssen, sich mit ihren Active Directory Anmeldeinformationen bei AWS Anwendungen und Diensten anzumelden. Sie können AD Connector auch verwenden, um Amazon EC2 EC2-Instances mit Ihrer bestehenden Active Directory Domain zu verbinden. Verwenden Sie Simple AD, wenn Sie ein niedriges , kostengünstiges Verzeichnis mit Active Directory Basiskompatibilität benötigen, das Samba 4-kompatible

Was müssen Sie als Nächstes tun?	Empfohlene AWS Directory Service Optionen
	Anwendungen unterstützt, oder wenn Sie LDAP-Komp atibilität für LDAP-fähige Anwendungen benötigen.
Ich entwickle SaaS-Anwendungen.	Verwenden Sie Amazon Cognito, wenn Sie umfangrei che SaaS-Anwendungen entwickeln und ein skalierbares Verzeichnis benötigen, um Ihre Abonnenten zu verwalten und zu authentifizieren, die mit Social Media-Identitäten arbeiten.

Weitere Informationen zu AWS Directory Service Verzeichnisoptionen finden Sie unter So wählen Sie Lösungen auf. Active DirectoryAWS

AWS Directory Service Optionen

AWS Directory Service beinhaltet mehrere Verzeichnistypen, aus denen Sie wählen können. Weitere Informationen finden Sie auf einer der folgenden Registerkarten:

AWS Directory Service for Microsoft Active Directory

Der AWS Directory Service für Microsoft Active Directory, auch AWS Managed Microsoft AD genannt, wird von einem echten Microsoft Windows Server Active Directory (AD) betrieben, das AWS in der AWS Cloud verwaltet wird. Damit können Sie eine Vielzahl von Active Directory-fähigen Anwendungen in die Cloud migrieren. AWS AWS Managed Microsoft AD funktioniert mit Microsoft SharePoint Microsoft SQL Server Always-On-Verfügbarkeitsgruppen und vielen .NET-Anwendungen. Es unterstützt auch AWS verwaltete Anwendungen und Dienste wie Amazon WorkSpaces, Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect und Amazon Relational Database Service für Microsoft SQL Server (Amazon RDS fürSQL Server, Amazon RDS für und Amazon RDS for Oracle PostgreSQL).

AWS Managed Microsoft AD ist für Anwendungen in der AWS Cloud zugelassen, die der Einhaltung des US-amerikanischen Health Insurance Portability and Accountability Act (HIPAA) oder des Payment Card Industry Data Security Standard (PCI DSS) unterliegen, wenn Sie die Compliance für Ihr Verzeichnis aktivieren.

Alle kompatiblen Anwendungen funktionieren mit Benutzeranmeldeinformationen, die Sie in AWS Managed Microsoft AD speichern, oder Sie können vertrauenswürdig eine Verbindung zu Ihrer vorhandenen AD-Infrastruktur herstellen und Anmeldeinformationen von einem lokal oder unter EC2 Active Directory laufenden Windows verwenden. Wenn Sie EC2-Instances mit Ihrem AWS Managed Microsoft AD verbinden, können Ihre Benutzer auf Windows-Workloads in der AWS Cloud mit derselben Windows Single Sign-On (SSO) -Erfahrung zugreifen wie beim Zugriff auf Workloads in Ihrem lokalen Netzwerk.

AWS Managed Microsoft AD unterstützt auch föderierte Anwendungsfälle mit Active Directory Anmeldeinformationen. Allein mit AWS Managed Microsoft AD können Sie sich bei der anmelden AWS Management Console. Mit AWS IAM Identity Centerkönnen Sie auch kurzfristige Anmeldeinformationen für die Verwendung mit dem AWS SDK und der CLI abrufen und vorkonfigurierte SAML-Integrationen verwenden, um sich bei vielen Cloud-Anwendungen anzumelden. Durch Hinzufügen Microsoft Entra Connect (früher bekannt alsAzure Active Directory Connect) und optional Active Directory Federation Service (AD FS) können Sie sich mit in AWS Managed Microsoft AD gespeicherten Anmeldeinformationen bei Microsoft Office 365 und anderen Cloud-Anwendungen anmelden.

Der Service umfasst die wichtigsten Funktionen, mit denen Sie Ihr Schema erweitern, Passwortrichtlinien verwalten und eine sichere LDAP-Kommunikation über Secure Socket Layer (SSL)/Transport Layer Security (TLS) aktivieren können. Sie können auch die Multi-Faktor-Authentifizierung (MFA) für AWS Managed Microsoft AD aktivieren, um eine zusätzliche Sicherheitsebene zu bieten, wenn Benutzer über das Internet auf AWS Anwendungen zugreifen. Da Active Directory es sich um ein LDAP-Verzeichnis handelt, können Sie AWS Managed Microsoft AD auch für die Linux Secure Shell (SSH) -Authentifizierung und für andere LDAP-fähige Anwendungen verwenden.

AWS bietet Überwachung, tägliche Snapshots und Wiederherstellung als Teil des Dienstes. Sie fügen Benutzer und Gruppen zu AWS Managed Microsoft AD hinzu und verwalten Gruppenrichtlinien mithilfe vertrauter Active Directory Tools, die auf einem Windows Computer ausgeführt werden, der zur AWS Managed Microsoft AD-Domäne gehört. Sie können das Verzeichnis auch skalieren, indem Sie zusätzliche Domain-Controller bereitstellen, und verbessern die Anwendungsleistung, indem Sie Anfragen über eine größere Anzahl von Domain-Controllern verteilen.

AWS Managed Microsoft AD ist in zwei Editionen erhältlich: Standard und Enterprise.

- Standard Edition: AWS Managed Microsoft AD (Standard Edition) ist als primäres Verzeichnis für kleine und mittelgroße Unternehmen mit bis zu 5 000 Mitarbeitern optimiert. Es bietet

genügend Speicherkapazität für bis zu 30.000* Verzeichnisobjekte, wie beispielsweise Benutzer, Gruppen und Computer.

- Enterprise Edition: AWS Managed Microsoft AD (Enterprise Edition) ist für Unternehmen und Organisationen mit bis zu 500 000* Verzeichnisobjekten ausgelegt.

* Die Obergrenzen sind Annäherungswerte. Ihr Verzeichnis kann mehr oder weniger Verzeichnisobjekte unterstützen, abhängig von der Größe Ihrer Objekte und dem Verhalten und den Leistungsanforderungen Ihrer Anwendungen.

Wann sollte dies verwendet werden?

AWS Managed Microsoft AD ist die beste Wahl, wenn Sie aktuelle Active Directory Funktionen zur Unterstützung von AWS Anwendungen oder Windows Workloads benötigen, einschließlich Amazon Relational Database Service für. Microsoft SQL Server Es ist auch am besten, wenn Sie eine eigenständige Lösung Active Directory in der AWS Cloud benötigen, die Office 365 unterstützt, oder wenn Sie ein LDAP-Verzeichnis zur Unterstützung Ihrer Linux-Anwendungen benötigen. Weitere Informationen finden Sie unter AWS Verwaltetes Microsoft AD.

AD Connector

AD Connector ist ein Proxy-Service, der eine einfache Möglichkeit bietet, kompatible AWS Anwendungen wie Amazon WorkSpaces, Amazon und Amazon QuickSight EC2 für Windows Server Instances mit Ihren vorhandenen lokalen Microsoft Active Directory Systemen zu verbinden. Mit AD Connector können Sie einfach ein Dienstkonto zu Ihrem hinzufügenActive Directory. Außerdem ist es mit AD Connector nicht mehr notwendig, Verzeichnisse zu synchronisieren. Die Kosten und die Komplexität des Hostings einer komplexen Verbund-Infrastruktur fallen weg.

Wenn Sie Benutzer zu AWS Anwendungen wie Amazon hinzufügen QuickSight, liest AD Connector Ihre vorhandenen, Active Directory um Listen mit Benutzern und Gruppen zu erstellen, aus denen Sie auswählen können. Wenn sich Benutzer bei den AWS Anwendungen anmelden, leitet AD Connector Anmeldeanfragen zur Authentifizierung an Ihre lokalen Active Directory Domänencontroller weiter. AD Connector funktioniert mit vielen AWS Anwendungen und Diensten WorkSpaces, darunter Amazon WorkDocs, Amazon QuickSight, Amazon Chime, Amazon Connect und Amazon WorkMail. Sie können Ihre Windows EC2-Instances auch über AD Connector mit Ihrer lokalen Active Directory Domain verbinden, indem Sie Seamless Domain Join verwenden. Mit AD Connector können Ihre Benutzer auch auf die AWS Ressourcen zugreifen

AWS Management Console und diese verwalten, indem sie sich mit ihren vorhandenen Active Directory Anmeldeinformationen anmelden. AD Connector ist nicht kompatibel mit RDS SQL Server.

Sie können AD Connector auch verwenden, um die Multi-Faktor-Authentifizierung (MFA) für Ihre AWS Anwendungsbenutzer zu aktivieren, indem Sie sie mit Ihrer vorhandenen RADIUS-basierten MFA-Infrastruktur verbinden. Dies sorgt für eine zusätzliche Sicherheitsebene, wenn Benutzer auf AWS -Anwendungen zugreifen.

Mit AD Connector verwalten Sie Ihre weiterhin Active Directory wie bisher. Sie fügen beispielsweise neue Benutzer und Gruppen hinzu und aktualisieren Kennwörter mithilfe von Active Directory Standard-Verwaltungstools vor OrtActive Directory. Auf diese Weise können Sie Ihre Sicherheitsrichtlinien wie Ablauf von Kennwörtern, Kennwortverlauf und Kontosperrungen konsistent durchsetzen, unabhängig davon, ob Benutzer auf Ressourcen vor Ort oder in der AWS Cloud zugreifen.

Wann sollte dies verwendet werden?

AD Connector ist die beste Wahl, wenn Sie Ihr vorhandenes lokales Verzeichnis mit kompatiblen AWS Diensten verwenden möchten. Weitere Informationen finden Sie unter AD Connector.

Simple AD

Simple AD ist ein Microsoft Active Directory — kompatibles Verzeichnis AWS Directory Service , das von Samba 4 unterstützt wird. Simple AD unterstützt grundlegende Active Directory Funktionen wie Benutzerkonten, Gruppenmitgliedschaften, Beitritt zu einer Linux-Domäne oder Windows basierten EC2-Instances, Kerberos-basiertes SSO und Gruppenrichtlinien. AWS bietet Überwachung, tägliche Snapshots und Wiederherstellung als Teil des Service.

Simple AD ist ein eigenständiges Verzeichnis in der Cloud, in dem Sie Benutzeridentitäten erstellen und verwalten und den Zugriff auf Anwendungen verwalten können. Sie können viele vertraute Anwendungen und Tools verwendenActive Directory, für die grundlegende Funktionen erforderlich sind. Active Directory Simple AD ist mit den folgenden AWS Anwendungen kompatibel: Amazon WorkSpaces WorkDocs, Amazon QuickSight, Amazon und Amazon WorkMail. Sie können sich auch AWS Management Console mit Simple AD AD-Benutzerkonten anmelden und AWS Ressourcen verwalten.

Simple AD unterstützt keine Multi-Faktor-Authentifizierung (MFA), Vertrauensstellungen, dynamische DNS-Updates, Schemaerweiterungen, Kommunikation über LDAPS, PowerShell

AD-Cmdlets oder FSMO-Rollenübertragung. Simple AD ist nicht kompatibel mit RDS SQL Server. Kunden, die die Funktionen eines aktuellen Verzeichnisses benötigen oder beabsichtigen MicrosoftActive Directory, ihr Verzeichnis mit RDS SQL Server zu verwenden, sollten stattdessen AWS Managed Microsoft AD verwenden. Bitte überprüfen Sie, ob Ihre erforderlichen Anwendungen vollständig mit Samba 4 kompatibel sind, bevor Sie Simple AD verwenden. Weitere Informationen finden Sie unter https://www.samba.org.

Wann sollte dies verwendet werden?

Sie können Simple AD als eigenständiges Verzeichnis in der Cloud verwenden, um Windows Workloads zu unterstützen, die grundlegende Active Directory Funktionen und kompatible AWS Anwendungen benötigen, oder um Linux-Workloads zu unterstützen, die einen LDAP-Dienst benötigen. Weitere Informationen finden Sie unter Simple AD.

Amazon Cognito

Amazon Cognito ist ein Benutzerverzeichnis, das Registrierung und Anmeldung für mobile Apps oder Webanwendungen über Amazon-Cognito-Benutzerpools hinzufügt.

Wann sollte dies verwendet werden?

Sie können Amazon Cognito auch für die Erstellung benutzerdefinierter Registrierungsfelder verwenden und die Metadaten in Ihrem Benutzerverzeichnis speichern. Dieser vollständig verwaltete Service unterstützt Hunderte Millionen von Benutzern. Weitere Informationen finden Sie unter Amazon-Cognito-Benutzerpools im Amazon-Cognito-Entwicklerhandbuch.

Eine Liste der unterstützten Verzeichnistypen pro Region finden Sie unter Verfügbarkeit in der Region für AWS Directory Service.

Arbeiten mit Amazon EC2

Ein grundlegendes Verständnis von Amazon EC2 ist wichtig, um AWS Directory Service zu nutzen. Wir empfehlen, dass Sie zuerst die folgenden Themen lesen:

- Was ist Amazon EC2? im Amazon EC2 EC2-Benutzerhandbuch.
- Starten von EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch.
- Sicherheitsgruppen im Amazon EC2 EC2-Benutzerhandbuch.
- Was ist Amazon VPC? im Amazon-VPC-Benutzerhandbuch.

- Hinzufügen eines Hardware Virtual Private Gateway zu Ihrer VPC im Amazon-VPC-Benutzerhandbuch.

Erste Schritte mit AWS Directory Service

Falls Sie dies noch nicht getan haben, müssen Sie auch ein AWS Konto erstellen und den AWS Identity and Access Management Dienst verwenden, um den Zugriff zu kontrollieren.

Um damit arbeiten zu können AWS Directory Service, müssen Sie die Voraussetzungen für AWS Directory Service for Microsoft Active Directory, AD Connector oder Simple AD erfüllen. Weitere Informationen finden Sie unter AWS Voraussetzungen für verwaltetes Microsoft AD, AD-Connector-Voraussetzungen oder Simple-AD-Voraussetzungen.

Melden Sie sich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/signup.
2. Folgen Sie den Online-Anweisungen.

   Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS Management Consoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen finden Sie unter Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer (Konsole) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

  Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal.

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter Einen Berechtigungssatz erstellen.AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Anweisungen finden Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen.

Weitere Informationen

- Weitere Informationen zur Anmeldung AWS Management Console als IAM Identity Center-Benutzer finden Sie unter Anmelden im IAM Identity Center-Zugriffsportal.
- Weitere Informationen zur Anmeldung AWS Management Console als IAM-Benutzer finden Sie unter Als IAM-Benutzer anmelden. AWS Management Console
- Weitere Informationen zur Verwendung von IAM-Richtlinien zur Steuerung des Zugriffs auf Ihre AWS Directory Service Ressourcen finden Sie unter. Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Directory Service

AWS Verwaltetes Microsoft AD

AWS Directory Service ermöglicht es Ihnen, Microsoft Active Directory (AD) als verwalteten Dienst auszuführen. AWS Der Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet, wird von Windows Server 2019 unterstützt. Wenn Sie diesen Verzeichnistyp auswählen und starten, wird er als hochverfügbares Paar von Domain-Controllern erstellt, die mit Ihrer Virtual Private Cloud (Amazon VPC) verbunden sind. Die Domain-Controller werden in verschiedenen Availability Zones einer Region Ihrer Wahl ausgeführt. Host-Überwachung und Wiederherstellung, Datenreplikation, Snapshots und Software-Updates werden automatisch für Sie konfiguriert und verwaltet.

Mit AWS Managed Microsoft AD können Sie verzeichnissensitive Workloads in der AWS Cloud ausführen, einschließlich benutzerdefinierter.NET Microsoft SharePoint - und SQL Server-basierter Anwendungen. Sie können auch eine Vertrauensstellung zwischen AWS Managed Microsoft AD in der AWS Cloud und Ihren vorhandenen lokalen Systemen konfigurieren MicrosoftActive Directory, sodass Benutzer und Gruppen Zugriff auf Ressourcen in beiden Domänen erhalten. AWS IAM Identity Center

AWS Directory Service macht es einfach, Verzeichnisse in der AWS Cloud einzurichten und auszuführen oder Ihre AWS Ressourcen mit vorhandenen lokalen Microsoft Active Directory Ressourcen zu verbinden. Nachdem Ihr Verzeichnis erstellt wurde, können Sie es für eine Vielzahl von Aufgaben verwenden:

- Verwalten von Benutzern und Gruppen
- Bereitstellen von Single Sign-On für Anwendungen und Services
- Erstellen und Anwenden von Gruppenrichtlinien
- Vereinfachen Sie die Bereitstellung und Verwaltung von cloudbasiertem Linux und Workloads Microsoft Windows
- Sie können AWS Managed Microsoft AD verwenden, um die Multi-Faktor-Authentifizierung zu aktivieren, indem Sie es in Ihre bestehende RADIUS-basierte MFA-Infrastruktur integrieren und so eine zusätzliche Sicherheitsebene bieten, wenn Benutzer auf Anwendungen zugreifen. AWS
- Stellen Sie eine sichere Verbindung zu Amazon EC2, Linux und Windows Instances her

> **Note**
>
> AWS verwaltet die Lizenzierung Ihrer Windows Server-Instances für Sie. Sie müssen lediglich für die Instances bezahlen, die Sie verwenden. Sie müssen auch keine zusätzlichen Windows-Server-Clientzugriffslizenzen (CALs) erwerben, da der Zugriff im Preis enthalten ist. Jede Instance verfügt über zwei Remoteverbindungen, die nur für Administratorzwecke bestimmt sind. Wenn Sie mehr als zwei Verbindungen benötigen oder diese Verbindungen für andere Zwecke als für Administratorzwecke benötigen, müssen Sie möglicherweise zusätzliche Remote-Desktop-Services-CALs für die Verwendung auf AWS einrichten.

Lesen Sie die Themen in diesem Abschnitt, um mit der Erstellung eines AWS verwalteten Microsoft AD-Verzeichnisses, dem Aufbau einer Vertrauensstellung zwischen AWS Managed Microsoft AD und Ihren lokalen Verzeichnissen und der Erweiterung Ihres AWS Managed Microsoft AD-Schemas zu beginnen.

Themen

Verwandte Blogartikel zum Thema AWS Sicherheit

- So delegieren Sie die Verwaltung Ihres AWS verwalteten Microsoft AD-Verzeichnisses an Ihre lokalen Active Directory-Benutzer
- So konfigurieren Sie mit AWS Managed Microsoft AD noch strengere Kennwortrichtlinien, um Ihre Sicherheitsstandards zu erfüllen AWS Directory Service
- So erhöhen Sie die Redundanz und Leistung Ihres AWS Directory Service for AWS Managed Microsoft AD durch Hinzufügen von Domain-Controllern

- So aktivieren Sie die Verwendung von Remote-Desktops, indem Sie den Microsoft Remote Desktop Licensing Manager auf AWS Managed Microsoft AD bereitstellen
- So greifen AWS Management Console Sie mithilfe von AWS Managed Microsoft AD und Ihren lokalen Anmeldeinformationen auf
- So aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Dienste mithilfe von AWS Managed Microsoft AD und lokalen Anmeldeinformationen
- Wie können Sie sich mithilfe Ihres lokalen Active Directory ganz einfach bei AWS Diensten anmelden

Erste Schritte mit AWS Managed Microsoft AD

AWS Managed Microsoft AD erstellt ein vollständig verwaltetes Microsoft Active Directory System, das von Windows Server 2019 unterstützt wird AWS Cloud und auf den Funktionsebenen 2012 R2 Forest und Domain betrieben wird. Wenn Sie ein Verzeichnis mit AWS Managed Microsoft AD erstellen, AWS Directory Service erstellt zwei Domänencontroller und fügt den DNS-Dienst in Ihrem Namen hinzu. Die Domain-Controller werden in verschiedenen Subnetzen in einer Amazon VPC erstellt. Durch diese Redundanz wird sichergestellt, dass Ihr Verzeichnis auch bei einem Ausfall zugänglich bleibt. Wenn Sie weitere Domain-Controller benötigen, können Sie diese später hinzufügen. Weitere Informationen finden Sie unter Bereitstellen zusätzlicher Domain-Controller.

Themen

- AWS Voraussetzungen für verwaltetes Microsoft AD
- Erstellen Sie Ihr AWS verwaltetes Microsoft AD
- Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt
- Berechtigungen für das Administratorkonto

AWS Voraussetzungen für verwaltetes Microsoft AD

Um ein AWS verwaltetes Microsoft AD zu erstellenActive Directory, benötigen Sie eine Amazon-VPC mit den folgenden Komponenten:

- Mindestens zwei Subnetze. Jedes dieser Subnetze muss sich in einer anderen Availability Zone befinden.
- Die VPC muss über Standard-Hardware-Tenancy verfügen.

- Sie können kein AWS verwaltetes Microsoft AD in einer VPC mithilfe von Adressen im 198.18.0.0/15-Adressraum erstellen.

Wenn Sie Ihre AWS verwaltete Microsoft AD-Domäne in eine bestehende lokale Active Directory Domäne integrieren müssen, müssen Sie die Funktionsebenen Gesamtstruktur und Domäne für Ihre lokale Domäne auf Windows Server 2003 oder höher einstellen.

AWS Directory Service verwendet eine Struktur mit zwei VPCs. Die EC2-Instances, aus denen Ihr Verzeichnis besteht, laufen außerhalb Ihres AWS Kontos und werden von verwaltet. AWS Sie haben zwei Netzwerkadapter `ETH0` und `ETH1`. `ETH0` ist der Verwaltungsadapter und existiert außerhalb Ihres Kontos. `ETH1` wird in Ihrem Konto erstellt.

Der IP-Verwaltungsbereich des ETH0-Netzwerks Ihres Verzeichnisses ist 198.18.0.0/15.

AWS IAM Identity Center Voraussetzungen

Wenn Sie planen, IAM Identity Center mit AWS Managed Microsoft AD zu verwenden, müssen Sie sicherstellen, dass Folgendes zutrifft:

- Ihr AWS verwaltetes Microsoft AD-Verzeichnis ist im Verwaltungskonto Ihrer AWS Organisation eingerichtet.
- Ihre Instanz von IAM Identity Center befindet sich in derselben Region, in der Ihr AWS verwaltetes Microsoft AD-Verzeichnis eingerichtet ist.

Weitere Informationen finden Sie unter Voraussetzungen für IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

Voraussetzungen für Multifaktor-Authentifizierung

Um die Multi-Faktor-Authentifizierung mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis zu unterstützen, müssen Sie entweder Ihren lokalen oder cloudbasierten RADIUS-Server (Remote Authentication Dial-In User Service) wie folgt konfigurieren, damit er Anfragen von Ihrem AWS verwalteten Microsoft AD-Verzeichnis annehmen kann. AWS

1. Erstellen Sie auf Ihrem RADIUS-Server zwei RADIUS-Clients, die beide AWS verwalteten Microsoft AD-Domänencontroller (DCs) in AWS repräsentieren. Sie müssen beide Clients mit den folgenden allgemeinen Parametern konfigurieren (Ihr RADIUS-Server kann abweichen):
   - Adresse (DNS oder IP): Dies ist die DNS-Adresse für eines der AWS verwalteten Microsoft AD-DCs. Beide DNS-Adressen befinden sich in der AWS Directory Service Console auf der

Detailseite des AWS verwalteten Microsoft AD-Verzeichnisses, in dem Sie MFA verwenden möchten. Die angezeigten DNS-Adressen stellen die IP-Adressen für beide AWS verwalteten Microsoft AD-DCs dar, die von AWS verwendet werden.

> **Note**
>
> Wenn Ihr RADIUS-Server DNS-Adressen unterstützt, müssen Sie nur eine RADIUS-Client-Konfiguration erstellen. Andernfalls müssen Sie eine RADIUS-Client-Konfiguration für jeden Domain-Controller in AWS Managed Microsoft AD erstellen.

- Portnummer: Konfigurieren Sie die Portnummer, für die Ihr RADIUS-Server RADIUS-Client-Verbindungen akzeptiert. Der Standard-RADIUS-Port ist 1812.
- Gemeinsamer geheimer Schlüssel: Geben Sie einen gemeinsamen geheimen Schlüssel ein oder generieren sie einen, der vom RADIUS-Server für die Verbindung mit RADIUS-Clients verwendet wird.
- Protokoll: Möglicherweise müssen Sie das Authentifizierungsprotokoll zwischen den AWS verwalteten Microsoft AD-DCs und dem RADIUS-Server konfigurieren. Zu den unterstützten Protokollen zählen PAP, CHAP, MS-CHAPv1 und MS- CHAPv2. MS-CHAPv2 wird empfohlen, da es die höchste Sicherheit der drei Optionen bietet.
- Anwendungs-Name: Dies kann optional in einigen RADIUS-Servern sein, und bestimmt in der Regel die Anwendung in Nachrichten oder Berichten.

2. Konfigurieren Sie Ihr vorhandenes Netzwerk so, dass eingehender Verkehr von den RADIUS-Clients (DNS-Adressen von AWS verwalteten Microsoft AD DCs, siehe Schritt 1) zu Ihrem RADIUS-Serverport zugelassen wird.
3. Fügen Sie der Amazon EC2-Sicherheitsgruppe in Ihrer AWS verwalteten Microsoft AD-Domain eine Regel hinzu, die eingehenden Datenverkehr von der zuvor definierten DNS-Adresse und Portnummer des RADIUS-Servers zulässt. Weitere Informationen finden Sie unter Hinzufügen von Regeln zu einer Sicherheitsgruppe im EC2-Benutzerhandbuch.

Weitere Informationen zur Verwendung von AWS Managed Microsoft AD mit MFA finden Sie unterAktivieren Sie die Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD.

Erstellen Sie Ihr AWS verwaltetes Microsoft AD

Zum Erstellen eines neuen Verzeichnisses führen Sie folgende Schritte aus. Bevor Sie dieses Verfahren beginnen, stellen Sie sicher, dass Sie die in AWS Voraussetzungen für verwaltetes Microsoft AD angegebenen Voraussetzungen erfüllt haben.

So erstellen Sie ein AWS verwaltetes Microsoft AD-Verzeichnis

1. Wählen Sie im Navigationsbereich AWS Directory Service -Konsole den Eintrag Verzeichnisse und wählen Sie Verzeichnis einrichten aus.
2. Wählen Sie auf der Seite Verzeichnistyp auswählen die Option AWS Managed Microsoft AD aus und klicken Sie dann auf Weiter.
3. Geben Sie auf der Seite Enter directory information (Verzeichnisinformationen eingeben) die folgenden Informationen ein:

   Edition

   Wählen Sie zwischen der Standard Edition oder der Enterprise Edition von AWS Managed Microsoft AD. Weitere Informationen zu Editionen finden Sie unter AWS Directory Service für Microsoft Active Directory.

   DNS-Name des Verzeichnisses

   Den vollständig qualifizierten Namen für das Verzeichnis, z. B. `corp.example.com`.

   > **Note**
   >
   > Wenn Sie Amazon Route 53 für DNS verwenden möchten, muss sich der Domainname Ihres AWS Managed Microsoft AD von Ihrem Route 53-Domainnamen unterscheiden. Probleme mit der DNS-Auflösung können auftreten, wenn Route 53 und AWS Managed Microsoft AD denselben Domainnamen verwenden.

   NetBIOS-Name des Verzeichnisses

   Die kurzen Namen für das Verzeichnis, z. B. `CORP`.

   Verzeichnisbeschreibung

   Eine optionale Beschreibung des Verzeichnisses.

Administratorpasswort

Das Passwort für den Verzeichnisadministrator. Mit der Verzeichniserstellung wird ein Administratorkonto mit dem Benutzernamen `Admin` und diesem Passwort angelegt.

Das Passwort darf das Wort „admin“ nicht beinhalten.

Das Verzeichnisadministrator-Passwort unterscheidet zwischen Groß-/ Kleinschreibung und muss zwischen 8 und 64 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:

- Kleinbuchstaben (a – z)
- Großbuchstaben (A – Z)
- Zahlen (0 – 9)
- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Confirm password (Passwort bestätigen)

Geben Sie das Administratorpasswort erneut ein.

4. Geben Sie auf der Seite Choose VPC and subnets (VPC und Subnetze wählen) die folgenden Informationen an und wählen Sie dann Next (Weiter).

   VPC

   Die VPC für das Verzeichnis.

   Subnets

   Wählen Sie Subnetze für die Domain-Controller aus. Die beiden Subnetze müssen zu verschiedenen Availability-Zonen gehören.

5. Überprüfen Sie auf der Seite Review & create (Überprüfen und erstellen) die Verzeichnisinformationen und nehmen Sie gegebenenfalls Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen). Das Erstellen des Verzeichnisses dauert 20 bis 40 Minuten. Sobald sie erstellt wurden, ändert sich der Status in Active.

Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt

Wenn Sie ein Active Directory mit AWS Managed Microsoft AD erstellen, AWS Directory Service führt in Ihrem Namen die folgenden Aufgaben aus:

- Erstellt automatisch eine Elastic-Network-Schnittstelle (ENI) und ordnet sie jedem Ihrer Domain-Controller zu. Jede dieser ENIs ist für die Konnektivität zwischen Ihrer VPC und den AWS Directory Service Domänencontrollern unerlässlich und sollte niemals gelöscht werden. Sie können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, AWS Directory Service anhand der Beschreibung identifizieren: "Netzwerkschnittstelle für Verzeichnis-ID AWS wurde erstellt“. Weitere Informationen finden Sie unter Elastic Network Interfaces im Amazon EC2 EC2-Benutzerhandbuch. Der Standard-DNS-Server von AWS Managed Microsoft AD Active Directory ist der VPC-DNS-Server bei Classless Inter-Domain Routing (CIDR) +2. Weitere Informationen finden Sie unter Amazon DNS-Server im Amazon VPC-Benutzerhandbuch.

  > **Note**
  >
  > Domain-Controller werden standardmäßig in zwei Availability Zones in einer Region bereitgestellt und mit Ihrer Amazon VPC (VPC) verbunden. Backups werden automatisch einmal täglich erstellt, und die Amazon EBS (EBS) -Volumes werden verschlüsselt, um sicherzustellen, dass die Daten im Ruhezustand gesichert sind. Domain-Controller, die ausfallen, werden automatisch in derselben Availability Zone unter Verwendung derselben IP-Adresse ersetzt, und eine vollständige Notfallwiederherstellung kann unter Verwendung des letzten Backups durchgeführt werden.

- Stellt Active Directory innerhalb Ihrer VPC mit zwei Domain-Controllern für Fehlertoleranz und hohe Verfügbarkeit bereit. Nachdem das Verzeichnis erfolgreich erstellt wurde und Aktiv ist, können weitere Domain-Controller bereitgestellt werden, um die Ausfallsicherheit und Leistung zu erhöhen. Weitere Informationen finden Sie unter Bereitstellen zusätzlicher Domain-Controller.

  > **Note**
  >
  > AWS erlaubt nicht die Installation von Monitoring-Agents auf AWS verwalteten Microsoft AD-Domänencontrollern.

- Erstellt eine AWS -Sicherheitsgruppe, die einen Netzwerkfilter für ein- und ausgehenden Datenverkehr Ihrer Domain-Controller einrichtet. Die Standardregel für ausgehenden Datenverkehr erlaubt den gesamten Datenverkehr, ENIs oder Instanzen, die an die erstellte AWS Sicherheitsgruppe angehängt sind. Die standardmäßige Regel für eingehenden Datenverkehr erlaubt nur den Datenverkehr über Ports, die von Active Directory aus jeder Quelle (0.0.0.0/0) benötigt werden. Die 0.0.0.0/0-Regeln führen nicht zu Sicherheitslücken, da der Datenverkehr zu den Domänencontrollern auf den Datenverkehr von Ihrer VPC, von anderen Peer-VPCs oder von

Netzwerken beschränkt ist, die Sie über AWS Transit Gateway oder Virtual Private AWS Direct Connect Network verbunden haben. Zur zusätzlichen Sicherheit sind den erstellten ENIs keine Elastic IPs zugeordnet und Sie haben keine Berechtigung, diesen ENIs eine Elastic IP zuzuordnen. Daher ist der einzige eingehende Datenverkehr, der mit Ihrem AWS verwalteten Microsoft AD kommunizieren kann, lokaler VPC- und VPC-gerouteter Verkehr. Seien Sie äußerst vorsichtig, wenn Sie versuchen, diese Reglen zu ändern, da Sie die Fähigkeit zur Kommmunikation mit Ihren Domain-Controllern beeinträchtigen können. Weitere Informationen finden Sie unter Bewährte Methoden für AWS Managed Microsoft AD. Die folgenden AWS Sicherheitsgruppenregeln werden standardmäßig erstellt:

Regeln für eingehenden Datenverkehr

Protokoll	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
ICMP	N/A	0.0.0.0/0	Ping	LDAP Keep Alive, DFS
TCP und UDP	53	0.0.0.0/0	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauensstellungen
TCP und UDP	88	0.0.0.0/0	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauensstellungen auf Gesamtstrukturebene

Protokoll	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP und UDP	389	0.0.0.0/0	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP und UDP	445	0.0.0.0/0	SMB/CIFS	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP und UDP	464	0.0.0.0/0	Kerberos Passwort ändern/einrichten	Replikation, Benutzer- und Computerauthentifizierung, Vertrauensstellungen
TCP	135	0.0.0.0/0	Replikation	RPC, EPM

Protokoll	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP	636	0.0.0.0/0	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	1024 - 65535	0.0.0.0/0	RPC	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	3268 - 3269	0.0.0.0/0	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
UDP	123	0.0.0.0/0	Windows-Uhrzeit	Windows-Uhrzeit, Vertrauensstellungen

Protokoll	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
UDP	138	0.0.0.0/0	DFSN & NetLogon	DFS, Gruppenrichtlinie
Alle	Alle	sg-###### ############	Gesamter Datenverkehr	

Regeln für ausgehenden Datenverkehr

Protokoll	Port-Bereich	Bestimmungsort	Datenverkehrstyp	Verwendung von Active Directory
Alle	Alle	sg-###### ############	Gesamter Datenverkehr	

- Weitere Informationen zu den von Active Directory verwendeten Ports und Protokollen finden Sie in der Microsoft-Dokumentation unter Serviceübersicht und Netzwerkportanforderungen für Windows.
- Erstellt ein Verzeichnisadministratorkonto mit dem Benutzernamen Admin und dem angegebenen Passwort. Dieses Konto befindet sich unter der OU Benutzer (Beispiel: Corp > Benutzer). Sie verwenden dieses Konto, um Ihr Verzeichnis in der AWS Cloud zu verwalten. Weitere Informationen finden Sie unter Berechtigungen für das Administratorkonto.

  > **Important**
  >
  > Achten Sie darauf, dieses Passwort zu speichern. AWS Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen werden. Sie können ein Passwort jedoch über die AWS Directory Service Konsole oder mithilfe der ResetUserPasswordAPI zurücksetzen.

- Erstellt die folgenden drei Organisationeinheiten unter dem Domainstamm:

Name der Organisationseinheit	Beschreibung
AWS Delegierte Gruppen	Speichert alle Gruppen, die Sie verwenden können, um AWS bestimmte Berechtigungen an Ihre Benutzer zu delegieren.
AWS Reserviert	Speichert alle AWS verwaltungsspezifischen Konten.

<yourdomainname>	Der Name dieser Organisationseinheit basiert auf dem NetBIOS-Namen, den Sie eingegeben haben, als Sie Ihr Verzeichnis erstellt haben. Wenn Sie keinen NetBIOS-Namen angegeben haben, wird dieser standardmäßig auf den ersten Teil Ihres Verzeichnis-DNS-Namens gesetzt (z. B. im Falle von corp.example.com wäre der NetBIOS-Name corp). Diese Organisationseinheit gehört all Ihren AWS zugehörigen Verzeichnisobjekten AWS und enthält diese, über die Sie Vollzugriff haben. Zwei untergeordnete OUs existieren unter dieser Organisationseinheit standardmäßig, Computer und Benutzer. Beispielsweise:
	• Corp
	  • Computers (Computer)
	  • Benutzer

- Erstellt die folgenden Gruppen in der Organisationseinheit AWS Delegated Groups:

Group name (Gruppenname)	Beschreibung
AWS Operatoren für delegierte Konten	Mitglieder dieser Sicherheitsgruppe verfügen über begrenzte Funktionen zur Kontoverwaltung, wie beispielsweise das Zurücksetzen von Passwörtern

Group name (Gruppenname)	Beschreibung
AWS Delegierte Active-Directory-basierte Aktivierungsadministratoren	Mitglieder dieser Sicherheitsgruppe können Active-Directory-Volumenlizenzaktivierungsobjekte erstellen, die es Unternehmen ermöglichen, Computer über eine Verbindung zu ihrer Domain zu aktivieren.
AWS Delegiertes Hinzufügen von Arbeitsstationen zu Domänenbenutzern	Mitglieder dieser Sicherheitsgruppe können einer Domain 10 Computer hinzufügen.
AWS Delegierte Administratoren	Mitglieder dieser Sicherheitsgruppe können AWS Managed Microsoft AD verwalten, haben volle Kontrolle über alle Objekte in Ihrer Organisationseinheit und können Gruppen verwalten, die in der Organisationseinheit AWS Delegated Groups enthalten sind.
AWS Delegiert: Darf Objekte authentifizieren	Mitgliedern dieser Sicherheitsgruppe wird die Möglichkeit gegeben, sich bei Computerressourcen in der AWS reservierten Organisationseinheit zu authentifizieren (nur für lokale Objekte mit aktivierter selektiver Authentifizierung als Trusts erforderlich).
AWS Delegiert: Zur Authentifizierung bei Domänencontrollern zugelassen	Mitglieder dieser Sicherheitsgruppe erhalten die Möglichkeit, sich bei Computerressourcen in der OU Domain-Controller zu authentifizieren (nur für On-Premises-Objekte mit Vertrauensstellungen mit aktivierter selektiver Authentifizierung erforderlich).
AWS Delegierte Administratoren für die Gültigkeitsdauer gelöschter Objekte	Mitglieder dieser Sicherheitsgruppe können das DeletedObjectLifetime MSDS-Objekt ändern, das festlegt, wie lange ein gelöschtes Objekt für die Wiederherstellung aus dem AD-Papierkorb verfügbar ist.

Group name (Gruppenname)	Beschreibung
AWS Delegierte Administratoren verteilter Dateisysteme	Mitglieder dieser Sicherheitsgruppe können FRS-, DFS-R- und DFS-Namensräume hinzufügen.
AWS Delegierte Administratoren von Domainnamensystemen	Mitglieder dieser Sicherheitsgruppe können das in Active-Directory-integrierte DNS verwalten.
AWS Delegierte Administratoren des Dynamic Host Configuration Protocol	Mitglieder dieser Sicherheitsgruppe können Windows DHCP-Servern im Unternehmen autorisieren.
AWS Delegierte Administratoren von Enterpris e Certificate Authority	Mitglieder dieser Sicherheitsgruppe können die Microsoft Enterprise Certificate Authority-Infrastruktur bereitstellen und verwalten.
AWS Delegierte, fein abgestufte Administr atoren für Kennwortrichtlinien	Mitglieder dieser Sicherheitsgruppe können vorab festgelegte differenzierte Passwortr ichtlinien abändern.
AWS Delegierte FSx-Administratoren	Mitglieder dieser Sicherheitsgruppe haben die Möglichkeit, Amazon-FSx-Ressourcen zu verwalten.
AWS Delegierte Gruppenrichtlinien-Administ ratoren	Mitglieder dieser Sicherheitsgruppe können Verwaltungsaufgaben für Gruppenrichtlinien durchführen (erstellen, bearbeiten, löschen, verlinken).
AWS Delegierte Kerberos-Delegierungsadmini stratoren	Mitglieder dieser Sicherheitsgruppe können eine Delegation auf Computer- und Benutzerk ontenobjekten aktivieren.
AWS Delegierte Administratoren für verwaltete Dienstkonten	Mitglieder dieser Sicherheitsgruppe können Managed Service-Konten erstellen und löschen.

Group name (Gruppenname)	Beschreibung
AWS Delegierte, nicht konforme MS-NPRC-Geräte	Mitglieder dieser Sicherheitsgruppe werden von der Anforderung einer Secure Channel Kommunikation mit Domain-Controllern ausgenommen. Diese Gruppe ist für Computerkonten vorgesehen.
AWS Delegierte Administratoren für den Fernzugriffsdienst	Mitglieder dieser Sicherheitsgruppe können RAS-Server aus der Gruppe der RAS- und IAS-Server hinzufügen und entfernen.
AWS Delegierte Administratoren für replizierte Verzeichnisänderungen	Mitglieder dieser Sicherheitsgruppe können Profilinformationen in Active Directory mit dem SharePoint Server synchronisieren.
AWS Delegierte Serveradministratoren	Mitglieder dieser Sicherheitsgruppe sind in der lokalen Administratorgruppe auf allen mit der Domain verknüpften Computern enthalten.
AWS Delegierte Sites- und Services-Administratoren	Mitglieder dieser Sicherheitsgruppe können das Default-First-Site-Name-Objekt an Active-Directory-Standorten und in Active-Directory-Services umbenennen.
AWS Delegierte Systemverwaltungsadministratoren	Mitglieder dieser Sicherheitsgruppe können Objekte im Systemverwaltungscontainer erstellen und verwalten.
AWS Delegierte Administratoren für die Terminalserver-Lizenzierung	Mitglieder dieser Sicherheitsgruppe können der Terminal Server License Servers-Gruppe Terminal Server License Server hinzufügen und sie daraus entfernen.
AWS Delegierte Administratoren mit Benutzerprinzipalnamensuffixen	Mitglieder dieser Sicherheitsgruppe können Suffixe für den Benutzer-Prinzipalnamen hinzufügen und entfernen.

- Erstellt die folgenden Gruppenrichtlinienobjekte (GPOs) und wendet sie an:

> **Note**
>
> Sie sind nicht berechtigt, diese GPOs zu löschen, zu ändern oder die Verknüpfung aufzuheben. Dies ist beabsichtigt, da sie der Verwendung vorbehalten AWS sind. Sie können sie bei Bedarf mit OUs verknüpfen, die Sie kontrollieren.

Gruppenrichtlinienname	Gilt für	Beschreibung
Standard-Domainrichtlinie	Domain	Beinhaltet Domainpasswort und Kerberos-Richtlinien.
ServerAdmins	Alle Computerkonten, die keine Domain-Controller sind	Fügt die „AWS Delegierten Serveradministratoren“ als Mitglied der Gruppe BUILTIN\ Administrators hinzu.
AWS Reservierte Richtlinie: Benutzer	AWS Reservierte Benutzerk onten	Legt die empfohlenen Sicherheitseinstellungen für alle Benutzerkonten in der AWS reservierten Organisat ionseinheit fest.
AWS Verwaltete Active Directory-Richtlinie	Alle Domain-Controller	Legt die empfohlenen Sicherheitseinstellungen auf allen Domain-Controllern fest.
TimePolicyNT5DS	Alle Domain-Controller, die nicht PDCe sind	Legt für alle Nicht-PDC e-Domain-Controller die Zeitrichtlinie fest, dass sie Windows Time (NT5DS) verwenden.
TimePolicyPDC	Der PDCe-Domain-Controller	Legt fest, dass die Zeitricht linie des PDCe-Domain-Controllers Network Time Protocol (NTP) verwendet.

Gruppenrichtlinienname	Gilt für	Beschreibung
Standardrichtlinie für Domain-Controller	Nicht verwendet	Stattdessen wird die AWS verwaltete Active Directory -Richtlinie verwendet, die während der Domänener stellung bereitgestellt wird.

Wenn Sie die Einstellungen der einzelnen Richtlinien sehen möchten, können Sie diese von einer domainverbundenen Windows-Instance mit aktivierter Gruppenrichtlinien-Verwaltungskonsole (GPMC) aus einsehen.

Berechtigungen für das Administratorkonto

Wenn Sie einen AWS Directory Service für das Microsoft Active Directory-Verzeichnis erstellen, AWS wird eine Organisationseinheit (OU) erstellt, in der alle AWS zugehörigen Gruppen und Konten gespeichert werden. Weitere Informationen über diese OU finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt. Dies umfasst auch das Admin-Konto. Das Admin-Konto verfügt über die Berechtigungen zur Durchführung allgemeiner administrativer Aktivitäten für Ihre OU:

- Hinzufügen, Aktualisieren oder Löschen von Benutzern, Gruppen und Computern. Weitere Informationen finden Sie unter Benutzer und Gruppen in AWS Managed Microsoft AD verwalten.
- Hinzufügen von Ressourcen zu Ihrer Domain, etwa Datei- oder Druckserver, und anschließendes Gewähren der zugehörigen Ressourcenberechtigungen für Benutzer und Gruppen in der OU.
- Erstellen weiterer OUs und Container.
- Delegieren Sie die Autorität für zusätzliche OUs und Container. Weitere Informationen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.
- Erstellen und Verknüpfen von Gruppenrichtlinien.
- Wiederherstellen von gelöschten Objekten aus dem Active Directory-Papierkorb.
- Führen Sie Active Directory- und Windows PowerShell DNS-Module im Active Directory-Webdienst aus.

- Erstellen und konfigurieren von gruppenverwalteten Service-Konten. Weitere Informationen finden Sie unter Gruppenverwaltete Service-Konten.
- Konfigurieren einer eingeschränkten Kerberos-Delegierung. Weitere Informationen finden Sie unter Eingeschränkte Kerberos-Delegierung.

Das Administratorkonto verfügt zudem über die Rechte zum Ausführen der folgenden domainübergreifenden Aktivitäten:

- Verwalten von DNS-Konfigurationen (Hinzufügen, Entfernen oder Aktualisieren von Datensätzen, Zonen und Weiterleitungen)
- Aufrufen von DNS-Ereignisprotokollen
- Anzeigen von Sicherheitsereignisprotokollen

Nur die hier aufgelisteten Aktionen können mit dem Administratorkonto ausgeführt werden. Das Administratorkonto hat keine Berechtigungen für verzeichnisbezogene Aktionen außerhalb Ihrer OU, etwa in der übergeordneten OU.

Important

AWS Domänenadministratoren haben vollen Administratorzugriff auf alle Domänen, auf denen gehostet wird AWS. Weitere Informationen zum AWS Umgang mit Inhalten, einschließlich Verzeichnisinformationen, die AWS Sie auf AWS Systemen speichern, finden Sie in Ihrer Vereinbarung mit AWS und in den häufig gestellten Fragen zum Datenschutz.

Note

Es wird empfohlen, dieses Konto nicht zu löschen oder umzubenennen. Wenn Sie das Konto nicht mehr verwenden möchten, empfehlen wir Ihnen, ein langes Passwort (maximal 64 zufällige Zeichen) festzulegen und dann das Konto zu deaktivieren.

Privilegierte Enterprise- und Domainadministrator-Konten

AWS wechselt das integrierte Administratorkennwort alle 90 Tage automatisch zu einem zufälligen Passwort. Jedes Mal, wenn das integrierte Administratorkennwort für den menschlichen Gebrauch

angefordert wird, wird ein AWS Ticket erstellt und beim AWS Directory Service Team protokolliert. Die Kontoanmeldeinformationen werden verschlüsselt und über sichere Kanäle verwaltet. Außerdem können die Anmeldeinformationen für das Administratorkonto nur vom AWS Directory Service Managementteam angefordert werden.

Für die operative Verwaltung Ihres Verzeichnisses AWS hat es die ausschließliche Kontrolle über Konten mit Unternehmensadministrator- und Domänenadministratorrechten. Dies beinhaltet die ausschließliche Kontrolle über das Active Directory-Administratorkonto. AWS schützt dieses Konto, indem die Passwortverwaltung mithilfe eines Passwort-Tresors automatisiert wird. AWS Erstellt während der automatischen Rotation des Administratorkennworts ein temporäres Benutzerkonto und gewährt ihm Domänenadministratorrechte. Dieses temporäre Konto wird im Falle eines Passwortrotationsfehlers im Administratorkonto als Backup verwendet. AWS Löscht nach AWS erfolgreicher Rotation des Administratorkennworts das temporäre Administratorkonto.

Normalerweise wird das Verzeichnis vollständig automatisiert AWS betrieben. Falls ein Automatisierungsprozess ein Betriebsproblem nicht lösen AWS kann, muss sich möglicherweise ein Support-Techniker bei Ihrem Domänencontroller (DC) anmelden, um die Diagnose durchzuführen. AWS Implementiert in diesen seltenen Fällen ein Anforderungs-/Benachrichtigungssystem, um den Zugriff zu gewähren. Bei diesem Vorgang erstellt die AWS Automatisierung ein zeitlich begrenztes Benutzerkonto in Ihrem Verzeichnis, das über Domänenadministratorberechtigungen verfügt. AWS ordnet das Benutzerkonto dem Techniker zu, der mit der Bearbeitung Ihres Verzeichnisses beauftragt ist. AWS zeichnet diese Zuordnung in unserem Protokollsystem auf und stellt dem Techniker die zu verwendenden Anmeldeinformationen zur Verfügung. Alle durchgeführten Aktionen des Technikers werden in den Windows-Ereignisprotokollen protokolliert. Wenn die zugeordnete Zeit verstrichen ist, löscht die Automatisierung das Benutzerkonto.

Sie können administrative Aktivitäten überwachen, indem Sie das Protokoll-Weiterleitungsfeature Ihres Verzeichnisses verwenden. Mit dieser Funktion können Sie die AD Security-Ereignisse an Ihr CloudWatch System weiterleiten, wo Sie Überwachungslösungen implementieren können. Weitere Informationen finden Sie unter Protokollweiterleitung aktivieren.

Die Sicherheitsereignis-IDs 4 624, 4 672 und 4 648 werden alle protokolliert, wenn sich jemand interaktiv bei einem DC anmeldet. Sie können das Windows Security-Ereignisprotokoll jedes DCs mit der Ereignisanzeige Microsoft Management Console (MMC) von einem Windows-Computer aus einsehen, der einer Domain angeschlossen ist. Sie können auch Protokollweiterleitung aktivieren alle CloudWatch Sicherheitsereignisprotokolle an Logs in Ihrem Konto senden.

Es kann gelegentlich vorkommen, dass Benutzer innerhalb der AWS reservierten Organisationseinheit erstellt und gelöscht wurden. AWS ist verantwortlich für die Verwaltung und

Sicherheit aller Objekte in dieser Organisationseinheit und allen anderen Organisationseinheiten oder Containern, deren Zugriff und Verwaltung wir Ihnen nicht delegiert haben. Möglicherweise sehen Sie Erstellungen und Löschungen in dieser Organisationseinheit. Dies liegt daran, dass das Domänenadministratorkennwort AWS Directory Service mithilfe von Automatisierung regelmäßig gewechselt wird. Wenn das Passwort rotiert wird, wird ein Backup erstellt, falls die Rotation fehlschlägt. Sobald die Rotation erfolgreich ist, wird das Backup-Konto automatisch gelöscht. Für den seltenen Fall, dass zur Fehlerbehebung interaktiver Zugriff auf die DCs erforderlich ist, wird außerdem ein temporäres Benutzerkonto für einen AWS Directory Service Techniker erstellt. Sobald ein Techniker seine Arbeit abgeschlossen hat, wird das temporäre Benutzerkonto gelöscht. Beachten Sie, dass jedes Mal, wenn interaktive Anmeldeinformationen für ein Verzeichnis angefordert werden, das AWS Directory Service Managementteam benachrichtigt wird.

Wichtige Konzepte für AWS Managed Microsoft AD

Sie können AWS Managed Microsoft AD besser nutzen, wenn Sie mit den folgenden wesentlichen Konzepten vertraut sind.

Themen

Active-Directory-Schema

Ein Schema ist die Definition von Attributen und Klassen, die Teil eines verteilten Verzeichnisses sind, ähnlich wie Felder und Tabellen in einer Datenbank. Schemas umfassen eine Reihe von Regeln, die die Art und das Format der Daten bestimmen, die hinzugefügt oder in der Datenbank gespeichert werden. Die Benutzerklasse ist ein Beispiel für eine Klasse, die in der Datenbank gespeichert ist. Beispielsweise können Benutzerklasse-Attribute Vorname, Nachname, Telefonnummer und so weiter sein.

Schemaelemente

Attribute, Klassen und Objekte sind die grundlegenden Elemente zum Erstellen von Objektdefinitionen im Schema. Im Folgenden finden Sie Details zu Schemaelementen, die Sie kennen sollten, bevor Sie mit der Erweiterung Ihres AWS-Managed-Microsoft-AD-Schemas beginnen.

Attribute

Schemaattribute können mit den Feldern in einer Datenbank verglichen werden. Jedes Schemaattribut hat mehrere Eigenschaften, die die Merkmale des Attributs definieren. Die Eigenschaft, die von LDAP-Clients zum Lesen und Schreiben des Attributs verwendet wird, lautet beispielsweise `LDAPDisplayName`. Die Eigenschaft `LDAPDisplayName` muss für alle Attribute und Klassen eindeutig sein. Eine vollständige Liste der Attributeigenschaften finden Sie auf der MSDN-Website im Bereich mit den Merkmalen von Attributen. Weitere Informationen zum Erstellen eines neuen Attributs finden Sie auf der MSDN-Website im Bereich zum Definieren eines neuen Attributs.

Klassen

Klassen sind vergleichbar mit Tabellen in einer Datenbank und haben ebenfalls verschiedene definierbare Eigenschaften. `objectClassCategory` definiert zum Beispiel die Kategorie der Klasse. Eine vollständige Liste der Klasseneigenschaften finden Sie auf der MSDN-Website im Bereich mit den Merkmalen von Objektklassen. Weitere Informationen zum Erstellen einer neuen Klasse finden Sie auf der MSDN-Website im Bereich zum Definieren einer neuen Klasse.

Objekt-ID (OID)

Alle Klassen und Attribute müssen für alle Ihre Objekte eine eindeutige OID aufweisen. Softwareanbieter müssen eine eigene OID abrufen, damit die Eindeutigkeit gewährleistet werden kann. Die Eindeutigkeit verhindert Konflikte, wenn dasselbe Attribut von mehreren Anwendungen für unterschiedliche Zwecke genutzt wird. Damit die Eindeutigkeit gewährleistet wird, können Sie eine Stamm-OID von einer Namensregistrierungsstelle gemäß ISO anfordern. Sie haben auch die Möglichkeit, eine Basis-OID von Microsoft zu erhalten. Weitere Informationen zu OIDs und zum Anfordern von OIDs finden Sie auf der MSDN-Website im Bereich zu Objektkennungen.

Mit einem Schema verknüpfte Attribute

Einige Attribute sind über Forward- und Back-Links zwischen zwei Klassen verknüpft. Das beste Beispiel hierfür sind Gruppen. Wenn Sie eine Gruppe aufrufen, sehen Sie die zugehörigen Mitglieder. Wenn Sie einen Benutzer aufrufen, sehen Sie, zu welchen Gruppen er gehört. Wenn Sie einer Gruppe einen Benutzer hinzufügen, erstellt Active Directory einen Forward-Link zur Gruppe. Zudem fügt Active Directory einen Back-Link von der Gruppe zum Benutzer hinzu. Beim Erstellen eines Attributs, das verknüpft werden soll, muss eine eindeutige Link-ID generiert werden. Weitere Informationen finden Sie auf der MSDN-Website im Bereich zu verknüpften Attributen.

Verwandte Themen

- Wann sollte das Schema von AWS Managed Microsoft AD erweitert werden?
- Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas

Patchen und Wartung für AWS Managed Microsoft AD

AWS Directory Service for Microsoft Active Directory, auch als AWS DS für AWS Managed Microsoft AD bezeichnet, ist eigentlich Microsoft Active Directory Domain Services (AD DS), das als verwalteter Service bereitgestellt wird. Das System verwendet Microsoft Windows Server 2019 für die Domain-Controller (DCs). AWS fügt den Domain-Controllern Software für die Verwaltung von Diensten hinzu. AWS aktualisiert (patcht) Domain-Controller, um neue Funktionalität hinzuzufügen und die Software von Microsoft Windows Server auf dem aktuellen Stand zu halten. Während des Patchings kann Ihr Verzeichnis weiterhin genutzt werden.

Sicherstellen der Verfügbarkeit

Standardmäßig besteht jedes Verzeichnis aus zwei DCs, die jeweils in einer anderen Availability Zone installiert sind. Nach Ihrer Wahl können Sie DCs hinzufügen, um die Verfügbarkeit weiter zu erhöhen. Für kritische Umgebungen, die hohe Verfügbarkeit und Fehlertoleranz erfordern, empfehlen wir den Einsatz zusätzlicher DCs. AWSpatcht Ihre DCs sequentiell. Während dieser Zeit ist der DC, der aktiv patcht, nicht verfügbar. AWS Wenn ein oder mehrere Domain-Controller vorübergehend außer Betrieb sind, verschiebt AWS das Patching auf einen späteren Zeitpunkt, bis für das Verzeichnis wieder mindestens zwei ausgeführte Domain-Controller verfügbar sind. Auf diese Weise können Sie die anderen funktionierenden DCs während des Patch-Prozesses verwenden, der in der Regel 30 bis 45 Minuten pro DC dauert, wobei diese Zeit jedoch variieren kann. Um sicherzustellen, dass Ihre Anwendungen einen funktionierenden DC erreichen können, wenn einer oder mehrere Ihrer DCs aus irgendeinem Grund nicht verfügbar ist bzw. sind, wie beispielsweise auch beim Patching, sollten Ihre Anwendungen den Windows DC Locator Service nutzen und keine statischen DC-Adressen verwenden.

Verstehen des Patch-Zeitplans

Um die Microsoft Windows Server-Software auf Ihren DCs auf dem aktuellen Stand zu halten, nutzt AWS Microsoft-Updates. Da Microsoft monatlich Rollup-Patches für Windows Server bereitstellt, testet AWS das Rollup so gut wie möglich und wendet es möglichst innerhalb von drei Kalenderwochen auf alle Kunden-DCs an. Darüber hinaus prüft AWS Updates, die Microsoft außerhalb des monatlichen Rollups veröffentlicht, abhängig von ihrer Anwendbarkeit auf DCs und

ihrer Priorität. Im Fall von Sicherheits-Patches, die Microsoft als kritisch oder wichtig einordnet und die für DCs relevant sind, strebt AWS an, den Patch innerhalb von fünf Tagen zu testen und bereitzustellen.

Gruppenverwaltete Service-Konten

Mit Windows Server 2012 hat Microsoft eine neue Methode eingeführt, wie Administratoren Service-Konten verwalten können, sogenannte gruppenverwaltete Service-Konten (group Managed Service Accounts, gMSAs). Dank gMSAs müssen die Service-Administratoren die Passwortsynchronisierung zwischen Service-Instances nicht mehr manuell verwalten. Stattdessen kann ein Administrator einfach ein gMSA in Active Directory erstellen und dann mehrere Service-Instances konfigurieren, um dieses einzelne gMSA zu verwenden.

Um Benutzern in AWS Managed Microsoft AD die nötigen Berechtigungen zu erteilen, damit diese ein gMSA erstellen können, müssen Sie ihre Konten der Sicherheitsgruppe AWS Delegated Managed Service Account Administrators als Mitglied hinzufügen. Standardmäßig ist das Admin-Konto ein Mitglied dieser Gruppe. Weitere Informationen zu gMSAs finden Sie auf der TechNet Microsoft-Website unter Group Managed Service Accounts Overview.

Zugehöriger Blog-Post zur Sicherheit in AWS

- Wie AWS Managed Microsoft AD zur Vereinfachung der Bereitstellung und zur Verbesserung der Sicherheit von Active Directory-Integrated .NET-Anwendungen beiträgt

Eingeschränkte Kerberos-Delegierung

Die eingeschränkte Kerberos-Delegierung ist ein Feature in Windows Server. Mit diesem Feature erhalten Service-Administratoren die Möglichkeit, Vertrauensgrenzen für Anwendungen anzugeben und zu erzwingen, indem der Umfang begrenzt wird, in dem die Anwendungsservices für einen Benutzer agieren können. Dies kann nützlich sein, wenn Sie konfigurieren müssen, welche Front-End-Service-Konten etwas an ihre Back-End-Services delegieren können. Die eingeschränkte Kerberos-Delegierung verhindert auch, dass sich Ihr gMSA mit beliebigen Services für Ihre Active Directory-Benutzer verbindet, womit potenzieller Missbrauch durch einen nicht autorisierten Entwickler vermieden wird.

Angenommen, Benutzer jsmith meldet sich bei einer HR-Anwendung an. Sie möchten, dass der SQL Server die Datenbankberechtigungen von jsmith anwendet. Standardmäßig öffnet SQL Server die Datenbankverbindung jedoch mit den Anmeldeinformationen für das Dienstkonto, die

für das jeweilige Konto gelten hr-app-service, und nicht mit den konfigurierten Berechtigungen von jsmith. Sie müssen der Anwendung für die HR-Gehaltsabrechnung den Zugriff auf die SQL Server-Datenbank unter Verwendung der Berechtigungen von jsmith ermöglichen. Dazu aktivieren Sie die eingeschränkte Kerberos-Delegierung für das hr-app-service Dienstkonto in Ihrem AWS verwalteten Microsoft AD-Verzeichnis in. AWS Wenn sich jsmith anmeldet, stellt Active Directory ein Kerberos-Ticket aus, das Windows automatisch verwendet, wenn jsmith versucht, auf andere Dienste im Netzwerk zuzugreifen. Die Kerberos-Delegierung ermöglicht es dem hr-app-service Konto, das Kerberos-Ticket von jsmith beim Zugriff auf die Datenbank wiederzuverwenden, wodurch beim Öffnen der Datenbankverbindung spezifische Berechtigungen für jsmith zugewiesen werden.

Um Berechtigungen zu erteilen, mit denen Benutzer in AWS Managed Microsoft AD die eingeschränkte Kerberos-Delegierung konfigurieren können, müssen Sie ihre Konten der Sicherheitsgruppe AWS Delegated Kerberos Delegation Administrators als Mitglieder hinzufügen. Standardmäßig ist das Admin-Konto ein Mitglied dieser Gruppe. Weitere Informationen zur eingeschränkten Kerberos-Delegierung finden Sie unter Übersicht über die eingeschränkte Kerberos-Delegierung auf der Microsoft-Website. TechNet

Die ressourcenbasierte eingeschränkte Delegierung wurde mit Windows Server 2012 eingeführt. Sie bietet dem Back-End-Service-Administrator die Möglichkeit, die eingeschränkte Delegierung für den Service zu konfigurieren.

Bewährte Methoden für AWS Managed Microsoft AD

Im Folgenden finden Sie einige Vorschläge und Richtlinien, die Sie berücksichtigen sollten, um Probleme zu vermeiden und das Beste aus AWS Managed Microsoft AD herauszuholen.

Einrichten: Voraussetzungen

Beachten Sie die folgenden Richtlinien, bevor Sie Ihr Verzeichnis erstellen.

Sicherstellen, dass Sie den richtigen Verzeichnistyp verwenden

AWS Directory Service bietet mehrere Möglichkeiten zur Verwendung Microsoft Active Directory mit anderen AWS Diensten. Sie können den Verzeichnisdienst mit den Funktionen wählen, die Sie benötigen, ohne Ihr Budget zu überlasten:

- AWS Der Directory Service für Microsoft Active Directory ist ein funktionsreicher, verwalteter Dienst, der in der Microsoft Active Directory AWS Cloud gehostet wird. AWS Managed Microsoft

AD ist die beste Wahl, wenn Sie mehr als 5.000 Benutzer haben und eine Vertrauensbeziehung zwischen einem AWS gehosteten Verzeichnis und Ihren lokalen Verzeichnissen einrichten möchten.

- AD Connector verbindet einfach Ihr vorhandenes lokales System Active Directory mit AWS. AD Connector ist die beste Wahl, wenn Sie Ihr vorhandenes On-Premises-Verzeichnis mit AWS - Services verwenden möchten.
- Simple AD ist ein niedriges, kostengünstiges Verzeichnis mit grundlegender Active Directory Kompatibilität. Es unterstützt 5 000 oder weniger Benutzer, Samba-4-kompatible Anwendungen und LDAP-Kompatibilität für LDAP-fähige Anwendungen.

Einen detaillierteren Vergleich der AWS Directory Service Optionen finden Sie unterWelche sollte man auswählen.

Sicherstellen, dass Ihre VPCs und Instances korrekt konfiguriert sind

Um eine Verbindung zu Ihren Verzeichnissen herzustellen, sie zu verwalten und zu nutzen, müssen Sie die VPCs, denen die Verzeichnisse zugeordnet sind, ordnungsgemäß konfigurieren. Weitere Informationen über die Anforderungen zur VPC-Sicherheit und Netzwerken finden Sie unter AWS Voraussetzungen für verwaltetes Microsoft AD, AD-Connector-Voraussetzungen oder Simple-AD-Voraussetzungen.

Wenn Sie Ihrer Domain eine Instance hinzufügen, stellen Sie sicher, dass Sie eine Verbindung und Remote-Zugriff auf Ihre Instance haben, wie in Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory beschrieben.

Sich der eigenen Grenzen bewusst sein

Erfahren Sie mehr über die verschiedenen Beschränkungen für Ihren spezifischen Verzeichnistyp. Der verfügbare Speicherplatz und die Gesamtgröße Ihrer Objekte sind die einzigen Einschränkungen in Bezug auf die Anzahl der Objekte, die Sie in Ihrem Verzeichnis speichern können. Einzelheiten zu dem von Ihnen ausgewählten Verzeichnis finden Sie unter AWS Verwaltete Microsoft AD-Kontingente, Kontingente für AD Connector oder Kontingente für Simple AD.

Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut

AWS erstellt eine Sicherheitsgruppe und fügt sie den elastischen Netzwerkschnittstellen des Domänencontrollers Ihres Verzeichnisses hinzu. Diese Sicherheitsgruppe blockiert unnötigen

Datenverkehr zum Domain-Controller und lässt Datenverkehr zu, der für die Active-Directory-Kommunikation erforderlich ist. AWS konfiguriert die Sicherheitsgruppe so, dass nur die Ports geöffnet werden, die für die Active-Directory-Kommunikation erforderlich sind. In der Standardkonfiguration akzeptiert die Sicherheitsgruppe Datenverkehr zu diesen Ports von jeder beliebigen IP-Adresse aus. AWS hängt die Sicherheitsgruppe an die Schnittstellen Ihrer Domänencontroller an, auf die von Ihren Peering-VPCs aus zugegriffen werden kann oder deren Größe geändert wurde. Der Zugriff auf diese Schnittstellen ist nicht über das Internet möglich, auch wenn Sie Routing-Tabellen ändern, die Netzwerkverbindungen zu Ihrer VPC ändern und den NAT Gateway-Service konfigurieren. Daher können nur Instances und Computer, die über einen Netzwerkpfad in die VPC verfügen, auf das Verzeichnis zugreifen. Dies vereinfacht die Einrichtung, weil es nicht mehr erforderlich ist, spezifische Adressbereiche zu konfigurieren. Stattdessen konfigurieren Sie Routen und Sicherheitsgruppen in der VPC, die Datenverkehr von vertrauenswürdigen Instances und Computern aus zulassen.

Ändern der Verzeichnissicherheitsgruppe

Wenn Sie die Sicherheit der Sicherheitsgruppen Ihrer Verzeichnisse erhöhen wollen, können Sie sie so abändern, dass sie Datenverkehr von einer restriktiveren IP-Adressliste akzeptieren. Beispielsweise könnten Sie die akzeptierten Adressen von 0.0.0.0/0 in einen CIDR-Bereich ändern, der spezifisch für ein einzelnes Subnetz oder einen Computer ist. Ebenso könnten Sie die Zieladressen einschränken, mit denen Ihre Domain-Controller kommunizieren können. Nehmen Sie diese Änderungen nur vor, wenn Sie verstehen, wie Sicherheitsgruppenfilter funktionieren. Weitere Informationen finden Sie unter Amazon-EC2-Sicherheitsgruppen für Linux-Instances im Amazon-EC2-Benutzerhandbuch. Unsachgemäße Änderungen können zum Verlust der Kommunikation mit den vorgesehenen Computern und Instanzen führen. AWS empfiehlt, nicht zu versuchen, zusätzliche Ports für den Domänencontroller zu öffnen, da dies die Sicherheit Ihres Verzeichnisses beeinträchtigt. Sehen Sie sich das AWS -Modell übergreifender Verantwortlichkeit genau an.

> **Warning**
>
> Es ist technisch möglich, dass Sie die Sicherheitsgruppen, die Ihr Verzeichnis verwendet, anderen EC2-Instances zuordnen, die Sie erstellen. AWS Empfiehlt jedoch, von dieser Vorgehensweise abzuraten. AWS kann Gründe haben, die Sicherheitsgruppe ohne vorherige Ankündigung zu ändern, um den Funktions- oder Sicherheitsanforderungen des verwalteten Verzeichnisses gerecht zu werden. Solche Änderungen wirken sich auf alle Instances aus, die Sie der Verzeichnis-Sicherheitsgruppe zuordnen. Außerdem entsteht durch die Zuordnung der Verzeichnis-Sicherheitsgruppe zu Ihren EC2-Instances ein potenzielles Sicherheitsrisiko für Ihre EC2-Instances. Die Verzeichnis-Sicherheitsgruppe akzeptiert

Datenverkehr auf erforderlichen Active Directory-Ports von jeder beliebigen IP-Adresse aus. Wenn Sie diese Sicherheitsgruppe einer EC2-Instance zuordnen, die eine öffentliche IP-Adresse im Internet hat, kann jeder Computer im Internet über die geöffneten Ports mit Ihrer EC2-Instance kommunizieren.

Einrichten: Erstellen Ihres Verzeichnisses

Hier finden Sie einige Vorschläge, wie Sie Ihr Verzeichnis erstellen.

Ihre Administratoren-ID und das Passwort nicht vergessen

Wenn Sie Ihr Verzeichnis einrichten, geben Sie ein Passwort für das Administratorkonto ein. Diese Konto-ID lautet Admin für AWS Managed Microsoft AD. Merken Sie sich das Passwort, das Sie für dieses Konto erstellen. Andernfalls können Sie keine Objekte in Ihrem Verzeichnis hinzufügen.

Erstellen einer DHCP-Optionsliste

Wir empfehlen, dass Sie einen DHCP-Optionssatz für Ihr AWS Directory Service Verzeichnis erstellen und den DHCP-Optionssatz der VPC zuweisen, in der sich Ihr Verzeichnis befindet. Auf diese Weise können alle Instances in dieser VPC auf die angegebene Domain zeigen und DNS-Server können ihre Domain-Namen auflösen.

Weitere Informationen zu den DHCP-Optionen finden Sie unter Erstellen oder ändern Sie einen DHCP-Optionssatz.

Aktivieren Sie die Einstellung für die bedingte Weiterleitung

Die folgenden Einstellungen für die bedingte Weiterleitung Speichern Sie diese bedingte Weiterleitung in Active Directory und replizieren Sie sie wie folgt: sollten aktiviert sein. Durch die Aktivierung dieser Einstellungen wird verhindert, dass die Einstellung für die bedingte Weiterleitung verschwindet, wenn ein Knoten aufgrund eines Infrastruktur- oder Überlastungsausfalls ersetzt wird.

Bereitstellen zusätzlicher Domain-Controller

Standardmäßig werden zwei Domänencontroller AWS erstellt, die sich in separaten Availability Zones befinden. Dies sorgt für Fehlerresilienz während des Software-Patchings und anderen Ereignissen, aufgrund derer ein Domain-Controller möglicherweise nicht erreichbar oder nicht verfügbar ist. Wir empfehlen, zusätzliche Domain-Controller bereitzustellen, um die Resilienz weiter zu erhöhen und die

Leistung der horizontalen Skalierung bei einem längerfristigen Ereignis sicherzustellen, das sich auf den Zugriff auf einen Domain-Controller oder eine Availability Zone auswirkt.

Weitere Informationen finden Sie unter Den Windows-DC-Suchservice verwenden.

Einschränkungen für Benutzernamen für AWS -Anwendungen verstehen

AWS Directory Service unterstützt die meisten Zeichenformate, die bei der Erstellung von Benutzernamen verwendet werden können. Es gibt jedoch Zeichenbeschränkungen, die für Benutzernamen gelten, die für die Anmeldung bei AWS Anwendungen wie WorkSpaces Amazon, Amazon oder Amazon WorkDocs verwendet werden. WorkMail QuickSight Diese Einschränkungen verlangen, dass die folgenden Zeichen nicht verwendet werden:

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

> **Note**
>
> Das Symbol @ ist zulässig, wenn es einem UPN-Suffix vorausgeht.

Verwenden Ihres Verzeichnisses

Hier finden Sie einige Vorschläge zur Verwendung Ihres Verzeichnisses.

Keine vordefinierten Benutzer, Gruppen und Organisationseinheiten ändern

Wenn Sie AWS Directory Service zum Starten eines Verzeichnisses verwenden, AWS wird eine Organisationseinheit (OU) erstellt, die alle Objekte Ihres Verzeichnisses enthält. Diese OU erhält den NetBIOS-Namen, den Sie beim Erstellen des Verzeichnisses eingegeben haben, und befindet sich im Domainstamm. Der Domänenstamm gehört und wird von diesem verwaltet AWS. Ebenso werden mehrere Gruppen und Benutzer erstellt.

Diese vordefinierten Objekte nicht verschieben, löschen oder auf andere Weise ändern! Dies kann dazu führen, dass sowohl Sie als auch Sie nicht auf Ihr Verzeichnis zugreifen können. AWS Weitere Informationen finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.

Automatisch mit Domains verbinden

Beim Starten einer Windows-Instanz, die Teil einer AWS Directory Service Domäne sein soll, ist es oft am einfachsten, der Domäne im Rahmen der Instanzerstellung beizutreten, anstatt die Instanz später manuell hinzuzufügen. Um eine Domain automatisch hinzuzufügen, wählen Sie einfach das richtige Verzeichnis für Domain join directory beim Starten einer neuen Instance. Details finden Sie in Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory.

Vertrauensstellungen korrekt einrichten

Beachten Sie beim Einrichten einer Vertrauensstellung zwischen Ihrem AWS verwalteten Microsoft AD-Verzeichnis und einem anderen Verzeichnis die folgenden Richtlinien:

- Der Vertrauenstyp muss auf beiden Seiten übereinstimmen (Gesamtstruktur oder Extern)
- Stellen Sie sicher, dass die Vertrauensrichtung korrekt eingerichtet ist, wenn Sie eine unidirektionale Vertrauensstellung verwenden (Ausgehend von der Trusting Domain, Eingehend auf der Trusted Domain)
- Sowohl vollqualifizierte Domainnamen (FQDNs) als auch NetBIOS-Namen müssen zwischen Gesamtstrukturen/Domains eindeutig sein

Weitere Details und Anweisungen zum Einrichten einer Vertrauensstellung finden Sie unter Erstellen einer Vertrauensstellung.

Verwalten Ihres Verzeichnisses

Beachten Sie die folgenden Vorschläge für die Verwaltung von Ihrem Verzeichnis.

Die Leistung Ihres Domain-Controllers verfolgen

Um Skalierungsentscheidungen zu optimieren und die Stabilität und Leistung von Verzeichnissen zu verbessern, empfehlen wir die Verwendung von CloudWatch Metriken. Weitere Informationen finden Sie unter Ihre Domain-Controller mit Leistungsmetriken überwachen.

Anweisungen zum Einrichten von Domänencontroller-Metriken mithilfe der CloudWatch Konsole finden Sie unter So automatisieren Sie die AWS verwaltete Microsoft AD-Skalierung auf der Grundlage von Nutzungsmetriken im AWS Sicherheitsblog.

Schemaerweiterungen sorgfältig planen

Wenden Sie Schemaerweiterungen gut durchdacht an, um Ihr Verzeichnis nach wichtigen und häufigen Abfragen zu indizieren. Achten Sie darauf, keinen zu umfangreichen Index zu verwenden, da Indizes viel Verzeichnisspeicherplatz beanspruchen und schnell ändernde indizierte Werte zu Leistungsproblemen führen können. Zum Hinzufügen von Indizes müssen Sie eine Lightweight Directory Access Protocol (LDAP) Directory Interchange Format (LDIF)-Datei erstellen und Ihre Schemaänderung erweitern. Weitere Informationen finden Sie unter Ihr Schema erweitern.

Über Load Balancer

Verwenden Sie keinen Load Balancer vor den AWS verwalteten Microsoft AD-Endpunkten. Microsoft hat Active Directory (AD) für die Nutzung eines Domain-Controller (DC)-Erkennungsalgorithmus entwickelt, der den reaktionsschnellsten DC ohne externen Lastausgleich findet. Externe Network Load Balancer erkennen aktive DCs nur ungenau. Dies kann dazu führen, dass Ihre Anwendung an einen DC gesendet wird, der noch nicht bereit ist. Weitere Informationen finden Sie unter Load Balancers and Active Directory auf Microsoft. Dort wird empfohlen TechNet , Anwendungen so zu reparieren, dass Active Directory korrekt verwendet wird, anstatt externe Load Balancer zu implementieren.

Ein Backup Ihrer Instance erstellen

Wenn Sie einer vorhandenen AWS Directory Service Domäne manuell eine Instanz hinzufügen möchten, erstellen Sie zunächst eine Sicherungskopie oder erstellen Sie einen Snapshot dieser Instanz. Dies ist besonders wichtig, wenn der Beitritt zu einer Linux-Instance erfolgt. Einige der Verfahren zum Hinzufügen einer Instance können, wenn sie nicht richtig durchgeführt werden, Ihre Instance nicht erreichbar oder nicht verwendungsfähig machen. Weitere Informationen finden Sie unter Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen.

SNS-Messaging einrichten

Mit Amazon Simple Notification Service (Amazon SNS) können Sie E-Mail- oder Text-Nachrichten (SMS) erhalten, wenn sich der Status Ihres Verzeichnisses ändert. Sie werden benachrichtigt, wenn Ihr Verzeichnis von einem Active-Status in einen Impaired- oder Inoperable-Status übergeht. Außerdem erhalten Sie eine Benachrichtigung, wenn das Verzeichnis in einen aktiven Status zurückkehrt.

Denken Sie auch daran, dass Sie, wenn Sie ein SNS-Thema haben AWS Directory Service, von dem Nachrichten empfangen werden, Ihr Verzeichnis einem anderen SNS-Thema zuordnen sollten,

bevor Sie dieses Thema aus der Amazon SNS-Konsole löschen. Andernfalls riskieren Sie, wichtige Verzeichnis-Statusmeldungen zu verpassen. Informationen zum Einrichten von Amazon SNS; finden Sie unter Konfiguration von Verzeichnisstatusbenachrichtigungen mit Amazon SNS.

Verzeichnisdienst-Einstellungen anwenden

AWS Mit Managed Microsoft AD können Sie Ihre Sicherheitskonfiguration an Ihre Compliance- und Sicherheitsanforderungen anpassen. AWS Managed Microsoft AD stellt die Konfiguration auf allen Domänencontrollern in Ihrem Verzeichnis bereit und verwaltet sie, auch wenn neue Regionen oder zusätzliche Domänencontroller hinzugefügt werden. Sie können diese Sicherheitseinstellungen für alle Ihre neuen und vorhandenen Verzeichnisse konfigurieren und anwenden. Sie können dies in der Konsole tun, indem Sie den Schritten in Sicherheitseinstellungen für Verzeichnisse bearbeiten oder über die UpdateSettings API folgen.

Weitere Informationen finden Sie unter Verzeichnis-Sicherheitseinstellungen konfigurieren.

Amazon Enterprise-Anwendungen vor dem Löschen eines Verzeichnisses entfernen

Bevor Sie ein Verzeichnis löschen, das mit einer oder mehreren Amazon Enterprise Applications wie Amazon WorkSpaces Application Manager, Amazon WorkDocs, Amazon oder Amazon WorkMail Relational Database Service (Amazon RDS) verknüpft ist, müssen Sie zunächst jede Anwendung entfernen. WorkSpaces AWS Management Console Weitere Informationen zum Entfernen dieser Anwendungen finden Sie unter Löschen Sie Ihr AWS verwaltetes Microsoft AD.

Beim Zugriff auf die SYSVOL- und NETLOGON-Freigaben SMB 2.x-Clients verwenden

Client-Computer verwenden Server Message Block (SMB), um auf die SYSVOL- und NETLOGON-Freigaben auf AWS verwalteten Microsoft AD-Domänencontrollern für Gruppenrichtlinien, Anmeldeskripts und andere Dateien zuzugreifen. AWS Managed Microsoft AD unterstützt nur SMB Version 2.0 (SMBv2) und neuer.

Die Protokolle SMBv2 und neuere Version fügen eine Reihe von Features hinzu, die die Clientleistung verbessern und die Sicherheit Ihrer Domain-Controller und Clients erhöhen. Diese Änderung folgt den Empfehlungen vom United States Computer Emergency Readiness Team und von Microsoft, SMBv1 zu deaktivieren.

> **Important**
>
> Wenn Sie derzeit SMBv1-Clients für den Zugriff auf die SYSVOL- und NETLOGON-Freigaben Ihres Domain-Controllers verwenden, müssen Sie diese Clients aktualisieren, um

SMBv2 oder neuer zu verwenden. Ihr Verzeichnis wird ordnungsgemäß funktionieren, aber Ihre SMBv1-Clients können keine Verbindung zu den SYSVOL- und NETLOGON-Freigaben Ihrer AWS verwalteten Microsoft AD-Domänencontroller herstellen und können auch keine Gruppenrichtlinien verarbeiten.

SMBv1-Clients arbeiten mit allen anderen vorhandenen SMBv1-kompatiblen Dateiservern. AWS Empfiehlt jedoch, dass Sie alle Ihre SMB-Server und -Clients auf SMBv2 oder neuer aktualisieren. Weitere Informationen zur Deaktivierung von SMBv1 und zur Aktualisierung auf neuere SMB-Versionen auf Ihren Systemen finden Sie in diesen Beiträgen auf Microsoft und in der Dokumentation. TechNet Microsoft

Verfolgen von SMBv1-Remoteverbindungen

Sie können das Microsoft-Windows-SMBServer/Audit Windows-Ereignisprotokoll überprüfen, wenn Sie eine Remoteverbindung mit dem AWS verwalteten Microsoft AD-Domänencontroller herstellen. Alle Ereignisse in diesem Protokoll weisen auf SMBv1-Verbindungen hin. Im Folgenden finden Sie ein Beispiel für die Informationen, die Sie in einem dieser Protokolle finden können:

SMB1-Zugriff

Clientadresse: ###.###.###.###

Leitfaden:

Dieses Ereignis deutet darauf hin, dass ein Client versucht hat, mithilfe von SMB1 auf den Server zuzugreifen. Um die Überwachung des SMB1-Zugriffs zu beenden, verwenden Sie das Cmdlet Set-. Windows PowerShell SmbServerConfiguration

Programmieren Ihrer Anwendungen

Stellen Sie folgende Überlegungen an, ehe Sie Ihre Anwendungen programmieren:

Den Windows-DC-Suchservice verwenden

Verwenden Sie bei der Entwicklung von Anwendungen den Windows DC Locator Service oder den Dynamic DNS (DDNS) -Dienst Ihres AWS verwalteten Microsoft AD, um nach Domänencontrollern (DCs) zu suchen. Nehmen Sie keine Hartkodierung an Anwendungen mit der Adresse eines Domain-Controllers vor. Der DC-Suchdienst sorgt für eine Verteilung der Verzeichnislast und

ermöglicht Ihnen die Nutzung einer horizontalen Skalierung durch das Hinzufügen von Domain-Controllern zu Ihrer Bereitstellung. Wenn Sie Ihre Anwendung an einen bestimmten DC binden und ein Patchen oder eine Wiederherstellung des DCs durchgeführt wird, verliert Ihre Anwendung den Zugriff auf den DC und kann die restlichen DCs nicht nutzen. Darüber hinaus kann eine feste DC-Kodierung dazu führen, dass ein einzelner DC zu einem Hotspot wird. In extremen Fällen kann dies dazu führen, dass Ihr DC nicht mehr reagiert. Solche Fälle können auch dazu führen, dass die AWS Verzeichnisautomatisierung das Verzeichnis als beeinträchtigt kennzeichnet und Wiederherstellungsprozesse auslöst, die den nicht reagierenden DC ersetzen.

Auslastungstests vor der Inbetriebnahme

Führen Sie Labortests mit Objekten und Anforderungen durch, die Ihren Produktions-Workload darstellen, um sicherzustellen, dass das Verzeichnis entsprechend der Arbeitslast Ihrer Anwendung skaliert wird. Wenn Sie weitere Kapazitäten benötigen, führen Sie den Test mit zusätzlichen DCs durch, während Anforderungen an die DCs verteilt werden. Weitere Informationen finden Sie unter Bereitstellen zusätzlicher Domain-Controller.

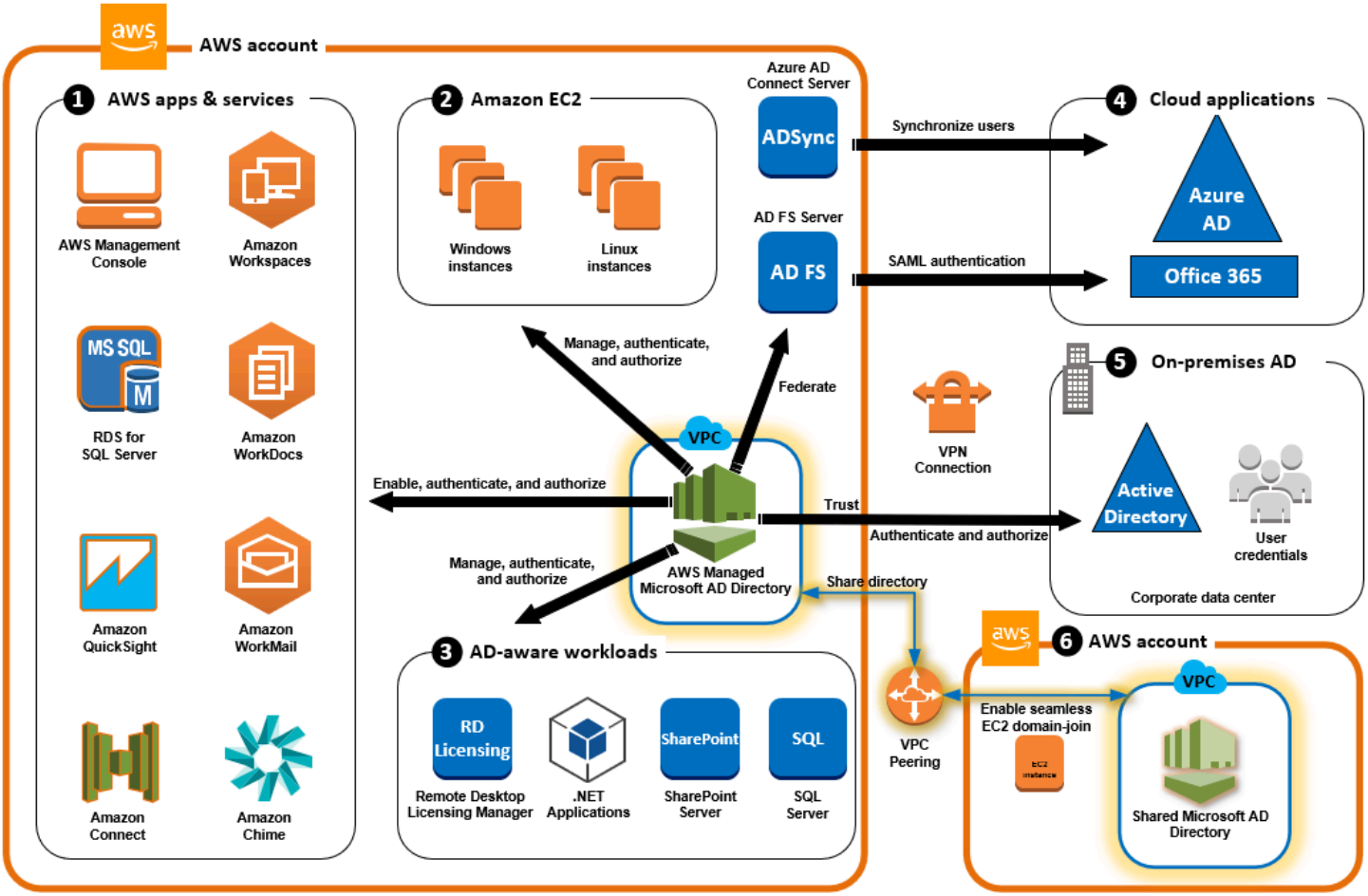
Effiziente LDAP-Abfragen verwenden

Umfassende LDAP-Abfragen für einen Domain-Controller bei tausenden von Objekten können umfangreiche CPU-Zyklen auf einem einzelnen DC verursachen und ein Hot Spotting nach sich ziehen. Dies kann Auswirkungen auf Anwendungen haben, die während der Abfrage denselben DC verwenden.

Anwendungsfälle für AWS Managed Microsoft AD

Mit AWS Managed Microsoft AD können Sie ein einzelnes Verzeichnis für mehrere Anwendungsfälle gemeinsam nutzen. Sie können beispielsweise ein Verzeichnis für die Authentifizierung und Autorisierung des Zugriffs für .NET-Anwendungen, Amazon RDS für SQL Server mit aktivierter Windows-Authentifizierung und Amazon Chime für Messaging und Videokonferenzen freigeben.

Das folgende Diagramm zeigt einige Anwendungsfälle für Ihr AWS verwaltetes Microsoft AD-Verzeichnis. Dazu gehört die Möglichkeit, Ihren Benutzern Zugriff auf externe Cloud-Anwendungen zu gewähren und es Ihren lokalen Active Directory-Benutzern zu ermöglichen, Ressourcen in der AWS Cloud zu verwalten und darauf zuzugreifen.



Verwenden Sie AWS Managed Microsoft AD für einen der folgenden Geschäftsanwendungsfälle.

Themen

- Anwendungsfall 1: Melden Sie sich mit Active Directory-Anmeldeinformationen bei AWS Anwendungen und Diensten an
- Anwendungsfall 2: Verwalten von Amazon EC2-Instances
- Anwendungsfall 3: Stellen Sie Verzeichnisdienste für Ihre Active Directory-fähigen Workloads bereit
- Anwendungsfall 4: für Office 365 und andere Cloud-Anwendungen AWS IAM Identity Center
- Anwendungsfall 5: Erweitern Sie Ihr lokales Active Directory auf die Cloud AWS
- Anwendungsfall 6: Teilen Sie Ihr Verzeichnis, um Amazon EC2 EC2-Instances kontenübergreifend AWS nahtlos mit einer Domain zu verbinden

Anwendungsfall 1: Melden Sie sich mit Active Directory-Anmeldeinformationen bei AWS Anwendungen und Diensten an

Sie können mehrere AWS Anwendungen und Dienste wie AWS Client VPN,, AWS Management Console, Amazon Chime AWS IAM Identity Center, Amazon Connect, Amazon FSx, Amazon QuickSight, Amazon RDS for SQL Server, Amazon WorkDocs WorkMail, Amazon aktivieren und WorkSpacesIhr AWS verwaltetes Microsoft AD-Verzeichnis verwenden. Wenn Sie eine AWS Anwendung oder einen Dienst in Ihrem Verzeichnis aktivieren, können Ihre Benutzer mit ihren Active Directory-Anmeldeinformationen auf die Anwendung oder den Dienst zugreifen.

Sie können Ihren Benutzern beispielsweise ermöglichen, sich AWS Management Console mit ihren Active Directory-Anmeldeinformationen bei anzumelden. Dazu aktivieren Sie das AWS Management Console als Anwendung in Ihrem Verzeichnis und weisen dann Ihre Active Directory-Benutzer und -Gruppen IAM-Rollen zu. Wenn sich Ihre Benutzer bei der anmelden AWS Management Console, übernehmen sie eine IAM-Rolle zur Verwaltung von AWS Ressourcen. Auf diese Weise können Sie Ihren Benutzern ganz einfach Zugriff auf die AWS Management Console gewähren, ohne eine separate SAML-Infrastruktur konfigurieren und verwalten zu müssen.

Um die Endbenutzererfahrung weiter zu verbessern, können Sie Single Sign-On-Funktionen für Amazon aktivieren WorkDocs, sodass Ihre Benutzer WorkDocs von einem Computer aus, der mit dem Verzeichnis verbunden ist, auf Amazon zugreifen können, ohne ihre Anmeldeinformationen separat eingeben zu müssen.

Sie können Benutzerkonten in Ihrem Verzeichnis oder in Ihrem lokalen Active Directory Zugriff gewähren, sodass sie sich AWS CLI mit ihren vorhandenen Anmeldeinformationen und Berechtigungen zur AWS Ressourcenverwaltung anmelden können, indem Sie den vorhandenen Benutzerkonten IAM-Rollen direkt zuweisen. AWS Management Console

Integration von FSx for Windows File Server mit AWS Managed Microsoft AD

Die Integration von FSx for Windows File Server mit AWS Managed Microsoft AD bietet ein vollständig verwaltetes natives Microsoft Windows-basiertes Server Message Block (SMB) - Protokolldateisystem, mit dem Sie Ihre Windows-basierten Anwendungen und Clients (die gemeinsam genutzten Dateispeicher verwenden) problemlos dorthin verschieben können. AWS Obwohl FSx für Windows File Server in ein selbstverwaltetes Microsoft Active Directory integriert werden kann, gehen wir hier nicht auf dieses Szenario ein.

Gängige Amazon FSx Anwendungsfälle und Ressourcen

Dieser Abschnitt enthält einen Verweis auf Ressourcen zu gängigen FSx for Windows File Server Server-Integrationen mit AWS Managed Microsoft AD-Anwendungsfällen. Jeder der Anwendungsfälle in diesem Abschnitt beginnt mit einer grundlegenden Konfiguration von AWS Managed Microsoft AD und FSx für Windows File Server. Weitere Informationen darüber, wie Sie diese Konfigurationen erstellen, finden Sie unter:

- Erste Schritte mit AWS Managed Microsoft AD
- Erste Schritte mit Amazon FSx

FSx für Windows File Server als persistenter Speicher auf Windows Containern

Amazon Elastic Container Service (ECS) unterstützt jetzt Windows-Container auf Container-Instances, die mit Amazon-ECS-optimierten Windows-Server-AMI gestartet werden. Die Windows-Container-Instances verwenden eine eigene Version des Amazon-ECS-Container-Agenten. Auf dem Amazon-ECS-optimierten Windows-AMI wird der Amazon-ECS-Container-Agent als Service auf dem Host ausgeführt.

Amazon ECS unterstützt die Active Directory-Authentifizierung für Windows-Container über ein spezielles Service-Konto namens group Managed Service Account (gMSA). Da Windows-Container nicht mit einer Domain verbunden werden können, müssen Sie einen Windows-Container für die Ausführung mit dem gMSA konfigurieren.

Verwandte Elemente

- Verwenden von FSx für Windows File Server als persistenter Speicher auf Windows Containern
- Gruppenverwaltete Service-Konten

Amazon AppStream 2.0-Unterstützung

Amazon AppStream 2.0 ist ein vollständig verwalteter Anwendungs-Streaming-Dienst. Er bietet eine Reihe von Lösungen, mit denen Benutzer Daten über ihre Anwendungen speichern und darauf zugreifen können. Amazon FSx with AppStream 2.0 stellt mithilfe von Amazon FSx ein persönliches persistentes Speicherlaufwerk bereit und kann so konfiguriert werden, dass ein gemeinsam genutzter Ordner für den Zugriff auf gemeinsame Dateien bereitgestellt wird.

Verwandte Elemente

- Exemplarische Vorgehensweise 4: Verwenden von Amazon FSx mit Amazon 2.0 AppStream
- Amazon FSx mit Amazon AppStream 2.0 verwenden
- Verwenden von Active Directory mit 2.0 AppStream

Unterstützung für Microsoft SQL Server

FSx for Windows File Server kann als Speicheroption für Microsoft SQL Server 2012 (ab 2012 Version 11.x) und neuere Systemdatenbanken (einschließlich Master, Model, MSDB und TempDB) sowie für Database-Engine-Benutzerdatenbanken verwendet werden.

Verwandte Elemente

- SQL Server mit SMB-Fileshare-Speicher installieren
- Ihre Hochverfügbarkeitsbereitstellungen von Microsoft SQL Server mit FSx für Windows File Server vereinfachen
- Gruppenverwaltete Service-Konten

Unterstützung von Stammordnern und Roaming-Benutzerprofilen

FSx für Windows File Server kann verwendet werden, um Daten aus den Stammordnern von Active-Directory-Benutzern und Meine Dokumente an einem zentralen Ort zu speichern. FSx für Windows File Server kann auch zum Speichern von Daten aus Roaming-Benutzerprofilen verwendet werden.

Verwandte Elemente

- Windows-Home-Verzeichnisse leicht gemacht mit Amazon FSx
- Bereitstellen von Roaming-Benutzerprofilen
- Verwenden von FSx for Windows File Server mit WorkSpaces

Unterstützung für die Dateifreigaben im Netzwerk

Dateifreigaben im Netzwerk in einem FSx für Windows File Server bieten eine verwaltete und skalierbare Filesharing-Lösung. Ein Anwendungsfall sind zugeordnete Laufwerke für Clients, die manuell oder über Gruppenrichtlinien erstellt werden können.

Verwandte Elemente

- Exemplarische Vorgehensweise 6: Leistung mit Shards aufskalieren
- Zuordnung von Laufwerken
- Verwenden von FSx for Windows File Server mit WorkSpaces

Unterstützung für die Installation von Gruppenrichtlinien-Software

Da Größe und Leistung des Ordners SYSVOL begrenzt sind, sollten Sie es als bewährte Methode vermeiden, Daten wie Softwareinstallationsdateien in diesem Ordner zu speichern. Als mögliche Lösung für dieses Problem kann FSx für Windows File Server so konfiguriert werden, dass alle Softwaredateien gespeichert werden, die mithilfe von Gruppenrichtlinien installiert wurden.

Verwandte Elemente

- Verwenden Sie Gruppenrichtlinien, um Software remote zu installieren

Unterstützung für Windows-Server-Backup-Ziele

FSx für Windows File Server kann in Windows Server Backup mithilfe der UNC-Dateifreigabe als Ziellaufwerk konfiguriert werden. In diesem Fall würden Sie den UNC-Pfad zu Ihrem FSx für Windows File Server anstelle des angehängten EBS-Volumes angeben.

Verwandte Elemente

- Eine Wiederherstellung des Systemstatus Ihres Servers durchführen

Amazon FSx unterstützt auch AWS Managed Microsoft AD Directory Sharing. Weitere Informationen finden Sie hier:

- Freigeben Ihres Verzeichnisses
- Amazon FSx mit AWS Managed Microsoft AD in einer anderen VPC oder einem anderen Konto verwenden

Amazon RDS-Integration mit AWS Managed Microsoft AD

Amazon RDS unterstützt die externe Authentifizierung von Datenbankbenutzern über Kerberos und Microsoft Active Directory. Kerberos ist ein Netzwerk-Authentifizierungsprotokoll, das Tickets und symmetrische Schlüsselkryptographie verwendet, um die Notwendigkeit der Übertragung von

Passwörtern über das Netzwerk zu vermeiden. Die Unterstützung von Amazon RDS für Kerberos und Active Directory bietet die Vorteile von Single Sign-On und zentralisierter Authentifizierung von Datenbankbenutzern, so dass Sie Ihre Benutzeranmeldeinformationen in Active Directory behalten können.

Um mit diesem Anwendungsfall zu beginnen, müssen Sie zunächst eine grundlegende AWS Managed Microsoft AD- und Amazon RDS-Konfiguration einrichten.

- Erste Schritte mit AWS Managed Microsoft AD
- Erste Schritte mit Amazon RDS

Alle unten genannten Anwendungsfälle beginnen mit einem Basismodell von AWS Managed Microsoft AD und Amazon RDS und behandeln die Integration von Amazon RDS mit AWS Managed Microsoft AD.

- Verwenden der Windows-Authentifizierung mit einer DB-Instance von Amazon RDS für SQL Server
- Verwenden der Kerberos-Authentifizierung für MySQL
- Verwenden der Kerberos-Authentifizierung mit Amazon RDS für Oracle
- Verwenden der Kerberos-Authentifizierung mit Amazon RDS für PostgreSQL

Amazon RDS unterstützt auch AWS Managed Microsoft AD Directory Sharing. Weitere Informationen finden Sie hier:

- Freigeben Ihres Verzeichnisses
- Kontenübergreifendes Verbinden Ihrer Amazon-RDS-DB-Instances mit einer einzelnen freigegebenen Domain

Weitere Informationen zum Hinzufügen von Amazon RDS für SQL Server zu Ihrem Active Directory finden Sie unter Einbinden von Amazon RDS für SQL Server in Ihrem selbstverwalteten Active Directory.

.NET-Anwendung, die Amazon RDS für SQL Server mit verwalteten Gruppenkonten verwendet

Sie können Amazon RDS für SQL Server in eine grundlegende .NET-Anwendung integrieren und Managed Service Accounts (gMSAs) gruppieren. Weitere Informationen finden Sie unter So hilft AWS Managed Microsoft AD, die Bereitstellung zu vereinfachen und die Sicherheit von Active Directory-integrierten .NET-Anwendungen zu verbessern

Anwendungsfall 2: Verwalten von Amazon EC2-Instances

Mithilfe vertrauter Active Directory-Verwaltungstools können Sie Active Directory-Gruppenrichtlinienobjekte (GPOs) anwenden, um Ihre Amazon EC2 für Windows- oder Linux-Instances zentral zu verwalten, indem Sie Ihre Instances mit Ihrer AWS verwalteten Microsoft AD-Domäne verbinden.

Darüber hinaus können sich Ihre Benutzer mit ihren Active Directory-Anmeldeinformationen bei Ihren Instances anmelden. Dadurch müssen keine individuellen Instance-Anmeldeinformationen verwendet oder private Schlüsseldateien (PEM) verteilt werden. Dies erleichtert es Ihnen, Benutzern sofort Zugriff zu gewähren oder zu entziehen, indem Sie die Active Directory-Benutzerverwaltungstools verwenden, die Sie bereits verwenden.

Anwendungsfall 3: Stellen Sie Verzeichnisdienste für Ihre Active Directory-fähigen Workloads bereit

AWS Managed Microsoft AD ist ein echtes Microsoft Active Directory, mit dem Sie herkömmliche Active Directory-fähige Workloads wie Remote Desktop Licensing Manager und Microsoft SharePoint und Microsoft SQL Server Always On in der Cloud ausführen können. AWS AWS Managed Microsoft AD hilft Ihnen auch dabei, die Sicherheit von Active Directory-integrierten .NET-Anwendungen zu vereinfachen und zu verbessern, indem Sie Group Managed Service Accounts (gMSAs) und Kerberos Constrained Delegation (KCD) verwenden.

Anwendungsfall 4: für Office 365 und andere Cloud-Anwendungen AWS IAM Identity Center

Sie können AWS Managed Microsoft AD verwenden, AWS IAM Identity Center um Cloud-Anwendungen bereitzustellen. Sie können Microsoft Entra Connect (früher bekannt alsAzure Active Directory Connect) verwenden, um Ihre Benutzer mit Microsoft Entra (früher bekannt als Azure Active Directory (AzureAD)) zu synchronisieren, und dann Active Directory Federation Services (AD FS) verwenden, sodass Ihre Benutzer mit ihren Active Directory-Anmeldeinformationen auf Microsoft Office 365 und andere SAML 2.0-Cloudanwendungen zugreifen können.

Durch die Integration von AWS Managed Microsoft AD mit IAM Identity Center werden Ihrem AWS verwalteten Microsoft AD und/oder Ihren lokalen vertrauenswürdigen Domänen SAML-Funktionen hinzugefügt. Nach der Integration können Ihre Benutzer IAM Identity Center mit Diensten nutzen, die SAML unterstützen, einschließlich Cloud-Anwendungen AWS Management Console und Drittanbieter-Cloud-Anwendungen wie Office 365, Concur und Salesforce, ohne eine SAML-

Infrastruktur konfigurieren zu müssen. Eine Demonstration, wie Sie Ihren lokalen Benutzern die Nutzung von IAM Identity Center ermöglichen, finden Sie im folgenden Video. YouTube

> **Note**
>
> AWS Single Sign-On wurde in IAM Identity Center umbenannt.

Anwendungsfall 5: Erweitern Sie Ihr lokales Active Directory auf die Cloud AWS

Wenn Sie bereits über eine Active Directory-Infrastruktur verfügen und diese bei der Migration von Active Directory-fähigen Workloads in die AWS Cloud verwenden möchten, kann AWS Managed Microsoft AD helfen. Sie können Active Directory-Vertrauensstellungen verwenden, um AWS Managed Microsoft AD mit Ihrem vorhandenen Active Directory zu verbinden. Das bedeutet, dass Ihre Benutzer mit ihren lokalen Active Directory-Anmeldeinformationen auf Active Directory-fähige AWS Anwendungen und Anwendungen zugreifen können, ohne dass Sie Benutzer, Gruppen oder Kennwörter synchronisieren müssen.

Ihre Benutzer können sich beispielsweise mit ihren vorhandenen Active Directory-Benutzernamen AWS Management Console und WorkSpaces -Passwörtern bei Amazon und Amazon anmelden. Wenn Sie Active Directory-fähige Anwendungen verwenden, z. B. SharePoint mit AWS Managed Microsoft AD, können Ihre angemeldeten Windows-Benutzer außerdem auf diese Anwendungen zugreifen, ohne die Anmeldeinformationen erneut eingeben zu müssen.

Sie können Ihre lokale Active Directory-Domäne auch migrieren, AWS um sich von der betrieblichen Belastung Ihrer Active Directory-Infrastruktur zu befreien, indem Sie das Active Directory Migration Toolkit (ADMT) zusammen mit dem Password Export Service (PES) für die Migration verwenden.

Anwendungsfall 6: Teilen Sie Ihr Verzeichnis, um Amazon EC2 EC2-Instances kontenübergreifend AWS nahtlos mit einer Domain zu verbinden

Durch die gemeinsame Nutzung Ihres Verzeichnisses für mehrere AWS Konten können Sie AWS Dienste wie Amazon EC2 einfach verwalten, ohne für jedes Konto und jede VPC ein Verzeichnis betreiben zu müssen. Sie können Ihr Verzeichnis über jedes beliebige AWS -Konto und jede beliebige Amazon VPC innerhalb einer AWS -Region nutzen. Auf diese Weise können Sie verzeichnisfähige Workloads einfacher und kosteneffektiver mit einem einzelnen Verzeichnis über

Konten und VPCs hinweg verwalten. Beispiel: Sie können Ihre für EC2-Instances bereitgestellte Windows-Workloads jetzt mithilfe eines Verzeichnisses in AWS Managed Microsoft AD problemlos über mehrere Konten und VPC hinweg verwalten.

Wenn Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnis mit einem anderen AWS Konto teilen, können Sie die Amazon EC2 EC2-Konsole verwenden oder AWS Systems ManagerIhre Instances von einer beliebigen Amazon VPC innerhalb des Kontos und AWS der Region aus nahtlos verbinden. Sie können schnell verzeichnisfähige Workloads auf EC2-Instances bereitstellen, ohne manuell eine Verbindung Ihrer Instances mit einer Domain herstellen oder Verzeichnisse in jedem Konto und der VPC bereitstellen zu müssen. Weitere Informationen finden Sie unter Freigeben Ihres Verzeichnisses.

So verwalten Sie AWS Managed Microsoft AD

In diesem Abschnitt werden alle Verfahren für den Betrieb und die Wartung einer AWS verwalteten Microsoft AD-Umgebung aufgeführt.

Themen

- Ihr Verzeichnis in AWS Managed Microsoft AD sichern
- Ihr AWS Managed Microsoft AD überwachen
- Multi-Region-Replikation
- Freigeben Ihres Verzeichnisses
- Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory
- Benutzer und Gruppen in AWS Managed Microsoft AD verwalten
- Connect zu Ihrer vorhandenen Active Directory-Infrastruktur her
- Connect Ihr AWS Managed Microsoft AD mit Microsoft Entra Connect Sync
- Ihr Schema erweitern
- Ihr Verzeichnis in AWS Managed Microsoft AD verwalten
- Benutzern und Gruppen den Zugriff auf AWS -Ressourcen gewähren
- Ermöglichen Sie den Zugriff auf AWS Anwendungen und Dienste
- Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren
- Bereitstellen zusätzlicher Domain-Controller
- Benutzer von Active Directory zu AWS Managed Microsoft AD migrieren

Ihr Verzeichnis in AWS Managed Microsoft AD sichern

In diesem Abschnitt wird beschrieben, wie Sie Ihre Umgebung in AWS Managed Microsoft AD sichern.

Themen

Kennwortrichtlinien für AWS Managed Microsoft AD verwalten

AWS Mit Managed Microsoft AD können Sie verschiedene Passwort- und Kontosperrrichtlinien (auch als differenzierte Kennwortrichtlinien bezeichnet) für Benutzergruppen definieren und zuweisen, die Sie in Ihrer AWS verwalteten Microsoft AD-Domäne verwalten. Wenn Sie ein AWS verwaltetes Microsoft AD-Verzeichnis erstellen, wird eine Standard-Domänenrichtlinie erstellt und auf die angewendetActive Directory. Diese Richtlinie enthält folgende Einstellungen:

Richtlinie	Einstellung
Passwortverlauf erzwingen	24 gespeicherte Passwörter
Maximales Passwortalter	42 Tage *
Minimales Passwortalter	1 Tag
Mindestlänge für Passwörter	7 Zeichen
Das Passwort muss Komplexitätsanforderungen entsprechen	Aktiviert
Passwörter unter Verwendung umkehrbarer Verschlüsselung speichern	Disabled

* Hinweis: Das maximale Passwortalter von 42 Tagen schließt das Admin-Passwort mit ein.

Sie können z. B. eine weniger strenge Richtlinieneinstellung für Mitarbeiter festlegen, die nur Zugriff auf Informationen mit niedriger Empfindlichkeit haben. Für leitende Angestellte, die regelmäßig auf vertrauliche Informationen zugreifen, können Sie strengere Einstellungen festlegen.

Im Folgenden finden Sie Ressourcen, in denen Sie mehr über Microsoft Active Directory detaillierte Kennwortrichtlinien und Sicherheitsrichtlinien erfahren können:

- Konfigurieren Sie die Einstellungen für Sicherheitsrichtlinien
- Anforderungen an die Komplexität von Passwörtern
- Sicherheitsüberlegungen zur Komplexität von Passwörtern

AWS bietet eine Reihe detaillierter Kennwortrichtlinien in AWS Managed Microsoft AD, die Sie konfigurieren und Ihren Gruppen zuweisen können. Um die Richtlinien zu konfigurieren, können Sie Microsoft Standardrichtlinientools wie das Active DirectoryAdministrative Center verwenden. Informationen zu den ersten Schritten mit den Microsoft Richtlinientools finden Sie unterInstallieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD.

Wie werden Passwortrichtlinien angewendet

Je nachdem, ob das Passwort zurückgesetzt oder geändert wurde, gibt es Unterschiede in der Art und Weise, wie die detaillierten Passwortrichtlinien angewendet werden. Domänenbenutzer können ihr eigenes Passwort ändern. Ein Active Directory Administrator oder Benutzer mit den erforderlichen Berechtigungen kann Benutzerkennwörter zurücksetzen. Weitere Informationen finden Sie in der folgenden Tabelle.

Richtlinie	Passwort zurückgesetzt	Passwort ändern
Passwortverlauf erzwingen	 Nein	 Ja
Maximales Passwortalter	 Ja	 Ja

Richtlinie	Passwort zurückgesetzt	Passwort ändern
Minimales Passwortalter	 Nein	 Ja
Mindestlänge für Passwörter	 Ja	 Ja
Das Passwort muss Komplexitätsanforderungen entsprechen	 Ja	 Ja

Diese Unterschiede haben Auswirkungen auf die Sicherheit. Wenn beispielsweise das Passwort eines Benutzers zurückgesetzt wird, werden die Richtlinien „Kennwortverlauf durchsetzen“ und „Mindestalter für Kennwörter“ nicht durchgesetzt. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu den Sicherheitsüberlegungen im Zusammenhang mit der Durchsetzung von Richtlinien für den Kennwortverlauf und das Mindestalter für Kennwörter.

Themen

- Unterstützte Richtlinieneinstellungen
- Delegieren, wer Ihre Passwortrichtlinien verwalten kann
- Passwortrichtlinien an Ihre Benutzer zuweisen

Verwandter Blogartikel zum Thema AWS Sicherheit

- So konfigurieren Sie mit AWS Managed Microsoft AD noch strengere Kennwortrichtlinien, um Ihre Sicherheitsstandards zu erfüllen AWS Directory Service

Unterstützte Richtlinieneinstellungen

AWS Managed Microsoft AD umfasst fünf detaillierte Richtlinien mit einem nicht bearbeitbaren Prioritätswert. Die Richtlinien umfassen verschiedene Eigenschaften, die Sie konfigurieren können, um die Stärke von Passwörtern und Kontosperrmaßnahmen bei Anmeldefehlern zu verstärken. Sie können die Richtlinien auf null oder mehr Active Directory-Gruppen zuweisen. Wenn ein Endbenutzer Mitglied mehrerer Gruppen ist und mehr als eine Kennwortrichtlinie erhält, erzwingt Active Directory die Richtlinie mit dem niedrigsten Prioritätswert.

AWS vordefinierte Kennwortrichtlinien

In der folgenden Tabelle sind die fünf Richtlinien aufgeführt, die in Ihrem AWS verwalteten Microsoft AD-Verzeichnis enthalten sind, sowie deren zugewiesener Prioritätswert. Weitere Informationen finden Sie unter Precedence.

Richtlinienname	Precedence
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

Eigenschaften der Passwortrichtlinie

Sie können die folgenden Eigenschaften in Ihren Passwortrichtlinien bearbeiten, um konform zu den Compliance-Standards für Ihre geschäftlichen Anforderungen zu arbeiten.

- Richtlinienname
- Passwortverlauf erzwingen
- Mindestlänge für Passwörter
- Minimales Passwortalter
- Maximales Passwortalter
- Passwörter unter Verwendung umkehrbarer Verschlüsselung speichern

- Das Passwort muss Komplexitätsanforderungen entsprechen

Sie können die Prioritätswerte für diese Richtlinien nicht ändern. Weitere Informationen dazu, wie sich diese Einstellungen auf die Kennwortdurchsetzung auswirken, finden Sie unter AD DS: Detaillierte Kennwortrichtlinien auf der TechNetMicrosoft-Website. Allgemeine Informationen zu diesen Richtlinien finden Sie unter Passwortrichtlinie auf der TechNetMicrosoft-Website.

Kontosperrungsrichtlinien

Sie können auch die folgenden Eigenschaften Ihrer Passwortrichtlinien ändern, um anzugeben, ob und wie Active Directory ein Konto sperren soll, wenn es fehlgeschlagene Anmeldeversuche gab:

- Anzahl der zulässigen fehlgeschlagenen Anmeldeversuche
- Dauer der Kontosperrung
- Zurücksetzen der fehlgeschlagene Anmeldeversuche nach einer bestimmten Zeitdauer

Allgemeine Informationen zu diesen Richtlinien finden Sie unter Kontosperrungsrichtlinie auf der TechNetMicrosoft-Website.

Precedence

Richtlinien mit einem niedrigeren Prioritätswert haben höhere Priorität. Sie weisen Passwortrichtlinien Active Directory-Sicherheitsgruppen zu. Sie sollten einer Sicherheitsgruppe nur eine einzelne Richtlinie zuordnen, während ein einzelner Benutzer mehrere Passwortrichtlinien erhalten kann. Angenommen, `jsmith` ist ein Mitglied der HR-Gruppe und auch ein Mitglied der MANAGERS-Gruppe. Wenn Sie CustomerPSO-05 (mit einer Priorität von 50) der HR-Gruppe zuordnen, und CustomerPSO-04 (mit einer Priorität von 40) der MANAGERS-Gruppe, hat CustomerPSO-04 die höhere Priorität und Active Directory wendet diese Richtlinie auf `jsmith` an.

Wenn Sie einem Benutzer oder einer Gruppe mehrere Richtlinien zuweisen, bestimmt Active Directory die resultierenden Richtlinie wie folgt:

1. Es gilt eine Richtlinie, die Sie direkt dem Benutzerobjekt zuweisen.
2. Wenn dem Benutzerobjekt nicht direkt eine Richtlinie zugewiesen wird, gilt die Richtlinie mit dem niedrigsten Wert aller Prioritäten, die der Benutzer aufgrund einer Gruppenmitgliedschaft erhalten hat.

Weitere Informationen finden Sie unter AD DS: Detaillierte Kennwortrichtlinien auf der TechNetMicrosoft-Website.

Delegieren, wer Ihre Passwortrichtlinien verwalten kann

Sie können Berechtigungen zur Verwaltung von Kennwortrichtlinien an bestimmte Benutzerkonten delegieren, die Sie in Ihrem AWS verwalteten Microsoft AD erstellt haben, indem Sie die Konten der Sicherheitsgruppe AWS Delegated Fine Grained Password Policy Administrators hinzufügen. Wenn ein Konto Mitglied dieser Gruppe wird, hat das Konto die Berechtigungen, die zuvor aufgelisteten Passwortrichtlinien zu bearbeiten und zu konfigurieren.

So delegieren Sie, wer Passwortrichtlinien verwalten kann

1. Starten Sie das Active Directory-Verwaltungscenter (ADAC) von jeder verwalteten EC2-Instance aus, die Sie Ihrer AWS verwalteten Microsoft AD-Domäne hinzugefügt haben.
2. Wechseln Sie zur Baumansicht und gehen Sie zur OU AWS Delegated Groups. Weitere Informationen über diese OU finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.
3. Suchen Sie die Benutzergruppe AWS Delegated Fine Grained Password Policy Administrators. Fügen Sie dieser Gruppe Benutzer oder Gruppen aus Ihrer Domain hinzu.

Passwortrichtlinien an Ihre Benutzer zuweisen

Benutzerkonten, die Mitglied der Sicherheitsgruppe AWS Delegated Fine Grained Password Policy Administrators sind, können das folgende Verfahren verwenden, um Benutzern und Sicherheitsgruppen Richtlinien zuzuweisen.

So weisen Sie Ihren Benutzern Passwortrichtlinien zu

1. Starten Sie das Active Directory-Verwaltungscenter (ADAC) von jeder verwalteten EC2-Instance aus, die Sie Ihrer AWS verwalteten Microsoft AD-Domäne hinzugefügt haben.
2. Wechseln Sie in die Tree View und öffnen Sie System\Password Settings Container.
3. Doppelklicken Sie auf die differenzierte Richtlinie, die Sie bearbeiten möchten. Klicken Sie auf Add, um die Richtlinieneigenschaften zu bearbeiten und der Richtlinie Benutzer oder Sicherheitsgruppen hinzuzufügen. Weitere Informationen über die standardmäßigen differenzierten Richtlinien in AWS Managed Microsoft AD finden Sie unter AWS vordefinierte Kennwortrichtlinien.

4. Führen Sie den folgenden PowerShell Befehl aus, um zu überprüfen, ob die Kennwortrichtlinie angewendet wurde:

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

> **Note**
>
> Vermeiden Sie die Verwendung des Befehls `net user`, da seine Ergebnisse ungenau sein könnten.

Wenn Sie keine der fünf Kennwortrichtlinien in Ihrem AWS verwalteten Microsoft AD-Verzeichnis konfigurieren, verwendet Active Directory die Standard-Domänengruppenrichtlinie. Weitere Informationen über die Verwendung von Password Settings Container finden Sie in diesem Microsoft Blog Post.

Aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD

Sie können die Multi-Faktor-Authentifizierung (MFA) für Ihr AWS verwaltetes Microsoft AD-Verzeichnis aktivieren, um die Sicherheit zu erhöhen, wenn Ihre Benutzer ihre AD-Anmeldeinformationen für den Zugriff angeben. Unterstützte Amazon-Enterprise-Anwendungen Wenn Sie die MFA aktivieren, geben Ihre Benutzer wie gewöhnlich ihren Benutzernamen und ihr Passwort (erster Faktor) ein. Darüber hinaus müssen sie jedoch einen Authentifizierungscode eingeben (zweiter Faktor), der von Ihrer virtuellen oder Hardware-MFA-Lösung bereitgestellt wird. Diese Faktoren zusammen erhöhen die Sicherheit, indem Sie Zugriffe auf Ihre Amazon Enterprise-Anwendungen verhindern, es sei denn, Benutzer geben gültige Anmeldeinformationen und einen gültigen MFA-Code ein.

Zum Aktivieren der MFA müssen Sie entweder über eine MFA-Lösung in Form eines Remote Authentication Dial-In User Service (RADIUS)-Servers verfügen oder über ein MFA-Plugin für einen RADIUS-Server, der bereits in Ihrer On-Premises-Infrastruktur vorhanden ist. Ihre MFA-Lösung sollte einmalige Sicherheitscodes (OTPs, One Time Passcodes) implementieren, die Benutzer von einem Hardwaregerät oder einer Software erhalten, die auf einem Gerät, beispielsweise einem Mobiltelefon, ausgeführt wird.

RADIUS ist ein branchenübliches Client/Server-Protokoll, das Authentifizierung, Autorisierung und Kontoverwaltung ermöglicht, sodass Benutzer eine Verbindung zu Netzwerkdiensten herstellen können. AWS Managed Microsoft AD umfasst einen RADIUS-Client, der eine Verbindung zu

dem RADIUS-Server herstellt, auf dem Sie Ihre MFA-Lösung implementiert haben. Der RADIUS-Server überprüft den Benutzernamen und den OTP-Code. Wenn Ihr RADIUS-Server den Benutzer erfolgreich validiert, authentifiziert AWS Managed Microsoft AD den Benutzer dann gegenüber Active Directory. Nach erfolgreicher Active Directory-Authentifizierung können Benutzer dann auf die AWS Anwendung zugreifen. Für die Kommunikation zwischen dem AWS verwalteten Microsoft AD RADIUS-Client und Ihrem RADIUS-Server müssen Sie AWS Sicherheitsgruppen konfigurieren, die die Kommunikation über Port 1812 ermöglichen.

Sie können die Multi-Faktor-Authentifizierung für Ihr AWS verwaltetes Microsoft AD-Verzeichnis aktivieren, indem Sie das folgende Verfahren ausführen. Weitere Informationen zum Konfigurieren Ihres RADIUS-Servers für AWS Directory Service und MFA finden Sie unter Voraussetzungen für Multifaktor-Authentifizierung.

Überlegungen

Im Folgenden finden Sie einige Überlegungen zur Multi-Faktor-Authentifizierung für Ihr AWS verwaltetes Microsoft AD:

- Die Multifaktor-Authentifizierung ist für Simple AD nicht verfügbar. MFA kann jedoch für Ihr AD-Connector-Verzeichnis aktiviert werden. Weitere Informationen finden Sie unter Multifaktor-Authentifizierung für AD Connector aktivieren.
- MFA ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.
- Wenn Sie AWS Managed Microsoft AD für die externe Kommunikation verwenden möchten, empfehlen wir Ihnen, für diese Kommunikation ein Network Address Translation (NAT) -Internet-Gateway oder ein Internet Gateway außerhalb des AWS Netzwerks zu konfigurieren.
  - Wenn Sie die externe Kommunikation zwischen Ihrem AWS Managed Microsoft AD und Ihrem im AWS Netzwerk gehosteten RADIUS-Server unterstützen möchten, wenden Sie sich bitte an AWS Support.

Aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD

Das folgende Verfahren zeigt Ihnen, wie Sie die Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD aktivieren.

1. Identifizieren Sie die IP-Adresse Ihres RADIUS-MFA-Servers und Ihres AWS verwalteten Microsoft AD-Verzeichnisses.

2. Bearbeiten Sie Ihre Virtual Private Cloud (VPC) -Sicherheitsgruppen, um die Kommunikation über Port 1812 zwischen Ihren AWS verwalteten Microsoft AD-IP-Endpunkten und Ihrem RADIUS-MFA-Server zu ermöglichen.
3. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
4. Wählen Sie den Verzeichnis-ID-Link für Ihr AWS verwaltetes Microsoft AD-Verzeichnis.
5. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie MFA aktivieren möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
6. Wählen Sie im Abschnitt Multi-factor authentication (Mehrfaktoren-Authentifizierung) die Option Actions (Aktionen) und dann Enable (Aktivieren) aus.
7. Geben Sie auf der Seite Multi-Faktor-Authentifizierung (MFA) aktivieren die folgenden Werte ein:

   Label anzeigen

   Geben Sie einen Labelnamen an.

   DNS-Name oder IP-Adressen des RADIUS-Servers

   Die IP-Adressen Ihrer RADIUS-Server-Endpunkte oder die IP-Adresse Ihres RADIUS-Server-Load Balancer. Sie können mehrere IP-Adressen getrennt durch ein Komma eingeben (z. B. `192.0.0.0,192.0.0.12`).

   > **Note**
   >
   > RADIUS MFA gilt nur für die Authentifizierung des Zugriffs auf die AWS Management Console oder auf Amazon Enterprise-Anwendungen und -Services wie WorkSpaces Amazon oder Amazon QuickSight Chime. Es bietet keine MFA für Windows-Workloads, die auf EC2-Instances ausgeführt werden, oder für die Anmeldung bei einer EC2-Instance. AWS Directory Service unterstützt die RADIUS Challenge/Response-Authentifizierung nicht.
   > Benutzer müssen ihren MFA-Code bei der Eingabe ihres Benutzernamens und Passworts zur Hand haben. Alternativ müssen Sie eine Lösung verwenden, die MFA out-of-band wie die SMS-Textverifizierung für den Benutzer durchführt. In out-of-

band MFA-Lösungen müssen Sie sicherstellen, dass Sie den RADIUS-Timeoutwert entsprechend Ihrer Lösung festlegen. Wenn Sie eine out-of-band MFA-Lösung verwenden, fordert die Anmeldeseite den Benutzer auf, einen MFA-Code einzugeben. In diesem Fall müssen Benutzer ihr Passwort sowohl in das Passwortfeld als auch in das MFA-Feld eingeben.

Port

Der Port, den Ihr RADIUS-Server für die Kommunikation verwendet. Ihr lokales Netzwerk muss eingehenden Datenverkehr über den Standard-RADIUS-Serverport (UDP:1812) von den Servern zulassen. AWS Directory Service

Shared secret code (Gemeinsamer geheimer Code)

Der gemeinsame geheime Code, der bei der Erstellung Ihrer RADIUS-Endpunkte angegeben wurde.

Confirm shared secret code (Gemeinsamen geheimen Code bestätigen)

Bestätigen Sie den gemeinsamen geheimen Code für Ihre RADIUS-Endpunkte.

Protocol (Protokoll)

Wählen Sie das Protokoll aus, das bei der Erstellung Ihrer RADIUS-Endpunkte angegeben wurde.

Server-Timeout (in Sekunden)

Die Zeit in Sekunden, die gewartet werden muss, bis der RADIUS-Server antwortet. Dies muss ein Wert zwischen 1 und 50 sein.

> **Note**
>
> Wir empfehlen, Ihr RADIUS-Server-Timeout auf 20 Sekunden oder weniger zu konfigurieren. Wenn das Timeout 20 Sekunden überschreitet, kann das System es nicht erneut mit einem anderen RADIUS-Server versuchen, was zu einem Timeout-Fehler führen kann.

Maximale Wiederholungen von RADIUS-Anfragen

Die Anzahl der Kommunikationsversuche mit dem RADIUS-Server. Dies muss ein Wert zwischen 0 und 10 sein.

Die Multifaktor-Authentifizierung ist verfügbar, wenn sich der RADIUS-Status in Enabled ändert.

8. Wählen Sie Enable (Aktivieren) aus.

Unterstützte Amazon-Enterprise-Anwendungen

Alle Amazon Enterprise IT-Anwendungen WorkSpaces, einschließlich Amazon, Amazon WorkDocs, Amazon WorkMail QuickSight, und der Zugriff auf AWS IAM Identity Center und AWS Management Console werden unterstützt, wenn AWS Managed Microsoft AD und AD Connector mit MFA verwendet werden.

Informationen zur Konfiguration des grundlegenden Benutzerzugriffs auf Amazon Enterprise-Anwendungen, AWS Single Sign-On und deren AWS Management Console Verwendung AWS Directory Service finden Sie unter Ermöglichen Sie den Zugriff auf AWS Anwendungen und Dienste undDen Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren.

Verwandter Blogartikel zum Thema AWS Sicherheit

- So aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Dienste mithilfe von AWS Managed Microsoft AD und lokalen Anmeldeinformationen

Sicheres LDAP oder LDAPS aktivieren

Lightweight Directory Access Protocol (LDAP) ist ein Standard-Kommunikationsprotokoll zum Lesen und Schreiben von Daten in und aus Active Directory. Einige Anwendungen verwenden LDAP, um Benutzer und Gruppen in Active Directory hinzuzufügen, zu entfernen oder zu suchen, oder um Anmeldeinformationen zur Authentifizierung von Benutzern in Active Directory zu transportieren. Jede LDAP-Kommunikation umfasst einen Client (z. B. eine Anwendung) und einen Server (z. B. Active Directory).

Standardmäßig ist die Kommunikation über LDAP nicht verschlüsselt. Auf diese Weise ist es für einen böswilligen Benutzer möglich, eine Software zur Netzwerk-Überwachung zu verwenden,

um über das Kabel übertragenen Datenpakete einzusehen. Aus diesem Grund fordern viele Unternehmenssicherheitsrichtlinien, dass Organisationen die gesamte LDAP-Kommunikation verschlüsseln.

Um diese Form der Datenexposition zu minimieren, bietet AWS Managed Microsoft AD eine Option: Sie können LDAP über Secure Sockets Layer (SSL) /Transport Layer Security (TLS), auch bekannt als LDAPS, aktivieren. Mit LDAPS können Sie die Sicherheit über das Kabel hinweg verbessern. Sie können Compliance-Anforderungen auch erfüllen, indem Sie die gesamte Kommunikation zwischen Ihren LDAP-fähigen Anwendungen und AWS Managed Microsoft AD verschlüsseln.

AWS Managed Microsoft AD bietet Unterstützung für LDAPS in den folgenden Bereitstellungsszenarien:

- Serverseitiges LDAPS verschlüsselt die LDAP-Kommunikation zwischen Ihren kommerziellen oder selbst entwickelten LDAP-fähigen Anwendungen (die als LDAP-Clients agieren) und AWS Managed Microsoft AD (als LDAP-Server). Weitere Informationen finden Sie unter Serverseitiges LDAPS mithilfe von AWS Managed Microsoft AD aktivieren.
- Das clientseitige LDAPS verschlüsselt die LDAP-Kommunikation zwischen AWS Anwendungen wie (die als LDAP-Clients agieren) und Ihrem selbstverwalteten WorkSpaces (lokalen) Active Directory (das als LDAP-Server fungiert). Weitere Informationen finden Sie unter Aktivieren Sie clientseitiges LDAPS mit AWS Managed Microsoft AD.

Themen

Serverseitiges LDAPS mithilfe von AWS Managed Microsoft AD aktivieren

Die serverseitige Unterstützung des Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) verschlüsselt die LDAP-Kommunikation zwischen Ihren kommerziellen oder selbst entwickelten LDAP-fähigen Anwendungen und Ihrem verwalteten Microsoft AD-Verzeichnis. AWS Dies trägt dazu bei, die Sicherheit über die gesamte Leitung hinweg zu verbessern und die Compliance-Anforderungen mithilfe des Verschlüsselungsprotokolls Secure Sockets Layer (SSL) zu erfüllen.

Serverseitiges LDAPS aktivieren

Ausführliche Anweisungen zur Einrichtung und Konfiguration serverseitiger LDAPS und Ihres Zertifizierungsstellenservers (CA) finden Sie unter So aktivieren Sie serverseitiges LDAPS für Ihr AWS verwaltetes Microsoft AD-Verzeichnis im Sicherheitsblog. AWS

Ein Großteil der Einrichtung erfolgt über die Amazon-EC2-Instance, die Sie für die Verwaltung Ihrer Domain-Controller in AWS Managed Microsoft AD verwenden. Die folgenden Schritte führen Sie durch die Aktivierung von LDAPS für Ihre Domain in der Cloud. AWS

Wenn Sie Ihre PKI-Infrastruktur mithilfe von Automatisierung einrichten möchten, können Sie die Microsoft Public Key Infrastructure on AWS QuickStart Guide verwenden. Insbesondere sollten Sie den Anweisungen in der Anleitung folgen, um die Vorlage für Microsoft PKI in eine bestehende VPC auf AWS bereitstellen zu laden. Stellen Sie nach dem Laden der Vorlage sicher, dass Sie **`AWSManaged`** auswählen, wenn Sie zur Option Typ der Active-Directory-Domainservices gelangen. Wenn Sie den QuickStart Leitfaden verwendet haben, können Sie direkt zu Schritt 3: Eine Zertifikatvorlage erstellen diesem Thema springen.

Themen

Schritt 1: Delegieren, wer LDAPS aktivieren kann

Um serverseitiges LDAPS zu aktivieren, müssen Sie Mitglied der Gruppe Admins oder AWS Delegated Enterprise Certificate Authority Administrators in Ihrem AWS verwalteten Microsoft AD-Verzeichnis sein. Alternativ können Sie der standardmäßige Administratorbenutzer sein (Admin-Konto). Wenn Sie möchten, können Sie einen anderen Benutzer als das Admin-Konto dazu veranlassen, LDAPS einzurichten. In diesem Fall fügen Sie diesen Benutzer der Gruppe Admins oder AWS Delegated Enterprise Certificate Authority Administrators in Ihrem AWS Managed Microsoft AD-Verzeichnis hinzu.

Schritt 2: Ihre Zertifizierungsstelle einrichten

Bevor Sie serverseitiges LDAPS aktivieren können, müssen Sie ein Zertifikat erstellen. Dieses Zertifikat muss von einem Microsoft Enterprise CA-Server ausgestellt werden, der mit Ihrer AWS

verwalteten Microsoft AD-Domäne verbunden ist. Nachdem das Zertifikat erstellt wurde, muss es auf jedem Ihrer Domain-Controller in dieser Domain installiert werden. Dieses Zertifikat ermöglicht, dass der LDAP-Service auf den Domain-Controllern darauf achtet, ob SSL-Verbindungen von LDAP-Clients angefordert werden, und diese automatisch akzeptiert.

> **Note**
>
> Serverseitiges LDAPS mit AWS Managed Microsoft AD unterstützt keine Zertifikate, die von einer eigenständigen Zertifizierungsstelle ausgestellt wurden. Darüber hinaus unterstützt es keine Zertifikate von einer Drittanbieter-Zertifizierungsstelle.

Abhängig von Ihren geschäftlichen Anforderungen können Sie die folgenden Optionen für das Einrichten oder Herstellen einer Verbindung mit einer Zertifizierungsstelle in Ihrer Domain haben:

- Eine untergeordnete Microsoft Enterprise CA erstellen — (empfohlen) Mit dieser Option können Sie einen untergeordneten Microsoft Enterprise CA Server in der AWS Cloud bereitstellen. Der Server kann Amazon EC2 so verwenden, dass es mit Ihrer vorhandenen Microsoft-Stammzertifizierungsstelle funktioniert. Weitere Informationen zum Einrichten einer untergeordneten Microsoft-Unternehmenszertifizierungsstelle finden Sie unter Schritt 4: Hinzufügen einer Microsoft Enterprise-CA zu Ihrem AWS Microsoft AD-Verzeichnis unter So aktivieren Sie serverseitige LDAPS für Ihr AWS verwaltetes Microsoft AD-Verzeichnis.
- Eine Microsoft-Unternehmensstammzertifizierungsstelle erstellen — Mit dieser Option können Sie mithilfe von Amazon EC2 eine Microsoft-Unternehmensstammzertifizierungsstelle in der AWS Cloud erstellen und diese mit Ihrer AWS verwalteten Microsoft AD-Domain verbinden. Diese Root-Zertifizierungsstelle kann das Zertifikat für Ihren Domain-Controller ausstellen. Weitere Informationen zum Einrichten einer neuen Stammzertifizierungsstelle finden Sie unter Schritt 3: Installieren und Konfigurieren einer Offline-Zertifizierungsstelle unter So aktivieren Sie serverseitiges LDAPS für Ihr AWS verwaltetes Microsoft AD-Verzeichnis.

Weitere Informationen darüber, wie Sie Ihre EC2-Instance mit der Domain verbinden, finden Sie unter Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory.

Schritt 3: Eine Zertifikatvorlage erstellen

Nachdem Ihre Unternehmenszertifizierungsstelle eingerichtet wurde, können Sie die Zertifikatvorlage für Kerberos-Authentifizierung konfigurieren.

Erstellen einer Zertifikatvorlage

1. Starten Sie Microsoft Windows Server Manager. Wählen Sie Tools > Zertifizierungsstelle aus.
2. Erweitern Sie im Fenster Zertifizierungsstelle die Zertifizierungsstellenstruktur im linken Fensterbereich. Klicken Sie mit der rechten Maustaste auf Zertifikatsvorlagen und wählen Sie Verwalten.
3. Klicken Sie im Fenster Konsole für Zertifikatsvorlagen mit der rechten Maustaste auf Kerberos-Authentifizierung und wählen Sie Vorlage duplizieren.
4. Das Fenster Eigenschaften der neuen Vorlage wird geöffnet.
5. Gehen Sie im Fenster Eigenschaften der neuen Vorlage zur Registerkarte Kompatibilität und gehen Sie dann wie folgt vor:
   a. Ändern Sie die Zertifizierungsstelle auf das Betriebssystem, das Ihrer CA entspricht.
   b. Wenn ein Fenster mit den resultierenden Änderungen angezeigt wird, wählen Sie OK aus.
   c. Ändern Sie den Zertifizierungsempfänger auf Windows 10/Windows Server 2016.

      > **Note**
      >
      > AWS Managed Microsoft AD wird von Windows Server 2019 unterstützt.

   d. Wenn Fenster mit den resultierenden Änderungen angezeigt werden, wählen Sie OK aus.
6. Klicken Sie auf die Registerkarte Allgemein und ändern Sie den Anzeigenamen der Vorlage in LDAPOverSSL oder einen anderen Namen, den Sie bevorzugen.
7. Klicken Sie auf die Registerkarte Sicherheit und wählen Sie Domain-Controller im Abschnitt Gruppen- oder Benutzernamen. Vergewissern Sie sich im Abschnitt Berechtigungen für Domain-Controller, dass die Kontrollkästchen Lesen, Registrieren und Auto-Registrierung aktiviert sind.
8. Wählen Sie OK, um die Zertifikatsvorlage LDAPOverSSL (oder den oben angegebenen Namen) zu erstellen. Schließen Sie das Fenster der Zertifikatsvorlagen-Konsole.
9. Klicken Sie im Fenster Zertifizierungsstelle mit der rechten Maustaste auf Zertifikatsvorlagen und wählen Sie Neu > Zertifikatsvorlage zum Ausstellen.
10. Wählen Sie im Fenster Zertifikatsvorlagen aktivieren die Option LDAPOverSSL (oder den Namen, den Sie oben angegeben haben), und wählen Sie dann OK.

Schritt 4: Sicherheitsgruppenregeln hinzufügen

Im letzten Schritt müssen Sie die Amazon-EC2-Konsole öffnen und Sicherheitsgruppenregeln hinzufügen. Diese Regeln ermöglichen es Ihren Domain-Controllern, eine Verbindung zu Ihrer Unternehmenszertifizierungsstelle herzustellen, um ein Zertifikat anzufordern. Dazu fügen Sie Regeln für den eingehenden Datenverkehr hinzu, sodass Ihre Enterprise CA eingehenden Datenverkehr von Ihren Domain-Controllern akzeptieren kann. Anschließend fügen Sie Regeln für ausgehenden Datenverkehr von Ihren Domain-Controllern zur Enterprise-Zertifizierungsstelle hinzu.

Sobald beide Regeln konfiguriert wurden, fordern Ihre Domain-Controller automatisch ein Zertifikat von Ihrer Enterprise CA an und aktivieren LDAPS für Ihr Verzeichnis. Der LDAP-Service auf Ihren Domain-Controllern kann jetzt LDAPS-Verbindungen akzeptieren.

Konfigurieren von Sicherheitsgruppenregeln

1. Navigieren Sie zu Ihrer Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2 und melden Sie sich mit Administratoranmeldeinformationen an.
2. Wählen Sie links die Option Security Groups unter Network & Security.
3. Wählen Sie im Hauptbereich die AWS Sicherheitsgruppe für Ihre CA aus.
4. Wählen Sie die Registerkarte Inbound (Eingehend) und anschließend Edit (Bearbeiten) aus.
5. Führen Sie im Dialogfeld Edit inbound rules die folgenden Schritte aus:
   - Klicken Sie auf Add Rule (Regel hinzufügen).
   - Wählen Sie All traffic für Type und Custom für Source.
   - Geben Sie die AWS Sicherheitsgruppe Ihres Verzeichnisses (z. B. sg-123456789) in das Feld neben Quelle ein.
   - Wählen Sie Speichern.
6. Wählen Sie nun die AWS Sicherheitsgruppe Ihres AWS Managed Microsoft AD-Verzeichnisses aus. Wählen Sie die Registerkarte Outbound und anschließend Edit.
7. Führen Sie im Dialogfeld Edit outbound rules die folgenden Schritte aus:
   - Klicken Sie auf Add Rule (Regel hinzufügen).
   - Wählen Sie All traffic für Type und Custom für Destination.
   - Geben Sie die AWS Sicherheitsgruppe Ihrer CA in das Feld neben Ziel ein.
   - Wählen Sie Speichern.

Sie können die LDAPS-Verbindung zum AWS Managed Microsoft AD-Verzeichnis mit dem LDP-Tool testen. Das Tool LDP ist in den Active Directory Administrative Tools enthalten. Weitere Informationen finden Sie unter Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD.

> **Note**
>
> Bevor Sie die LDAPS-Verbindung testen, müssen Sie bis zu 30 Minuten warten, bis die untergeordnete Zertifizierungsstelle ein Zertifikat für Ihre Domain-Controller ausgestellt hat.

Weitere Informationen zu serverseitigen LDAPS und ein Anwendungsbeispiel für die Einrichtung finden Sie unter So aktivieren Sie serverseitiges LDAPS für Ihr AWS verwaltetes Microsoft AD-Verzeichnis im Sicherheitsblog. AWS

Aktivieren Sie clientseitiges LDAPS mit AWS Managed Microsoft AD

Die clientseitige Unterstützung des Lightweight Directory Access Protocol Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) in AWS Managed Microsoft AD verschlüsselt die Kommunikation zwischen selbstverwaltetem (lokalem) Microsoft Active Directory (AD) und Anwendungen. AWS Beispiele für solche Anwendungen sind WorkSpaces, AWS IAM Identity Center QuickSight, Amazon und Amazon Chime. Diese Verschlüsselung hilft Ihnen, die Identitätsdaten Ihrer Organisation besser zu schützen und Ihre Sicherheitsanforderungen zu erfüllen.

Voraussetzungen

Bevor Sie clientseitiges LDAPS aktivieren, müssen Sie die folgenden Anforderungen erfüllen.

Themen

- Schaffen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrem selbstverwalteten Microsoft Active Directory
- Serverzertifikate in Active Directory bereitstellen
- Anforderungen an das Zertifikat der Zertifizierungsstelle
- Netzwerkanforderungen

Schaffen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrem selbstverwalteten Microsoft Active Directory

Zunächst müssen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD einrichten, um clientseitige Microsoft Active Directory LDAPS zu aktivieren. Weitere Informationen finden Sie unter the section called “Erstellen einer Vertrauensstellung”.

Serverzertifikate in Active Directory bereitstellen

Um clientseitiges LDAPS aktivieren zu können, müssen Sie Serverzertifikate für jeden Domain-Controller in Ihrem Active Directory abrufen und installieren. Diese Zertifikate werden vom LDAP-Service verwendet, um SSL-Verbindungen von LDAP-Clients zu überwachen und automatisch zu akzeptieren. Sie können SSL-Zertifikate verwenden, die entweder von einer internen Active Directory Certificate Services (ADCS)-Bereitstellung ausgestellt oder von einem kommerziellen Aussteller erworben werden. Weitere Informationen zu Active Directory-Serverzertifikatanforderungen finden Sie unter LDAP over SSL (LDAPS) Certificate auf der Microsoft-Website.

Anforderungen an das Zertifikat der Zertifizierungsstelle

Ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das den Aussteller Ihrer Serverzertifikate darstellt, ist für den clientseitigen LDAPS-Betrieb erforderlich. Zertifizierungsstellenzertifikate (CA-Zertifikate) werden mit den Serverzertifikaten abgeglichen, die von den Active-Directory-Domain-Controllern zur Verschlüsselung der LDAP-Kommunikation bereitgestellt werden. Beachten Sie die folgenden Zertifizierungsstellenzertifikat-Anforderungen:

- Die Enterprise Certification Authority (CA) ist erforderlich, um clientseitiges LDAPS zu aktivieren. Sie können entweder den Active Directory Zertifikatsdienst, eine kommerzielle Zertifizierungsstelle eines Drittanbieters oder verwenden. AWS Certificate Manager Weitere Informationen zur Microsoft Enterprise Certificate Authority finden Sie in der MicrosoftDokumentation.
- Es können nur Zertifikate registriert werden, die noch mehr als 90 Tage lang gültig sind.
- Zertifikate müssen im PEM-Format (Privacy-Enhanced Mail) vorliegen. Wenn Sie Zertifizierungsstellenzertifikate aus Active Directory exportieren, wählen Sie base64-codiertes X.509 (.CER) als Exportdateiformat aus.
- Pro AWS verwaltetem Microsoft AD-Verzeichnis können maximal fünf (5) CA-Zertifikate gespeichert werden.
- Zertifikate, die den RSASSA-PSS-Signaturalgorithmus verwenden, werden nicht unterstützt.
- Zertifizierungsstellenzertifikate, die mit jedem Serverzertifikat in jeder vertrauenswürdigen Domain verbunden sind, müssen registriert werden.

Netzwerkanforderungen

AWS Der LDAP-Verkehr von Anwendungen wird ausschließlich auf TCP-Port 636 ausgeführt, ohne dass ein Fallback auf den LDAP-Port 389 erfolgt. Für die Windows LDAP-Kommunikation, die Replikation, Vertrauensstellungen und mehr unterstützt, wird jedoch weiterhin LDAP-Port 389 mit Windows-nativer Sicherheit verwendet. Konfigurieren Sie AWS Sicherheitsgruppen und Netzwerkfirewalls, um TCP-Kommunikation auf Port 636 in AWS Managed Microsoft AD (ausgehend) und selbstverwaltetem Active Directory (eingehend) zu ermöglichen. Lassen Sie den LDAP-Port 389 zwischen AWS Managed Microsoft AD und selbstverwaltetem Active Directory geöffnet.

Clientseitiges LDAPS aktivieren

Um clientseitiges LDAPS zu aktivieren, importieren Sie das Zertifikat der Zertifizierungsstelle (CA) in AWS Managed Microsoft AD und aktivieren Sie dann LDAPS in Ihrem Verzeichnis. Nach der Aktivierung fließt der gesamte LDAP-Verkehr zwischen AWS -Anwendungen und Ihrem selbstverwalteten Active Directory mit SSL-Kanalverschlüsselung (Secure Sockets Layer).

Sie können zwei verschiedene Verfahren nutzen, um client-seitiges LDAPS für Ihr Verzeichnis zu aktivieren. Sie können entweder die Methode oder die AWS Management Console Methode verwenden. AWS CLI

> **Note**
>
> Clientseitiges LDAPS ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.

Themen

Schritt 1: Registrieren Sie ein Zertifikat in AWS Directory Service

Verwenden Sie eine der folgenden Methoden, um ein Zertifikat in zu registrieren AWS Directory Service.

Methode 1: Um Ihr Zertifikat in AWS Directory Service (AWS Management Console) zu registrieren

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie das Zertifikat registrieren möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Client-side LDAPS (clientseitiges LDAPS) das Menü Actions (Aktionen) aus und klicken Sie dann auf Register certificate (Zertifikat registrieren).
5. Klicken Sie im Dialogfeld Register a CA certificate (Registrieren eines CA-Zertifikats) auf die Option Browse (Durchsuchen), wählen Sie dann das Zertifikat aus und klicken Sie anschließend auf die Option Open (Öffnen).
6. Wählen Sie die Option Register certificate (Zertifikat registrieren) aus.

Methode 2: Um Ihr Zertifikat in AWS Directory Service (AWS CLI) zu registrieren

- Führen Sie den folgenden Befehl aus. Zeigen Sie für die Zertifikatdaten auf den Speicherort der Zertifizierungsstellen-Zertifikatdatei. In der Antwort wird eine Zertifikat-ID angegeben.

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

Schritt 2: Den Registrierungsstatus überprüfen

Um sich den Status einer Zertifikatsregistrierung oder eine Liste der registrierten Zertifikate anzeigen zu lassen, nutzen Sie eines der folgenden Verfahren.

Methode 1: Um den Registrierungsstatus des Zertifikats in AWS Directory Service (AWS Management Console) zu überprüfen

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Überprüfen Sie den aktuellen Status der Zertifikatregistrierung, der in der Spalte Registration status (Registrierungsstatus) angezeigt wird. Wenn sich der Wert des Registrierungsstatus in Registered (Registriert) ändert, ist Ihr Zertifikat erfolgreich registriert worden.

Methode 2: Um den Status der Zertifikatsregistrierung in AWS Directory Service (AWS CLI) zu überprüfen

- Führen Sie den folgenden Befehl aus. Wenn der Statuswert `Registered` zurückgegeben wird, wurde Ihr Zertifikat erfolgreich registriert.

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

Schritt 3: Clientseitiges LDAPS aktivieren

Verwenden Sie eine der folgenden Methoden, um clientseitiges LDAPS in zu aktivieren. AWS Directory Service

> **Note**
>
> Sie müssen mindestens ein Zertifikat erfolgreich registriert haben, bevor Sie das clientseitige LDAPS aktivieren können.

Methode 1: Um clientseitiges LDAPS in () zu aktivieren AWS Directory ServiceAWS Management Console

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Wählen Sie Enable (Aktivieren) aus. Steht diese Option nicht zur Verfügung, überprüfen Sie, ob ein gültiges Zertifikat erfolgreich registriert wurde, und versuchen Sie es dann erneut.
3. Wählen Sie im Dialogfeld Enable client-side LDAPS (Client-seitiges LDAPS aktivieren) die Option Enable (Aktivieren).

Methode 2: Um clientseitiges LDAPS in () zu aktivieren AWS Directory ServiceAWS CLI

- Führen Sie den folgenden Befehl aus.

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

Schritt 4: Den LDAPS-Status überprüfen

Verwenden Sie eine der folgenden Methoden, um den LDAPS-Status in zu überprüfen. AWS Directory Service

Methode 1: Um den LDAPS-Status in AWS Directory Service () zu überprüfen AWS Management Console

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Wenn der Statuswert als Enabled (Aktiviert) angezeigt wird, wurde das LDAPS erfolgreich konfiguriert.

Methode 2: Um den LDAPS-Status in AWS Directory Service () zu überprüfen AWS CLI

- Führen Sie den folgenden Befehl aus. Wenn der Statuswert `Enabled` zurückgibt, wurde das LDAPS erfolgreich konfiguriert.

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

Clientseitiges LDAPS überprüfen

Verwenden Sie diese Befehle, um Ihre LDAPS-Konfiguration zu verwalten.

Sie können zwei verschiedene Verfahren nutzen, um client-seitige LDAPS-Einstellungen zu verwalten. Sie können entweder die AWS Management Console Methode oder die AWS CLI Methode verwenden.

Zertifikatsdetails anzeigen

Nutzen Sie eines der folgenden Verfahren, um zu sehen, wann ein Zertifikat abläuft.

Methode 1: Um die Zertifikatsdetails in AWS Directory Service (AWS Management Console) anzuzeigen

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie das Zertifikat anzeigen möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) werden unter CA certificates (CA-Zertifikate) Informationen zum Zertifikat angezeigt.

Methode 2: Um die Zertifikatsdetails in AWS Directory Service (AWS CLI) anzuzeigen

- Führen Sie den folgenden Befehl aus. Verwenden Sie für die Zertifikat-ID den von `register-certificate` oder `list-certificates` zurückgegebenen Bezeichner.

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

Ein Zertifikat abmelden

Nutzen Sie eines der folgenden Verfahren, um ein Zertifikat abzumelden.

> **Note**
>
> Wenn nur ein Zertifikat registriert ist, müssen Sie zuerst LDAPS deaktivieren, bevor Sie das Zertifikat abmelden können.

Methode 1: Um ein Zertifikat in AWS Directory Service () abzumelden AWS Management Console

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.

2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie das Zertifikat deregistrieren möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) die Option Actions (Aktionen) und klicken Sie dann auf Deregister certificate (Zertifikat abmelden).
5. Wählen Sie im Dialogfeld Deregister a CA certificate (Ein CA-Zertifikat abmelden) die Option Deregister (Abmelden).

Methode 2: Um ein Zertifikat in () abzumelden AWS Directory ServiceAWS CLI

- Führen Sie den folgenden Befehl aus. Verwenden Sie für die Zertifikat-ID den von `register-certificate` oder `list-certificates` zurückgegebenen Bezeichner.

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

Clientseitiges LDAPS deaktivieren

Nutzen Sie eines der folgenden Verfahren, um clientseitiges LDAPS zu deaktivieren.

Methode 1: Um clientseitiges LDAPS in () zu deaktivieren AWS Directory ServiceAWS Management Console

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region, in der Sie das clientseitige LDAPS deaktivieren möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.

- Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.

4. Wählen Sie im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) die Option Disable (Deaktivieren) aus.
5. Klicken Sie im Dialogfeld Disable client-side LDAPS (Clientseitiges LDAPS deaktivieren) auf Disable (Deaktivieren).

Methode 2: Um clientseitiges LDAPS in () zu deaktivieren AWS Directory ServiceAWS CLI

- Führen Sie den folgenden Befehl aus.

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

Probleme bei der Zertifikatsregistrierung

Die Registrierung Ihrer AWS verwalteten Microsoft AD-Domänencontroller mit den CA-Zertifikaten kann bis zu 30 Minuten dauern. Wenn Sie Probleme mit der Zertifikatsregistrierung haben und Ihre AWS verwalteten Microsoft AD-Domänencontroller neu starten möchten, können Sie sich an uns wenden. AWS Support Informationen zum Erstellen eines Supportfalls finden Sie unter Erstellen von Supportanfragen und Fallmanagement.

Compliance für AWS Managed Microsoft AD verwalten

Sie können AWS Managed Microsoft AD verwenden, um Ihre Active Directory-fähigen Anwendungen in der AWS Cloud zu unterstützen, die den folgenden Compliance-Anforderungen unterliegen. Ihre Anwendungen genügen jedoch den Compliance-Anforderungen nicht, wenn Sie Simple AD verwenden.

Unterstützte Compliance-Standards

AWS Managed Microsoft AD wurde nach den folgenden Standards geprüft und kann als Teil von Lösungen verwendet werden, für die Sie eine Konformitätszertifizierung benötigen.

AWS Managed Microsoft AD erfüllt die Sicherheitsanforderungen des Federal Risk and Authorization Management Program (FedRAMP) und wurde vom FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) für die FedRAMP Moderate and High Baseline ausgezeichnet. Weitere Informationen zu FedRAMP finden Sie unter FedRAMP-Compliance.

AWS Managed Microsoft AD verfügt über eine Konformitätsbescheinigung für den Payment Card Industry (PCI) Data Security Standard (DSS) Version 3.2 auf Service Provider Level 1. Kunden, die AWS Produkte und Dienste zum Speichern, Verarbeiten oder Übertragen von Karteninhaberdaten verwenden, können AWS Managed Microsoft AD verwenden, um ihre eigene PCI-DSS-Konformitätszertifizierung zu verwalten.

Weitere Informationen zu PCI DSS, einschließlich der Möglichkeit, eine Kopie des AWS PCI Compliance Package anzufordern, finden Sie unter PCI DSS Level 1. Wichtig ist, dass Sie in AWS Managed Microsoft AD detaillierte Kennwortrichtlinien konfigurieren müssen, damit sie den PCI-DSS-Standards der Version 3.2 entsprechen. Einzelheiten dazu, welche Richtlinien durchgesetzt werden müssen, finden Sie im folgenden Abschnitt mit dem Titel Aktivieren der PCI-Konformität für Ihr AWS verwaltetes Microsoft AD-Verzeichnis.

AWS hat sein Compliance-Programm nach dem Health Insurance Portability and Accountability Act (HIPAA) um AWS Managed Microsoft AD als HIPAA-fähigen Service erweitert. Wenn Sie ein Business Associate Agreement (BAA) mit abgeschlossen haben AWS, können Sie AWS Managed Microsoft AD verwenden, um Ihre HIPAA-kon formen Anwendungen zu erstellen.

AWS bietet ein Whitepaper mit Fokus auf HIPAA für Kunden, die mehr darüber erfahren möchten, wie sie Gesundheitsinformationen verarbeiten und speichern können AWS . Weitere Informationen finden Sie unter HIPAA-Compliance.

Gemeinsame Verantwortlichkeit

Sicherheit, einschließlich FedRAMP-, HIPAA- und PCI-Compliance, ist eine gemeinsame Verantwortlichkeit. Es ist wichtig zu verstehen, dass der Compliance-Status von AWS Managed Microsoft AD nicht automatisch für Anwendungen gilt, die Sie in der AWS Cloud ausführen. Sie müssen sicherstellen, dass Ihre Nutzung der AWS Dienste den Standards entspricht.

Eine vollständige Liste der verschiedenen AWS Compliance-Programme, die AWS Managed Microsoft AD unterstützt, finden Sie unter AWS Services im Umfang nach Compliance-Programmen.

Aktivieren Sie die PCI-Konformität für Ihr AWS verwaltetes Microsoft AD-Verzeichnis

Um die PCI-Konformität für Ihr AWS verwaltetes Microsoft AD-Verzeichnis zu aktivieren, müssen Sie detaillierte Kennwortrichtlinien konfigurieren, wie sie in der PCI-DSS-Konformitätsbescheinigung (AOC) und der Haftungsübersicht von beschrieben sind. AWS Artifact

Weitere Informationen über differenzierte Passwortrichtlinien finden Sie unter Kennwortrichtlinien für AWS Managed Microsoft AD verwalten.

Ihre Netzwerksicherheitskonfiguration in AWS Managed Microsoft AD verbessern

Die AWS-Sicherheitsgruppe, die für das Verzeichnis in AWS Managed Microsoft AD bereitgestellt wird, ist mit den minimalen eingehenden Netzwerkports konfiguriert, die erforderlich sind, um alle bekannten Anwendungsfälle für Ihr Verzeichnis in AWS Managed Microsoft AD zu unterstützen.

Weitere Informationen zur bereitgestellten AWS-Sicherheitsgruppe finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.

Um die Netzwerksicherheit Ihres Verzeichnisses in AWS Managed Microsoft AD weiter zu verbessern, können Sie die AWS-Sicherheitsgruppe auf der Grundlage der unten aufgeführten allgemeinen Szenarien ändern.

Themen

Unterstützung nur für AWS-Anwendungen

Alle Benutzerkonten werden nur in Ihrem AWS Managed Microsoft AD bereitgestellt und können mit unterstützten AWS-Anwendungen verwendet werden, z. B. mit den folgenden:

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

Sie können die folgende AWS-Sicherheitsgruppenkonfiguration verwenden, um den gesamten unwichtigen Datenverkehr zu Ihren Domain-Controllern in AWS Managed Microsoft AD zu blockieren.

> **Note**
>
> - Folgendes ist mit dieser AWS-Sicherheitsgruppenkonfiguration nicht kompatibel:
>   - Amazon EC2-Instances
>   - Amazon FSx

- Amazon RDS für MySQL
- Amazon RDS für Oracle
- Amazon RDS für PostgreSQL
- Amazon RDS für SQL Server
- WorkSpaces
- Active-Directory-Vertrauensstellungen
- Mit der Domain verbundene Clients oder Server

Regeln für eingehenden Datenverkehr

Keine.

Regeln für ausgehenden Datenverkehr

Keine.

Nur AWS-Anwendungen mit Vertrauensunterstützung

Alle Benutzerkonten werden in Ihrem AWS Managed Microsoft AD oder in vertrauenswürdigem Active Directory eingerichtet, um mit unterstützten AWS-Anwendungen verwendet zu werden, z. B. mit den folgenden:

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

Sie können die bereitgestellte AWS-Sicherheitsgruppenkonfiguration so ändern, dass der gesamte nicht wesentliche Datenverkehr zu Ihren Domain-Controllern in AWS Managed Microsoft AD blockiert wird.

Note

- Folgendes ist mit dieser AWS-Sicherheitsgruppenkonfiguration nicht kompatibel:
  - Amazon EC2-Instances
  - Amazon FSx
  - Amazon RDS für MySQL
  - Amazon RDS für Oracle
  - Amazon RDS für PostgreSQL
  - Amazon RDS für SQL Server
  - WorkSpaces
  - Active-Directory-Vertrauensstellungen
  - Mit der Domain verbundene Clients oder Server
- Bei dieser Konfiguration müssen Sie sicherstellen, dass das „On-Premises-CIDR-Netzwerk“ sicher ist.
- TCP 445 wird nur für die Vertrauensstellung verwendet und kann entfernt werden, nachdem die Vertrauensstellung eingerichtet wurde.
- TCP 636 ist nur erforderlich, wenn LDAP über SSL verwendet wird.

Regeln für eingehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP und UDP	53	On-Premises-CIDR	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauensstellungen
TCP und UDP	88	On-Premises-CIDR	Kerberos	Benutzer- und Computera

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
				uthentifizierung, Vertrauen sstellungen auf Gesamtstr ukturebene
TCP und UDP	389	On-Premises-CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP und UDP	464	On-Premises-CIDR	Kerberos Passwort ändern/ei nrichten	Replikation, Benutzer- und Computera uthentifizierung, Vertrauen sstellungen
TCP	445	On-Premises-CIDR	SMB/CIFS	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien-Vertraue nsstellungen
TCP	135	On-Premises-CIDR	Replikation	RPC, EPM

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP	636	On-Premises-CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	49152–65535	On-Premises-CIDR	RPC	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	3268 - 3269	On-Premises-CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
UDP	123	On-Premises-CIDR	Windows-Uhrzeit	Windows-Uhrzeit, Vertrauensstellungen

Regeln für ausgehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
Alle	Alle	On-Premises-CIDR	Gesamter Datenverkehr	

AWS -Anwendungen und native Active-Directory-Workload-Unterstützung

Benutzerkonten werden nur in Ihrem AWS Managed Microsoft AD bereitgestellt und können mit unterstützten AWS-Anwendungen verwendet werden, z. B. mit den folgenden:

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

Sie können die bereitgestellte AWS-Sicherheitsgruppenkonfiguration so ändern, dass der gesamte nicht wesentliche Datenverkehr zu Ihren Domain-Controllern in AWS Managed Microsoft AD blockiert wird.

> **Note**
>
> - Active-Directory-Vertrauensstellungen können nicht zwischen Ihrem Verzeichnis in AWS Managed Microsoft AD und Ihrer On-Premises-Domain erstellt und verwaltet werden.
> - Sie müssen sicherstellen, dass das „Client CIDR-Netzwerk“ sicher ist.
> - TCP 636 ist nur erforderlich, wenn LDAP über SSL verwendet wird.
> - Wenn Sie eine Enterprise CA mit dieser Konfiguration verwenden möchten, müssen Sie eine ausgehende Regel „TCP, 443, CA CIDR“ erstellen.

Regeln für eingehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP und UDP	53	Client-CIDR	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauensstellungen
TCP und UDP	88	Client-CIDR	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauensstellungen auf Gesamtstrukturebene
TCP und UDP	389	Client-CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung,

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
				Gruppenrichtlinien, Vertrauensstellungen
TCP und UDP	445	Client-CIDR	SMB/CIFS	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien-Vertrauensstellungen
TCP und UDP	464	Client-CIDR	Kerberos Passwort ändern/einrichten	Replikation, Benutzer- und Computerauthentifizierung, Vertrauensstellungen
TCP	135	Client-CIDR	Replikation	RPC, EPM
TCP	636	Client-CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP	49152–65535	Client-CIDR	RPC	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	3268 - 3269	Client-CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	9389	Client-CIDR	SOAP	AD-DS-Web-Services
UDP	123	Client-CIDR	Windows-Uhrzeit	Windows-Uhrzeit, Vertrauensstellungen
UDP	138	Client-CIDR	DFSN und NetLogon	DFS, Gruppenrichtlinie

Regeln für ausgehenden Datenverkehr

Keine.

AWS-Anwendungen und native Active-Directory-Workload-Unterstützung mit Vertrauensstellung

Alle Benutzerkonten werden in Ihrem AWS Managed Microsoft AD oder in vertrauenswürdigem Active Directory eingerichtet, um mit unterstützten AWS-Anwendungen verwendet zu werden, z. B. mit den folgenden:

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

Sie können die bereitgestellte AWS-Sicherheitsgruppenkonfiguration so ändern, dass der gesamte nicht wesentliche Datenverkehr zu Ihren Domain-Controllern in AWS Managed Microsoft AD blockiert wird.

> **Note**
>
> - Sie müssen dafür sorgen, dass die Netzwerke „On-premises-CIDR“ und „Client CIDR“ sicher sind.
> - TCP 445 mit „On-Premises-CIDR“ wird nur für die Vertrauensstellung verwendet und kann entfernt werden, nachdem die Vertrauensstellung eingerichtet wurde.
> - TCP 445 mit „Client CIDR“ sollte offen gelassen werden, da es für die Verarbeitung der Gruppenrichtlinien erforderlich ist.

- TCP 636 ist nur erforderlich, wenn LDAP über SSL verwendet wird.
- Wenn Sie eine Enterprise CA mit dieser Konfiguration verwenden möchten, müssen Sie eine ausgehende Regel „TCP, 443, CA CIDR“ erstellen.

Regeln für eingehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP und UDP	53	On-Premises-CIDR	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauensstellungen
TCP und UDP	88	On-Premises-CIDR	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauensstellungen auf Gesamtstrukturebene
TCP und UDP	389	On-Premises-CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP und UDP	464	On-Premises-CIDR	Kerberos Passwort ändern/einrichten	Replikation, Benutzer- und Computerauthentifizierung, Vertrauensstellungen
TCP	445	On-Premises-CIDR	SMB/CIFS	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien-Vertrauensstellungen
TCP	135	On-Premises-CIDR	Replikation	RPC, EPM
TCP	636	On-Premises-CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP	49152–65535	On-Premises-CIDR	RPC	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	3268 - 3269	On-Premises-CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
UDP	123	On-Premises-CIDR	Windows-Uhrzeit	Windows-Uhrzeit, Vertrauensstellungen
TCP und UDP	53	Client-CIDR	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauensstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP und UDP	88	Client-CIDR	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauensstellungen auf Gesamtstrukturebene
TCP und UDP	389	Client-CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP und UDP	445	Client-CIDR	SMB/CIFS	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien-Vertrauensstellungen
TCP und UDP	464	Client-CIDR	Kerberos Passwort ändern/einrichten	Replikation, Benutzer- und Computerauthentifizierung, Vertrauensstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
TCP	135	Client-CIDR	Replikation	RPC, EPM
TCP	636	Client-CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	49152–65535	Client-CIDR	RPC	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	3268 - 3269	Client-CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP	9389	Client-CIDR	SOAP	AD-DS-Web-Services

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
UDP	123	Client-CIDR	Windows-Uhrzeit	Windows-Uhrzeit, Vertrauensstellungen
UDP	138	Client-CIDR	DFSN und NetLogon	DFS, Gruppenrichtlinie

Regeln für ausgehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
Alle	Alle	On-Premises-CIDR	Gesamter Datenverkehr	

Verzeichnis-Sicherheitseinstellungen konfigurieren

Sie können differenzierte Verzeichniseinstellungen für Ihr AWS Managed Microsoft AD konfigurieren, um Ihre Compliance- und Sicherheitsanforderungen zu erfüllen, ohne dass sich der betriebliche Workload erhöht. In den Verzeichniseinstellungen können Sie die Secure-Channel-Konfiguration für die in Ihrem Verzeichnis verwendeten Protokolle und Codes aktualisieren. Sie haben beispielsweise die Möglichkeit, einzelne Legacy-Chiffren, wie RC4 oder DES, und Protokolle, wie SSL 2.0/3.0 und TLS 1.0/1.1, zu deaktivieren. AWS Managed Microsoft AD stellt die Konfiguration dann auf allen Domain-Controllern in Ihrem Verzeichnis bereit, verwaltet Domain-Controller-Neustarts und behält diese Konfiguration bei, wenn Sie den Umfang erweitern oder zusätzliche AWS-Regionen bereitstellen. Alle verfügbaren Einstellungen finden Sie unter Liste der Verzeichnis-Sicherheitseinstellungen.

Sicherheitseinstellungen für Verzeichnisse bearbeiten

Sie können die Einstellungen für jedes Ihrer Verzeichnisse konfigurieren und bearbeiten.

Um Verzeichniseinstellungen zu bearbeiten

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die AWS-Directory-Service-Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Suchen Sie unter Netzwerk und Sicherheit nach Verzeichniseinstellungen und wählen Sie dann Einstellungen bearbeiten aus.
4. Ändern Sie unter Einstellungen bearbeiten den Wert für die Einstellungen, die Sie bearbeiten möchten. Wenn Sie eine Einstellung bearbeiten, ändert sich ihr Status von Standard auf Bereit zur Aktualisierung. Wenn Sie die Einstellung bereits bearbeitet haben, ändert sich ihr Status von Aktualisiert in Bereit zur Aktualisierung. Wählen Sie dann Überprüfen aus.
5. Unter Einstellungen überprüfen und aktualisieren sehen Sie sich den Abschnitt Verzeichniseinstellungen an und stellen Sie sicher, dass alle neuen Werte korrekt sind. Wenn Sie weitere Änderungen an Ihren Einstellungen vornehmen möchten, wählen Sie Einstellungen bearbeiten. Wenn Sie mit Ihren Änderungen zufrieden sind und bereit sind, die neuen Werte zu implementieren, wählen Sie Einstellungen aktualisieren. Anschließend kehren Sie zur Verzeichnis-ID-Seite zurück.

> **Note**
>
> Unter Verzeichniseinstellungen können Sie den Status Ihrer aktualisierten Einstellungen einsehen. Während die Einstellungen implementiert werden, wird im Status die Meldung Wird aktualisiert angezeigt. Sie können keine anderen Einstellungen bearbeiten, solange für eine Einstellung unter Status die Option Wird aktualisiert angezeigt wird. Der Status zeigt Aktualisiert an, wenn die Einstellung mit Ihrer Änderung erfolgreich aktualisiert wurde. Der Status zeigt Fehlgeschlagen an, wenn die Einstellung nicht mit Ihrer Änderung aktualisiert werden kann.

Fehlgeschlagene Sicherheitseinstellungen für Verzeichnisse

Wenn während einer Aktualisierung der Einstellungen ein Fehler auftritt, wird der Status als Fehlgeschlagen angezeigt. Bei einem fehlgeschlagenen Status werden die Einstellungen nicht auf die neuen Werte aktualisiert, und die ursprünglichen Werte bleiben implementiert. Sie können erneut versuchen, diese Einstellungen zu aktualisieren oder sie auf ihre vorherigen Werte zurückzusetzen.

So beheben Sie fehlgeschlagene Einstellungsaktualisierungen

- Wählen Sie unter Verzeichniseinstellungen die Option Fehlgeschlagene Einstellungen beheben aus. Führen Sie dann einen der folgenden Schritte aus:
  - Um Ihre Einstellungen auf ihren ursprünglichen Wert vor dem Fehlerstatus zurückzusetzen, wählen Sie Fehlgeschlagene Einstellungen wiederherstellen aus. Wählen Sie dann im Popup-Modal die Option Wiederherstellen.
  - Um erneut zu versuchen, Ihre Verzeichniseinstellungen zu aktualisieren, wählen Sie Fehlgeschlagene Einstellungen erneut versuchen. Wenn Sie weitere Änderungen an Ihren Verzeichniseinstellungen vornehmen möchten, bevor Sie die fehlgeschlagenen Aktualisierungen erneut versuchen, wählen Sie Weiter bearbeiten. Wählen Sie unter Fehlgeschlagene Aktualisierungen überprüfen und erneut versuchen die Option Einstellungen aktualisieren aus.

Liste der Verzeichnis-Sicherheitseinstellungen

Die folgende Liste enthält den Typ, den Einstellungsnamen, den API-Namen, mögliche Werte und die Einstellungsbeschreibung für alle verfügbaren Verzeichnissicherheitseinstellungen.

TLS 1.2 und AES 256/256 sind die Standardsicherheitseinstellungen für Verzeichnisse, wenn alle anderen Sicherheitseinstellungen deaktiviert sind. Sie können nicht deaktiviert werden.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
Zertifikatsbasierte Authentifizierung	Certificate Backdating Compension	CERTIFICATE_BACKDATING_COMPENSATION	Jahre: 0 bis 50 Monate: 0 bis 11 Tage: 0 bis 30 Stunden: 0 bis 23 Minuten: 0 bis 59 Sekunden: 0 bis 59	Geben Sie einen Wert an, der angibt, wie lange ein Zertifikat einem Benutzer in Active Directory vorausgehen kann und noch für die Authentif

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
				izierung in Active Directory verwendet werden kann. Der Standardwert beträgt 10 Minuten. Sie können diesen Wert zwischen 1 Sekunde und 50 Jahren einstellen. Um diese Einstellung zu konfigurieren, müssen Sie den Kompatibilitätstyp für Strong Certificate Binding Enforcement auswählen. Weitere Informationen finden Sie unter KB5014754 – Änderungen der zertifikatsbasierten

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
				Authentifizierung auf Windows-Domain-Controllern in der Microsoft-Supportdokumentation.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	Certificate Strong Enforcent	CERTIFICATE_STRONG_ENFORCEMENT	Kompatibilität, vollständige Durchsetzung	Geben Sie einen der folgenden Durchsetzungstypen an: • Kompatibilität (Standard): Authentifizierung ist zulässig, wenn ein Zertifikat nicht eindeutig einem Benutzer zugeordnet werden kann. Wenn das Zertifikat älter ist als das Benutzerkonto in Active Directory, müssen Sie auch die Certificate Backdating Compensation festlegen

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
				, da andernfalls die Authentifizierung fehlschlägt. • Vollständige Durchsetzung: Authentifizierung ist nicht zulässig, wenn ein Zertifikat nicht eindeutig einem Benutzer zugeordnet werden kann. Wenn Sie diesen Durchsetzungstyp wählen, kann die Certificate Backdating Compensation nicht konfiguriert werden.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
				Weitere Informationen finden Sie unter KB5014754 – Änderungen der zertifikatsbasierten Authentifizierung auf Windows-Domain-Controllern in der Microsoft-Supportdokumentation.
Sicherer Kanal: Code	AES 128/128	AES_128_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den AES-128/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	DES 56/56	DES_56_56	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den DES-56/56-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.
	RC2 40/128	RC2_40_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC2-40/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	RC2 56/128	RC2_56_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC2-56/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.
	RC2 128/128	RC2_128_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC2-128/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	RC4 40/128	RC4_40_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC4-40/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.
	RC4 56/128	RC4_56_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC4-56/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	RC4 64/128	RC4_64_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC4-64/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.
	RC4 128/128	RC4_128_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den RC4-128/128-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	Triple DES 168/168	3DES_168_168	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den Triple-DES-168/168-Verschlüsselungscode für die Secure-Channel-Kommunikation zwischen Domain-Controllern in Ihrem Verzeichnis.
Sicherer Kanal: Protokoll	PCT 1.0	PCT_1_0	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie das PCT-1.0-Protokoll für die Secure-Channel-Kommunikation (Server und Client) auf den Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	SSL 2.0	SSL_2_0	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie das SSL-2.0-Protokoll für die Secure-Channel-Kommunikation (Server und Client) auf den Domain-Controllern in Ihrem Verzeichnis.
	SSL 3.0	SSL_3_0	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie das SSL-3.0-Protokoll für die Secure-Channel-Kommunikation (Server und Client) auf den Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsnam	API-Name	Mögliche Werte	Beschreibung der Einstellung
	TLS 1.0	TLS_1_0	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie das TLS-1.0-Protokoll für die Secure-Channel-Kommunikation (Server und Client) auf den Domain-Controllern in Ihrem Verzeichnis.
	TLS 1.1	TLS_1_1	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie das TLS-1.1-Protokoll für die Secure-Channel-Kommunikation (Server und Client) auf den Domain-Controllern in Ihrem Verzeichnis.

Einrichten von AWS Private CA Connector für AD

Sie können Ihr AWS Managed Microsoft AD in AWS Private Certificate Authority (CA) integrieren, um Zertifikate für Ihre mit der Active-Directory-Domain verbundenen Benutzer, Gruppen und Maschinen auszustellen und zu verwalten. AWS Private CA Mit Connector für Active Directory können Sie einen vollständig verwalteten AWS Private CA Drop-In-Ersatz für Ihre selbstverwalteten CAs verwenden, ohne lokale Agenten oder Proxyserver bereitstellen, patchen oder aktualisieren zu müssen.

> **Note**
>
> Die serverseitige LDAPS-Zertifikatsregistrierung für Domain-Controller in AWS Managed Microsoft AD mit AWS Private CA Connector für Active Directory wird nicht unterstützt. Informationen zum Aktivieren von serverseitigem LDAPS für Ihr Verzeichnis finden Sie unter So aktivieren Sie serverseitiges LDAPS für Ihr Verzeichnis in AWS Managed Microsoft AD.

Sie können die AWS Private CA Integration mit Ihrem Verzeichnis über die Directory-Service-Konsole, die AWS Private CA -Connector-for-Active-Directory-Konsole oder durch Aufrufen der `CreateTemplate`-API einrichten. Informationen zum Einrichten der Private-CA-Integration über die - AWS Private CA Connector-for-Active-Directory-Konsole finden Sie unter Erstellen einer Konnektorvorlage. Im Folgenden finden Sie Schritte zum Einrichten dieser Integration über die AWS Directory Service Konsole.

So richten Sie AWS Private CA Connector für AD ein

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die - AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit unter AWS Private CA Connector für AD die Option AWS Private CA Connector für AD einrichten aus. Die Seite Private CA-Zertifikat erstellen für Active Directory wird angezeigt. Führen Sie die Schritte in der -Konsole aus, um Ihre Private CA für den Active DirectoryKonnektor zu erstellen, um sich bei Ihrer Private CA zu registrieren. Weitere Informationen finden Sie unter Einen Konnektor erstellen.
4. Nachdem Sie Ihren Connector erstellt haben, folgen Sie den nachstehenden Schritten, um Details anzuzeigen, darunter den Status des Connectors und den Status der zugehörigen Private CA.

So zeigen Sie AWS Private CA Connector für AD an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die - AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Unter Netzwerk und Sicherheit können Sie unter AWS Private CA Connector für AD Ihre Private-CA-Konnektoren und zugehörige Private CA einsehen. Standardmäßig sehen Sie die folgenden Felder:

    a. AWS Private CA Konnektor-ID – Die eindeutige Kennung für einen AWS Private CA Konnektor. Wenn Sie darauf klicken, wird die Detailseite dieses AWS Private CA Konnektors angezeigt.

    b. AWS Private CA Betreff – Informationen über den definierten Namen für die CA. Wenn Sie darauf klicken, gelangen Sie zur Detailseite dieses AWS Private CA.

    c. Status – Basierend auf einer Statusprüfung für den AWS Private CA Connector und die AWS Private CA. Wenn beide Prüfungen erfolgreich sind, wird Aktiv angezeigt. Wenn eine der Prüfungen fehlschlägt, wird 1/2 Prüfungen fehlgeschlagen angezeigt. Wenn beide Prüfungen fehlschlagen, wird Fehlgeschlagen angezeigt. Weitere Informationen über den Status „fehlgeschlagen“ erhalten Sie, wenn Sie den Mauszeiger über den Hyperlink bewegen, um zu erfahren, welche Prüfung fehlgeschlagen ist. Folgen Sie den Anweisungen in der Konsole, um das Problem zu beheben.

    d. Erstellungsdatum – Der Tag, an dem der AWS Private CA Connector erstellt wurde.

Weitere Informationen finden Sie unter Konnektor-Details anzeigen.

Ihr AWS Managed Microsoft AD überwachen

Sie können Ihr Verzeichnis in AWS Managed Microsoft AD mit folgenden Methoden überwachen:

Themen

Erläuterungen zum Verzeichnisstatus

Im Folgenden sind die verschiedenen Zustandsangaben für ein Verzeichnis aufgeführt.

Aktiv

Das Verzeichnis funktioniert normal. AWS Directory Service hat keine Probleme für Ihr Verzeichnis erkannt.

Erstellen

Das Verzeichnis wird gerade erstellt. Die Verzeichniserstellung nimmt in der Regel 20 bis 45 Minuten in Anspruch, kann jedoch je nach Systemauslastung abweichen.

Deleted (Gelöscht)

Das Verzeichnis wurde gelöscht. Alle Ressourcen für das Verzeichnis wurden freigegeben. Ein Verzeichnis, das diesen Zustand erreicht hat, kann nicht wiederhergestellt werden.

Wird gelöscht

Das Verzeichnis wird gerade gelöscht. Das Verzeichnis bleibt in diesem Zustand, bis es vollständig gelöscht ist. Sobald ein Verzeichnis diesen Zustand erreicht, kann der Löschvorgang nicht mehr abgebrochen werden und das Verzeichnis ist nicht wiederherstellbar.

Fehlgeschlagen

Das Verzeichnis konnte nicht erstellt werden. Löschen Sie dieses Verzeichnis. Falls das Problem weiterhin besteht, kontaktieren Sie das AWS Support -Zentrum.

Beeinträchtigt

Das Verzeichnis wird nicht fehlerfrei ausgeführt. Mindestens ein Problem wurde erkannt und vermutlich wird nicht bei allen Verzeichnisvorgängen die volle Leistungskapazität erreicht. Es gibt viele mögliche Gründe dafür, dass sich das Verzeichnis in diesem Zustand befindet. Darunter fallen normale betriebliche Wartungsaktivitäten wie das Patchen oder die EC2-Instance-Rotation, das temporäre Hot-Spotting durch eine Anwendung auf einem Ihrer Domain-Controller oder Änderungen, die Sie an Ihrem Netzwerk vorgenommen haben und die versehentlich die Verzeichniskommunikation stören. Weitere Informationen finden Sie unter Problembehandlung bei AWS verwaltetem Microsoft AD, Fehlerbehebung in AD Connector, Beheben von Fehlern in Simple AD. AWS Behebt Probleme im Zusammenhang mit normalen Wartungsarbeiten innerhalb von 40 Minuten. Falls das Verzeichnis nach der Konsultation des Themas Fehlerbehebung länger als 40 Minuten den Status Beeinträchtigt aufweist, sollten Sie das AWS Support -Zentrum kontaktieren.

> **Important**
>
> Stellen Sie keinen Snapshot für ein Verzeichnis mit dem Status „Impaired“ (Beeinträchtigt) wieder her. Nur selten ist eine Snapshot-Wiederherstellung nötig, um Beeinträchtigungen zu beheben. Weitere Informationen finden Sie unter Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen.

Angefragt

Eine Anforderung zum Erstellen Ihres Verzeichnisses steht zurzeit an.

RestoreFailed

Die Wiederherstellung des Verzeichnisses anhand eines Snapshots ist fehlgeschlagen. Versuchen Sie die Wiederherstellung erneut. Falls das Problem weiterhin besteht, versuchen Sie es mit einem anderen Snapshot oder wenden Sie sich an das AWS Support -Zentrum.

Restoring (Wiederherstellung läuft)

Das Verzeichnis wird zurzeit anhand eines automatischen oder manuellen Snapshots wiederhergestellt. Die Wiederherstellung anhand eines Snapshots dauert in der Regel einige Minuten, abhängig von der Größe der Verzeichnisdaten im Snapshot.

Konfiguration von Verzeichnisstatusbenachrichtigungen mit Amazon SNS

Mit Amazon Simple Notification Service (Amazon SNS) können Sie E-Mail- oder Textnachrichten (SMS) erhalten, wenn sich der Status Ihres Verzeichnisses ändert. Sie werden benachrichtigt, wenn Ihr Verzeichnis vom Status Aktiv in den Status Beeinträchtigt wechselt. Außerdem erhalten Sie eine Benachrichtigung, wenn das Verzeichnis in einen aktiven Status zurückkehrt.

So funktioniert’s

Amazon SNS verwendet „Themen“ zum Sammeln und Verteilen von Nachrichten. Jedes Thema hat einen oder mehrere Subscriber, die zu diesem Thema veröffentlichte Nachrichten empfangen. Mit den folgenden Schritten können Sie ein Amazon SNS SNS-Thema AWS Directory Service als Herausgeber hinzufügen. Wenn AWS Directory Service eine Änderung des Status Ihres Verzeichnisses festgestellt wird, wird eine Nachricht zu diesem Thema veröffentlicht, die dann an die Abonnenten des Themas gesendet wird.

Sie können mehrere Verzeichnisse als Publisher zu einem einzelnen Thema zuordnen. Sie können auch Verzeichnis-Statusmeldungen zu Themen hinzufügen, die Sie zuvor in Amazon SNS erstellt haben. Sie haben umfassende Kontrolle, wer ein Thema veröffentlichen und abonnieren kann. Umfassende Informationen zu Amazon SNS finden Sie unter Was ist Amazon SNS?.

> **Note**
>
> Verzeichnisstatusbenachrichtigungen sind eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.

So aktivieren Sie SNS Messaging für Ihr Verzeichnis

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Directory Service Konsole.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie SNS-Nachrichten aktivieren möchten, und wählen Sie dann die Registerkarte Wartung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Wartung.
4. Wählen Sie im Abschnitt Verzeichnisüberwachung die Option Aktionen und dann Benachrichtigung erstellen aus.
5. Wählen Sie auf der Seite Benachrichtigung erstellen die Option Benachrichtigungstyp auswählen und dann Neue Benachrichtigung erstellen aus. Wenn Sie bereits über ein SNS-Thema verfügen, können Sie Vorhandenes SNS-Thema zuordnen wählen, um Status-Nachrichten aus diesem Verzeichnis zu diesem Thema zu senden.

> **Note**
>
> Wenn Sie Neue Benachrichtigung erstellen wählen, jedoch denselben Themen-Namen für ein SNS-Thema wählen, das bereits vorhanden ist, erstellt Amazon SNS kein neues Thema, sondern fügt die neue Abonnement-Information zum vorhandenen Thema hinzu. Wenn Sie Vorhandenes SNS-Thema zuordnen wählen, können Sie immer nur ein SNS-Thema wählen, das sich in derselben Region wie das Verzeichnis befindet.

6. Wählen Sie Empfängertyp und geben Sie die Kontaktinformationen für den Empfänger ein. Wenn Sie eine Telefonnummer für SMS eingeben, verwenden Sie nur Zahlen. Geben Sie keine Gedankenstriche, Leerzeichen oder Klammern ein.
7. (Optional) Geben Sie einen Namen für Ihr Thema und einen SNS-Anzeigenamen ein. Der Anzeigename ist ein kurzer Name von bis zu 10 Zeichen, der in alle SMS-Nachrichten zu diesem Thema aufgenommen wird. Bei der Verwendung der SMS-Option ist der Anzeigename erforderlich.

> **Note**
>
> Wenn Sie mit einem IAM-Benutzer oder einer IAM-Rolle angemeldet sind, für die nur die DirectoryServiceFullAccessverwaltete Richtlinie gilt, muss Ihr Themenname mit „DirectoryMonitoring“ beginnen. Wenn Sie Ihren Themennamen anpassen möchten, benötigen Sie zusätzliche Berechtigungen für SNS.

8. Wählen Sie Erstellen.

Wenn Sie zusätzliche SNS-Abonnenten angeben möchten, z. B. eine zusätzliche E-Mail-Adresse, Amazon SQS SQS-Warteschlangen oder AWS Lambda, können Sie dies von der Amazon SNS SNS-Konsole aus tun.

Verzeichnis-Status-Nachrichten aus einem Thema entfernen

1. Melden Sie sich bei der an und öffnen Sie die Konsole AWS Management Console .AWS Directory Service
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

- Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Statusnachrichten entfernen möchten, und wählen Sie dann die Registerkarte Wartung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
- Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Wartung.

4. Wählen Sie im Abschnitt Verzeichnisüberwachung einen SNS-Themennamen in der Liste aus, klicken Sie auf Aktionen und dann auf Entfernen.
5. Wählen Sie Remove (Entfernen) aus.

Dadurch wird Ihr Verzeichnis als Publisher für das ausgewählte SNS-Thema entfernt. Wenn Sie das gesamte Thema löschen möchten, können Sie dies von der Amazon SNS SNS-Konsole aus tun.

> **Note**
>
> Stellen Sie vor dem Löschen eines Amazon-SNS-Themas mithilfe der SNS-Konsole sicher, dass kein Verzeichnis Status-Nachrichten zu diesem Thema sendet.
> Wenn Sie ein Amazon-SNS-Thema mithilfe der SNS-Konsole löschen, wird diese Änderung nicht sofort in der Directory-Services-Konsole sichtbar. Sie würden nur benachrichtigt werden, wenn das nächste Mal ein Verzeichnis eine Nachricht zu diesem gelöschten Thema veröffentlicht. In diesem Fall würden Sie einen aktualisierten Status auf der Registerkarte Monitoring sehen, der angibt, dass das Thema nicht gefunden wurde.
> Um zu vermeiden, dass wichtige Verzeichnisstatusmeldungen übersehen werden, verknüpfen Sie Ihr Verzeichnis daher mit einem anderen Amazon SNS SNS-Thema AWS Directory Service, bevor Sie ein Thema löschen, von dem Nachrichten empfangen werden.

Ihre Verzeichnisprotokolle von AWS Managed Microsoft AD überprüfen

Sicherheitsprotokolle von Domain-Controller-Instances in AWS Managed Microsoft AD werden für ein Jahr archiviert. Sie können Ihr Verzeichnis in AWS Managed Microsoft AD auch so konfigurieren, dass Domain-Controller-Protokolle nahezu in Echtzeit an Amazon CloudWatch Logs weitergeleitet werden. Weitere Informationen finden Sie unter Protokollweiterleitung aktivieren.

AWS protokolliert die folgenden Ereignisse für die Compliance.

Überwachungskategorie	Richtlinieneinstellung	Audit-Status
Kontoanmeldung	Audit Validierung Anmeldeinformationen	Erfolg, Fehler
	Andere Ereignisse bei der Kontoanmeldung prüfen	Erfolg, Fehler
Kontenverwaltung	Audit Computerkonten-Management	Erfolg, Fehler
	Audit Andere Kontenmanagement-Ereignisse	Erfolg, Fehler
	Audit Sicherheitsgruppen-Management	Erfolg, Fehler
	Audit Benutzerkonten-Management	Erfolg, Fehler
Detaillierte Nachverfolgung	DPAPI-Aktivität prüfen	Erfolg, Fehler
	PNP-Aktivität prüfen	Herzlichen Glückwunsch
	Audit Prozesserstellung	Erfolg, Fehler
DS-Zugriff	Audit Verzeichnisservice-Zugriff	Erfolg, Fehler
	Audit Verzeichnisservice-Änderungen	Erfolg, Fehler
Anmeldung/Abmeldung	Kontosperre prüfen	Erfolg, Fehler
	Audit-Abmeldung	Herzlichen Glückwunsch
	Audit-Anmeldung	Erfolg, Fehler
	Andere Anmelde-/Abmeldeereignisse prüfen	Erfolg, Fehler

Überwachungskategorie	Richtlinieneinstellung	Audit-Status
	Audit Spezielle Anmeldung	Erfolg, Fehler
Objektzugriff	Andere Objektzugriffsereignisse prüfen	Erfolg, Fehler
	Audit Wechseldatenträger	Erfolg, Fehler
	Audit Zentrales Zugriffsrichtlinien-Staging	Erfolg, Fehler
Richtlinienänderungen	Audit Richtlinienänderungen	Erfolg, Fehler
	Audit Authentifizierungsrichtlinienänderungen	Erfolg, Fehler
	Audit Autorisierungsrichtlinienänderung	Erfolg, Fehler
	Änderung der MPSSVC-Richtlinie auf Regelebene prüfen	Herzlichen Glückwunsch
	Andere Richtlinienänderungen prüfen	Fehler
Privilegierte Nutzung	Audit Sensible privilegierte Nutzung	Erfolg, Fehler
System (System)	Audit IPsec-Treiber	Erfolg, Fehler
	Andere Weitere Systemereignisse	Erfolg, Fehler
	Audit Sicherheitsstatusänderung	Erfolg, Fehler
	Audit Sicherheitssystemerweiterung	Erfolg, Fehler

Überwachungskategorie	Richtlinieneinstellung	Audit-Status
	Audit Systemintegrität	Erfolg, Fehler

Protokollweiterleitung aktivieren

Sie können die AWS Directory Service-Konsole oder APIs verwenden, um Domain-Controller-Sicherheitsereignisprotokolle an Amazon CloudWatch Logs. weiterzuleiten. Dies hilft Ihnen, Ihre Anforderungen an die Richtlinien für die Sicherheitsüberwachung, -prüfung und -aufbewahrung von Protokollen zu erfüllen, indem die Transparenz der Sicherheitsereignisse in Ihrem Verzeichnis gewährleistet wird.

CloudWatch Logs kann diese Ereignisse auch an andere AWS-Konten, AWS-Services oder Anwendungen von Drittanbietern weiterleiten. Dies erleichtert Ihnen die zentrale Überwachung und Konfiguration von Warnungen, um ungewöhnliche Aktivitäten nahezu in Echtzeit zu erkennen und proaktiv darauf zu reagieren.

Nach der Aktivierung können Sie die CloudWatch-Logs-Konsole zum Abrufen der Daten aus der Protokollgruppe verwenden, die Sie beim Aktivieren des Service angegeben haben. Diese Protokollgruppe enthält die Sicherheitsprotokolle aus Ihren Domain-Controllern.

Weitere Informationen über Protokollgruppen und das Lesen ihrer Daten finden Sie unter Arbeiten mit Protokollgruppen und Protokollstreams im Benutzerhandbuch zu Amazon CloudWatch Logs.

> **Note**
>
> Die Protokollweiterleitung ist ein regionales Feature von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.

So aktivieren Sie die Protokollweiterleitung

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie die Verzeichnis-ID des Verzeichnisses in AWS Managed Microsoft AD aus, die Sie freigeben möchten.

3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Protokollweiterleitung aktivieren möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.

4. Wählen Sie im Abschnitt Log forwarding die Option Enable.
5. Wählen Sie im Dialogfeld Enable log forwarding to CloudWatch (Protokollweiterleitung an CloudWatch aktivieren) eine der folgenden Optionen:

   a. Wählen Sie Neue CloudWatch-Protokollgruppe erstellen, geben Sie unter CloudWatch-Protokollgruppenname einen Namen an, auf den Sie sich in CloudWatch Logs beziehen können.

   b. Wählen Sie Choose an existing CloudWatch log group und unter Existing CloudWatch log groups eine Protokollgruppe im Menü aus.

6. Prüfen Sie die Preisinformationen und die Verknüpfung und wählen Sie dann Enable aus.

So deaktivieren Sie die Protokollweiterleitung

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie die Verzeichnis-ID des Verzeichnisses in AWS Managed Microsoft AD aus, die Sie freigeben möchten.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Protokollweiterleitung deaktivieren möchten, und wählen Sie dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.

4. Wählen Sie im Abschnitt Log forwarding die Option Disable.
5. Sobald Sie die Informationen im Dialogfeld Disable log forwarding gelesen haben, wählen Sie Disable (Deaktivieren).

Verwenden der CLI zum Aktivieren der Protokollweiterleitung

Bevor Sie den `ds create-log-subscription`-Befehl verwenden, müssen Sie zunächst eine Amazon-CloudWatch-Protokollgruppe und anschließend eine IAM-Ressourcenrichtlinie erstellen, die dieser Gruppe die erforderlichen Berechtigungen zuweisen. Um mithilfe der CLI die Protokollweiterleitung zu aktivieren, führen Sie die folgenden Schritte aus.

Schritt 1: Eine Protokollgruppe in CloudWatch Logs erstellen

Erstellen Sie eine Protokollgruppe, die Sicherheitsprotokolle von Ihren Domain-Controllern erhält. Wir empfehlen, dem Namen `/aws/directoryservice/` voranzustellen, dies ist jedoch nicht erforderlich. Beispiele:

EXAMPLE CLI COMMAND (BEISPIEL FÜR DEN CLI-BEFEHL)

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

EXAMPLE POWERSHELL COMMAND (BEISPIEL FÜR DEN POWERSHELL-BEFEHL)

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

Anweisungen zum Erstellen einer CloudWatch-Logs-Gruppe finden Sie unter Erstellen einer Protokollgruppe in CloudWatch Logs im Benutzerhandbuch zu Amazon CloudWatch Logs.

Schritt 2: Eine CloudWatch-Logs-Ressourcenrichtlinie in IAM erstellen

Erstellen Sie eine CloudWatch-Logs-Ressourcenrichtlinie, die AWS Directory Service-Rechte zum Hinzufügen von Protokollen zu der neuen Protokollgruppe gewährt, die Sie in Schritt 1 erstellt haben. Sie können entweder den genauen ARN für die Protokollgruppe angeben, um den Zugriff von AWS Directory Service auf andere Protokollgruppen einzuschränken, oder einen Platzhalter verwenden, um alle Protokollgruppen einzuschließen. Die folgende Beispielrichtlinie verwendet die Platzhaltermethode, um zu identifizieren, dass alle Protokollgruppen, die mit `/aws/directoryservice/` beginnen, für das AWS-Konto, in dem sich Ihr Verzeichnis befindet, enthalten sind.

```
{
    "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/*"
        }
    ]
}
```

Sie müssen diese Richtlinie in einer Textdatei (z. B. DSPolicy.json) auf Ihrer lokalen Workstation speichern, da Sie sie über die CLI ausführen müssen. Beispiele:

EXAMPLE CLI COMMAND (BEISPIEL FÜR DEN CLI-BEFEHL)

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

EXAMPLE POWERSHELL COMMAND (BEISPIEL FÜR DEN POWERSHELL-BEFEHL)

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

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

Schritt 3: Ein AWS Directory Service-Protokollabonnement erstellen

In diesem letzten Schritt können Sie nun die Protokollweiterleitung aktivieren, indem Sie das Protokollabonnement erstellen. Beispiele:

EXAMPLE CLI COMMAND (BEISPIEL FÜR DEN CLI-BEFEHL)

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

EXAMPLE POWERSHELL COMMAND (BEISPIEL FÜR DEN POWERSHELL-BEFEHL)

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

Ihre Domain-Controller mit Leistungsmetriken überwachen

AWS Directory Service ist in Amazon integriert CloudWatch , um Ihnen wichtige Leistungskennzahlen für jeden Domain-Controller in Ihrem zu bietenActive Directory. Das bedeutet, dass Sie Leistungsindikatoren für Domain-Controller, wie z. B. die CPU- und Speicherauslastung, überwachen können. Sie können auch Alarme konfigurieren und automatische Aktionen einleiten, um auf Zeiten hoher Auslastung zu reagieren. Sie können beispielsweise einen Alarm für eine CPU-Auslastung von Domain-Controllern über 70 Prozent konfigurieren und ein SNS-Thema erstellen, das Sie benachrichtigt, wenn dies der Fall ist. Sie können dieses SNS-Thema verwenden, um Automatisierungen zu initiieren, z. B. AWS Lambda Funktionen, um die Anzahl Ihrer Active Directory Domain-Controller zu erhöhen.

Weitere Informationen zur Überwachung Ihrer Domain-Controller finden Sie unter Ermitteln Sie, wann Domänencontroller mit CloudWatch Metriken hinzugefügt werden sollen.

Im Zusammenhang mit Amazon fallen Gebühren an CloudWatch. Weitere Informationen finden Sie unter CloudWatchAbrechnung und Kosten.

> **Important**
>
> Leistungskennzahlen für Domänencontroller mit CloudWatch sind in der Region Kanada West (Calgary) nicht verfügbar.

Leistungskennzahlen für Domänencontroller finden Sie unter CloudWatch

In der CloudWatch Amazon-Konsole werden die Metriken für einen bestimmten Service zunächst nach dem Namespace des Dienstes gruppiert. Sie können Metrikfilter hinzufügen, die diesem Namespace untergeordnet sind. Gehen Sie wie folgt vor, um den richtigen Namespace und die richtige untergeordnete Metrik zu finden, die für die Einrichtung von Messobjekten für AWS verwaltete Microsoft AD-Domänencontroller in erforderlich sind. CloudWatch

So finden Sie Messwerte für Domänencontroller in der Konsole CloudWatch

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie aus der Liste der Metriken den Namespace Directory Service und dann aus der Liste die Metrik AWS Managed Microsoft AD.

Anweisungen zum Einrichten von Domänencontroller-Metriken mithilfe der CloudWatch Konsole finden Sie unter So automatisieren Sie die AWS verwaltete Microsoft AD-Skalierung auf der Grundlage von Nutzungsmetriken im AWS Sicherheitsblog.

Ermitteln Sie, wann Domänencontroller mit CloudWatch Metriken hinzugefügt werden sollen

Der Lastenausgleich zwischen all Ihren Domänencontrollern ist wichtig für die Widerstandsfähigkeit und Leistung IhrerActive Directory. Um Ihnen zu helfen, die Leistung Ihrer Domänencontroller in AWS Managed Microsoft AD zu optimieren, empfehlen wir Ihnen, zunächst wichtige Messwerte zu überwachen, CloudWatch um eine Ausgangsbasis zu bilden. Während dieses Vorgangs analysieren Sie Ihre Auslastung Active Directory im Zeitverlauf, um Ihre durchschnittliche Auslastung und Active Directory Spitzenauslastung zu ermitteln. Nachdem Sie Ihren Ausgangswert ermittelt haben, können Sie diese Messwerte regelmäßig überwachen, um festzustellen, wann Sie einen Domänencontroller zu Ihrem hinzufügen solltenActive Directory.

Die folgenden Metriken sollten Sie regelmäßig überwachen. Eine vollständige Liste der verfügbaren Domänencontroller-Metriken CloudWatch finden Sie unterAWS Verwaltete Microsoft AD-Leistungsindikatoren.

- Domain-Controller-spezifische Metriken, wie z. B.:
  - Prozessor
  - Arbeitsspeicher
  - Logische Festplatte
  - Netzwerkschnittstelle
- AWS Verwaltete verzeichnisspezifische Metriken für Microsoft AD, z. B.:
  - LDAP-Suchen
  - Bindungen
  - DNS-Abfragen
  - Verzeichnis-Lesevorgänge
  - Verzeichnis-Schreibvorgänge

Anweisungen zum Einrichten von Domänencontroller-Metriken mithilfe der CloudWatch Konsole finden Sie unter So automatisieren Sie die AWS verwaltete Microsoft AD-Skalierung auf der Grundlage von Nutzungsmetriken im AWS Sicherheitsblog. Allgemeine Informationen zu Metriken in CloudWatch finden Sie unter Verwenden von CloudWatch Amazon-Metriken im CloudWatch Amazon-Benutzerhandbuch.

Allgemeine Informationen zur Planung von Domänencontrollern finden Sie unter Kapazitätsplanung für Active Directory Domänendienste auf der Microsoft-Website.

AWS Verwaltete Microsoft AD-Leistungsindikatoren

In der folgenden Tabelle sind alle Leistungsindikatoren aufgeführt, die in Amazon CloudWatch zur Nachverfolgung der Domain-Controller- und Verzeichnisleistung in AWS Managed Microsoft AD verfügbar sind.

Metrik-Kategorie	Metrikname
Datenbank ==> Instances (NTDSA)	Datenbank-Cache % Treffer
	Durchschnittliche Latenz von I/O-Datenbank-Lesevorgängen
	I/O-Datenbank Lesevorgänge/Sek
	Durchschnittliche Latenz von I/O-Protokollschreibvorgängen
DirectoryServices (NTDS)	LDAP-Bindungszeit
	DRA Ausstehende Replikationsvorgänge
	DRA Ausstehende Replikationssynchronisierungen
DNS	Rekursive Abfragen/Sek.
	Rekursive fehlgeschlagene Abfragen/Sek.
	Empfangene TCP-Abfragen/Sek.
	Gesamt empfangene DNS-Abfragen/Sek.
	Gesamt gesendete Antworten/Sek.
	Empfangene UDP-Abfragen/Sek.

Metrik-Kategorie	Metrikname
LogicalDisk	Durchschn. Länge der Datenträgerwartesc hlange
	% freier Speicherplatz
Arbeitsspeicher	% übertragene Bytes im Gebrauch
	Langfristige durchschnittliche Standby-Cache-Lebensdauer (S)
Netzwerkschnittstelle	Gesendete Byte/Sek.
	Empfangene Bytes/Sek.
	Aktuelle Bandbreite
NTDS	Geschätzte Verzögerung in der ATQ-Warte schlange
	ATQ-Anforderungslatenz
	Lesevorgänge pro Sekunde im DS-Verzeichnis
	DS-Verzeichnis-Suchen/Sek
	Schreibvorgänge im DS-Verzeichnis pro Sekunde
	LDAP-Clientsitzungen
	LDAP-Suchen/Sekunde
	Erfolgreiche LDAP-Bindungen/Sekunde
Prozessor	% Prozessorzeit
Systemweite Sicherheitsstatistiken	Kerberos-Authentifizierungen
	NTLM-Authentifizierungen

Multi-Region-Replikation

Die Multi-Region-Replikation kann verwendet werden, um Ihre Verzeichnisdaten in AWS Managed Microsoft AD automatisch über mehrere hinweg zu replizieren AWS-Regionen. Diese Replikation kann die Leistung von Benutzern und Anwendungen an verteilten geografischen Standorten verbessern. AWS Managed Microsoft AD verwendet die native Active-Directory-Replikation, um die Daten Ihres Verzeichnisses sicher in die neue Region zu replizieren.

Die Multi-Region-Replikation wird nur für die Enterprise Edition von AWS Managed Microsoft AD unterstützt.

In den meisten Regionen, in denen AWS Managed Microsoft AD verfügbar ist, können Sie die automatische Replikation mit mehreren Regionen verwenden.

Important

Die Multi-Region-Replikation ist in den folgenden Opt-In-Regionen nicht verfügbar:

- Afrika (Kapstadt) af-south-1
- Asien-Pazifik (Hongkong) ap-east-1
- Asien-Pazifik (Hyderabad) ap-south-2
- Asien-Pazifik (Jakarta) ap-southeast-3
- Asien-Pazifik (Melbourne) ap-southeast-4
- Kanada West (Calgary) ca-west-1
- Europa (Mailand) eu-south-1
- Europa (Spanien) eu-south-2
- Europa (Zürich) eu-central-2
- Israel (Tel Aviv) il-central-1
- Naher Osten (Bahrain) me-south-1
- Naher Osten (VAE) me-central-1

Weitere Informationen zu Opt-in-Regionen und deren Aktivierung finden Sie unter Angeben, welche AWS-Regionen Ihr Konto verwenden kann im AWS Account Management - Handbuch.

Vorteile

Bei der Multi-Region-Replikation in AWS Managed Microsoft AD verwenden Active-Directory-fähige Anwendungen das -Verzeichnis lokal für hohe Leistung und die Multi-Regions-Funktion für Ausfallsicherheit. Sie können die Multi-Region-Replikation mit Active-Directory-fähigen Anwendungen wie SharePoint und SQL Server Always On sowie mit AWS Services wie Amazon RDS für SQL Server und FSx für Windows File Server verwenden. Im Folgenden finden Sie weitere Vorteile der Multi-Region-Replikation.

- Damit können Sie eine einzelne Instance von AWS Managed Microsoft AD global, schnell bereitstellen und die hohe Belastung der Selbstverwaltung einer globalen Active-Directory-Infrastruktur beseitigen.
- Es erleichtert und kostengünstiger für Sie, Windows- und Linux-Workloads in mehreren AWS Regionen bereitzustellen und zu verwalten. Die automatisierte Multi-Region-Replikation ermöglicht eine optimale Leistung in Ihren globalen Active-Directory-fähigen Anwendungen. Alle Anwendungen, die in Windows- oder Linux-Instances bereitgestellt werden, verwenden AWS Managed Microsoft AD lokal in der Region, wodurch Antworten auf Benutzeranfragen aus der nächstgelegenen Region möglich sind.
- Das bietet Resilienz in mehreren Regionen. Managed Microsoft AD wird in der hochverfügbaren AWS AWS verwalteten Infrastruktur bereitgestellt und übernimmt automatisierte Softwareupdates, Überwachung, Wiederherstellung und die Sicherheit der zugrunde liegenden Active-Directory-Infrastruktur in allen -Regionen. So können Sie sich auf die Entwicklung Ihrer Anwendungen konzentrieren.

Themen

Globale und regionale Features

Wenn Sie Ihrem Verzeichnis mithilfe der Multi-Region-Replikation eine - AWS Region hinzufügen, AWS Directory Service erweitert den Umfang aller Funktionen, sodass sie regionsfähig werden.

Diese Features sind auf verschiedenen Registerkarten der Detailseite aufgeführt, die angezeigt wird, wenn Sie die ID eines Verzeichnisses in der AWS Directory Service -Konsole auswählen. Das bedeutet, dass alle Features auf der Grundlage der Region aktiviert, konfiguriert oder verwaltet werden, die Sie im Bereich Multi-Region-Replikation der Konsole auswählen. Änderungen, die Sie an Features in jeder Region vornehmen, werden entweder global oder pro Region angewendet.

Die Multi-Region-Replikation wird nur für die Enterprise Edition von AWS Managed Microsoft AD unterstützt.

Globale Features

Alle Änderungen, die Sie an globalen Features vornehmen, während die Primäre -Region ausgewählt ist, werden auf alle Regionen angewendet.

Sie können die Features, die global verwendet werden, auf der Seite mit den Verzeichnisdetails identifizieren, da neben ihnen der Eintrag Auf alle replizierten Regionen angewendet angezeigt wird. Wenn Sie in der Liste eine andere Region ausgewählt haben, bei der es sich nicht um die primäre Region handelt, können Sie alternativ die global verwendeten Features identifizieren, da dort die Option Von primärer Region geerbt angezeigt wird.

Regionale Funktionen

Alle Änderungen, die Sie an einem Feature in einer Zusätzliche Region vornehmen, werden nur auf diese Region angewendet.

Sie können die regionalen Features auf der Seite mit den Verzeichnisdetails identifizieren, da neben ihnen nicht die Option Auf alle replizierten Regionen angewendet oder Von primärer Region geerbt angezeigt wird.

Primäre Regionen im Vergleich zu zusätzlichen Regionen

Bei der Multi-Region-Replikation verwendet AWS Managed Microsoft AD die folgenden beiden Arten von Regionen, um zu unterscheiden, wie globale oder regionale Funktionen auf Ihr Verzeichnis angewendet werden sollen.

Primäre -Region

Die ursprüngliche Region, in der Sie Ihr Verzeichnis zuerst erstellt haben, wird als primäre Region bezeichnet. Von der primären Region aus können Sie nur globale Vorgänge auf Verzeichnisebene durchführen, wie das Erstellen von Vertrauensstellungen für Active Directory und das Aktualisieren des AD-Schemas.

Die primäre Region kann immer als die erste Region identifiziert werden, die im Abschnitt Multi-Region-Replikation ganz oben in der Liste angezeigt wird und auf – Primär endet. Beispiel: USA Ost (Nord-Virginia) – Primär.

Alle Änderungen, die Sie an Globale Features vornehmen, während die Primärregion ausgewählt ist, werden auf alle Regionen angewendet.

Sie können Regionen nur hinzufügen, solange die Primärregion ausgewählt ist. Weitere Informationen finden Sie unter Eine replizierte Region hinzufügen.

Zusätzliche Region

Alle Regionen, die Sie Ihrem Verzeichnis hinzugefügt haben, werden als zusätzliche Regionen bezeichnet.

Obwohl einige Features global für alle Regionen verwaltet werden können, werden andere für jede Region einzeln verwaltet. Um ein Feature für eine zusätzliche Region (nicht die primäre Region) zu verwalten, müssen Sie zuerst die zusätzliche Region aus der Liste im Abschnitt Multi-Region-Replikation auf der Seite mit den Verzeichnisdetails auswählen. Anschließend können Sie mit der Verwaltung des Features fortfahren.

Alle Änderungen, die Sie an Regionale Funktionen vornehmen, während eine zusätzliche Region ausgewählt ist, werden nur auf diese Region angewendet.

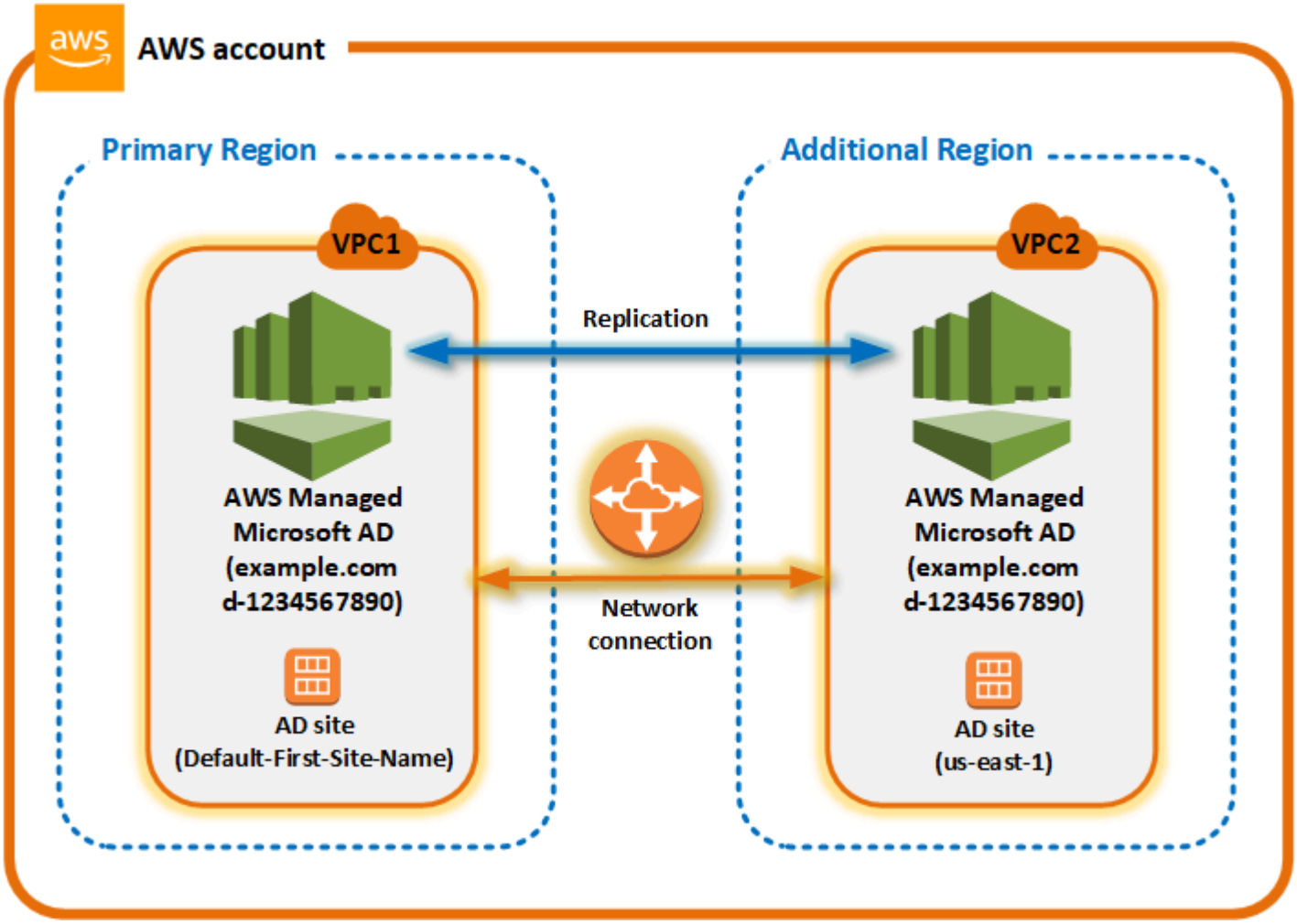
So funktioniert die Multi-Region-Replikation

Mit der Multi-Region-Replikationsfunktion eliminiert AWS Managed Microsoft AD die undifferenzierte, schwerwiegende Arbeit der Verwaltung einer globalen Active-Directory-Infrastruktur. Bei der Konfiguration AWS repliziert alle Kundenverzeichnisdaten, einschließlich Benutzer, Gruppen, Gruppenrichtlinien und Schema, über mehrere AWS Regionen hinweg.

Sobald eine neue Region hinzugefügt wurde, werden die folgenden Vorgänge automatisch ausgeführt, wie in der Abbildung dargestellt:

- AWS Managed Microsoft AD erstellt zwei Domain-Controller in der ausgewählten VPC und stellt sie in der neuen Region im selben AWS Konto bereit. Ihre Verzeichnis-ID (`directory_id`) bleibt in allen Regionen gleich. Sie können auf Wunsch später weitere Domain-Controller hinzufügen.
- AWS Managed Microsoft AD konfiguriert die Netzwerkverbindung zwischen der primären Region und der neuen Region.

- AWS Managed Microsoft AD erstellt einen neuen Active-Directory-Standort und gibt ihm denselben Namen wie die Region, z. B. us-east-1. Sie können ihn auch später mithilfe des Tools für Active-Directory-Standorte und -Services umbenennen.
- AWS Managed Microsoft AD repliziert alle Active-Directory-Objekte und -Konfigurationen in die neue Region, einschließlich Benutzer, Gruppen, Gruppenrichtlinien, Active-Directory-Vertrauensstellungen, Organisationseinheiten und Active-Directory-Schema. Active-Directory-Standortlinks sind für die Verwendung von Änderungsbenachrichtigungen konfiguriert. Wenn die Änderungsbenachrichtigung zwischen Standorten aktiviert ist, werden Änderungen mit derselben Häufigkeit an den Remotestandort weitergegeben, wie sie innerhalb des Quellstandorts weitergegeben werden. Dies gilt auch für Änderungen, die eine dringende Replikation rechtfertigen.
- Wenn dies die erste Region ist, die Sie hinzugefügt haben, macht AWS Managed Microsoft AD alle Funktionen auf mehrere Regionen aufmerksam. Weitere Informationen finden Sie unter Globale und regionale Features.



Active-Directory-Standorte

Die Multi-Region-Replikation unterstützt mehrere Active-Directory-Standorte (ein Active-Directory-Standort pro Region). Wenn eine neue Region hinzugefügt wird, erhält sie denselben Namen wie die Region, z. B. us-east-1. Sie können dies auch später mithilfe von Active-Directory-Standorten und -Services umbenennen.

AWS -Services

AWS -Services wie Amazon RDS für SQL Server und Amazon FSx stellen eine Verbindung zu den lokalen Instances des globalen Verzeichnisses her. Auf diese Weise können sich Ihre Benutzer einmal bei Active-Directory-fähigen Anwendungen anmelden, die in ausgeführt werden AWS , sowie bei AWS Services wie Amazon RDS für SQL Server in jeder - AWS Region. Dazu benötigen Benutzer Anmeldeinformationen von AWS Managed Microsoft AD oder On-Premises Active Directory, wenn Sie eine Vertrauensstellung zu Ihrem AWS Managed Microsoft AD haben.

Sie können die folgenden AWS Services mit der Multi-Region-Replikationsfunktion verwenden.

- Amazon EC2
- FSx für Windows File Server
- Amazon RDS für SQL Server
- Amazon RDS für Oracle
- Amazon RDS für MySQL
- Amazon RDS für PostgreSQL
- Amazon RDS für MariaDB
- Amazon Aurora für MySQL
- Amazon Aurora für PostgreSQL

Failover

Falls alle Domain-Controller in einer Region ausfallen, stellt AWS Managed Microsoft AD die Domain-Controller wieder her und repliziert die Verzeichnisdaten automatisch. In der Zwischenzeit bleiben die Domain-Controller in anderen Regionen betriebsbereit.

Eine replizierte Region hinzufügen

Wenn Sie eine Region mit der Multi-Region-Replikation Funktion hinzufügen, erstellt AWS Managed Microsoft AD zwei Domain-Controller in der ausgewählten AWS Region, Amazon Virtual

Private Cloud (VPC), und subnet. AWS Managed Microsoft AD erstellt auch die zugehörigen Sicherheitsgruppen, mit denen Windows-Workloads eine Verbindung zu Ihrem Verzeichnis in der neuen Region herstellen können. Außerdem werden diese Ressourcen mit demselben AWS Konto erstellt, in dem Ihr Verzeichnis bereits bereitgestellt ist. Dazu wählen Sie die Region aus, geben die VPC an und geben die Konfigurationen für die neue Region an.

Die Multi-Region-Replikation wird nur für die Enterprise Edition von AWS Managed Microsoft AD unterstützt.

Voraussetzungen

Bevor Sie mit den Schritten zum Hinzufügen einer neuen Replikationsregion fortfahren, empfehlen wir Ihnen, zunächst die folgenden erforderlichen Aufgaben zu überprüfen.

- Stellen Sie sicher, dass Sie über die erforderlichen AWS Identity and Access Management (IAM)-Berechtigungen, die Amazon-VPC-Einrichtung und die Subnetzeinrichtung in der neuen Region verfügen, in die Sie das Verzeichnis replizieren möchten.
- Wenn Sie Ihre vorhandenen On-Premises-Active-Directory-Anmeldeinformationen verwenden möchten, um auf Active-Directory-fähige Workloads in zuzugreifen und diese zu verwalten AWS, müssen Sie eine Active-Directory-Vertrauensstellung zwischen AWS Managed Microsoft AD und Ihrer On-Premises-AD-Infrastruktur erstellen. Weitere Informationen über Vertrauensstellungen finden Sie unter Connect zu Ihrer vorhandenen Active Directory-Infrastruktur her.
- Wenn zwischen Ihrem On-Premises-Active Directory eine Vertrauensstellung besteht und Sie eine replizierte Region hinzufügen möchten, müssen Sie überprüfen, ob Sie über die erforderliche Amazon-VPC- und Subnetzeinrichtung in der neuen Region verfügen, in die Sie das Verzeichnis replizieren möchten.

Eine Region hinzufügen

Gehen Sie wie folgt vor, um eine replizierte Region für Ihr Verzeichnis in AWS Managed Microsoft AD hinzuzufügen.

So fügen Sie eine replizierte Region hinzu

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite mit den Verzeichnisdetails unter Multi-Region-Replikation die primäre Region aus der Liste aus, und klicken Sie dann auf Region hinzufügen.

> **Note**
>
> Sie können Regionen nur hinzufügen, solange die primäre Region ausgewählt ist. Weitere Informationen finden Sie unter Primäre -Region.

4. Wählen Sie auf der Seite Region hinzufügen unter Region die Region, die Sie hinzufügen möchten, aus der Liste aus.
5. Wählen Sie unter VPC die VPC aus, die für diese Region verwendet werden soll.

> **Note**
>
> Diese VPC darf kein Classless Inter-Domain Routing (CIDR) haben, das sich mit einer VPC überschneidet, die von diesem Verzeichnis in einer anderen Region verwendet wird.

6. Wählen Sie unter Subnetze das Subnetz aus, das für diese Region verwendet werden soll.
7. Überprüfen Sie die Informationen unter Preise und wählen Sie dann Hinzufügen aus.
8. Wenn AWS Managed Microsoft AD den Bereitstellungsprozess des Domain-Controllers abgeschlossen hat, zeigt die Region den Status Aktiv an. Sie können diese Region nun nach Bedarf aktualisieren.

Nächste Schritte

Nachdem Sie Ihre neue Region hinzugefügt haben, sollten Sie die folgenden nächsten Schritte in Betracht ziehen:

- Stellen Sie bei Bedarf weitere Domain-Controller (bis zu 20) in Ihrer neuen Region bereit. Die Anzahl der Domain-Controller, wenn Sie eine neue Region hinzufügen, ist standardmäßig 2. Dies ist das Minimum, das für Fehlertoleranz und Hochverfügbarkeit erforderlich ist. Weitere Informationen finden Sie unter Zusätzliche Domain-Controller hinzufügen oder entfernen.
- Geben Sie Ihr Verzeichnis für mehrere AWS Konten pro Region frei. Konfigurationen für die Verzeichnisfreigabe werden nicht automatisch von der primären Region repliziert. Weitere Informationen finden Sie unter Freigeben Ihres Verzeichnisses.
- Aktivieren Sie die Protokollweiterleitung, um die Sicherheitsprotokolle Ihres Verzeichnisses mit Amazon CloudWatch Logs aus der neuen Region abzurufen. Wenn Sie die Protokollweiterleitung aktivieren, müssen Sie in jeder Region, in der Sie Ihr Verzeichnis repliziert haben, einen

Protokollgruppennamen angeben. Weitere Informationen finden Sie unter Protokollweiterleitung aktivieren.

- Aktivieren Sie die Überwachung des Amazon Simple Notification Service (Amazon SNS) für die neue Region, um den Status Ihres Verzeichnisses pro Region zu verfolgen. Weitere Informationen finden Sie unter Konfiguration von Verzeichnisstatusbenachrichtigungen mit Amazon SNS.

Eine replizierte Region löschen

Gehen Sie wie folgt vor, um eine Region für Ihr Verzeichnis in AWS Managed Microsoft AD zu löschen. Bevor Sie eine Region löschen, vergewissern Sie sich, dass sie keinen der folgenden Punkte aufweist:

- Autorisierte Anwendungen angehängt.
- Damit verknüpfte freigegebene Verzeichnisse.

So löschen Sie eine replizierte Region

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regionen und wählen Sie dann die Region aus, in der Ihr Verzeichnis gespeichert ist.
3. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
4. Wählen Sie auf der Seite Verzeichnisdetails unter Multi-Region-Replikation die Option Region löschen.
5. Überprüfen Sie im Dialogfeld Region löschen die Informationen und geben Sie dann zur Bestätigung den Namen der Region ein. Wählen Sie dann Löschen.

> **Note**
>
> Sie können die Region nicht aktualisieren, während sie gelöscht wird.

Freigeben Ihres Verzeichnisses

AWS Managed Microsoft AD ist eng in AWS Organizations integriert, um eine nahtlose Verzeichnisfreigabe über mehrere AWS-Konten hinweg zu ermöglichen. Sie können ein einzelnes Verzeichnis zur gemeinsamen Nutzung mit anderen vertrauenswürdigen AWS-Konten innerhalb der

gleichen Organisation oder mit anderen AWS-Konten außerhalb Ihrer Organisation freigeben. Sie können Ihr Verzeichnis auch freigeben, wenn Ihr AWS-Konto derzeit nicht Mitglied einer Organisation ist.

> **Note**
>
> AWS berechnet eine Zusatzgebühr für die Verzeichnisfreigabe. Weitere Informationen finden Sie auf der Seite Preise auf der AWS Directory Service-Website.

Durch die Verzeichnisfreigabe ist AWS Managed Microsoft AD eine kosteneffektivere Methode der Integration in Amazon EC2 für mehrere Konten und VPCs. Die Verzeichnisfreigabe ist in allen AWS-Regionen verfügbar, in denen AWS Managed Microsoft AD angeboten wird.

> **Note**
>
> In der AWS-Region China (Ningxia) ist dieses Feature nur verfügbar, wenn AWS Systems Manager (SSM) für die nahtlose Verbindung mit Ihren Amazon-EC2-Instances verwendet wird.

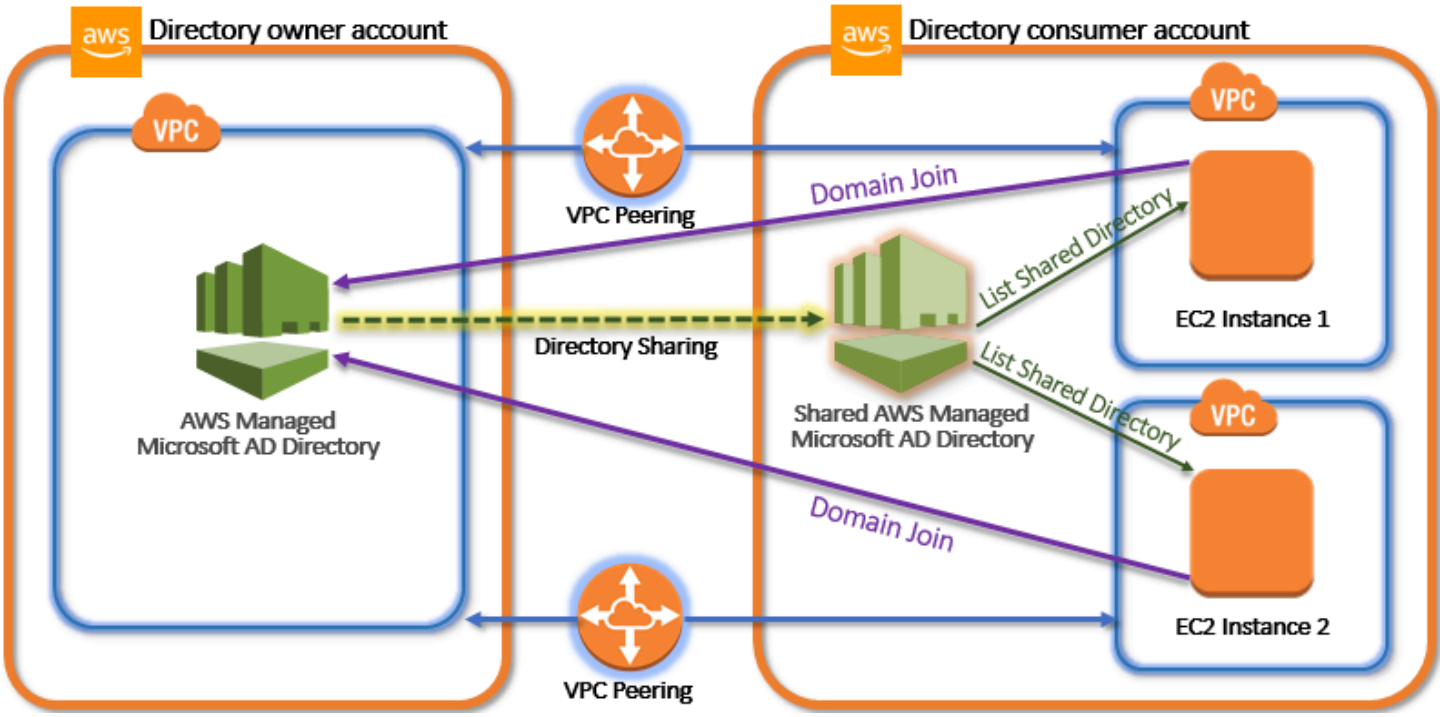
Weitere Informationen zur Verzeichnisfreigabe und Erhöhung der Reichweite Ihres Verzeichnisses in AWS Managed Microsoft AD über die Grenzen des AWS-Kontos hinaus finden Sie in den folgenden Themen.

Themen

- Schlüsselkonzepte der Verzeichnisfreigabe
- Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt
- Die Freigabe Ihres Verzeichnisses aufheben

Schlüsselkonzepte der Verzeichnisfreigabe

Sie profitieren mehr von dem Verzeichnisfreigabe-Feature, wenn Sie mit den folgenden wesentlichen Konzepten vertraut sind.



Konto des Verzeichniseigentümers

Ein Verzeichniseigentümer ist der Inhaber des AWS-Konto, dem das ursprüngliche Verzeichnis in Verzeichnisfreigabe-Beziehung gehört. Ein Administrator in diesem Konto initiiert den Verzeichnisfreigabe-Workflow durch Angabe der AWS-Konten, für die das Verzeichnis freigegeben werden soll. Verzeichniseigentümer können auf der Registerkarte Scale & Share (Skalieren und Freigeben) für ein bestimmtes Verzeichnis in der AWS Directory Service-Konsole einsehen, für wen sie ein Verzeichnis freigegeben haben.

Konto des Verzeichnisverbrauchers

In einer Verzeichnisfreigabe-Beziehung repräsentiert ein Verzeichnisverbraucher das AWS-Konto, für das der Verzeichniseigentümer das Verzeichnis freigegeben hat. Abhängig von der verwendeten Freigabemethode muss ein Administrator in diesem Konto möglicherweise zuerst eine vom Verzeichniseigentümer gesendete Einladung akzeptieren, bevor er mit der Verwendung des freigegebenen Verzeichnisses beginnen kann.

Der Verzeichnisfreigabevorgang erstellt im Konto des Verzeichniskonsumenten ein freigegebenes Verzeichnis. Dieses freigegebene Verzeichnis enthält die Metadaten, die der EC2-Instance eine nahtlose Verbindung mit der Domain ermöglichen, die das Originalverzeichnis im Verzeichniseigentümerkonto ausfindig macht. Jedes freigegebene Verzeichnis im Konto des

Verzeichniskonsumenten verfügt über eine eindeutige Kennung, die Shared directory ID (ID des freigegebenen Verzeichnisses).

Freigabemethoden

AWS Managed Microsoft AD bietet die folgenden beiden Verzeichnisfreigabemethoden:

- AWS Organizations – Diese Methode vereinfacht die Freigabe des Verzeichnisses innerhalb Ihrer Organisation, da Sie die Konten des Verzeichnisverbrauchers durchsuchen und validieren können. Zur Verwendung dieser Option muss für Ihre Organisation die Einstellung Alle Features aktiviert sein und Ihr Verzeichnis muss sich im Verwaltungskonto der Organisation befinden. Diese Freigabemethode vereinfacht Ihnen die Einrichtung, da die Verzeichniskonsumentenkonten Ihre Verzeichnisfreigabe-Anforderung nicht akzeptieren müssen. In der Konsole wird diese Methode als Freigabe dieses Verzeichnisses für AWS-Konten innerhalb Ihrer Organisation bezeichnet.
- Handshake – Diese Methode ermöglicht die Verzeichnisfreigabe, wenn Sie derzeit nicht AWS Organizations verwenden. Bei der Handshake-Methode muss das Verzeichniskonsumentenkonto die Verzeichnisfreigabe-Anfrage akzeptieren. In der Konsole wird diese Methode als Freigabe dieses Verzeichnisses für andere AWS-Konten bezeichnet.

Netzwerkkonnektivität

Netzwerkkonnektivität ist eine Voraussetzung für die Verwendung einer Verzeichnisfreigabebeziehung über AWS-Konten hinweg. AWS unterstützt viele Lösungen für die Verbindung Ihrer VPCs, darunter VPC-Peering, Transit Gateway und VPN. Lesen Sie zum Einstieg Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt.

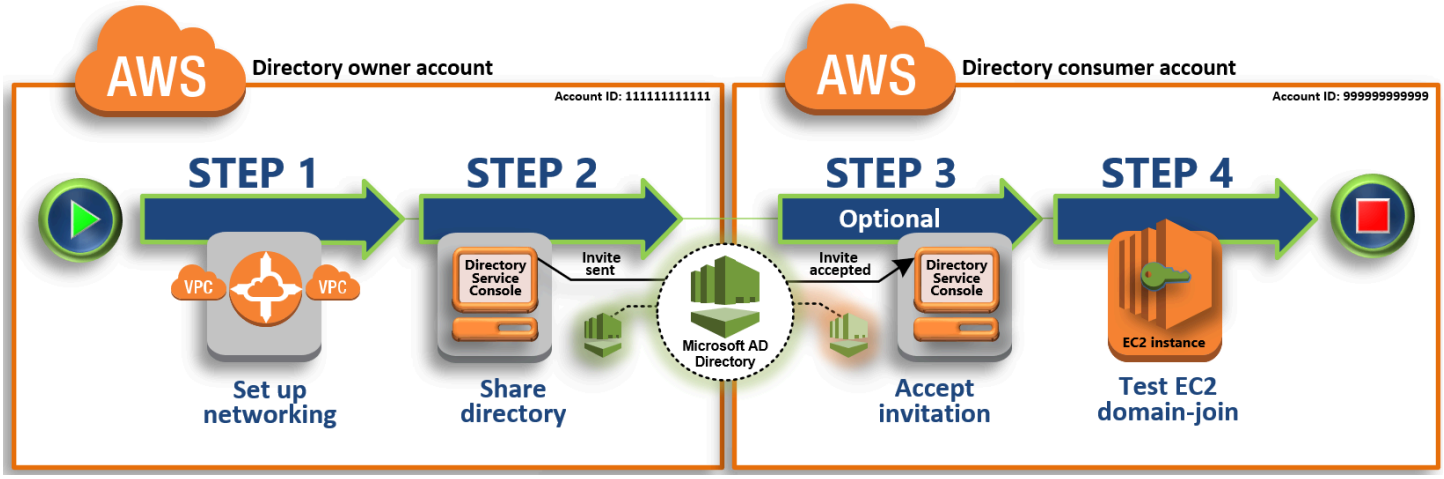
Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt

Dieses Tutorial zeigt Ihnen, wie Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnis (das Verzeichnisbesitzerkonto) mit einem anderen AWS-Konto (dem Verzeichnisverbraucherkonto) teilen können. Sobald die Netzwerkvoraussetzungen erfüllt sind, teilen Sie sich ein Verzeichnis für zwei Personen AWS-Konten. Danach erfahren Sie, wie Sie eine EC2-Instance nahtlos mit einer Domain in dem Verbraucherkonsumentenkonto verbinden.

Wir empfehlen, dass Sie zuerst die Schlüsselkonzepte der Verzeichnisfreigabe und den Inhalt der Anwendungsfälle durchgehen, bevor Sie mit dem Durcharbeiten dieses Tutorials beginnen. Weitere Informationen finden Sie unter Schlüsselkonzepte der Verzeichnisfreigabe.

Das Verfahren zur gemeinsamen Nutzung Ihres Verzeichnisses hängt davon ab, ob Sie das Verzeichnis für ein anderes AWS-Konto Mitglied derselben AWS Organisation oder für ein Konto außerhalb der AWS Organisation gemeinsam nutzen. Weitere Information über die Funktionsweise der Freigabe finden Sie unter Freigabemethoden.

Dieser Workflow umfasst vier grundlegende Schritte.



Schritt 1: Ihre Netzwerkumgebung einrichten

Im Verzeichniseigentümerkonto erfüllen Sie alle Netzwerkvoraussetzungen, die für den Verzeichnisfreigabevorgang erforderlich sind.

Schritt 2: Ihr Verzeichnis freigeben

Während Sie mit den Administrator-Anmeldeinformationen des Verzeichniseigentümers angemeldet sind, öffnen Sie die AWS Directory Service -Konsole und beginnen Sie mit dem Verzeichnisfreigabe-Workflow, der eine Einladung an das Konto des Verzeichniskonsumenten sendet.

Schritt 3: Einladung zum gemeinsamen Verzeichnis annehmen — optional

Während Sie mit den Anmeldeinformationen des Directory-Consumer-Administrators angemeldet sind, öffnen Sie die AWS Directory Service Konsole und akzeptieren die Einladung zur gemeinsamen Nutzung von Verzeichnissen.

Schritt 4: Die nahtlose Verbindung einer EC2-Instance für Windows Server mit einer Domain testen

Schließlich versuchen Sie als Verzeichniskonsumenten-Administrator, eine EC2-Instance mit Ihrer Domain zu verbinden, und überprüfen, ob der Vorgang erfolgreich war.

Weitere Ressourcen

- Anwendungsfall: Freigeben Ihres Verzeichnisses, um Amazon-EC2-Instances nahtlos über AWS-Konten hinweg mit einer Domain zu vereinzubinden
- AWS Blogartikel zum Thema Sicherheit: So verbinden Sie Amazon EC2 EC2-Instances von mehreren Konten und VPCs zu einem einzigen AWS verwalteten Microsoft AD-Verzeichnis

Schritt 1: Ihre Netzwerkumgebung einrichten

Bevor Sie mit den Schritten in diesem Tutorial beginnen, müssen Sie zuerst folgende Aufgaben ausführen:

- Erstellen Sie zwei neue zu AWS-Konten Testzwecken in derselben Region. Wenn Sie eine erstellen AWS-Konto, wird automatisch eine dedizierte Virtual Private Cloud (VPC) in jedem Konto erstellt. Notieren Sie sich die VPC-ID in jedem Konto. Sie benötigen sie zu einem späteren Zeitpunkt.
- Erstellen Sie mithilfe der Verfahren in diesem Schritt eine VPC-Peering-Verbindung zwischen den beiden VPCs in jedem Konto.

> **Note**
>
> Es gibt viele Möglichkeiten, Verzeichniseigentümer- und Verzeichniskonsumentenkonto-VPCs zu verbinden. In diesem Tutorial wird allerdings die VPC-Peering-Methode verwendet. Weitere VPC-Konnektivitätsoptionen finden Sie unter Netzwerkkonnektivität.

Eine VPC-Peering-Verbindung zwischen dem Konto des Verzeichniseigentümers und des Verzeichnisverbrauchers konfigurieren

Die von Ihnen erstellte VPC-Peering-Verbindung besteht zwischen der Verzeichniskonsumenten- und der Verzeichniseigentümer-VPC. Führen Sie die folgenden Schritte zum Konfigurieren einer VPC-Peering-Verbindung für Konnektivität mit dem Verzeichniskonsumentenkonto durch. Mit dieser Verbindung können Sie den Datenverkehr zwischen den beiden VPCs unter Verwendung privater IP-Adressen weiterleiten.

So erstellen Sie eine VPC-Peering-Verbindung zwischen dem Verzeichniseigentümer- und dem Verzeichniskonsumentenkonto

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Achten Sie darauf, sich bei dem Verzeichniseigentümerkonto als Benutzer mit Administrator-Anmeldeinformationen anzumelden.
2. Wählen Sie im Navigationsbereich Peering Connections aus. Wählen Sie dann Create Peering Connection (Peering-Verbindung erstellen).
3. Konfigurieren Sie die folgenden Informationen:
   - Peering connection name tag (Namens-Tag der Peering-Verbindung): Geben Sie einen Namen ein, der diese Verbindung mit der VPC im Verzeichniskonsumentenkonto eindeutig identifiziert.
   - VPC (Requester) (VPC (anfordernd)): Wählen Sie die VPC-ID für das Verzeichniseigentümerkonto aus.
   - Vergewissern Sie sich unter Select another VPC to peer with (Eine weitere VPC zum Verbinden per Peering auswählen) davon, dass My account (Mein Konto) und This region (Diese Region) ausgewählt sind.
   - VPC (Requester) (VPC (annehmend)): Wählen Sie die VPC-ID für das Verzeichniskonsumentenkonto aus.
4. Wählen Sie Create Peering Connection (Peering-Verbindung erstellen). Wählen Sie im Bestätigungsdialogfeld OK aus.

Da sich beide VPCs in derselben Region befinden, kann der Administrator des Verzeichniseigentümerkontos, der die VPC-Peering-Anfrage gesendet hat, die Peering-Anfrage auch im Namen des Verzeichniskonsumentenkontos akzeptieren.

So akzeptieren Sie die Peering-Anfrage im Namen des Verzeichniskonsumentenkontos

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Peering Connections aus.
3. Wählen Sie die ausstehende VPC-Peering-Verbindung aus. (Der Status muss noch akzeptiert werden.) Wählen Sie Actions (Aktionen), Accept Request (Anfrage akzeptieren).
4. Wählen Sie im Bestätigungsdialogfeld Yes, Accept aus. Wählen Sie im nächsten Bestätigungsdialogfeld Modify my route tables now (Meine Routing-Tabellen jetzt anpassen), um direkt zur Seite der Routing.Tabellen zu gelangen.

Wenn Ihre VPC-Peering-Verbindung nun aktiv ist, müssen Sie im Verzeichniseigentümerkonto einen Eintrag zu Ihrer VPC-Routing-Tabelle hinzufügen. Auf diese Weise wird die Weiterleitung des Datenverkehrs zur VPC im Verzeichniskonsumentenkonto ermöglicht.

So fügen Sie einen Eintrag zur VPC-Routingtabelle im Verzeichniseigentümerkonto hinzu

1. Wählen Sie im Bereich Routing-Tabellen der Amazon-VPC-Konsole die Routing-Tabelle für die Verzeichniseigentümer-VPC aus.
2. Wählen Sie auf der Registerkarte Routen Routen bearbeiten und wählen Sie dann Route hinzufügen.
3. Geben Sie in der Spalte Destination (Ziel) den CIDR-Block für die Verzeichniskonsumenten-VPC ein.
4. Geben Sie in der Spalte Target (Ziel) die VPC-Peering-Verbindungs-ID (wie z. B. **`pcx-123456789abcde000`**) für die Peering-Verbindung ein, die Sie zuvor im Verzeichniseigentümerkonto erstellt haben.
5. Wählen Sie Änderungen speichern aus.

So fügen Sie einen Eintrag zur VPC-Routingtabelle im Verzeichniskonsumentenkonto hinzu

1. Wählen Sie im Bereich Routing-Tabellen der Amazon-VPC-Konsole die Routing-Tabelle für die Verzeichnisverbraucher-VPC aus.
2. Wählen Sie auf der Registerkarte Routen Routen bearbeiten und wählen Sie dann Route hinzufügen.
3. Geben Sie in der Spalte Destination (Ziel) den CIDR-Block für die Verzeichniseigentümer-VPC ein.
4. Geben Sie in der Spalte Target (Ziel) die VPC-Peering-Verbindungs-ID (wie z. B. **`pcx-123456789abcde001`**) für die Peering-Verbindung ein, die Sie zuvor im Verzeichniskonsumentenkonto erstellt haben.
5. Wählen Sie Änderungen speichern aus.

Konfigurieren Sie die Sicherheitsgruppe Ihrer Verzeichniskonsumenten-VPCs unbedingt so, dass ausgehender Datenverkehr ermöglicht wird. Fügen Sie dazu die Active Directory-Protokolle und -Ports zur Regeltabelle für ausgehenden Datenverkehr hinzu. Weitere Informationen finden Sie unter Sicherheitsgruppen für Ihre VPC und Voraussetzungen für AWS Managed Microsoft AD.

Nächster Schritt

Schritt 2: Ihr Verzeichnis freigeben

Schritt 2: Ihr Verzeichnis freigeben

Verfahren Sie wie folgt, um über das Verzeichniseigentümerkonto mit dem Workflow für die Verzeichnisfreigabe zu beginnen.

> **Note**
>
> Die gemeinsame Nutzung von Verzeichnissen ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.

So geben Sie Ihr Verzeichnis über das Verzeichniseigentümerkonto frei

1. Melden Sie sich AWS Management Console mit Administratoranmeldedaten im Konto des Verzeichnisbesitzers an und öffnen Sie die AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie die Verzeichnis-ID des AWS verwalteten Microsoft AD-Verzeichnisses, das Sie teilen möchten.
4. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Ihr Verzeichnis freigeben möchten, und wählen Sie dann die Registerkarte Skalieren und Freigeben. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Skalieren und Freigeben.
5. Wählen Sie im Bereich Shared directories (Freigegebene Verzeichnisse) die Option Actions (Aktionen) and danach Create new shared directory (Neues freigegebenes Verzeichnis erstellen).
6. Wählen Sie auf der Seite Wählen Sie aus, mit welcher AWS-Konten Datei Sie teilen möchten, je nach Ihren Geschäftsanforderungen eine der folgenden Freigabemethoden aus:

a. Dieses Verzeichnis AWS-Konten innerhalb Ihrer Organisation teilen — Mit dieser Option können Sie aus einer Liste, in der AWS-Konten alle Informationen AWS-Konten innerhalb Ihrer AWS Organisation angezeigt werden, das Verzeichnis auswählen, mit dem Sie Ihr Verzeichnis teilen möchten. Sie müssen den vertrauenswürdigen Zugriff mit aktivieren, AWS Directory Service bevor Sie ein Verzeichnis teilen können. Weitere Informationen finden Sie unter So aktivieren oder deaktivieren Sie den vertrauenswürdigen Zugriff.

> **Note**
>
> Zur Verwendung dieser Option muss für Ihre Organisation die Einstellung Alle Features aktiviert sein und Ihr Verzeichnis muss sich im Verwaltungskonto der Organisation befinden.

   i. Wählen Sie unter AWS-Konten In Ihrer Organisation das Verzeichnis aus, für AWS-Konten das Sie das Verzeichnis gemeinsam nutzen möchten, und klicken Sie auf Hinzufügen.

   ii. Überprüfen Sie die Preisdetails und klicken Sie auf Share (Freigeben).

   iii. Fahren Sie mit Schritt 4 in dieser Anleitung fort. Da AWS-Konten sich alle in derselben Organisation befinden, müssen Sie Schritt 3 nicht ausführen.

b. Dieses Verzeichnis mit anderen teilen AWS-Konten — Mit dieser Option können Sie ein Verzeichnis mit Konten innerhalb oder außerhalb Ihrer AWS Organisation teilen. Sie können diese Option auch verwenden, wenn Ihr Verzeichnis nicht Mitglied einer AWS Organisation ist und Sie es mit einer anderen teilen möchten AWS-Konto.

   i. Geben Sie unter AWS-Konto -ID(s) alle die AWS-Konto -IDs ein, für die Sie das Verzeichnis freigeben möchten. Klicken Sie dann auf Hinzufügen.

   ii. Geben Sie unter Einen Hinweis senden eine Nachricht an den Administrator in dem anderen AWS-Konto ein.

   iii. Überprüfen Sie die Preisdetails und klicken Sie auf Share (Freigeben).

   iv. Fahren Sie mit Schritt 3 fort.

Nächster Schritt

Schritt 3: Einladung zum gemeinsamen Verzeichnis annehmen — optional

Schritt 3: Einladung zum gemeinsamen Verzeichnis annehmen — optional

Wenn Sie im vorherigen Verfahren die Option Freigabe dieses Verzeichnisses für andere AWS-Konten (Handshake-Methode) ausgewählt haben, sollten Sie den Workflow der Verzeichnisfreigabe mit diesem Verfahren abschließen. Wenn Sie die Option Dieses Verzeichnis AWS-Konten innerhalb Ihrer Organisation teilen ausgewählt haben, überspringen Sie diesen Schritt und fahren Sie mit Schritt 4 fort.

So akzeptieren Sie die Einladung für die Verzeichnisfreigabe

1. Melden Sie sich AWS Management Console mit Administratoranmeldedaten im Verzeichnis an und öffnen Sie die AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie im Navigationsbereich Directories shared with me (Mit mir geteilte Verzeichnisse).
3. Wählen Sie in der Spalte Shared directory ID (ID des freigegebenen Verzeichnisses) die Verzeichnis-ID aus, die sich im Zustand Pending acceptance (Annahme ausstehend) befindet.
4. Wählen Sie auf der Seite Shared directory details (Weitere Informationen zu dem freigegebenen Verzeichnis) die Option Review (Überprüfen) aus.
5. Überprüfen Sie im Dialogfeld Pending shared directory invitation (Ausstehende Einladung für ein freigegebenes Verzeichnis) Hinweis, Verzeichniseigentümer-Details und Informationen zu den Preisen. Wenn Sie damit einverstanden sind, wählen Sie Accept (Annehmen), um das Verzeichnis zu verwenden.

Nächster Schritt

Schritt 4: Die nahtlose Verbindung einer EC2-Instance für Windows Server mit einer Domain testen

Schritt 4: Die nahtlose Verbindung einer EC2-Instance für Windows Server mit einer Domain testen

Sie können eine der beiden folgenden Methoden verwenden, um die nahtlose Verbindung einer EC2-Instance mit eine Domain zu testen.

Methode 1: Domainverbindung mit der Amazon-EC2-Konsole testen

Verwenden Sie diese Schritte im Konto des Verzeichnisverbrauchers.

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie in der Navigationsleiste dasselbe Verzeichnis AWS-Region wie das bestehende Verzeichnis aus.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.
4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Windows-EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.
6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) Windows im Schnellstartbereich aus. Sie können das Windows Amazon Machine Image (AMI) in der Dropdown-Liste Amazon Machine Image (AMI) ändern.
7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen.

    a. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen.

    b. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels.

    c. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk.

    d. Wählen Sie Schlüsselpaar erstellen aus.

    e. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

    > **Important**
    >
    > Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.

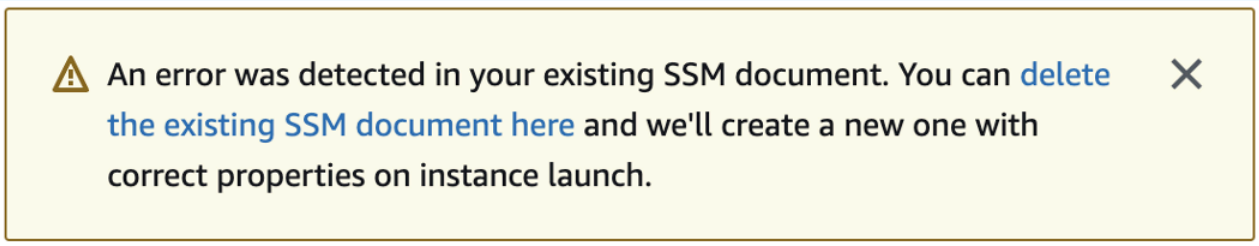
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.

11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

    Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.

12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>
>
> Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:
>
> - Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
> - Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den

richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Für das IAM-Instance-Profil können Sie ein vorhandenes IAM-Instance-Profil auswählen oder ein neues erstellen. Wählen Sie aus der Dropdownliste für das IAM-Instanzprofil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM DirectoryServiceAccess angehängt sind. Um ein neues zu erstellen, wählen Sie den Link Neues IAM-Profil erstellen und gehen Sie dann wie folgt vor:

    1. Wählen Sie Rolle erstellen aus.
    2. Wählen Sie unter Vertrauenswürdige Entität auswählen die Option AWS -Service aus.
    3. Wählen Sie unter Use case (Anwendungsfall) die Option EC2 aus.
    4. Wählen Sie in der Liste der Richtlinien unter Berechtigungen hinzufügen die Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM aus. DirectoryServiceAccess Geben Sie im Suchfeld **`SSM`** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess stellt die Berechtigungen zum Hinzufügen von Instances zu einer Gruppe bereit, die von verwaltet wird. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager -Benutzerhandbuch.

    5. Geben Sie auf der Seite Benennen, überprüfen und erstellen einen Rollennamen ein. Sie benötigen diesen Rollennamen, um mit der EC2-Instance verbunden zu werden.
    6. (Optional) Sie können im Feld Beschreibung eine Beschreibung des IAM-Instance-Profils angeben.
    7. Wählen Sie Rolle erstellen aus.
    8. Kehren Sie zur Seite Eine Instance starten zurück und wählen Sie das Aktualisierungssymbol neben dem IAM-Instance-Profil. Ihr neues IAM-Instance-Profil sollte in der Dropdown-Liste IAM-Instance-Profil sichtbar sein. Wählen Sie das neue Profil und belassen Sie die restlichen Einstellungen auf den Standardwerten.

16. Wählen Sie Launch Instance (Instance starten) aus.

Methode 2: Testen Sie den Domänenbeitritt mit AWS Systems Manager

Verwenden Sie diese Schritte im Konto des Verzeichnisverbrauchers. Um diesen Vorgang abzuschließen, benötigen Sie einige Informationen über das Besitzerkonto des Verzeichnisses, wie die Verzeichnis-ID, den Verzeichnisnamen und die DNS-IP-Adressen.

Voraussetzungen

- Einrichtung AWS Systems Manager.
  - Weitere Informationen zu Systems Manager finden Sie unter Allgemeine Einrichtung für AWS Systems Manager.
- Instances, denen Sie der AWS verwalteten Microsoft Active Directory-Domäne beitreten möchten, müssen über eine zugeordnete IAM-Rolle verfügen, die die von AmazonSSM ManagedInstanceCore und DirectoryServiceAccessAmazonSSM verwalteten Richtlinien enthält.
  - Weitere Informationen über diese verwalteten Richtlinien und andere Richtlinien, die Sie an ein IAM-Instance-Profil für Systems Manager anhängen können, finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager im AWS Systems Manager -Benutzerhandbuch. Informationen über verwaltete Richtlinien finden Sie unter AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Weitere Informationen zur Verwendung von Systems Manager zum Hinzufügen von EC2-Instances zu einer AWS verwalteten Microsoft Active Directory-Domäne finden Sie unter Wie verwende ich, AWS Systems Manager um eine laufende EC2-Windows-Instance mit meiner AWS Verzeichnisdienstdomäne zu verbinden? .

1. Öffnen Sie die AWS Systems Manager Konsole unterhttps://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich unter Knotenverwaltung die Option Befehl ausführen.
3. Wählen Sie Run Command (Befehl ausführen) aus.
4. Suchen Sie auf der Seite Befehl ausführen nach `AWS-JoinDirectoryServiceDomain`. Wenn es in den Suchergebnissen angezeigt wird, wählen Sie die Option `AWS-JoinDirectoryServiceDomain`.
5. Scrollen Sie nach unten bis zum Abschnitt Command Parameters (Befehlsparameter). Sie müssen die folgenden Parameter angeben:

> **Note**
>
> Sie können die Verzeichnis-ID, den Verzeichnisnamen und die DNS-IP-Adressen finden, indem Sie zur AWS Directory Service Konsole zurückkehren, mit mir gemeinsam genutzte Verzeichnisse und dann Ihr Verzeichnis auswählen. Ihre Verzeichnis-ID finden Sie im Abschnitt Geteilte Verzeichnisdetails. Sie finden die Werte für den Verzeichnisnamen und die DNS-IP-Adressen im Abschnitt Details zum Besitzerverzeichnis.

- Geben Sie als Verzeichnis-ID den Namen des AWS verwalteten Microsoft Active Directory ein.
- Geben Sie unter Verzeichnisname den Namen des AWS Managed Microsoft Active Directory (für das Konto des Verzeichnisinhabers) ein.
- Geben Sie für DNS-IP-Adressen die IP-Adressen der DNS-Server im AWS verwalteten Microsoft Active Directory (für das Verzeichnisbesitzerkonto) ein.

6. Wählen Sie für Ziele die Option Instances manuell auswählen und wählen Sie dann die Instances aus, die Sie mit der Domain verbinden möchten.
7. Lassen Sie den Rest des Formulars auf die Standardwerte eingestellt, blättern Sie auf der Seite nach unten und wählen Sie dann Run (Ausführen).
8. Der Befehlsstatus ändert sich von Ausstehend in Erfolgreich, sobald die Instances erfolgreich mit der Domain verbunden wurden. Sie können die Befehlsausgabe anzeigen, indem Sie die Instance-ID der Instance, die mit der Domain verbunden wurde, und die Option Ausgabe anzeigen auswählen.

Nach Abschluss von einem der Schritte sollten Sie jetzt mit der EC2-Instance der Domain beitreten können. Sobald Sie dies getan haben, können Sie sich mit einem Remote Desktop Protocol (RDP) - Client mit den Anmeldeinformationen Ihres AWS verwalteten Microsoft AD-Benutzerkontos bei Ihrer Instanz anmelden.

Die Freigabe Ihres Verzeichnisses aufheben

Gehen Sie wie folgt vor, um die Freigabe eines Verzeichnisses in AWS Managed Microsoft AD aufzuheben.

So heben Sie die Freigabe Ihres Verzeichnisses auf

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole unter Active Directory die Option Verzeichnisse.
2. Wählen Sie die Verzeichnis-ID des Verzeichnisses in AWS Managed Microsoft AD aus, dessen Freigabe Sie aufheben möchten..
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie die Freigabe eines Verzeichnisses aufheben möchten, und wählen Sie dann die Registerkarte Skalieren und Freigeben. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Skalieren und Freigeben.
4. Wählen Sie im Bereich Shared directories (Freigegebene Verzeichnisse) das freigegebene Verzeichnis aus, dessen Freigabe Sie aufheben möchten. Wählen Sie dann Actions (Aktionen) und Unshare (Freigabe aufheben).
5. Wählen Sie im Dialogfeld Unshare directory (Aufheben der Freigabe für ein Verzeichnis) die Option Unshare (Freigabe aufheben).

Weitere Ressourcen

- Anwendungsfall: Freigeben Ihres Verzeichnisses, um Amazon-EC2-Instances nahtlos über AWS-Konten hinweg mit einer Domain zu verbinden
- Blog-Artikel zur AWS-Sicherheit: Wie Sie Amazon-EC2-Instances aus mehreren Konten und VPCs mit einem einzelnen AWS Managed Microsoft AD Directory verbinden
- Kontenübergreifendes Verbinden Ihrer Amazon-RDS-DB-Instances mit einer einzelnen freigegebenen Domain

Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory

Sie können eine Amazon EC2 EC2-Instance nahtlos mit Ihrer Active Directory Domain verbinden, wenn die Instance gestartet wird. Weitere Informationen finden Sie unter Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory. Mit

Automation können Sie auch direkt von der AWS Directory Service Konsole aus eine EC2-Instance starten und sie mit AWS Systems Manager einer Active Directory Domain verbinden.

Wenn Sie eine EC2-Instance manuell mit Ihrer Active Directory Domain verbinden müssen, müssen Sie die Instance in der richtigen Region und Sicherheitsgruppe oder dem richtigen Subnetz starten und dann die Instance mit der Domain verbinden.

Um eine Remote-Verbindung zu diesen Instances herstellen zu können, benötigen Sie eine IP-Verbindung zu den Instances von dem Netzwerk aus, von dem aus Sie sich verbinden. In den meisten Fällen muss hierfür Ihrer VPC ein Internet-Gateway zugeordnet sein und die Instance muss eine öffentliche IP-Adresse haben.

Themen

Starten Sie die Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory

Mit diesem Verfahren wird eine Amazon EC2 Windows EC2-Verzeichnisverwaltungsinstanz gestartet, die AWS Systems Manager Automation zur Verwaltung Ihrer Verzeichnisse AWS Management

Console verwendet. Sie können dies auch erreichen, indem Sie die Option Automation AWS-CreateDS direkt ManagementInstance in der AWS Systems Manager Automation-Konsole ausführen.

Voraussetzungen

Um eine EC2-Instance für die Verzeichnisverwaltung von der Konsole aus zu starten, müssen Sie die folgenden Berechtigungen in Ihrem Konto aktiviert haben.

- `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`

Um eine EC2-Instanz für die Verzeichnisverwaltung in der AWS Management Console

1. Melden Sie sich an der AWS Directory Service -Konsole an.
2. Wählen Sie unter Active Directory die Option Verzeichnisse aus.
3. Wählen Sie die Verzeichnis-ID des Verzeichnisses, in dem Sie eine EC2-Instance für die Verzeichnisverwaltung starten möchten.
4. Wählen Sie auf der Verzeichnisseite in der oberen rechten Ecke Aktionen aus.
5. Wählen Sie in der Dropdownliste Aktionen die Option EC2-Instance für die Verzeichnisverwaltung starten aus.
6. Füllen Sie auf der Seite EC2-Instance für die Verzeichnisverwaltung starten unter Eingabeparameter alle Felder aus.

    a. (Optional) Sie können ein key pair für die Instance angeben. Wählen Sie aus der Dropdownliste Schlüsselpaarname — optional ein key pair aus.

    b. (Optional) Wählen Sie den AWS CLI Befehl View, um ein Beispiel zu sehen, das Sie in der AWS CLI zum Ausführen dieser Automatisierung verwenden.
7. Wählen Sie Absenden aus.

8. Sie kehren zur Verzeichnisseite zurück. Am oberen Bildschirmrand wird eine grüne Blinkleiste angezeigt, die darauf hinweist, dass Sie den Start erfolgreich eingeleitet haben.

Um die EC2-Instanz für die Verzeichnisverwaltung anzuzeigen

Wenn Sie keine EC2-Instances für ein Verzeichnis gestartet haben, wird ein Bindestrich (-) unter EC2-Instance für die Verzeichnisverwaltung angezeigt.

1. Wählen Sie unter Active Directory die Option Verzeichnisse und dann das Verzeichnis aus, das Sie anzeigen möchten.
2. Wählen Sie unter Verzeichnisdetails unter Verzeichnisverwaltung EC2-Instance eine oder alle Ihre Instances aus, die Sie anzeigen möchten.
3. Wenn Sie eine Instance auswählen, werden Sie zur EC2-Seite MIt Instance verbinden weitergeleitet, um einen Remote-Desktop mit Ihrer Instance zu verbinden.

Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory

Dieses Verfahren verbindet eine Amazon EC2 Windows EC2-Instance nahtlos mit Ihrem AWS Managed Microsoft AD. Wenn Sie einen nahtlosen Domänenbeitritt über mehrere Domänen hinweg durchführen müssen AWS-Konten, finden Sie weitere Informationen unterTutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt. Mehr Informationen zu Amazon EC2 finden Sie unter Was ist Amazon EC2?.

Um einer Amazon EC2 Windows EC2-Instance nahtlos beizutreten

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste dasselbe Verzeichnis AWS-Region wie das bestehende Verzeichnis aus.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.
4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Windows-EC2-Instance verwenden möchten.

5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.
6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) Windows im Schnellstartbereich aus. Sie können das Windows Amazon Machine Image (AMI) in der Dropdown-Liste Amazon Machine Image (AMI) ändern.
7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen.

   a. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen.

   b. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels.

   c. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk.

   d. Wählen Sie Schlüsselpaar erstellen aus.

   e. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

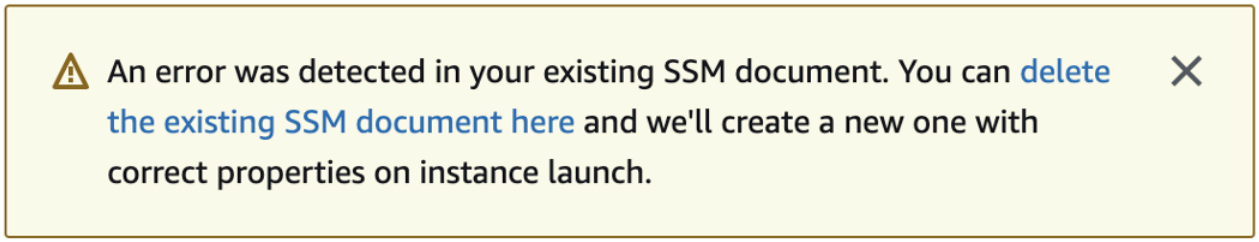
   > **Important**
   >
   > Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.

12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>
>
> Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:
>
> - Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
> - Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Für das IAM-Instance-Profil können Sie ein vorhandenes IAM-Instance-Profil auswählen oder ein neues erstellen. Wählen Sie aus der Dropdownliste für das IAM-Instanzprofil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM DirectoryServiceAccess angehängt sind. Um ein neues zu erstellen, wählen Sie den Link Neues IAM-Profil erstellen und gehen Sie dann wie folgt vor:

1. Wählen Sie Rolle erstellen aus.
2. Wählen Sie unter Vertrauenswürdige Entität auswählen die Option AWS -Service aus.
3. Wählen Sie unter Use case (Anwendungsfall) die Option EC2 aus.
4. Wählen Sie in der Liste der Richtlinien unter Berechtigungen hinzufügen die Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM aus. DirectoryServiceAccess Geben Sie im Suchfeld **SSM** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess stellt die Berechtigungen zum Hinzufügen von Instances zu einer Gruppe bereit, die von verwaltet wird. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager -Benutzerhandbuch.

5. Geben Sie auf der Seite Benennen, überprüfen und erstellen einen Rollennamen ein. Sie benötigen diesen Rollennamen, um mit der EC2-Instance verbunden zu werden.
6. (Optional) Sie können im Feld Beschreibung eine Beschreibung des IAM-Instance-Profils angeben.
7. Wählen Sie Rolle erstellen aus.
8. Kehren Sie zur Seite Eine Instance starten zurück und wählen Sie das Aktualisierungssymbol neben dem IAM-Instance-Profil. Ihr neues IAM-Instance-Profil sollte in der Dropdown-Liste IAM-Instance-Profil sichtbar sein. Wählen Sie das neue Profil und belassen Sie die restlichen Einstellungen auf den Standardwerten.

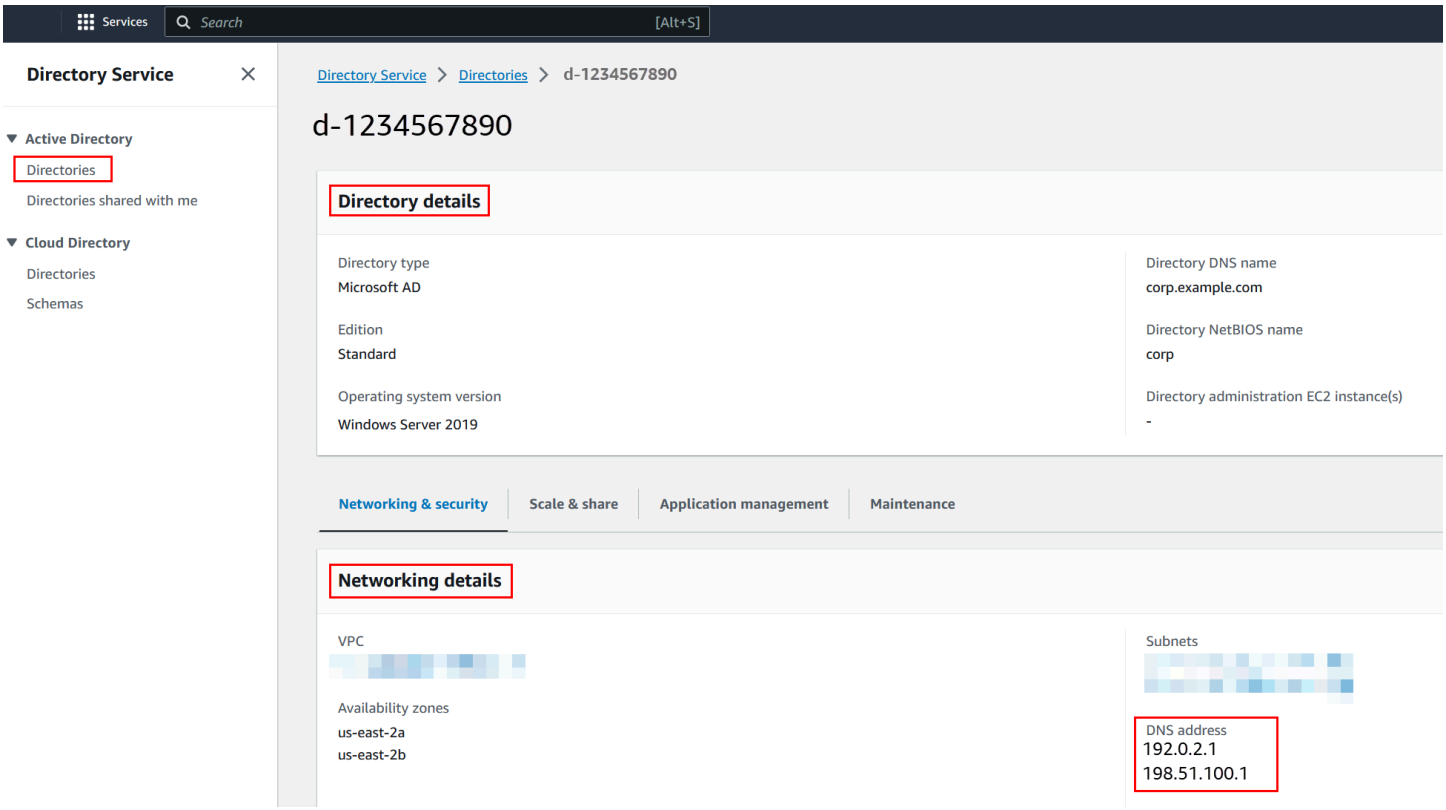
16. Wählen Sie Launch Instance (Instance starten) aus.

Manuelles Verbinden einer Amazon EC2 Windows EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory

Um eine bestehende Amazon EC2 Windows EC2-Instance manuell mit einem AWS Managed Microsoft AD zu verbindenActive Directory, muss die Instance mit den unter angegebenen

Parametern gestartet werden. Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory

Sie benötigen die IP-Adressen der AWS verwalteten Microsoft AD DNS-Server. Diese Informationen finden Sie in den Abschnitten Verzeichnisservices > Verzeichnisse > dem Verzeichnis-ID-Link für Ihr Verzeichnis > Verzeichnisdetails und Netzwerk und Sicherheit.



So verbinden Sie eine Windows-Instanz mit einem AWS verwalteten Microsoft AD Active Directory

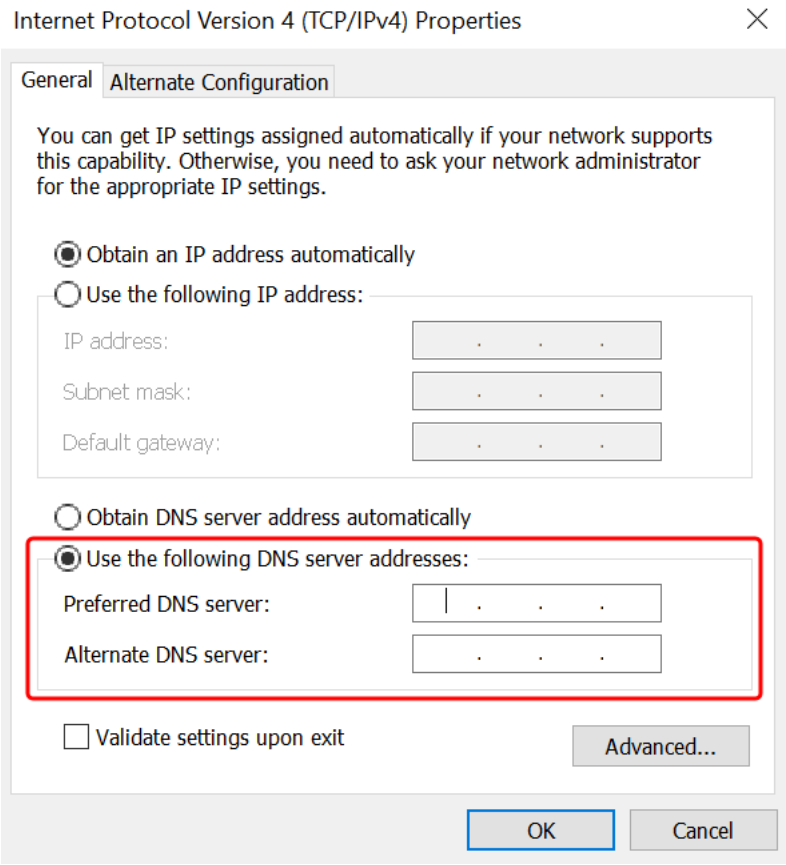
1. Verbinden Sie die Instance mithilfe eines beliebigen Remote Desktop Protocol-Clients.
2. Öffnen Sie in der Instance das Dialogfeld mit den Eigenschaften für TCP/IPv4.
   a. Öffnen Sie Network Connections.

> **Tip**
>
> Öffnen Sie Network Connections direkt, indem Sie folgenden Befehl über die Befehlszeile der Instance ausführen.
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

b. Öffnen Sie für eine beliebige aktivierte Netzwerkverbindung per Rechtsklick das Kontextmenü und wählen Sie dann Properties aus.

c. Öffnen Sie im Dialogfeld für die Verbindungseigenschaften (per Doppelklick) Internet Protocol Version 4.

3. Wählen Sie Folgende DNS-Serveradressen verwenden aus, ändern Sie die bevorzugten DNS-Server - und alternativen DNS-Serveradressen in die IP-Adressen Ihrer von AWS Managed Microsoft AD bereitgestellten DNS-Server und wählen Sie OK.



4. Öffnen Sie das Dialogfeld System Properties für die Instance, wählen Sie die Registerkarte Computer Name und wählen Sie Change.

> **Tip**
>
> Öffnen Sie das Dialogfeld System Properties direkt, indem Sie folgenden Befehl über die Befehlszeile der Instance ausführen.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Wählen Sie im Feld Mitglied von die Option Domäne aus, geben Sie den vollqualifizierten Namen Ihres AWS verwalteten Microsoft AD Active Directory ein, und klicken Sie auf OK.
6. Wenn Sie zur Eingabe des Namens und des Kennworts für den Domänenadministrator aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Kontos ein, das über Domänenbeitrittsrechte verfügt. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

   > **Note**
   >
   > Sie können entweder den vollqualifizierten Namen Ihrer Domäne oder den NetBIOS-Namen, gefolgt von einem umgekehrten Schrägstrich (\) und dann den Benutzernamen eingeben. Der Benutzername wäre Admin. Zum Beispiel **`corp.example.com\admin`** oder **`corp\admin`**.

7. Nachdem Sie in der Domain willkommen geheißen wurden, starten Sie die Instance neu, damit die Änderungen übernommen werden.

Nachdem Ihre Instanz der AWS verwalteten Microsoft AD Active Directory-Domäne hinzugefügt wurde, können Sie sich remote bei dieser Instanz anmelden und Dienstprogramme zur Verwaltung des Verzeichnisses installieren, z. B. zum Hinzufügen von Benutzern und Gruppen. Die Active Directory-Verwaltungstools können verwendet werden, um Benutzer und Gruppen zu erstellen. Weitere Informationen finden Sie unter Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD.

> **Note**
>
> Sie können Amazon Route 53 auch verwenden, um DNS-Abfragen zu verarbeiten, anstatt die DNS-Adressen auf Ihren Amazon EC2 EC2-Instances manuell zu ändern. Weitere Informationen finden Sie unter Integrieren der DNS-Auflösung Ihres Verzeichnisdienstes in Ihr Netzwerk Amazon Route 53 Resolver und Weiterleiten ausgehender DNS-Abfragen an Ihr Netzwerk.

Fügen Sie eine Amazon EC2 EC2-Linux-Instance nahtlos zu Ihrem AWS verwalteten Microsoft AD Active Directory hinzu

Durch dieses Verfahren wird eine Amazon EC2 EC2-Linux-Instance nahtlos mit Ihrem AWS verwalteten Microsoft AD Active Directory verbunden. Wenn Sie einen nahtlosen Domänenbeitritt über mehrere AWS Konten hinweg durchführen müssen, können Sie optional die gemeinsame Nutzung von Verzeichnissen aktivieren.

Die folgenden Linux-Instance-Distributionen und -Versionen werden unterstützt:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-Bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-Bit x86)
- Ubuntu Server 18.04 LTS und Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Versionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 unterstützen das Feature der nahtlosen Domainverbindung nicht.

Eine Demonstration des Prozesses zum nahtlosen Hinzufügen einer Linux-Instanz zu Ihrem AWS verwalteten Microsoft AD Active Directory finden Sie im folgenden YouTube Video.

Demo für nahtlose AD-Domainverbindung von Amazon EC2 für Linux

Voraussetzungen

Bevor Sie einen nahtlosen Domänenbeitritt zu einer Linux-Instance einrichten können, müssen Sie die Verfahren in diesem Abschnitt abschließen.

Ihr Servicekonto für die nahtlose Domainverbindung auswählen

Sie können Linux-Computer nahtlos mit Ihrer AWS verwalteten Microsoft AD Active Directory-Domäne verbinden. Dazu müssen Sie ein Benutzerkonto mit der Berechtigung zum Erstellen von Computerkonten verwenden, um die Rechner mit der Domain zu verbinden. Obwohl Mitglieder

der AWS delegierten Administratoren oder anderer Gruppen über ausreichende Berechtigungen verfügen, um Computer mit der Domain zu verbinden, raten wir davon ab, diese zu verwenden. Als bewährte Methode empfehlen wir Ihnen, ein Servicekonto zu verwenden, das über die erforderlichen Mindestberechtigungen verfügt, um die Computer mit der Domain zu verbinden.

Um ein Konto mit den Mindestberechtigungen zu delegieren, die für den Beitritt der Computer zur Domäne erforderlich sind, können Sie die folgenden PowerShell Befehle ausführen. Sie müssen diese Befehle von einem mit der Domain verbundenen Windows-Computer ausführen, auf dem Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD installiert ist. Darüber hinaus müssen Sie ein Konto verwenden, das die Berechtigung hat, die Berechtigungen für Ihre Computer-OU oder Ihren Container zu ändern. Der PowerShell Befehl legt Berechtigungen fest, die es dem Dienstkonto ermöglichen, Computerobjekte im Standardcontainer für Computer Ihrer Domäne zu erstellen.

```
$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"
```

Wenn Sie eine grafische Benutzeroberfläche (GUI) bevorzugen, können Sie den manuellen Prozess verwenden, der unter Zuweisen von Berechtigungen zu Ihrem Servicekonto beschrieben wird.

Die Secrets zum Speichern des Domain-Servicekontos erstellen

Sie können AWS Secrets Manager es zum Speichern des Domänendienstkontos verwenden.

So erstellen Sie Secrets und speichern die Kontoinformationen des Domainservices

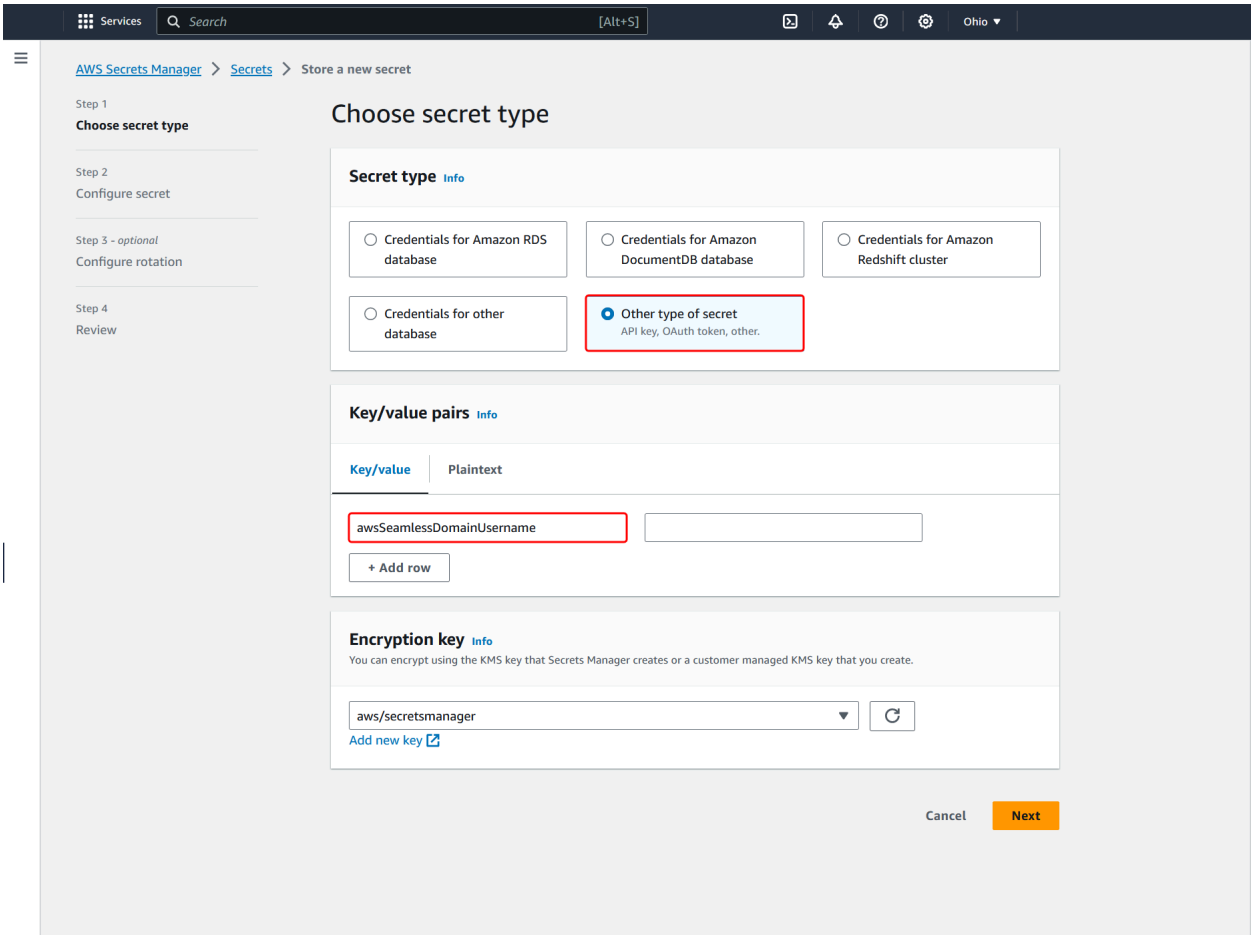
1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Secrets Manager Konsole unter https://console.aws.amazon.com/secretsmanager/.
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Gehen Sie auf der Seite Neues Geheimnis speichern wie folgt vor:

    a. Wählen Sie unter Geheimtyp die Option Andere Art von Geheimnissen aus.

    b. Gehen Sie unter Schlüssel/Wert-Paare wie folgt vor:

        i. Geben Sie im ersten Feld **`awsSeamlessDomainUsername`** ein. Geben Sie in derselben Zeile im nächsten Feld den Benutzernamen für Ihr Dienstkonto ein. Wenn Sie den PowerShell Befehl beispielsweise zuvor verwendet haben, wäre der Name des Dienstkontos**`awsSeamlessDomain`**.

        > **Note**
        >
        > Sie müssen **`awsSeamlessDomainUsername`** genau so eingeben, wie er lautet. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.



ii. Wählen Sie Zeile hinzufügen.

iii. Geben Sie in der neuen Zeile im ersten Feld **`awsSeamlessDomainPassword`** ein. Geben Sie in derselben Zeile im nächsten Feld das Passwort für Ihr Servicekonto ein.

> **Note**
>
> Sie müssen **`awsSeamlessDomainPassword`** genau so eingeben, wie er lautet. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.

iv. Behalten Sie unter Verschlüsselungsschlüssel den Standardwert bei`aws/secretsmanager`. AWS Secrets Manager verschlüsselt das Geheimnis immer, wenn Sie diese Option wählen. Sie können auch einen von Ihnen erstellten Schlüssel auswählen.

> **Note**
>
> Je nachdem AWS Secrets Manager, welches Geheimnis Sie verwenden, fallen Gebühren an. Die aktuelle vollständige Preisliste finden Sie unter AWS Secrets Manager – Preise.
> Sie können den AWS verwalteten Schlüssel`aws/secretsmanager`, den Secrets Manager erstellt, verwenden, um Ihre Geheimnisse kostenlos zu verschlüsseln. Wenn Sie Ihre eigenen KMS-Schlüssel zur Verschlüsselung Ihrer Geheimnisse erstellen, wird Ihnen der aktuelle AWS KMS Tarif AWS berechnet. Weitere Informationen finden Sie unter AWS Key Management Service -Preisgestaltung.

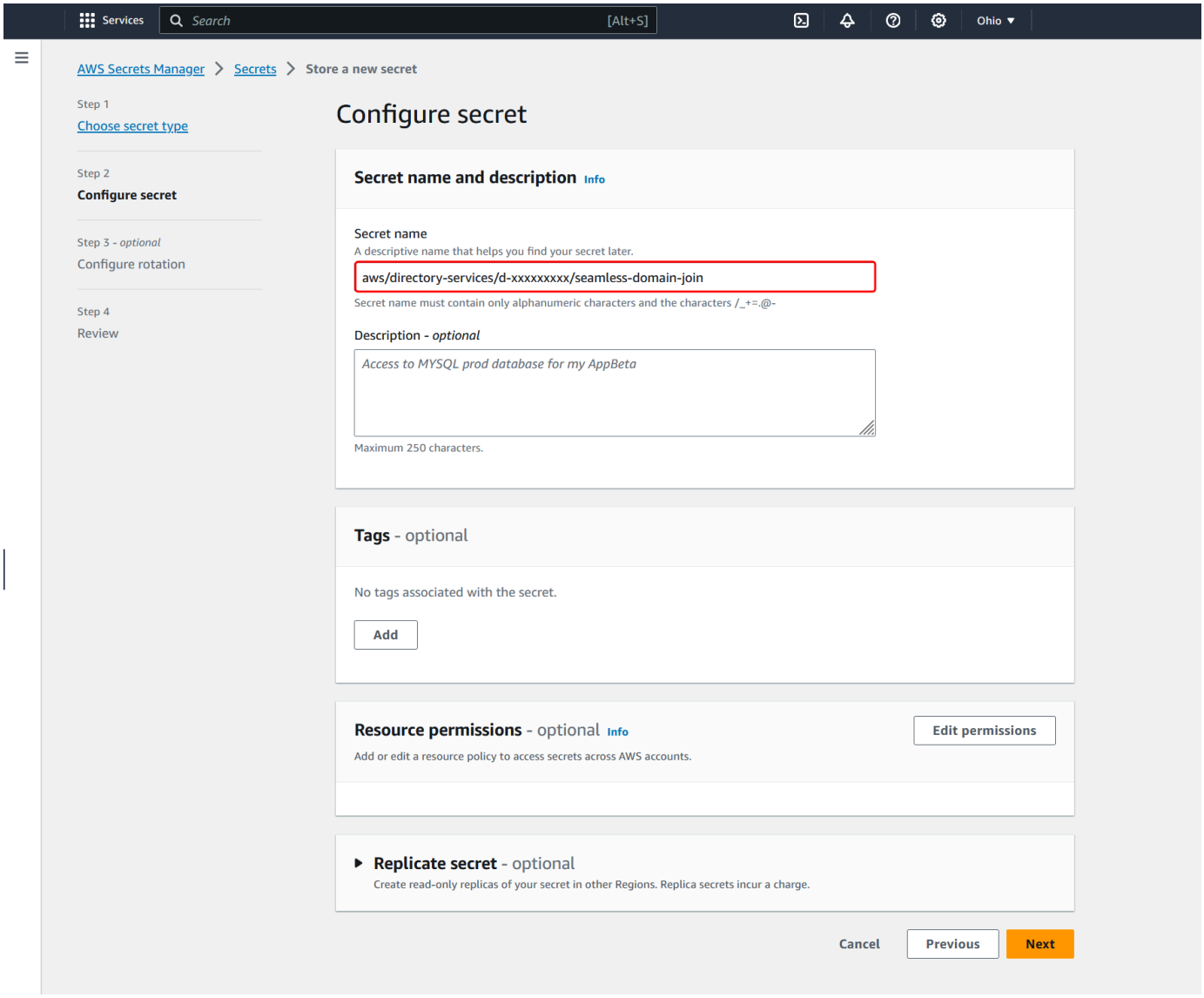
v. Wählen Sie Weiter aus.

4. Geben Sie unter Geheimer Name einen geheimen Namen ein, der Ihre Verzeichnis-ID enthält. Verwenden Sie dabei das folgende Format und ersetzen Sie *d-xxxxxxxxx* durch Ihre Verzeichnis-ID:

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

Dies wird verwendet, um Secrets in der Anwendung abzurufen.

> **Note**
>
> Sie müssen **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join** genau so eingeben, wie es ist, aber *d-xxxxxxxxxx* durch Ihre Verzeichnis-ID ersetzen. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.



5. Belassen Sie alles andere auf den eingestellten Standardwerte und wählen Sie dann Weiter.
6. Wählen Sie unter Automatische Rotation konfigurieren die Option Automatische Rotation deaktivieren und wählen Sie dann Weiter.

   Sie können die Rotation für dieses Geheimnis aktivieren, nachdem Sie es gespeichert haben.
7. Überprüfen Sie die Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen zu speichern. Die Secrets-Manager-Konsole zeigt Ihnen wieder die Liste der Secrets in Ihrem Konto an, in der Ihr neues Secret nun enthalten ist.
8. Wählen Sie Ihren neu erstellten Secret-Namen aus der Liste und notieren Sie sich den Wert des Secret-ARN. Sie brauchen diesen im nächsten Abschnitt.

Schalten Sie die Rotation für das geheime Domänendienstkonto ein

Wir empfehlen, dass Sie die geheimen Daten regelmäßig wechseln, um Ihre Sicherheitslage zu verbessern.

So aktivieren Sie die Rotation für das geheime Domänendienstkonto

- Folgen Sie den Anweisungen unter Automatische Rotation für AWS Secrets Manager geheime Daten einrichten im AWS Secrets Manager Benutzerhandbuch.

  Verwenden Sie für Schritt 5 die Rotationsvorlage Microsoft Active Directory-Anmeldeinformationen im AWS Secrets Manager Benutzerhandbuch.

  Hilfe finden Sie im AWS Secrets Manager Benutzerhandbuch unter Problembehandlung bei der AWS Secrets Manager Rotation.

Die erforderliche IAM-Richtlinie und -Rolle erstellen

Gehen Sie wie folgt vor, um eine benutzerdefinierte Richtlinie zu erstellen, die nur Lesezugriff auf Ihren Secrets Manager Seamless Domain Join Secret (den Sie zuvor erstellt haben) ermöglicht, und um eine neue DomainJoin LinuxEC2 IAM-Rolle zu erstellen.

Die IAM-Leserichtlinie zu Secrets Manager erstellen

Sie verwenden die IAM-Konsole, um eine Richtlinie zu erstellen, die schreibgeschützten Zugriff auf Ihr Secrets-Manager-Secret gewährt.

So erstellen Sie die IAM-Leserichtlinie zu Secrets Manager

1. Melden Sie sich AWS Management Console als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Dann öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Access Management die Option Richtlinien aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie die Registerkarte JSON aus und kopieren Sie den Text aus dem folgenden JSON-Richtliniendokument. Fügen Sie ihn dann in das JSON-Textfeld ein.

> **Note**
>
> Stellen Sie sicher, dass Sie die Region und den Ressourcen-ARN durch die tatsächliche Region und den ARN des Secrets ersetzen, den Sie zuvor erstellt haben.

```
{
    "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. Wählen Sie danach Next aus. Die Richtlinienvalidierung meldet mögliche Syntaxfehler. Weitere Informationen finden Sie unter Validierung von IAM-Richtlinien.
6. Geben Sie auf der Seite Richtlinie überprüfen einen Namen für die Richtlinie ein, z. B. **`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. Überprüfen Sie den Abschnitt Zusammenfassung, um die Berechtigungen einzusehen, die Ihre Richtlinie gewährt. Wählen Sie dann Richtlinie erstellen aus, um Ihre Änderungen zu speichern. Die neue Richtlinie erscheint in der Liste der verwalteten Richtlinien und ist nun bereit, einer Identität zugeordnet zu werden.

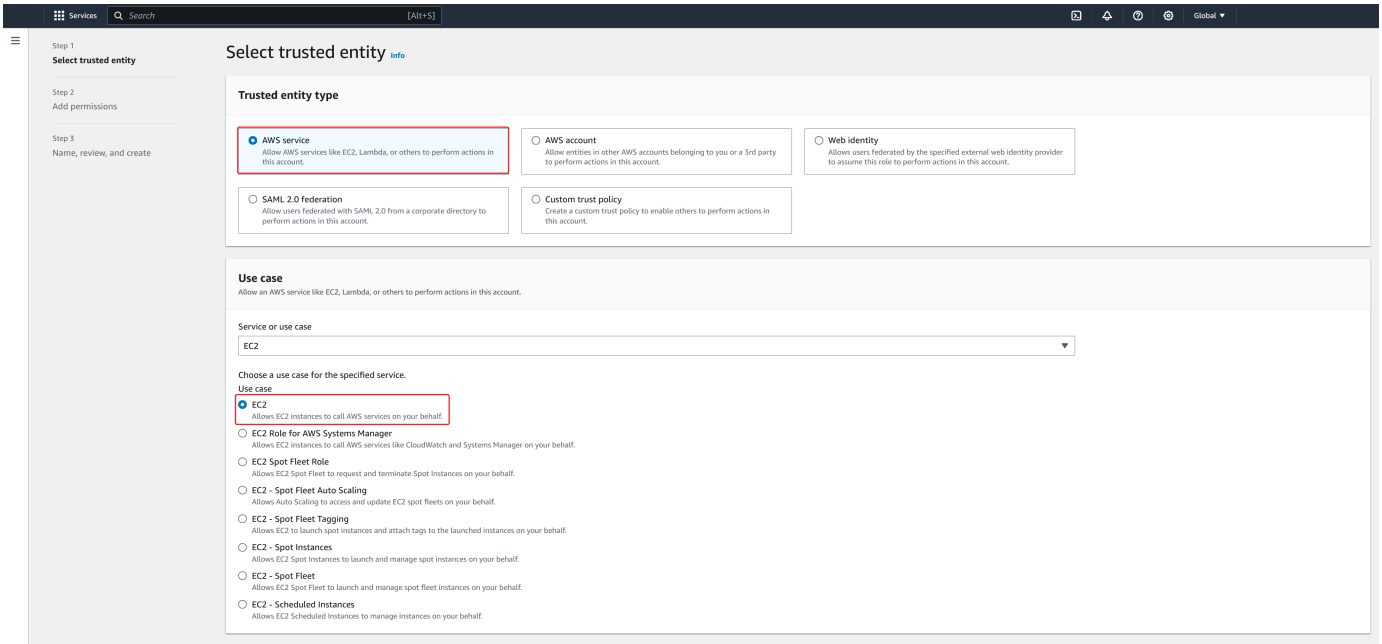
> **Note**
>
> Wir empfehlen Ihnen, eine Richtlinie pro Secret zu erstellen. Auf diese Weise wird sichergestellt, dass Instances nur auf das entsprechende Secret zugreifen können und die Auswirkungen einer Kompromittierung einer Instance minimiert werden.

Erstellen Sie die LinuxEC2-Rolle DomainJoin

Sie verwenden die IAM-Konsole, um die Rolle zu erstellen, die Sie für die Domainverbindung Ihrer Linux-EC2-Instance verwenden werden.

Um die LinuxEC2-Rolle zu erstellen DomainJoin

1. Melden Sie sich AWS Management Console als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Dann öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich unter Access Management die Option Rollen aus.
3. Wählen Sie im Inhaltsbereich die Option Rolle erstellen.
4. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität auswählen) die Option AWS -Service aus.
5. Wählen Sie unter Anwendungsfall die Option EC2 und dann Weiter aus.



6. Gehen Sie für Filterrichtlinien wie folgt vor:

   a. Geben Sie **`AmazonSSMManagedInstanceCore`** ein. Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

   b. Geben Sie **`AmazonSSMDirectoryServiceAccess`** ein. Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

   c. Geben Sie **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** ein (oder den Namen der Richtlinie, die Sie im vorherigen Verfahren erstellt haben). Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

d. Nachdem Sie die drei oben aufgeführten Richtlinien hinzugefügt haben, wählen Sie Rolle erstellen aus.

> **Note**
>
> AmazonSSM DirectoryServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einer Datei, die von Active Directory verwaltet wird. AWS Directory Service AmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager - Benutzerhandbuch.

7. Geben Sie im Feld Rollenname einen Namen für Ihre neue Rolle ein, z. B. **`LinuxEC2DomainJoin`** oder einen anderen Namen, den Sie bevorzugen.
8. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein.
9. (Optional) Wählen Sie unter Schritt 3: Stichwörter hinzufügen die Option Neues Tag hinzufügen aus, um Stichwörter hinzuzufügen. Tag-Schlüssel-Wert-Paare werden verwendet, um den Zugriff für diese Rolle zu organisieren, nachzuverfolgen oder zu kontrollieren.
10. Wählen Sie Rolle erstellen aus.

Treten Sie Ihrer Linux-Instance nahtlos bei

Nachdem Sie nun alle erforderlichen Aufgaben konfiguriert haben, können Sie das folgende Verfahren verwenden, um Ihrer EC2-Linux-Instance nahtlos beizutreten.

Um Ihrer Linux-Instance nahtlos beizutreten

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Regionsauswahl in der Navigationsleiste dasselbe Verzeichnis aus AWS-Region wie das bestehende Verzeichnis.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.

4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Linux EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.
6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) ein Linux-AMI aus, das Sie starten möchten.

> **Note**
>
> Das verwendete AMI muss AWS Systems Manager (SSM Agent) Version 2.3.1644.0 oder höher haben. Um die installierte SSM-Agent-Version in Ihrem AMI zu überprüfen, indem Sie eine Instance von diesem AMI aus starten, lesen Sie den Abschnitt Ermittlung der aktuell installierten SSM-Agent-Version. Wenn Sie den SSM Agent aktualisieren müssen, lesen Sie den Abschnitt Installieren und Konfigurieren von SSM Agent in EC2-Instances für Linux.
> SSM verwendet das `aws:domainJoin` Plugin, wenn eine Linux-Instance mit einer Domain verknüpft wird. Active Directory *`Das Plugin ändert den Hostnamen für die Linux-Instances in das Format EC2AMAZ- XXXXXXX.`* Weitere Informationen *`aws:domainJoin`* dazu finden Sie in der Plugin-Referenz zum AWS Systems Manager Befehlsdokument im Benutzerhandbuch.AWS Systems Manager

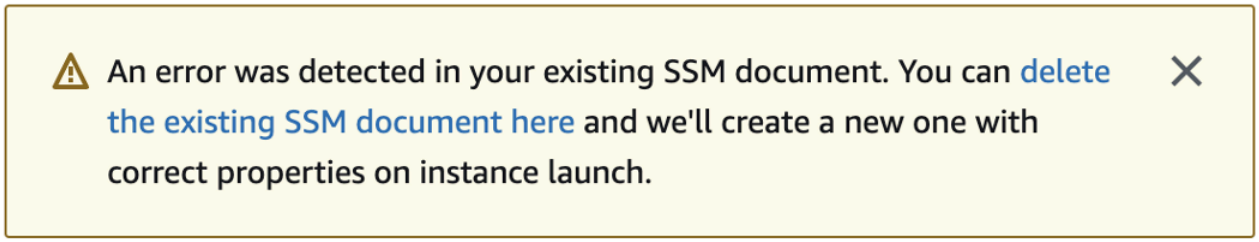
7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk. Wählen Sie Schlüsselpaar erstellen aus. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

> **Important**
>
> Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

    Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.
12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>

Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:

- Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
- Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Wählen Sie für das IAM-Instanzprofil die IAM-Rolle aus, die Sie zuvor im Abschnitt Voraussetzungen erstellt haben. Schritt 2: LinuxEC2-Rolle erstellen. DomainJoin
16. Wählen Sie Launch Instance (Instance starten) aus.

> **Note**
>
> Wenn Sie eine nahtlose Domainverbindung mit SUSE Linux durchführen, ist ein Neustart erforderlich, bevor die Authentifizierungen funktionieren. Um SUSE vom Linux-Terminal aus neu zu starten, geben Sie sudo reboot ein.

Manuelles Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory

Zusätzlich zu Amazon EC2 Windows-Instances können Sie auch bestimmte Amazon EC2 Linux-Instances zu Ihrem AWS Managed Microsoft AD Active Directory hinzufügen. Die folgenden Linux-Instance-Distributionen und -Versionen werden unterstützt:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-Bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-Bit x86)
- Ubuntu Server 18.04 LTS und Ubuntu Server 16.04 LTS
- CentOS 7 x86-64

- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Andere Linux-Distributionen und -Versionen können funktionieren, sind jedoch nicht getestet worden.

Verbinden Sie eine Linux-Instanz mit Ihrem AWS Managed Microsoft AD

Bevor Sie eine Amazon-Linux-, CentOS-, Red-Hat- oder Ubuntu-Instance mit Ihrem Verzeichnis verbinden können, muss die Instance zunächst wie unter Treten Sie Ihrer Linux-Instance nahtlos bei beschrieben gestartet werden.

> **Important**
>
> Einige der folgenden Verfahren können, wenn sie nicht richtig durchgeführt werden, Ihre Instance nicht erreichbar oder unbrauchbar machen. Aus diesem Grund empfehlen wir dringend, eine Sicherung anzufertigen oder einen Snapshot der Instance zu machen, bevor diese Verfahren ausgeführt werden.

So fügen Sie Ihrem Verzeichnis eine Linux-Instance hinzu

Folgen Sie den Schritten für Ihre spezifische Linux-Instance unter Verwendung einer der folgenden Registerkarten:

Amazon Linux

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre Amazon-Linux-64bit-Instance auf dem aktuellen Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen Amazon-Linux-Pakete auf Ihrer Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Hilfe bei der Bestimmung der Amazon-Linux-Version, die Sie verwenden, finden Sie unter Identifizieren von Amazon-Linux-Images im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Ein Konto in der *example.com* Domain, das eine Berechtigung zum Verbinden einer Domain hat. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

6. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

7. Stellen Sie nach dem Neustart der Instanz mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen Sie die Gruppe AWS Delegated Administrators zur Sudoer-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

   ```
   sudo visudo
   ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

CentOS

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der bereitgestellten DNS-Server verwendet. AWS Directory Service Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre CentOS 7-Instance auf dem aktuellen Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen CentOS 7-Pakete auf Ihre Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Ein Konto in der *example.com* Domain, das eine Berechtigung zum Verbinden einer Domain hat. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

6. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

7. Stellen Sie nach dem Neustart der Instanz mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen Sie die Gruppe AWS Delegated Administrators der Sudoer-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

   ```
   sudo visudo
   ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

Red Hat

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der bereitgestellten DNS-Server verwendet. AWS Directory Service Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Stellen Sie sicher, dass die Red Hat - 64bit-Instance auf dem neuesten Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen Red Hat-Pakete auf Ihrer Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

Das SaM AccountName für ein Konto in der Domäne *example.com*, das über Domänenbeitrittsrechte verfügt. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

6. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

7. Stellen Sie nach dem Neustart der Instanz mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen Sie die Gruppe AWS Delegated Administrators der Sudoer-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

   ```
   sudo visudo
   ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

   ```
   ## Add the "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

SUSE

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instance so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service-bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre SUSE Linux 15-Instance auf dem aktuellen Stand ist.
   a. Verbinden Sie das Paket-Repository.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Aktualisieren Sie SUSE.

   ```
   sudo zypper update -y
   ```

4. Installieren Sie die erforderlichen SUSE Linux 15-Pakete auf Ihrer Linux-Instance.

   > **Note**
   >
   > Einige dieser Pakete sind möglicherweise bereits installiert.
   > Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

   ```
   sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
   ```

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

   ```
   sudo realm join -U join_account example.com --verbose
   ```

   join_account

   Das sAM AccountName in der Domäne *example.com*, das über Domänenbeitrittsrechte verfügt. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden.

Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig qualifizierte DNS-Name Ihres Verzeichnisses.

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

Beachten Sie, dass beide folgenden Rückgaben erwartet werden.

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. Aktivieren Sie SSSD in PAM manuell.

```
sudo pam-config --add --sss
```

7. Bearbeiten Sie nsswitch.conf, um SSSD in nsswitch.conf zu aktivieren.

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. Fügen Sie die folgende Zeile zu /etc/pam.d/common-session hinzu, um bei der ersten Anmeldung automatisch ein Startverzeichnis zu erstellen.

```
sudo vi /etc/pam.d/common-session
```

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

9. Starten Sie die Instance neu, um den Domain-Beitrittsprozess abzuschließen.

```
sudo reboot
```

10. Verbinden Sie sich mit einem beliebigen SSH-Client erneut mit der Instance, um zu überprüfen, ob die Domainverbindung erfolgreich abgeschlossen wurde, und schließen Sie die weiteren Schritte ab.

    a. So überprüfen Sie, ob die Instance in der Domain registriert wurde

    ```
    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. So überprüfen Sie den Status des SSSD-Daemon

    ```
    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. So gestatten Sie einem Benutzer Zugriff über SSH und Konsole

```
sudo realm permit join_account@example.com
```

So gestatten Sie einer Domaingruppe den Zugriff über SSH und Konsole

```
sudo realm permit -g 'AWS Delegated Administrators'
```

So gestatten Sie allen Benutzern den Zugriff

```
sudo realm permit --all
```

12. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

    a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Starten Sie den SSH-Service neu.

    ```
    sudo systemctl restart sshd.service
    ```

    Alternative Vorgehensweise:

    ```
    sudo service sshd restart
    ```

13. 13. Stellen Sie nach dem Neustart der Instanz mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen Sie die Gruppe AWS Delegated Administrators der Sudoer-Liste hinzu, indem Sie die folgenden Schritte ausführen:

    a. Öffnen Sie die sudoers-Datei mit dem folgenden Befehl:

    ```
    sudo visudo
    ```

    b. Fügen Sie Folgendes am Ende der sudoers-Datei hinzu und speichern Sie die Datei.

    ```
    ## Add the "Domain Admins" group from the awsad.com domain.
    ```

```
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der bereitgestellten DNS-Server verwendet. AWS Directory Service Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Stellen Sie sicher, dass Ihre Ubuntu - 64bit-Instance auf dem neuesten Stand ist.

   ```
   sudo apt-get update
   sudo apt-get -y upgrade
   ```

4. Installieren Sie die erforderlichen Ubuntu-Pakete auf Ihrer Linux-Instance.

   > **Note**
   >
   > Einige dieser Pakete sind möglicherweise bereits installiert.
   > Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

   ```
   sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
   ```

5. Deaktivieren Sie die Reverse DNS-Auflösung und legen Sie den Standardbereich auf den FQDN Ihrer Domain fest. Ubuntu-Instances müssen im DNS reverse-auflösbar sein, bevor der Bereich genutzt werden kann. Andernfalls müssen Sie Reverse DNS in der /etc/krb5.conf wie folgt deaktivieren:

   ```
   sudo vi /etc/krb5.conf
   ```

   ```
   [libdefaults]
   ```

```
default_realm = EXAMPLE.COM
rdns = false
```

6. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

Das SaM AccountName für ein Konto in der Domäne *example.com*, das über Domänenbeitrittsrechte verfügt. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

7. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.
   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

```
sudo vi /etc/ssh/sshd_config
```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

```
PasswordAuthentication yes
```

   c. Starten Sie den SSH-Service neu.

```
sudo systemctl restart sshd.service
```

   Alternative Vorgehensweise:

```
sudo service sshd restart
```

8. Stellen Sie nach dem Neustart der Instanz mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen Sie die Gruppe AWS Delegated Administrators der Sudoer-Liste hinzu, indem Sie die folgenden Schritte ausführen:
   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

      ```
      sudo visudo
      ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

      ```
      ## Add the "AWS Delegated Administrators" group from the example.com domain.
      %AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
      ```

      (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

Einschränken des Kontoanmeldungszugriffs

Da alle Konten in Active Directory standardmäßig definiert sind, können sich alle Benutzer aus dem Verzeichnis bei der Instance anmelden. Mit ad_access_filter in sssd.conf können Sie festlegen, dass sich nur bestimmte Benutzer bei der Instance anmelden können. Beispielsweise:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Gibt an, dass Benutzer nur Zugriff auf die Instance haben, wenn sie Mitglied einer bestimmten Gruppe sind.

cn

Der allgemeine Name der Gruppe, die Zugriff haben soll. In diesem Beispiel ist der Name der Gruppe *admins*.

ou

Dies ist die Organisationseinheit, in der sich die oben genannte Gruppe befindet. In diesem Beispiel ist die OU *Testou*.

dc

Dies ist die Domainkomponente Ihrer Domain. In diesem Beispiel *example*.

dc

Hierbei handelt es sich um eine zusätzliche Domainkomponente. In diesem Beispiel *com*.

Sie müssen ad_access_filter manuell zu /etc/sssd/sssd.conf hinzufügen.

Öffnen Sie die Datei /etc/sssd/sssd.conf in einem Text-Editor.

```
sudo vi /etc/sssd/sssd.conf
```

Danach sieht sssd.conf wie folgt aus:

```
[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)
```

Damit die Konfiguration wirksam wird, müssen Sie den sssd-Service neu starten:

```
sudo systemctl restart sssd.service
```

Alternativ können Sie:

```
sudo service sssd restart
```

Da alle Konten in Active Directory standardmäßig definiert sind, können sich alle Benutzer aus dem Verzeichnis bei der Instance anmelden. Mit ad_access_filter in sssd.conf können Sie festlegen, dass sich nur bestimmte Benutzer bei der Instance anmelden können.

Beispielsweise:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Gibt an, dass Benutzer nur Zugriff auf die Instance haben, wenn sie Mitglied einer bestimmten Gruppe sind.

cn

Der allgemeine Name der Gruppe, die Zugriff haben soll. In diesem Beispiel ist der Name der Gruppe *admins*.

ou

Dies ist die Organisationseinheit, in der sich die oben genannte Gruppe befindet. In diesem Beispiel ist die OU *Testou*.

dc

Dies ist die Domainkomponente Ihrer Domain. In diesem Beispiel *example*.

dc

Hierbei handelt es sich um eine zusätzliche Domainkomponente. In diesem Beispiel *com*.

Sie müssen ad_access_filter manuell zu /etc/sssd/sssd.conf hinzufügen.

1. Öffnen Sie die Datei /etc/sssd/sssd.conf in einem Text-Editor.

   ```
   sudo vi /etc/sssd/sssd.conf
   ```

2. Danach sieht sssd.conf wie folgt aus:

   ```
   [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. Damit die Konfiguration wirksam wird, müssen Sie den sssd-Service neu starten:

```
sudo systemctl restart sssd.service
```

Alternativ können Sie:

```
sudo service sssd restart
```

ID-Zuordnung

Die ID-Zuordnung kann mit zwei Methoden durchgeführt werden, um eine einheitliche Benutzererfahrung zwischen UNIX/Linux-Benutzerkennungen (UID) und Gruppenkennungen (GID) sowie Windows- und Active Directory Security Identifier (SID) -Identitäten zu gewährleisten.

1. Zentralisiert
2. Verteilt

> **Note**
>
> Für die zentrale Zuordnung von Benutzeridentitäten Active Directory ist ein Portable Operating System Interface oder POSIX erforderlich.

Zentralisierte Zuordnung von Benutzeridentitäten

Active Directoryoder ein anderer LDAP-Dienst (Lightweight Directory Access Protocol) stellt den Linux-Benutzern UID und GID zur Verfügung. In Active Directory werden diese Identifikatoren in den Benutzerattributen gespeichert:

- UID — Der Linux-Benutzername (Zeichenfolge)
- UID-Nummer — Die Linux-Benutzer-ID-Nummer (Integer)
- GID-Nummer — Die Linux-Gruppen-ID-Nummer (Integer)

Um eine Linux-Instanz für die Verwendung der UID und GID zu konfigurierenActive Directory, legen Sie diese `ldap_id_mapping = False` in der Datei sssd.conf fest. Bevor Sie diesen Wert festlegen, stellen Sie sicher, dass Sie den Benutzern und Gruppen in eine UID, UID-Nummer und GID-Nummer hinzugefügt haben. Active Directory

Zuordnung verteilter Benutzeridentitäten

Wenn Sie Active Directory nicht über die POSIX-Erweiterung verfügen oder wenn Sie die Identitätszuweisung nicht zentral verwalten möchten, kann Linux die UID- und GID-Werte berechnen. Linux verwendet den eindeutigen Security Identifier (SID) des Benutzers, um die Konsistenz aufrechtzuerhalten.

Um die verteilte Benutzer-ID-Zuordnung zu konfigurieren, legen Sie dies `ldap_id_mapping = True` in der Datei sssd.conf fest.

Connect zur Linux-Instanz her

Wenn ein Benutzer die Verbindung zur Instance über einen SSH-Client herstellt, wird er zur Eingabe des Benutzernamens aufgefordert. Der Benutzer kann den Benutzernamen entweder im Format `username@example.com` oder `EXAMPLE\username` eingeben. Je nachdem, welche Linux-Distribution Sie verwenden, wird die Antwort etwa wie folgt aussehen:

Amazon Linux, Red Hat Enterprise Linux und 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%
```

Manuelles Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory mithilfe von Winbind

Sie können den Winbind-Dienst verwenden, um Ihre Amazon EC2 EC2-Linux-Instances manuell mit einer AWS verwalteten Microsoft AD Active Directory-Domain zu verbinden. Dadurch können Ihre vorhandenen lokalen Active Directory-Benutzer ihre Active Directory-Anmeldeinformationen verwenden, wenn sie auf die Linux-Instanzen zugreifen, die mit Ihrem AWS verwalteten Microsoft AD Active Directory verknüpft sind. Die folgenden Linux-Instance-Distributionen und -Versionen werden unterstützt:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-Bit x86)
- Amazon Linux 2023 AMI

- Red Hat Enterprise Linux 8 (HVM) (64-Bit x86)
- Ubuntu Server 18.04 LTS und Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Andere Linux-Distributionen und -Versionen können funktionieren, sind jedoch nicht getestet worden.

Verbinden Sie eine Linux-Instanz mit Ihrem AWS verwalteten Microsoft AD Active Directory

> **Important**
>
> Einige der folgenden Verfahren können, wenn sie nicht richtig durchgeführt werden, Ihre Instance nicht erreichbar oder unbrauchbar machen. Aus diesem Grund empfehlen wir dringend, eine Sicherung anzufertigen oder einen Snapshot der Instance zu machen, bevor diese Verfahren ausgeführt werden.

So fügen Sie Ihrem Verzeichnis eine Linux-Instance hinzu

Folgen Sie den Schritten für Ihre spezifische Linux-Instance unter Verwendung einer der folgenden Registerkarten:

Amazon Linux/CENTOS/REDHAT

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instance so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service-bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre Linux-Instance auf dem aktuellen Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen Samba-/Winbind-Pakete auf Ihrer Linux-Instance.

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-
clients
```

5. Erstellen Sie eine Sicherungskopie der `smb.conf`-Hauptdatei, damit Sie im Falle eines Fehlers auf diese zurückgreifen können:

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Öffnen Sie die ursprüngliche Konfigurationsdatei [`/etc/samba/smb.conf`] in einem Texteditor.

```
sudo vim /etc/samba/smb.conf
```

   Geben Sie die Informationen zur Active Directory-Domänenumgebung ein, wie im folgenden Beispiel gezeigt:

```
[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. Öffnen Sie die Hosts-Datei [`/etc/hosts`] in einem Texteditor.

```
sudo vim /etc/hosts
```

   Fügen Sie die private IP-Adresse Ihrer Linux-Instance wie folgt hinzu:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Wenn Sie Ihre IP-Adresse nicht in der `/etc/hosts`-Datei angegeben haben, erhalten Sie möglicherweise den folgenden DNS-Fehler, während Sie die Instance mit der Domain verbinden:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Dieser Fehler bedeutet, dass die Verbindung erfolgreich war, aber der Befehl [net ads] den DNS-Eintrag nicht im DNS registrieren konnte.

8. Verbinden Sie die Linux-Instance mit Active Directory mithilfe von net utility.

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

Ein Konto in der *example.com* Domain, das eine Berechtigung zum Verbinden einer Domain hat. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Ändern Sie die PAM-Konfigurationsdatei. Verwenden Sie den folgenden Befehl, um die erforderlichen Einträge für die winbind-Authentifizierung hinzuzufügen:

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. Stellen Sie den SSH-Service so ein, dass er die Passwortauthentifizierung zulässt, indem Sie die `/etc/ssh/sshd_config`-Datei bearbeiten.

    a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Starten Sie den SSH-Service neu.

    ```
    sudo systemctl restart sshd.service
    ```

    Alternative Vorgehensweise:

    ```
    sudo service sshd restart
    ```

11. Nachdem die Instance neu gestartet wurde, stellen Sie mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen die Root-Rechte für einen Domain-Benutzer oder eine Gruppe zur sudoers-Liste hinzu, indem Sie die folgenden Schritte ausführen:

    a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

    ```
    sudo visudo
    ```

    b. Fügen Sie die erforderlichen Gruppen oder Benutzer aus Ihrer Trusting- oder Trusted-Domain wie folgt hinzu und speichern Sie sie dann.

    ```
    ## 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
    ```

    (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

SUSE

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instance so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service-bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre SUSE Linux 15-Instance auf dem aktuellen Stand ist.

   a. Verbinden Sie das Paket-Repository.

   ```
   sudo SUSEConnect -p PackageHub/15.1/x86_64
   ```

   b. Aktualisieren Sie SUSE.

   ```
   sudo zypper update -y
   ```

4. Installieren Sie die erforderlichen Samba-/Winbind-Pakete auf Ihrer Linux-Instance.

   ```
   sudo zypper in -y samba samba-winbind
   ```

5. Erstellen Sie eine Sicherungskopie der `smb.conf`-Hauptdatei, damit Sie im Falle eines Fehlers auf diese zurückgreifen können:

   ```
   sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
   ```

6. Öffnen Sie die ursprüngliche Konfigurationsdatei [`/etc/samba/smb.conf`] in einem Texteditor.

   ```
   sudo vim /etc/samba/smb.conf
   ```

   Geben Sie die Informationen zu Ihrer Active-Directory-Domainumgebung ein, wie im folgenden Beispiel gezeigt:

   ```
   [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. Öffnen Sie die Hosts-Datei [`/etc/hosts`] in einem Texteditor.

```
sudo vim /etc/hosts
```

Fügen Sie die private IP-Adresse Ihrer Linux-Instance wie folgt hinzu:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Wenn Sie Ihre IP-Adresse nicht in der `/etc/hosts`-Datei angegeben haben, erhalten Sie möglicherweise den folgenden DNS-Fehler, während Sie die Instance mit der Domain verbinden:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Dieser Fehler bedeutet, dass die Verbindung erfolgreich war, aber der Befehl [net ads] den DNS-Eintrag nicht im DNS registrieren konnte.

8. Fügen Sie die Linux-Instance mit folgendem Befehl dem Verzeichnis hinzu.

```
sudo net ads join -U join_account@example.com
```

`join_account`

Das SaM AccountName in der Domäne *`example.com`*, das über Domänenbeitrittsrechte verfügt. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

`example.com`

Der vollständig qualifizierte DNS-Name Ihres Verzeichnisses.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Ändern Sie die PAM-Konfigurationsdatei. Verwenden Sie den folgenden Befehl, um die erforderlichen Einträge für die Winbind-Authentifizierung hinzuzufügen:

```
sudo pam-config --add --winbind --mkhomedir
```

10. Öffnen Sie die Konfigurationsdatei Name Service Switch [`/etc/nsswitch.conf`] in einem Texteditor.

```
vim /etc/nsswitch.conf
```

Fügen Sie die Winbind-Direktive hinzu, wie unten gezeigt.

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. Stellen Sie den SSH-Service so ein, dass er die Passwortauthentifizierung zulässt, indem Sie die `/etc/ssh/sshd_config`-Datei bearbeiten.

a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

```
sudo vim /etc/ssh/sshd_config
```

b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

```
PasswordAuthentication yes
```

c. Starten Sie den SSH-Service neu.

```
sudo systemctl restart sshd.service
```

Alternative Vorgehensweise:

```
sudo service sshd restart
```

12. Nachdem die Instance neu gestartet wurde, stellen Sie mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen der Liste sudoers die Root-Rechte eines Domainbenutzers oder einer -Gruppe hinzu, indem Sie die folgenden Schritte ausführen:

    a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

    ```
    sudo visudo
    ```

    b. Fügen Sie die erforderlichen Gruppen oder Benutzer aus Ihrer Trusting- oder Trusted-Domain wie folgt hinzu und speichern Sie sie dann.

    ```
    ## 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
    ```

    (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

Ubuntu

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instance so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service-bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Wenn Sie ihn manuell einrichten möchten, finden Sie im AWS Knowledge Center unter Wie weise ich einer privaten Amazon EC2 EC2-Instance einen statischen DNS-Server zu? Anleitungen zur Einrichtung des persistenten DNS-Servers für Ihre spezielle Linux-Distribution und -Version.
3. Überprüfen Sie, ob Ihre Linux-Instance auf dem aktuellen Stand ist.

    ```
    sudo yum -y update
    ```

    ```
    sudo apt-get -y upgrade
    ```

4. Installieren Sie die erforderlichen Samba-/Winbind-Pakete auf Ihrer Linux-Instance.

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. Erstellen Sie eine Sicherungskopie der `smb.conf`-Hauptdatei, damit Sie im Falle eines Fehlers auf diese zurückgreifen können.

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. Öffnen Sie die ursprüngliche Konfigurationsdatei [`/etc/samba/smb.conf`] in einem Texteditor.

```
sudo vim /etc/samba/smb.conf
```

   Geben Sie die Informationen zu Ihrer Active-Directory-Domainumgebung ein, wie im folgenden Beispiel gezeigt:

```
[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. Öffnen Sie die Hosts-Datei [`/etc/hosts`] in einem Texteditor.

```
sudo vim /etc/hosts
```

   Fügen Sie die private IP-Adresse Ihrer Linux-Instance wie folgt hinzu:

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> Wenn Sie Ihre IP-Adresse nicht in der `/etc/hosts`-Datei angegeben haben, erhalten Sie möglicherweise den folgenden DNS-Fehler, während Sie die Instance mit der Domain verbinden:
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> Dieser Fehler bedeutet, dass die Verbindung erfolgreich war, aber der Befehl [net ads] den DNS-Eintrag nicht im DNS registrieren konnte.

8. Verbinden Sie die Linux-Instance mit Active Directory mithilfe von net utility.

```
sudo net ads join -U join_account@example.com
```

`join_account@example.com`

Ein Konto in der *`example.com`* Domain, das eine Berechtigung zum Verbinden einer Domain hat. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

`example.com`

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. Ändern Sie die PAM-Konfigurationsdatei. Verwenden Sie den folgenden Befehl, um die erforderlichen Einträge für die Winbind-Authentifizierung hinzuzufügen:

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. Öffnen Sie die Konfigurationsdatei Name Service Switch [`/etc/nsswitch.conf`] in einem Texteditor.

```
vim /etc/nsswitch.conf
```

Fügen Sie die Winbind-Direktive hinzu, wie unten gezeigt.

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. Stellen Sie den SSH-Service so ein, dass er die Passwortauthentifizierung zulässt, indem Sie die `/etc/ssh/sshd_config`-Datei bearbeiten.

    a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

    ```
    sudo vim /etc/ssh/sshd_config
    ```

    b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

    ```
    PasswordAuthentication yes
    ```

    c. Starten Sie den SSH-Service neu.

    ```
    sudo systemctl restart sshd.service
    ```

    Alternative Vorgehensweise:

    ```
    sudo service sshd restart
    ```

12. Nachdem die Instance neu gestartet wurde, stellen Sie mit einem beliebigen SSH-Client eine Verbindung zu ihr her und fügen der Liste sudoers die Root-Rechte eines Domainbenutzers oder einer -Gruppe hinzu, indem Sie die folgenden Schritte ausführen:

    a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

    ```
    sudo visudo
    ```

    b. Fügen Sie die erforderlichen Gruppen oder Benutzer aus Ihrer Trusting- oder Trusted-Domain wie folgt hinzu und speichern Sie sie dann.

    ```
    ## 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
```

(Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

Connect zur Linux-Instanz her

Wenn ein Benutzer die Verbindung zur Instance über einen SSH-Client herstellt, wird er zur Eingabe des Benutzernamens aufgefordert. Der Benutzer kann den Benutzernamen entweder im Format `username@example.com` oder `EXAMPLE\username` eingeben. Je nachdem, welche Linux-Distribution Sie verwenden, wird die Antwort etwa wie folgt aussehen:

Amazon Linux, Red Hat Enterprise Linux und 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%
```

Manuelles Verbinden einer Amazon EC2 Mac-Instance mit Ihrem AWS verwalteten Microsoft AD Active Directory

Mit diesem Verfahren wird eine Amazon EC2 Mac-Instance manuell mit Ihrem AWS verwalteten Microsoft AD Active Directory verknüpft.

Voraussetzungen

- Amazon EC2 Mac-Instances benötigen Amazon EC2 Dedicated Hosts. Sie müssen einen dedizierten Host zuweisen und eine Instance auf dem Host starten. Weitere Informationen finden Sie unter Starten einer Mac-Instance im Amazon EC2 EC2-Benutzerhandbuch.
- Wir empfehlen, einen DHCP-Optionssatz für Ihr AWS verwaltetes Microsoft AD Active Directory zu erstellen. Dadurch können alle Instances in Ihrer Amazon VPC auf die angegebene Domain und die DNS-Server verweisen, um ihre Domainnamen aufzulösen. Weitere Informationen finden Sie unter Erstellen oder ändern Sie einen DHCP-Optionssatz.

> **Note**
>
> Die Preise für Dedicated Hosts variieren je nach der von Ihnen ausgewählten Zahlungsoption. Weitere Informationen finden Sie im Amazon EC2 EC2-Benutzerhandbuch unter Preise und Abrechnung.

Um einer Mac-Instance manuell beizutreten

1. Verwenden Sie den folgenden SSH-Befehl, um eine Verbindung zu Ihrer Mac-Instanz herzustellen. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Mac-Instanz finden Sie unter Connect zu Ihrer Mac-Instanz herstellen.

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

2. Nachdem Sie eine Verbindung zu Ihrer Mac-Instanz hergestellt haben, erstellen Sie mit dem folgenden Befehl ein Passwort für das *ec2-Benutzerkonto*:

```
sudo passwd ec2-user
```

3. Wenn Sie in der Befehlszeile dazu aufgefordert werden, geben Sie ein Passwort für das *ec2-Benutzerkonto* ein. Sie können Ihr Betriebssystem und Ihre Software aktualisieren, indem Sie das Verfahren unter Betriebssystem und Software aktualisieren im Amazon EC2 EC2-Benutzerhandbuch befolgen.

4. Verwenden Sie den folgenden Befehl *dsconfigad*, um Ihre Mac-Instanz mit der AWS verwalteten Microsoft AD Active Directory-Domäne zu verbinden. Stellen Sie sicher, dass Sie den Domänennamen, den Computernamen und die Organisationseinheit durch Ihre AWS verwalteten Microsoft AD Active Directory-Domäneninformationen ersetzen. Weitere Informationen finden Sie auf der Apple-Website unter Konfiguration des Domänenzugriffs im Verzeichnisdienstprogramm auf dem Mac.

> **Warning**
>
> Der Computername sollte keinen Bindestrich enthalten. Bindestriche verhindern möglicherweise die Verbindung zum AWS verwalteten Microsoft AD Active Directory.

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

Das folgende Beispiel zeigt, wie der Befehl aussehen sollte, wenn Sie einem Administratorbenutzer auf einer Mac-Instanz beitreten, die **myec2mac01** nach der **example.com** Domäne benannt ist:

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. Verwenden Sie den folgenden Befehl, um die AWS delegierten Administratoren zum Administratorbenutzer auf Ihrer Mac-Instanz hinzuzufügen:

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. Verwenden Sie den folgenden Befehl, um zu bestätigen, dass der Domänenbeitritt mit AWS verwaltetem Microsoft AD Active Directory erfolgreich war:

```
dsconfigad -show
```

Sie haben Ihre Mac-Instanz erfolgreich mit Ihrem AWS Managed Microsoft AD Active Directory verbunden. Sie können sich jetzt mit Ihren AWS Managed Microsoft AD Active Directory-Anmeldeinformationen bei Ihrer Mac-Instanz anmelden.

Wenn Sie sich zum ersten Mal bei Ihrer Mac-Instanz anmelden, sollte Ihnen die Option zur Verfügung stehen, sich als „Anderer“ Benutzer anzumelden. Zu diesem Zeitpunkt können Sie Ihre Active Directory-Domänenanmeldedaten verwenden, um sich bei der Mac-Instanz anzumelden. Wenn Ihnen nach Abschluss dieser Schritte nicht die Option „Andere“ auf dem Anmeldebildschirm angezeigt wird, melden Sie sich als ec2-user an und melden Sie sich dann ab.

Um sich über die grafische Benutzeroberfläche mit einem Domain-Benutzer anzumelden, folgen Sie den Schritten unter Connect zur grafischen Benutzeroberfläche (GUI) Ihrer Instance herstellen im Amazon EC2 EC2-Benutzerhandbuch.

Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD

Wenn Sie einen Computer mit Ihrem Verzeichnis verbinden möchten, muss Ihr Konto über die entsprechenden Berechtigungen verfügen.

Mit AWS Directory Service for Microsoft Active Directory verfügen Mitglieder der Gruppen Admins und AWS Delegated Server Administrators über diese Rechte.

Als bewährte Methode empfehlen wir Ihnen, ein Konto zu verwenden, das nur die mindestens erforderlichen Berechtigungen hat. Die folgenden Schritte veranschaulichen, wie Sie eine neue Gruppe mit dem Namen `Joiners` erstellen und die Berechtigungen, die für die Verbindung von Computern mit dem Verzeichnis erforderlich sind, an diese Gruppe delegieren.

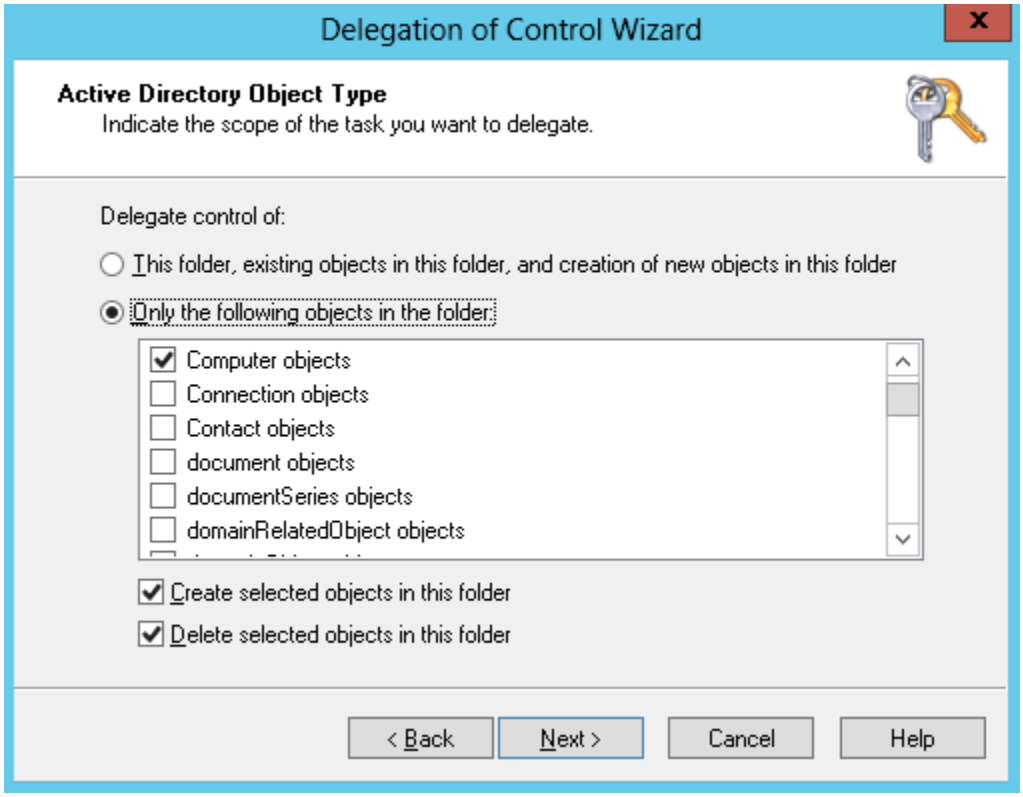
Sie müssen diesen Vorgang auf einem Computer durchführen, der mit Ihrem Verzeichnis verbunden ist und auf dem das MMC-Snap-In Active Directory Benutzer und Computer installiert ist. Außerdem müssen Sie als Domain-Administrator angemeldet sein.

So delegieren Sie Beitrittsberechtigungen für AWS Managed Microsoft AD

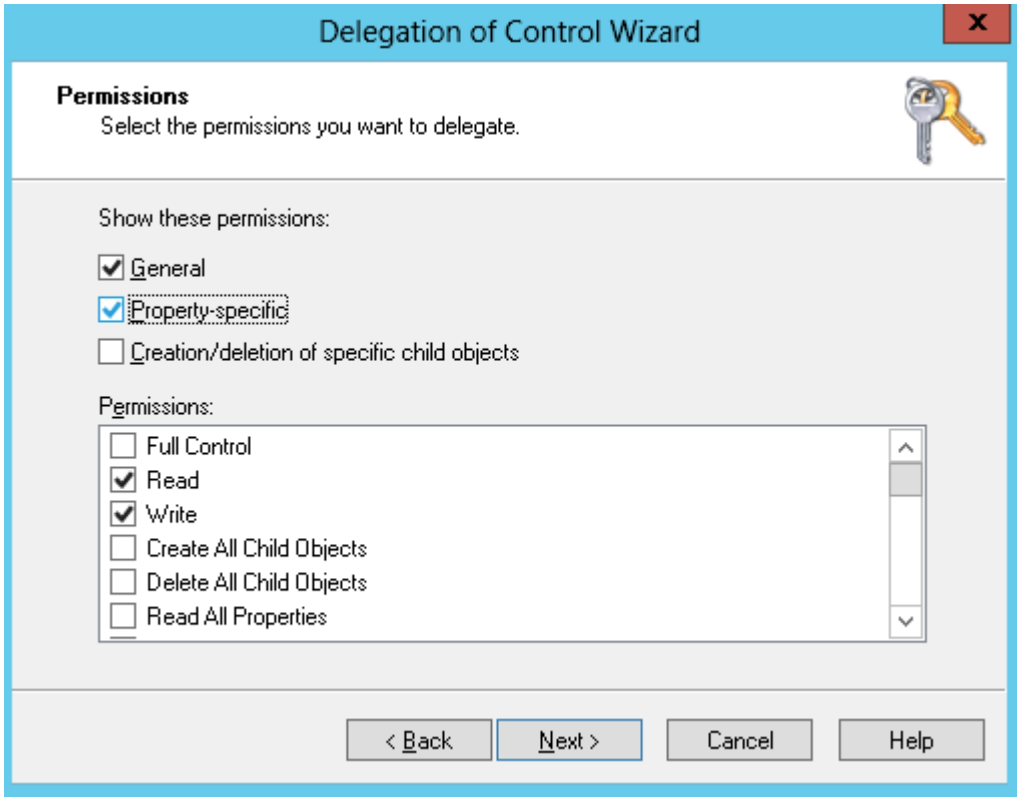
1. Öffnen Sie Active Directory User and Computers und wählen Sie die Organisationseinheit (Organizational Unit – OU) mit Ihrem NetBIOS-Namen in der Navigationsstruktur aus. Klicken Sie dann auf die OU Users.

   > **Important**
   >
   > Wenn Sie einen AWS Directory Service für Microsoft Active Directory starten, AWS wird eine Organisationseinheit (OU) erstellt, die alle Objekte Ihres Verzeichnisses enthält. Diese OU erhält den NetBIOS-Namen, den Sie beim Erstellen des Verzeichnisses eingegeben haben, und befindet sich im Domainstamm. Der Domänenstamm gehört und wird von diesem verwaltet AWS. Am Domainstamm selbst können Sie keine Änderungen vornehmen. Daher müssen Sie die **`Joiners`**-Gruppe in der OU mit Ihrem NetBIOS-Namen erstellen.

2. Öffnen Sie das Kontextmenü (Rechtsklick) für Users, wählen Sie New und dann Group.
3. Geben Sie im Dialogfeld New Object - Group Folgendes ein und klicken Sie auf OK.
   - Geben Sie in Group Name (Gruppenname) **`Joiners`** ein.
   - Wählen Sie für Group scope die Option Global.
   - Wählen Sie für Group type die Option Security.
4. Wählen Sie in der Navigationsstruktur unter Ihrem NetBIOS-Namen den Container Computers aus. Wählen Sie im Menü Action die Option Delegate Control aus.
5. Wählen Sie auf der Seite Delegation of Control Wizard Next und dann Add.
6. Geben Sie in das Dialogfeld Select Users, Computers, or Groups `Joiners` ein und klicken Sie auf OK. Wenn mehr als ein Objekt gefunden wurde, wählen Sie die oben erstellte Gruppe `Joiners`. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Tasks to Delegate Create a custom task to delegate und dann Next.
8. Wählen Sie Only the following objects in the folder und dann Computer objects.
9. Wählen Sie Create selected objects in this folder und Delete selected objects in this folder. Wählen Sie anschließend Weiter.



10. Wählen Sie Read und Write und dann Next.



11. Überprüfen Sie auf der Seite Den Assistenten für die Delegation der Kontrolle abschließen die Informationen und wählen Sie Fertigstellen.
12. Erstellen Sie einen Benutzer mit einem sicheren Passwort und fügen Sie diesen Benutzer zur Gruppe `Joiners` hinzu. Der Benutzer muss unter Ihrem NetBIOS-Namen im Container Users enthalten sein. Der Benutzer hat dann alle nötigen Berechtigungen, um Instances mit dem Verzeichnis zu verbinden.

Erstellen oder ändern Sie einen DHCP-Optionssatz

AWS empfiehlt, dass Sie einen DHCP-Optionssatz für Ihr AWS Directory Service Verzeichnis erstellen und den DHCP-Optionssatz der VPC zuweisen, in der sich Ihr Verzeichnis befindet. So können alle Instances in der entsprechenden VPC auf die angegebene Domain und die festgelegten DNS-Server verweisen, um ihre Domainnamen aufzulösen.

Weitere Informationen zur DHCP-Optionsliste finden Sie unter DHCP-Optionsliste im Amazon-VPC-Benutzerhandbuch.

So erstellen Sie eine DHCP-Optionsliste für Ihr Verzeichnis

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich DHCP Options Sets und anschließend Create DHCP Options Set aus.
3. Geben Sie auf der Seite DHCP-Optionsliste erstellen die folgenden Werte für Ihr Verzeichnis ein:

   Name

   Ein optionales Tag für die Optionsliste

   Domainname

   Den vollständig qualifizierten Namen Ihres Verzeichnisses, z. B. `corp.example.com`

   Domainnamenserver

   Die IP-Adressen der DNS-Server des von Ihnen AWS bereitgestellten Verzeichnisses.

> **Note**
>
> Sie finden diese Adressen, indem Sie im Navigationsbereich der AWS Directory Service -Konsole die Option Verzeichnisse und anschließend die ID des gewünschten Verzeichnisses auswählen.

NTP-Server

Lassen Sie dieses Feld leer.

NetBIOS-Namenserver

Lassen Sie dieses Feld leer.

NetBIOS-Knotentyp

Lassen Sie dieses Feld leer.

4. Wählen Sie Create DHCP Options Set (DHCP-Optionsliste erstellen). Die neue DHCP-Optionsliste wird in der Liste der DHCP-Optionen angezeigt.
5. Notieren Sie sich die ID der neuen DHCP-Optionsliste (dopt-*xxxxxxxx*). Sie verwenden dies, um die neue Optionsliste mit Ihrer VPC zu verknüpfen.

So ändern Sie die DHCP-Optionsliste, die mit einer VPC verknüpft ist

Nach dem Erstellen einer DHCP-Optionsliste sind keine Änderungen an den Optionen mehr möglich. Falls Ihre VPC verschiedene DHCP-Optionslisten nutzen soll, müssen Sie eine neue Liste erstellen und diese dann mit der VPC verknüpfen. Sie können Ihre VPC auch so einrichten, dass keine DHCP-Optionen verwendet werden.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie die VPC aus und klicken Sie dann auf Aktionen, VPC-Einstellungen bearbeiten.
4. Wählen Sie unter DHCP-Optionssatz einen Optionssatz aus oder wählen Sie Kein DHCP-Optionssatz und dann Speichern.

Um den mit einer VPC verknüpften DHCP-Optionssatz über die Befehlszeile zu ändern, gehen Sie wie folgt vor:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Benutzer und Gruppen in AWS Managed Microsoft AD verwalten

„Benutzer“ sind Einzelpersonen oder Entitäten, die Zugriff auf Ihr Verzeichnis haben. Gruppen sind sehr nützlich, um Berechtigungen zu erteilen oder zu verweigern, anstatt diese Berechtigungen für jeden einzelnen Benutzer erstellen zu müssen. Wenn ein Benutzer zu einer anderen Organisation wechselt, verschieben Sie diesen Benutzer in eine andere Gruppe. Er erhält dann automatisch die Berechtigungen für die neue Organisation.

Um Benutzer und Gruppen in einem AWS Directory Service-Verzeichnis zu erstellen, müssen Sie eine beliebige Instance (entweder On-Premises oder EC2) verwenden, die mit Ihrem AWS Directory Service-Verzeichnis verbunden wurde, und als Benutzer angemeldet sein, der die Berechtigung hat, Benutzer und Gruppen zu erstellen. Sie müssen außerdem die Active-Directory-Tools auf Ihrer EC2-Instance installieren, sodass Sie Ihre Benutzer und Gruppen mit dem Active-Directory-Snap-in Benutzer und Computer hinzufügen können.

Sie können eine vorkonfigurierte EC2-Instance mit vorinstallierten Active-Directory-Verwaltungstools von der AWS Directory Service-Managementkonsole aus bereitstellen. Weitere Informationen finden Sie unter Starten Sie die Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory.

Informationen dazu, wie Sie eine selbstverwaltete EC2-Instance mit Verwaltungstools bereitstellen und die erforderlichen Tools installieren müssen, finden Sie unter Schritt 3: Stellen Sie eine Amazon EC2 EC2-Instance bereit, um Ihr AWS verwaltetes Microsoft AD Active Directory zu verwalten.

> **Note**
>
> Für Ihre Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Dies ist die Standardeinstellung für neue Benutzerkonten und sie sollte nicht geändert werden. Weitere Informationen zu dieser Einstellung finden Sie im Microsoft TechNet unter Vorabauthentifizierung.

Im Folgenden erfahren Sie, wie Sie Benutzer und Gruppen erstellen und verwalten.

Themen

- Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD
- Erstellen eines Benutzers
- Löschen eines Benutzers
- Ein Benutzerpasswort zurücksetzen
- Erstellen einer Gruppe
- Hinzufügen eines Benutzers zu einer Gruppe

Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD

Um Ihre Active Directory von einer Amazon EC2 Windows Server-Instance aus zu verwalten, müssen Sie die Active Directory Domain Services and Active Directory Lightweight Directory Services Tools auf der Instance installieren. Verwenden Sie das folgende Verfahren, um diese Tools auf einer EC2 Windows Server-Instance zu installieren.

Voraussetzungen

Bevor Sie mit diesem Verfahren beginnen können, gehen Sie wie folgt vor:

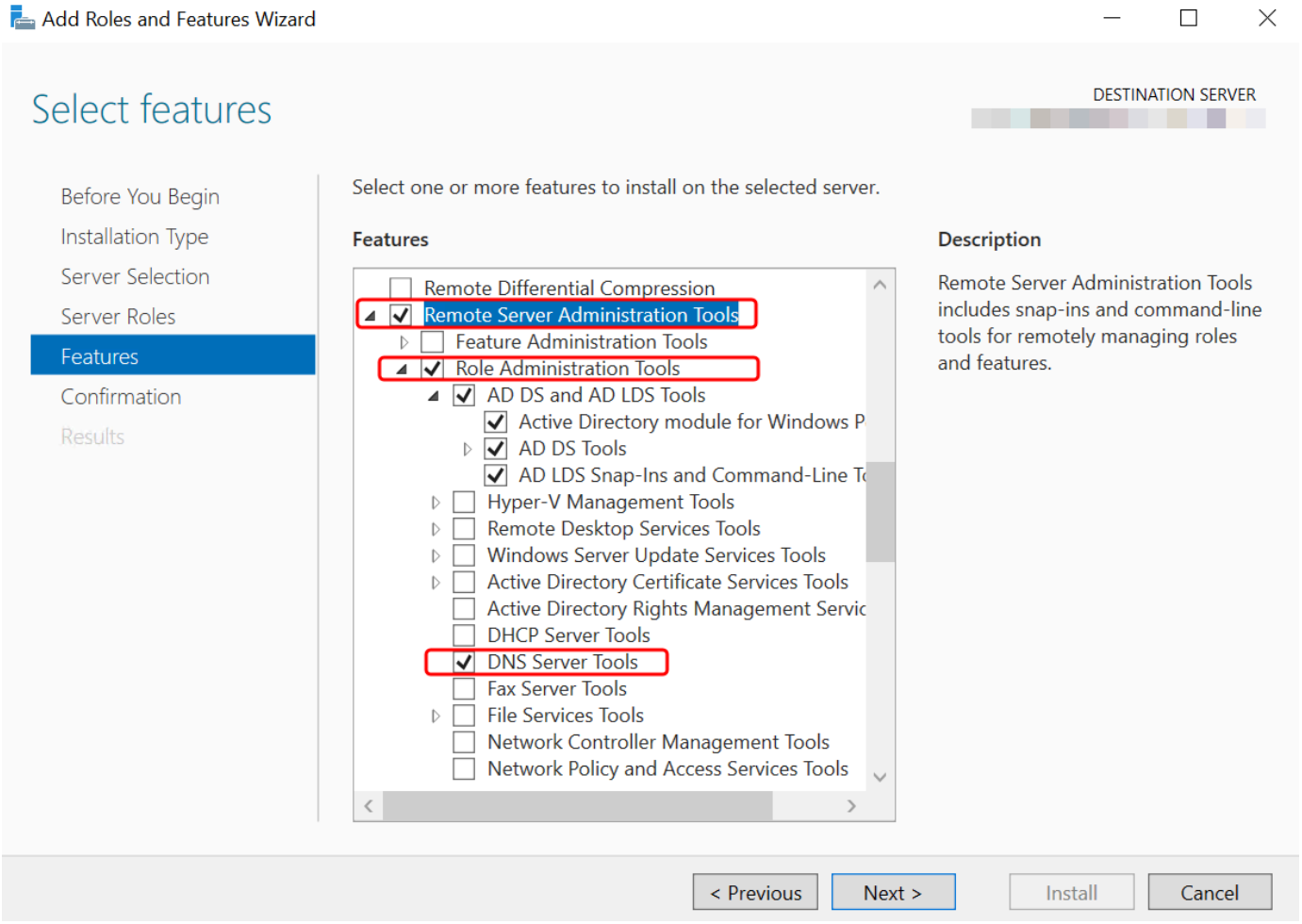
1. Erstellen Sie ein AWS verwaltetes Microsoft ADActive Directory. Weitere Informationen finden Sie unter Erstellen Sie Ihr AWS verwaltetes Microsoft AD.
2. Starten Sie eine EC2 Windows Server-Instance und fügen Sie sie Ihrem AWS verwalteten Microsoft AD Active Directory hinzu. Die EC2-Instance benötigt die folgenden Richtlinien, um Benutzer und Gruppen zu erstellen: **`AWSSSMManagedInstanceCore`** und. **`AmazonSSMDirectoryServiceAccess`** Weitere Informationen finden Sie unter Starten Sie die Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory und Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory.
3. Sie benötigen die Anmeldeinformationen für Ihren Active Directory Domain-Administrator. Diese Anmeldeinformationen wurden erstellt, als das AWS Managed Microsoft AD erstellt wurde. Wenn Sie das Verfahren unter befolgt habenErstellen Sie Ihr AWS verwaltetes Microsoft AD, enthält Ihr Administrator-Benutzername Ihren NetBIOS-Namen,**`corp\admin`**.

Installieren Sie die Active Directory-Verwaltungstools auf der EC2 Windows Server-Instanz

Um die Active Directory-Verwaltungstools auf einer EC2 Windows Server-Instanz zu installieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie in der Amazon-EC2-Konsole die Option Instances, wählen Sie die zuvor erstellte Windows-Server-Instance und wählen Sie dann Verbinden.
3. Wählen Sie auf der Seite Mit Instance verbinden die Option RDP-Client aus.
4. Wählen Sie auf der Registerkarte RDP-Client die Option Remotedesktop-Datei herunterladen und anschließend Passwort abrufen, um Ihr Passwort zu erhalten.
5. Wählen Sie unter Windows-Passwort abrufen die Option Datei mit privatem Schlüssel hochladen aus. Wählen Sie die .pem private Schlüsseldatei, die der Windows-Server-Instance zugeordnet ist. Nachdem Sie die private Schlüsseldatei hochgeladen haben, wählen Sie Passwort entschlüsseln.
6. Kopieren Sie im Dialogfeld Windows-Sicherheit Ihre lokalen Administratoranmeldeinformationen für den Windows Server-Computer, um sich anzumelden. Der Benutzername kann die folgenden Formate haben: ***NetBIOS-Name*****\admin** oder***DNS-Name*****\admin**. Dies **corp\admin** wäre beispielsweise der Benutzername, wenn Sie das Verfahren in befolgen würdenErstellen Sie Ihr AWS verwaltetes Microsoft AD.
7. Nachdem Sie sich bei der Windows Server-Instanz angemeldet haben, öffnen Sie den Server-Manager im Startmenü, indem Sie Server-Manager wählen.
8. Wählen Sie im Server-Manager-Dashboard die Option Rollen und Features hinzufügen.
9. Wählen Sie im Assistent zum Hinzufügen von Rollen und Features die Option Installationstyp und Rollenbasierte oder featurebasierte Installation aus. Klicken Sie dann auf Weiter.
10. Stellen Sie sicher, dass unter Serverauswahl der lokale Server ausgewählt ist. Wählen Sie dann im linken Navigationsbereich Features aus.
11. Wählen und öffnen Sie im Baum Features Remote Server Administration Tools, Role Administration Tools und AD DS und AD LDS Tools. Wenn AD DS- und AD LDS-Tools ausgewählt sind, werden Active DirectoryModul für Windows PowerShell, AD DS-Tools und AD LDS-Snap-Ins und Befehlszeilentools ausgewählt. Scrollen Sie nach unten und wählen Sie DNS Server Tools und dann Weiter.



12. Prüfen Sie die Informationen und klicken Sie auf Installieren. Nach Abschluss der Featureinstallation sind die Tools für Active Directory Domain Services (AD DS) und Active Directory Lightweight Directory Services (AD LDS) vom Startmenü im Ordner Verwaltungstools verfügbar.

Alternative Methoden zur Installation der Active Directory-Verwaltungstools auf einer EC2-Windows-Server-Instanz

- Hier sind einige andere Methoden zur Installation der Active Directory-Verwaltungstools:
  - Sie können optional wählen, ob Sie die Active Directory-Verwaltungstools mithilfe von installieren möchtenWindows PowerShell. Beispielsweise können Sie die Active Directory-Remoteverwaltungstools von einer PowerShell Eingabeaufforderung aus mit installieren`Install-WindowsFeature RSAT-ADDS`. Weitere Informationen finden Sie unter Install- WindowsFeature auf der Microsoft-Website.

- Sie können auch eine EC2-Instanz für die Verzeichnisverwaltung in der Datei starten, auf der bereits AWS Management Console die Active Directory-Domänendienste und die Active Directory Lightweight Directory Services Tools installiert sind, indem Sie die Verfahren unter befolgen. Starten Sie die Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory

Erstellen eines Benutzers

Gehen Sie wie folgt vor, um einen Benutzer mit einer EC2-Instance zu erstellen, die mit Ihrem Verzeichnis in AWS Managed Microsoft AD verbunden ist. Bevor Sie Benutzer erstellen können, müssen Sie die Verfahren unter Installation der Active-Directory-Verwaltungstools abschließen.

Sie können eine der folgenden Methoden verwenden, um einen Benutzer zu erstellen:

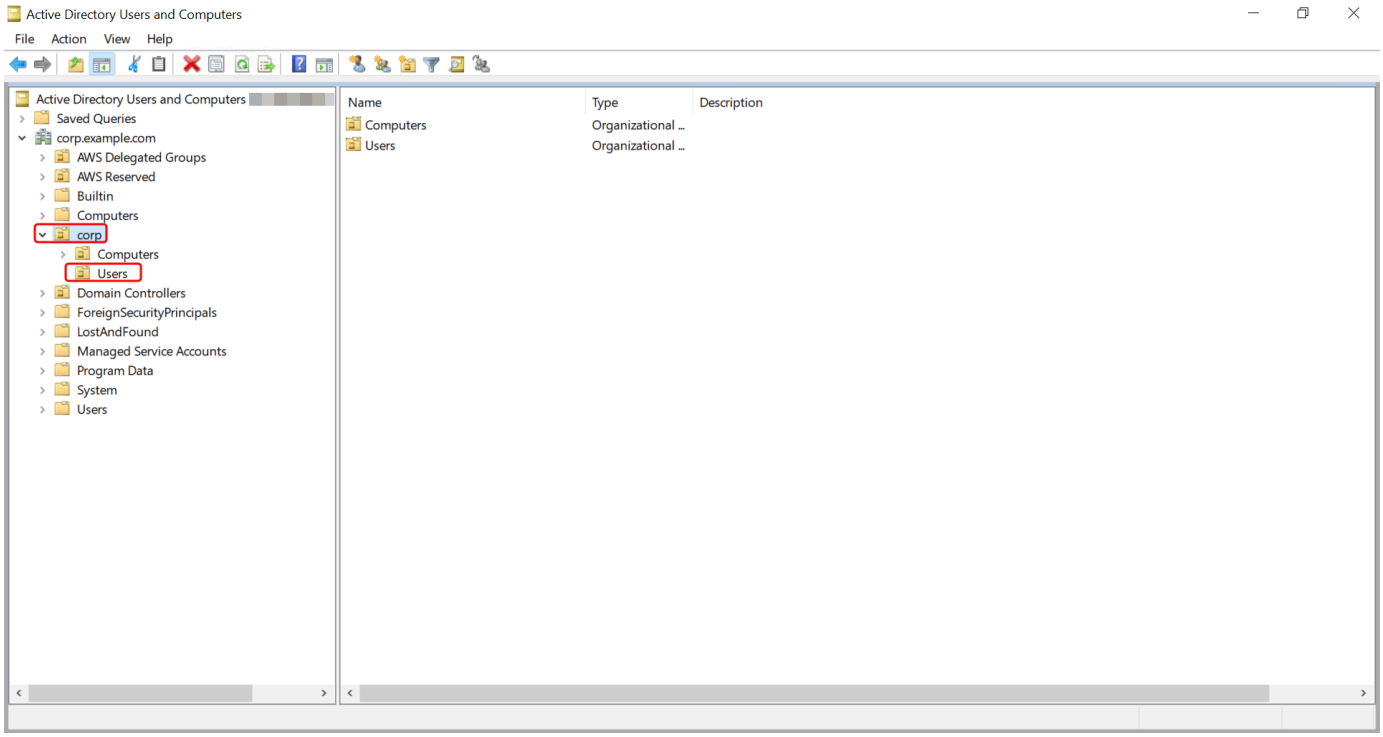
- Active DirectoryVerwaltungstools
- Windows PowerShell

Erstellen Sie einen Benutzer mit den Active Directory Administrationstools

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool „Active Directory-Benutzer und -Computer“ über das Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

   > **Tip**
   >
   > Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Wählen Sie in der Verzeichnisstruktur eine Organisationseinheit unter dem NetBIOS-Namen OU Ihres Verzeichnisses aus, in der Sie Ihren Benutzer speichern möchten (z. B.**`corp\Users`**). Weitere Hinweise zur OU-Struktur, die von den Verzeichnissen in verwendet wird AWS, finden Sie unterWas wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.



4. Wählen Sie im Menü Aktionen die Option Neu und wählen Sie dann Benutzer, um den Assistenten für neue Benutzer zu öffnen.
5. Geben Sie auf der ersten Seite des Assistenten die Werte für die folgenden Felder ein und wählen Sie dann Weiter aus.
   - First name (Vorname)
   - Last name (Nachname)
   - Benutzeranmeldename
6. Geben Sie auf der zweiten Seite des Assistenten für neue Benutzer ein temporäres Passwort in Passwort und Passwort bestätigen ein. Stellen Sie sicher, dass die Option Benutzer muss Passwort bei nächster Anmeldung ändern ausgewählt ist. Keine der anderen Optionen sollte ausgewählt sein. Wählen Sie Weiter aus.
7. Überprüfen Sie auf der dritten Seite des Assistenten, ob die Informationen zum neuen Benutzer richtig sind, und klicken Sie auf Beenden. Der neue Benutzer wird im Ordner Users angezeigt.

Erstellen Sie einen Benutzer in Windows PowerShell

1. Stellen Sie als Active Directory Administrator Connect zu der Instanz her, die mit Ihrer Active Directory Domain verbunden ist.
2. Öffnen Sie Windows PowerShell.

3. Geben Sie den folgenden Befehl ein **`jane.doe`** und ersetzen Sie den Benutzernamen durch den Benutzernamen des Benutzers, den Sie erstellen möchten. Sie werden aufgefordertWindows PowerShell, ein Passwort für den neuen Benutzer einzugeben. Weitere Informationen zu den Anforderungen an die Komplexität von Active Directory Kennwörtern finden Sie in der MicrosoftDokumentation. Weitere Informationen zum Befehl New-ADUser finden Sie in der Dokumentation. Microsoft

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

Löschen eines Benutzers

Gehen Sie wie folgt vor, um einen Benutzer zu löschen, der Ihrem AWS verwalteten Microsoft AD beigetreten istActive Directory.

Sie können eine der folgenden Methoden verwenden, um einen Benutzer zu löschen:

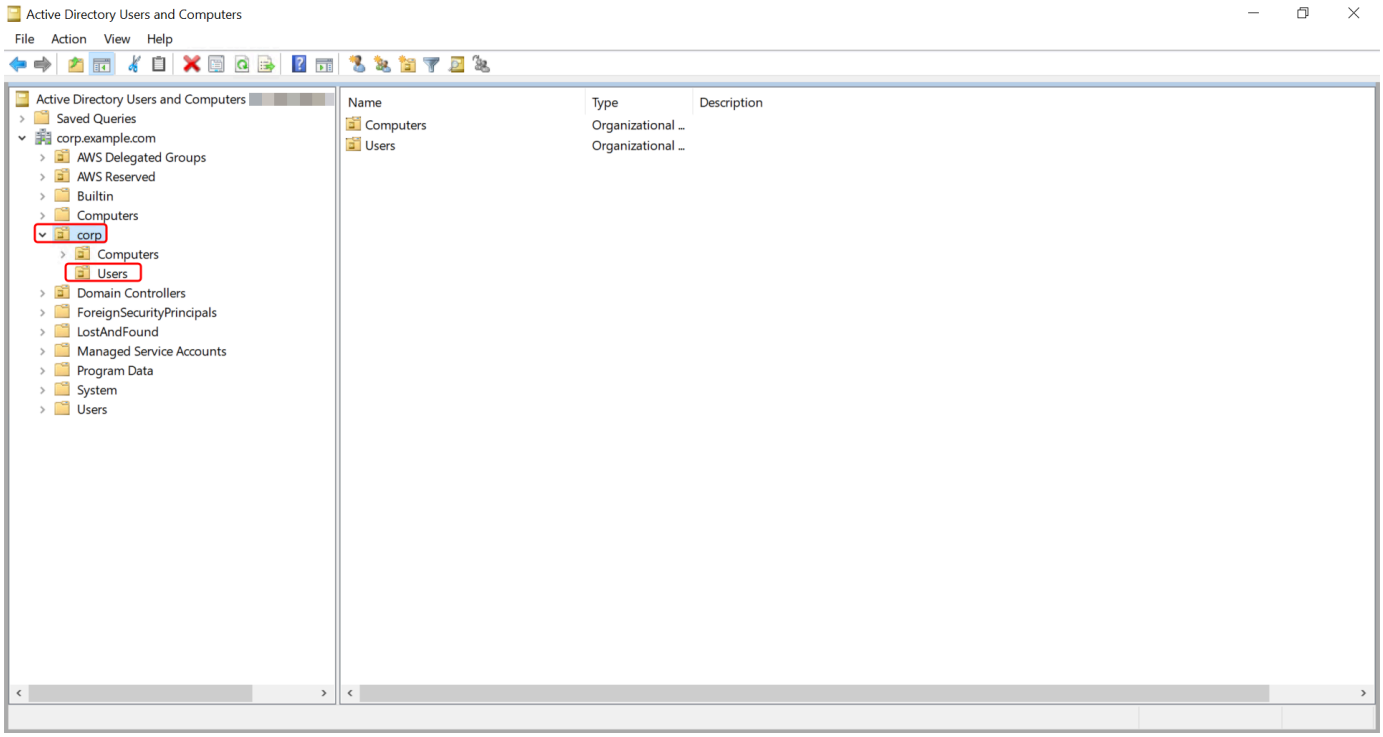
- Active DirectoryVerwaltungstools
- Windows PowerShell

Löschen Sie einen Benutzer mit den Active Directory Administrationstools

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool „Active Directory-Benutzer und -Computer“ über das Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

   > **Tip**
   >
   > Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Wählen Sie in der Verzeichnisstruktur die Organisationseinheit aus, die den Benutzer enthält, den Sie löschen möchten (z. B.**`corp\Users`**).



4. Wählen Sie den Benutzer aus, den Sie löschen möchten. Wählen Sie im Menü Aktionen die Option Löschen.
5. Es erscheint ein Dialogfeld, in dem Sie bestätigen müssen, dass Sie den Benutzer löschen möchten. Wählen Sie Ja, um den Benutzer zu löschen. Dadurch wird der ausgewählte Benutzer dauerhaft gelöscht.

Löschen Sie einen Benutzer in Windows PowerShell

1. Stellen Sie als Active Directory Administrator Connect zu der Instanz her, die mit Ihrer Active Directory Domain verbunden ist.
2. Öffnen Sie Windows PowerShell.
3. Geben Sie den folgenden Befehl ein **`jane.doe`** und ersetzen Sie den Benutzernamen durch den Benutzernamen des Benutzers, den Sie löschen möchten. Weitere Informationen zum Befehl Remove-ADUser finden Sie in der Dokumentation. Microsoft

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

Überlegungen zum AD-Papierkorb

Gelöschte Benutzer werden vorübergehend im AD-Papierkorb gespeichert. Weitere Informationen zum AD-Papierkorb finden Sie unter Der AD-Papierkorb: Grundlegendes, Implementieren, Bewährte Methoden und Problembehandlung im Blog Fragen Sie Microsoft das Directory Services Team.

Ein Benutzerpasswort zurücksetzen

Benutzer müssen sich an die Kennwortrichtlinien halten, wie sie in der definiert sindActive Directory. Manchmal kann dies dazu führen, dass Benutzer, einschließlich des Active Directory Administrators, ihr Passwort vergessen. In diesem Fall können Sie das Benutzerkennwort schnell zurücksetzen, indem Sie angeben, AWS Directory Service ob der Benutzer in AWS Managed Microsoft AD ansässig ist.

Sie müssen als Benutzer mit den erforderlichen Berechtigungen zum Zurücksetzen von Passwörtern angemeldet sein. Weitere Informationen zu Berechtigungen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Directory Service Ressourcen.

Sie können das Passwort für jeden Benutzer in Ihrem Konto zurücksetzen, Active Directory mit den folgenden Ausnahmen:

- Sie können das Passwort für jeden Benutzer innerhalb der Organisationseinheit (OU) zurücksetzen, das auf dem NetBIOS-Namen basiert, den Sie bei der Erstellung Ihres Active Directory verwendet haben. Wenn Sie beispielsweise das Verfahren in Erstellen Sie Ihr AWS verwaltetes Microsoft AD Ihrem NetBIOS-Namen befolgt haben, wäre der Name CORP und die Benutzerkennwörter, die Sie zurücksetzen könnten, wären Mitglieder der Organisationseinheit Corp/Users.
- Sie können das Kennwort eines Benutzers außerhalb der Organisationseinheit nicht zurücksetzen, das auf dem NetBIOS-Namen basiert, den Sie bei der Erstellung Ihres Active Directory verwendet haben. Beispielsweise können Sie das Passwort für einen Benutzer in der AWS reservierten Organisationseinheit nicht zurücksetzen. Weitere Informationen zur OU-Struktur für AWS Managed Microsoft AD finden Sie unterWas wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.

Weitere Informationen darüber, wie die Kennwortrichtlinien angewendet werden, wenn ein Passwort in AWS Managed Microsoft AD zurückgesetzt wird, finden Sie unterWie werden Passwortrichtlinien angewendet.

Sie können eine der folgenden Methoden verwenden, um ein Benutzerkennwort zurückzusetzen:

- AWS Management Console
- AWS CLI
- Windows PowerShell

Setzen Sie ein Benutzerkennwort zurück in AWS Management Console

1. Wählen Sie im Navigationsbereich der AWS Directory Service Konsole unter Active DirectoryVerzeichnisse aus, und wählen Sie dann Active Directory in der Liste das Objekt aus, für das Sie ein Benutzerkennwort zurücksetzen möchten.
2. Wählen Sie auf der Seite Verzeichnisdetails die Option Aktionen und anschließend die Option Benutzerpasswort zurücksetzen.
3. Geben Sie im Dialogfeld Benutzerkennwort zurücksetzen in das Feld Benutzername den Benutzernamen des Benutzers ein, dessen Passwort geändert werden muss.
4. Geben Sie ein Passwort unter Neues Passwort und Passwort bestätigen ein und wählen Sie dann Passwort zurücksetzen.

Setzen Sie ein Benutzerkennwort zurück in AWS CLI

1. Informationen zur AWS CLI Installation von finden Sie unter Installieren oder Aktualisieren der neuesten Version von AWS CLI.
2. Öffnen Sie das AWS CLI.
3. Geben Sie den folgenden Befehl ein und ersetzen Sie die Verzeichnis-ID, den Benutzernamen **`jane.doe`** und das Passwort **`P@ssw0rd`** durch Ihre Active Directory Verzeichnis-ID und die gewünschten Anmeldeinformationen. Weitere Informationen finden Sie reset-user-passwordin der AWS CLI Befehlsreferenz.

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

Setzen Sie ein Benutzerkennwort zurück in Windows PowerShell

1. Stellen Sie als Active Directory Administrator Connect zu der Instanz her, die mit Ihrer Active Directory Domain verbunden ist.
2. Öffnen Sie Windows PowerShell.

3. Geben Sie den folgenden Befehl ein und ersetzen Sie den Benutzernamen**`jane.doe`**, die Verzeichnis-ID und das Passwort **`P@ssw0rd`** durch Ihre Active Directory Verzeichnis-ID und die gewünschten Anmeldeinformationen. Weitere Informationen finden Sie unter UserPassword Reset-DS-Cmdlet.

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

Erstellen einer Gruppe

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe mit einer EC2-Instance zu erstellen, die mit Ihrem Verzeichnis in AWS Managed Microsoft AD verbunden ist. Bevor Sie Sicherheitsgruppen erstellen können, müssen Sie die Verfahren unter Installation der Active-Directory-Verwaltungstools abschließen.

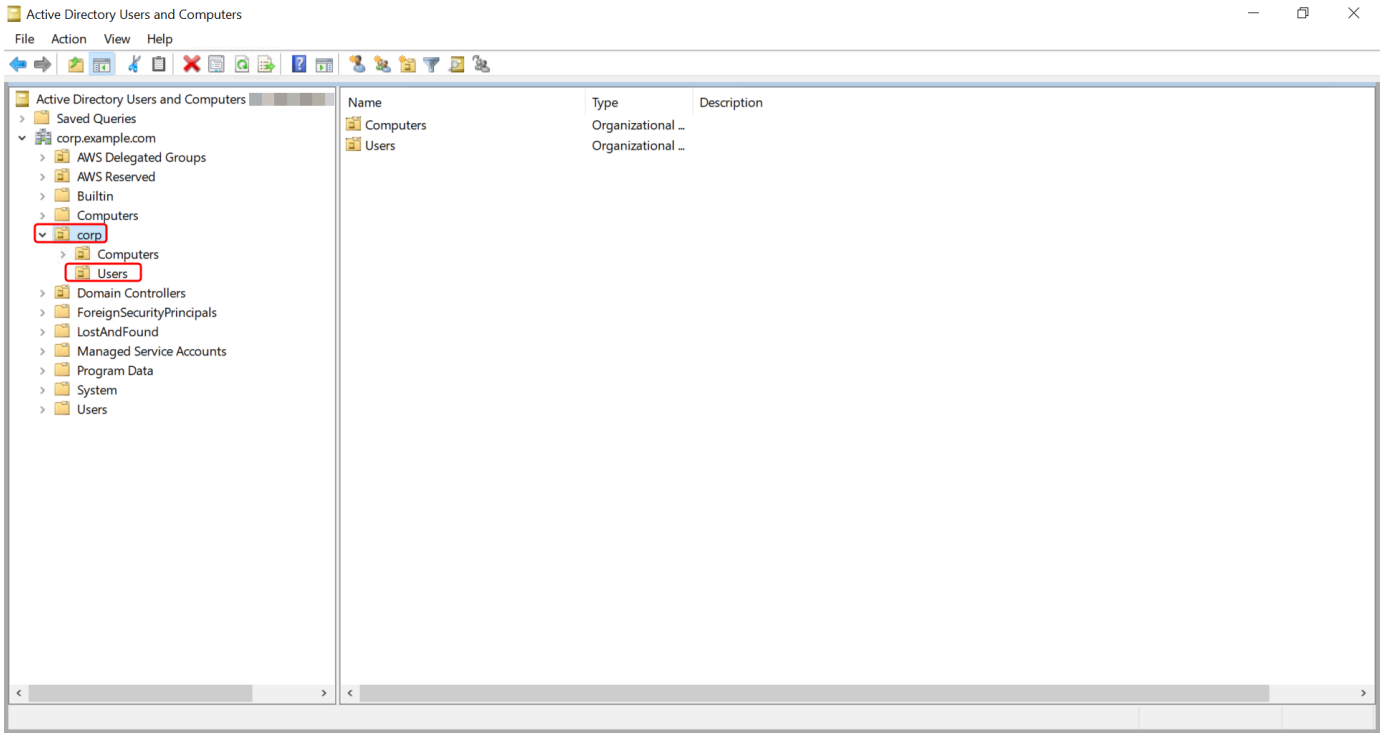
Sie können auch -Windows PowerShellBefehle verwenden, um Gruppen zu erstellen. Weitere Informationen finden Sie unter New-ADGroup in der Windows Server 2022- PowerShell Dokumentation.

So erstellen Sie eine Gruppe

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

   > **Tip**
   >
   > Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Wählen Sie in der Verzeichnisstruktur eine OU unter dem OU-NetBIOS-Namen Ihres Verzeichnisses aus, in der Sie Ihre Gruppe speichern möchten (z. B. Corp\Users). Weitere Informationen zur Organisationseinheitsstruktur, die von Verzeichnissen in verwendet wird AWS, finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.



4. Klicken Sie im MenüAction auf New und dann auf Group, um den Assistenten für neue Gruppen aufzurufen.
5. Geben Sie unter Gruppenname einen Namen für die Gruppe ein, wählen Sie einen Gruppenumfang, der Ihren Anforderungen entspricht, und wählen Sie als Gruppentyp Sicherheit. Weitere Informationen über den Gruppenumfang von Active Directory und Sicherheitsgruppen finden Sie unter Active-Directory-Sicherheitsgruppen in der Microsoft-Windows-Server-Dokumentation.
6. Klicken Sie auf OK. Die neue Sicherheitsgruppe wird im Ordner Benutzer angezeigt.

Hinzufügen eines Benutzers zu einer Gruppe

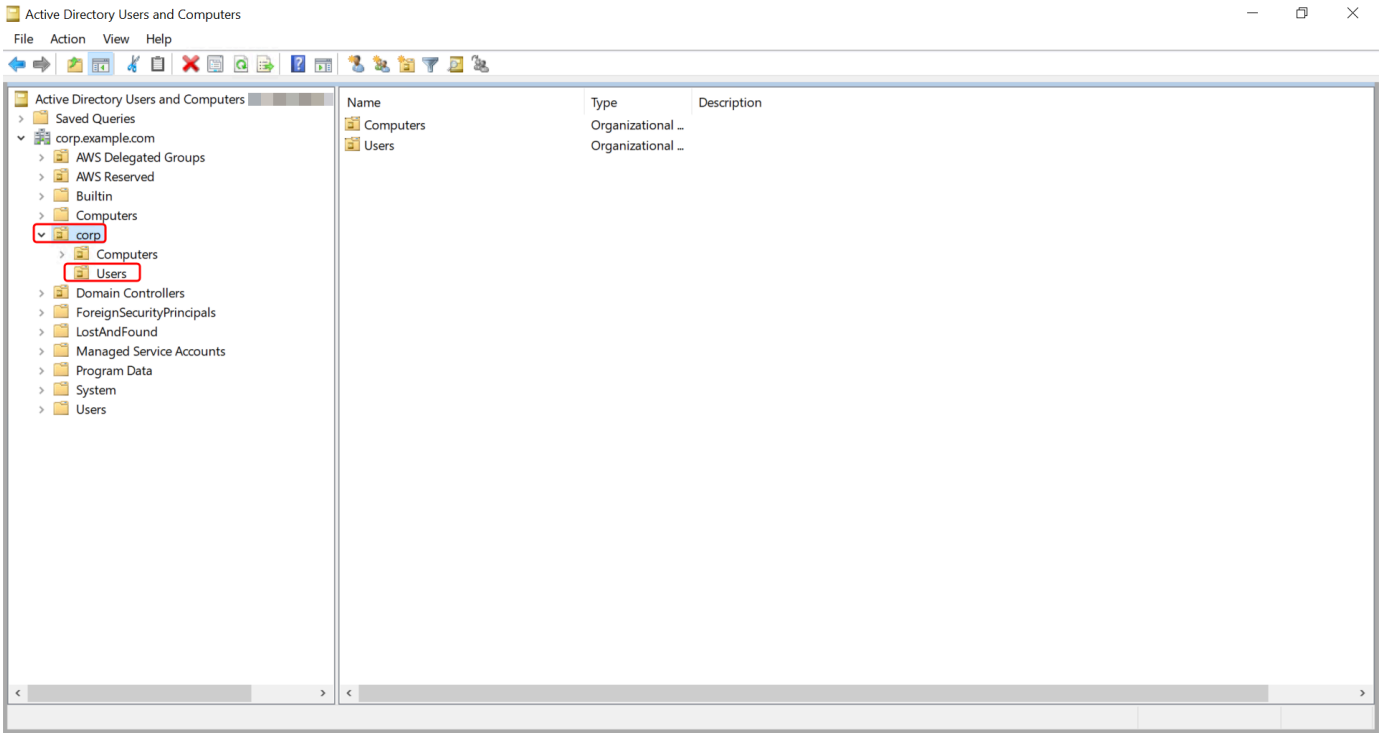
Gehen Sie wie folgt vor, um einen Benutzer zu einer Sicherheitsgruppe mit einer EC2-Instance hinzuzufügen, die mit Ihrem Verzeichnis in AWS Managed Microsoft AD verbunden ist.

So fügen Sie einen neuen Benutzer zu einer Gruppe hinzu

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

> **Tip**
>
> Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Wählen Sie in der Verzeichnisstruktur die OU unter der OU mit dem NetBIOS-Namen Ihres Verzeichnisses aus, in der Sie Ihre Gruppe gespeichert haben, und wählen Sie die Gruppe, der Sie einen Benutzer als Mitglied hinzufügen möchten.



4. Klicken Sie im Menü Aktionen auf Eigenschaften, um das Dialogfeld Eigenschaften für die Gruppe zu öffnen.
5. Wählen Sie die Registerkarte Mitglieder und klicken Sie auf Hinzufügen.
6. Geben Sie unter Geben Sie die zu wählenden Objektnamen ein den Benutzernamen ein, den Sie hinzufügen möchten, und klicken Sie auf OK. Der Name wird in der Mitgliederliste angezeigt. Klicken Sie erneut auf OK, um die Gruppenmitgliedschaft zu aktualisieren.
7. Stellen Sie sicher, dass der Benutzer jetzt Mitglied der Gruppe ist, indem Sie den Benutzer im Ordner Benutzer auswählen und im Aktionsmenü auf Eigenschaften klicken, um das

Eigenschaftendialogfeld zu öffnen. Wählen sie die Registerkarte Mitglied von. Sie sollten den Namen der Gruppe in der Liste der Gruppen sehen, zu der der Benutzer gehört.

Connect zu Ihrer vorhandenen Active Directory-Infrastruktur her

In diesem Abschnitt wird beschrieben, wie Sie Vertrauensbeziehungen zwischen AWS Managed Microsoft AD und Ihrer vorhandenen Active Directory-Infrastruktur konfigurieren.

Themen

Erstellen einer Vertrauensstellung

Sie können ein- und bidirektionale externe Vertrauensstellungen und Gesamtstruktur-Vertrauensstellungen zwischen Ihrem AWS Directory Service für Microsoft Active Directory und selbstverwalteten (lokalen) Verzeichnissen sowie zwischen mehreren AWS verwalteten Microsoft AD-Verzeichnissen in der Cloud konfigurieren. AWS AWS Managed Microsoft AD unterstützt alle drei Richtungen von Vertrauensbeziehungen: Eingehend, Ausgehend und Bidirektional (bidirektional).

Weitere Informationen zur Vertrauensstellung finden Sie unter Alles, was Sie über Vertrauensstellungen mit AWS Managed Microsoft AD wissen wollten.

> **Note**
>
> Beim Einrichten von Vertrauensstellungen müssen Sie sicherstellen, dass Ihr selbstverwaltetes Verzeichnis mit AWS Directory Service s kompatibel ist und bleibt. Weitere Informationen zu Ihren Verantwortlichkeiten finden Sie in unserem Modell für übergreifende Verantwortlichkeit.

AWS Managed Microsoft AD unterstützt sowohl externe als auch Forest-Trusts. Ein Beispielszenario, das Sie durch das Erstellen einer Gesamtstruktur-Vertrauensstellung führt, finden Sie unter Tutorial:

Eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD und Ihrer selbstverwalteten Active-Directory-Domain erstellen.

Für AWS Unternehmens-Apps wie Amazon Chime, Amazon Connect, Amazon, Amazon, Amazon und die ist eine bidirektionale Vertrauensstellung WorkSpaces erforderlich. QuickSight AWS IAM Identity Center WorkDocs WorkMail AWS Management Console AWS Managed Microsoft AD muss in der Lage sein, die Benutzer und Gruppen in Ihrem selbstverwalteten Active Directory System abzufragen.

Amazon EC2, Amazon RDS und Amazon FSx funktionieren entweder mit einer unidirektionalen oder einer bidirektionalen Vertrauensstellung.

Voraussetzungen

Eine Vertrauensstellung zu erstellen erfordert nur wenige Schritte, jedoch müssen Sie vor deren Einrichtung zuerst verschiedene vorbereitende Maßnahmen durchführen.

> **Note**
>
> AWS Managed Microsoft AD unterstützt kein Vertrauen in Single Label Domains.

Verbinden mit der VPC

Wenn Sie eine Vertrauensbeziehung mit Ihrem selbstverwalteten Verzeichnis aufbauen, müssen Sie zuerst Ihr selbstverwaltetes Netzwerk mit der Amazon VPC verbinden, die Ihr AWS verwaltetes Microsoft AD enthält. In der Firewall für Ihre selbstverwalteten und AWS verwalteten Microsoft AD-Netzwerke müssen die Netzwerkports geöffnet sein, die in der Microsoft Dokumentation zu WindowsServer 2008 und späteren Versionen aufgeführt sind.

Um Ihren NetBIOS-Namen anstelle Ihres vollständigen Domainnamens für die Authentifizierung mit Ihren AWS Anwendungen wie Amazon WorkDocs oder Amazon zu verwenden QuickSight, müssen Sie Port 9389 zulassen. Weitere Informationen zu Active Directory-Ports und -Protokollen finden Sie in der Dokumentation unter Serviceübersicht und Netzwerk-Port-Anforderungen für Windows. Microsoft

Das ist das Minimum an notwendigen Ports, um eine Verbindung mit Ihrem Verzeichnis herstellen zu können. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports.

Konfigurieren Ihrer VPC

Die VPC, die Ihr AWS verwaltetes Microsoft AD enthält, muss über die entsprechenden Regeln für ausgehenden und eingehenden Datenverkehr verfügen.

Konfigurieren Ihrer ausgehenden VPC-Regeln

1. Notieren Sie sich in der AWS Directory Service Konsole auf der Seite mit den Verzeichnisdetails Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
3. Wählen Sie Security Groups.
4. Suchen Sie nach Ihrer AWS Managed Microsoft AD-Verzeichnis-ID. Wählen Sie in den Suchergebnissen das Element mit der Beschreibung "Sicherheitsgruppe für Verzeichnis-ID-Verzeichniscontroller AWS erstellt“ aus.

   > **Note**
   >
   > Die ausgewählte Sicherheitsgruppe wird automatisch erzeugt, wenn Sie Ihr Verzeichnis zum ersten Mal erstellen.

5. Wählen Sie die Registerkarte Outbound Rules dieser Sicherheitsgruppe. Wählen Sie Edit und Add another rule. Geben Sie die folgenden Werte für die neue Regel ein:

   - Typ: All Traffic (Gesamter Datenverkehr)
   - Protocol: All (Alle)
   - Die Zieladresse bestimmt den Datenverkehr, der Ihre Domain-Controller verlassen kann, und wohin er in Ihrem selbstverwalteten Netzwerk gesendet werden kann. Geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich in CIDR-Notation an (z. B. 203.0.113.5/32). Sie können auch den Namen oder die ID einer anderen Sicherheitsgruppe in derselben Region angeben. Weitere Informationen finden Sie unter Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut.
6. Wählen Sie Speichern.

Kerberos-Vorabauthentifizierung aktivieren

Auf Ihren Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Weitere Informationen zu dieser Einstellung finden Sie unter Vorauthentifizierung bei Microsoft TechNet.

DNS-bedingte Weiterleitunge in Ihrer selbstverwalteten Domain konfigurieren

Sie müssen DNS bedingte Weiterleitungen auf Ihrer selbstverwalteten Domain einrichten. Einzelheiten zu bedingten Weiterleitungen finden Sie unter Zuweisen einer bedingten Weiterleitung TechNet für einen Domainnamen auf Microsoft.

Um die folgenden Schritte ausführen zu können, benötigen Sie Zugriff auf die folgenden Windows-Server-Tools Ihrer selbstverwalteten Domain:

- AD DS- und AD LDS-Tools
- DNS

So konfigurieren Sie bedingte Weiterleitungen auf Ihre selbstverwaltete Domain

1. Zunächst müssen Sie einige Informationen zu Ihrem AWS Managed Microsoft AD erhalten. Melden Sie sich bei der AWS Management Console an und öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie im Navigationsbereich Directories aus.
3. Wählen Sie die Verzeichnis-ID Ihres AWS Managed Microsoft AD.
4. Notieren Sie sich den vollqualifizierten Domainnamen (FQDN) und die DNS-Adressen Ihres Verzeichnisses.
5. Kehren Sie jetzt zu Ihrem selbstverwalteten Domain-Controller zurück. Öffnen Sie Server Manager.
6. Wählen Sie im Menü Tools den Eintrag DNS.
7. Erweitern Sie in der Konsolenstruktur den DNS-Server der Domain, für die Sie die Vertrauensstellung einrichten.
8. Wählen Sie in der Konsolenbaumstruktur Conditional Forwarders.
9. Wählen Sie im Menü Action den Eintrag New conditional forwarder.
10. Geben Sie unter DNS-Domäne den vollqualifizierten Domänennamen (FQDN) Ihres AWS verwalteten Microsoft AD ein, den Sie zuvor notiert haben.
11. Wählen Sie die IP-Adressen der Primärserver und geben Sie die DNS-Adressen Ihres AWS verwalteten Microsoft AD-Verzeichnisses ein, die Sie zuvor notiert haben.

    Nach der Eingabe der DNS-Adressen ist es möglich, einen "Timeout" oder "nicht lösbar" Fehler zu erhalten. Sie können diese Fehler in der Regel ignorieren.

12. Markieren Sie das Kontrollkästchen Store this conditional forwarder in Active Directory, and replicate as follows: All DNS servers in this domain. Wählen Sie OK aus.

Passwort der Vertrauensstellung

Wenn Sie eine Vertrauensstellung mit einer bestehenden Domain erstellen, können Sie die Domain mit den Windows Server Verwaltungs-Tools dort einrichten. Notieren Sie währenddessen das Passwort, das Sie für die Vertrauensstellung benutzen. Sie müssen dasselbe Passwort verwenden, wenn Sie die Vertrauensbeziehung auf dem AWS Managed Microsoft AD einrichten. Weitere Informationen finden Sie unter Managing Trusts auf Microsoft TechNet.

Sie sind jetzt bereit, die Vertrauensbeziehung in Ihrem AWS Managed Microsoft AD einzurichten.

NetBIOS und Domainnamen

Die NetBIOS- und Domainnamen müssen eindeutig sein und dürfen nicht identisch sein, um eine Vertrauensstellung aufzubauen.

Eine Vertrauensbeziehung erstellen, überprüfen oder löschen

> **Note**
>
> Vertrauensbeziehungen sind eine globale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in Primäre -Region ausgeführt werden. Die Änderungen werden automatisch auf alle replizierten Regionen angewendet. Weitere Informationen finden Sie unter Globale und regionale Features.

Um eine Vertrauensbeziehung mit Ihrem AWS Managed Microsoft AD aufzubauen

1. Öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Verzeichnisse Ihre AWS verwaltete Microsoft AD-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.

4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Option Actions (Aktionen) und dann Add trust relationship (Vertrauensstellung hinzufügen aus.
5. Geben Sie auf der Seite Eine Vertrauensstellung hinzufügen die erforderlichen Informationen ein, einschließlich Vertrauenstyps, des voll ständig qualifizierten Domainnamens (FQDN) Ihrer vertrauenswürdigen Domain, des Vertrauenspassworts und der Richtung der Vertrauensstellung.
6. (Optional) Wenn Sie nur autorisierten Benutzern den Zugriff auf Ressourcen in Ihrem AWS verwalteten Microsoft AD-Verzeichnis ermöglichen möchten, können Sie optional das Kontrollkästchen Selektive Authentifizierung aktivieren. Allgemeine Informationen zur selektiven Authentifizierung finden Sie unter Sicherheitsaspekte für Trusts bei Microsoft TechNet.
7. Geben Sie für Conditional forwarder die IP-Adresse Ihres selbstverwalteten DNS-Servers ein. Wenn Sie zuvor bereits bedingte Weiterleitungen erstellt haben, können Sie den FQDN Ihrer selbstverwalteten Domain anstelle einer DNS IP-Adresse eingeben.
8. (Optional) Wählen Sie Weitere IP-Adresse hinzufügen und geben Sie die IP-Adresse eines zusätzlichen selbstverwalteten DNS-Servers ein. Sie können diesen Schritt für jede anzuwendende DNS Server-Adresse bis zu insgesamt vier Adressen wiederholen.
9. Wählen Sie Hinzufügen aus.
10. Wenn der DNS-Server oder das Netzwerk Ihrer selbstverwalteten Domain einer öffentlichen IP-Adressumgebung (nicht RFC 1918) verwendet, wählen Sie die Registerkarte IP-Routing, Aktionen und dann Route hinzufügen aus. Geben Sie den IP-Adressblock Ihres DNS-Servers oder selbstverwalteten Netzwerks im CIDR-Format ein, z. B. 203.0.113.0/24. Dieser Schritt ist nicht erforderlich, wenn Ihr DNS-Server und Ihr selbstverwaltetes Netzwerk RFC 1918 IP-Adressumgebungen verwenden.

    > **Note**
    >
    > Wenn Sie eine öffentlichen IP-Adressumgebung verwenden, stellen Sie sicher, dass Sie keine der AWS -IP-Adressbereiche verwenden, da diese nicht genutzt werden können.

11. (Optional) Wir empfehlen, dass Sie auf der Seite Add routes (Routen hinzufügen) auch Add routes to the security group for this directory's VPC (Routen zur Sicherheitsgruppe für die VPC dieses Verzeichnisses hinzufügen) auswählen. So konfigurieren Sie die Sicherheitsgruppen wie oben unter „Konfigurieren Ihrer VPC” beschrieben. Diese Sicherheitsregeln betreffen eine interne Netzwerkschnittstelle, die nicht öffentlich zugänglich ist. Wenn diese Option nicht verfügbar ist, wird stattdessen eine Meldung angezeigt, dass Sie Ihre Sicherheitsgruppen bereits angepasst haben.

Sie müssen die Vertrauensstellung auf beiden Domains einrichten. Die Stellungen müssen wechselseitig sein. Wenn Sie beispielsweise eine ausgehende Vertrauensstellung in einer Domain erstellen, benötigen Sie auf der anderen eine eingehende.

Wenn Sie eine Vertrauensstellung mit einer bestehenden Domain erstellen, können Sie die Domain mit den Windows Server Verwaltungs-Tools dort einrichten.

Sie können mehrere Vertrauensstellungen zwischen Ihrem AWS verwalteten Microsoft AD und verschiedenen Active Directory-Domänen einrichten. Jedoch kann zeitgleich nur eine Vertrauensstellung pro Paar bestehen. Wenn Sie beispielsweise über eine bestehende, einseitige Vertrauensstellung in „Eingehender Richtung" verfügen und dann eine weitere „Ausgehender Richtung" einrichten möchten, müssen Sie die bestehende Vertrauensstellung löschen und eine neue „wechselseitige" erstellen.

Um eine ausgehende Vertrauensstellung zu überprüfen:

1. Öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Verzeichnisse Ihre AWS verwaltete Microsoft AD-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Vertrauensstellung aus, die Sie überprüfen möchten, dann Actions (Aktionen) und schließlich Verify trust relationship (Vertrauensstellung überprüfen).

Bei diesem Vorgang wird nur die ausgehende Richtung einer bidirektionalen Vertrauensstellung überprüft. AWS unterstützt nicht die Überprüfung eingehender Trusts. Weitere Informationen dazu, wie Sie eine Vertrauensstellung zu oder von Ihrem selbstverwalteten Active Directory überprüfen können, finden Sie unter Verify a Trust on Microsoft TechNet.

Um eine bestehende Vertrauensstellung zu löschen:

1. Öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Verzeichnisse Ihre AWS verwaltete Microsoft AD-ID aus.

3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.

4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Beziehung aus, die Sie löschen möchten, dann Actions (Aktionen) und schließlich Delete trust relationship (Vertrauensstellung löschen).
5. Wählen Sie Löschen.

Hinzufügen von IP-Routen bei der Verwendung von öffentlichen IP-Adressen

Mit AWS Directory Service für Microsoft Active Directory können Sie die vielen leistungsstarken Active-Directory-Features nutzen, wie beispielsweise die Einrichtung von Vertrauensstellungen mit anderen Verzeichnissen. Wenn die DNS-Server für die Netzwerke der anderen Verzeichnisse jedoch öffentliche (nicht RFC 1918) IP-Adressen verwenden, müssen Sie diese IP-Adressen als Teil der Konfiguration der Vertrauensstellung angeben. Anweisungen hierzu finden Sie unter Erstellen einer Vertrauensstellung.

In ähnlicher Weise müssen Sie auch die Information der IP-Adresse eingeben, wenn Sie Datenverkehr aus Ihrem AWS Managed Microsoft AD auf AWS zu einer gleichgestellten AWS-VPC routen. Das gilt für den Fall, dass die VPC öffentliche IP-Bereiche verwendet.

Wenn Sie die IP-Adressen wie in Erstellen einer Vertrauensstellung beschrieben hinzufügen, haben Sie die Option, Add routes to the security group for this directory's VPC auszuwählen. Diese Option sollte gewählt werden, es sei denn, Sie haben Ihre Sicherheitsgruppe vorher so angepasst, dass sie den erforderlichen Datenverkehr wie unten dargestellt erlaubt. Weitere Informationen finden Sie unter Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut.

Tutorial: Eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD und Ihrer selbstverwalteten Active-Directory-Domain erstellen

Dieses Tutorial führt Sie durch alle notwendigen Schritte, um eine Vertrauensstellung zwischen dem AWS Directory Service für Microsoft Active Directory und Ihrem selbstverwalteten (On-Premises)

Microsoft Active Directory einzurichten. Eine Vertrauensstellung zu erstellen, erfordert nur wenige Schritte, jedoch müssen Sie zuerst die folgenden vorbereitenden Schritte ausführen.

Themen

Weitere Informationen finden Sie auch unter:

Erstellen einer Vertrauensstellung

Voraussetzungen

In dieser praktischen Anleitung wird davon ausgegangen, dass Sie bereits über folgende Elemente verfügen:

> **Note**
>
> AWS Managed Microsoft AD unterstützt keine Vertrauensstellung mit Single Label Domain.

- So erstellen Sie ein Verzeichnis in AWS Managed Microsoft AD in AWS. Weitere Informationen hierzu finden Sie unter Erste Schritte mit AWS Managed Microsoft AD.
- Eine EC2-Instance, in der Windows ausgeführt wird und die diesem AWS Managed Microsoft AD hinzugefügt wurde. Weitere Informationen hierzu finden Sie unter Manuelles Verbinden einer Amazon EC2 Windows EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory.

  > **Important**
  >
  > Das Administratorkonto für Ihr AWS Managed Microsoft AD muss Administratorzugriff auf diese Instance haben.

- Folgende Windows Server-Tools müssen in der Instance installiert sein:
  - AD DS- und AD LDS-Tools
  - DNS

Weitere Informationen hierzu finden Sie unter Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD.

- Ein selbstverwaltetes (On-Premises) Microsoft Active Directory

  Sie müssen Administratorzugriff auf dieses Verzeichnis haben. Für dieses Verzeichnis müssen ebenfalls die oben genannten Windows Server-Tools verfügbar sein.

- Eine aktive Verbindung zwischen Ihrem selbstverwalteten Netzwerk und der VPC, die Ihr AWS Managed Microsoft AD enthält. Weitere Informationen hierzu finden Sie im Bereich mit den Konnektivitätsoptionen für Amazon Virtual Private Cloud.
- Eine korrekt eingestellte lokale Sicherheitsrichtlinie. Überprüfen Sie `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` und stellen Sie sicher, dass sie mindestens die drei folgenden benannten Pipes enthält:
  - netlogon
  - samr
  - lsarpc
- Der NetBIOS- und der Domainname müssen eindeutig sein und dürfen nicht identisch sein, um eine Vertrauensstellung aufzubauen

Weitere Informationen über die Voraussetzungen für die Einrichtung einer Vertrauensstellung finden Sie unter Erstellen einer Vertrauensstellung.

Praktische Anleitung zur Konfiguration

Für dieses Tutorial haben wir bereits ein AWS Managed Microsoft AD und eine selbstverwaltete Domain erstellt. Das selbstverwaltete Netzwerk ist mit der VPC von AWS Managed Microsoft AD verbunden. Im Folgenden sehen Sie die Eigenschaften der beiden Verzeichnisse:

AWS Managed Microsoft AD, das in AWS ausgeführt wird

- Domainname (FQDN): MyManagedAD.example.com
- NetBIOS-Name: MyManagedAD
- DNS-Adressen: 10.0.10.246, 10.0.20.121
- VPC-CIDR: 10.0.0.0/16

AWS Managed Microsoft AD befindet sich in der VPC-ID: vpc-12345678.

Selbstverwaltete oder AWS-Managed-Microsoft-AD-Domain

- Domainname (FQDN): corp.example.com
- NetBIOS-Name: CORP
- DNS-Adressen: 172.16.10.153
- Selbstverwaltetes CIDR: 172.16.0.0/16

Nächster Schritt

Schritt 1: Selbstverwaltete AD-Domain vorbereiten

Schritt 1: Selbstverwaltete AD-Domain vorbereiten

Zunächst müssen Sie auf Ihrer selbstverwalteten (On-Premises)-Domain einige voraussetzende Schritte durchführen.

Selbstverwaltete Firewall konfigurieren

Sie müssen Ihre selbstverwaltete Firewall so konfigurieren, dass die folgenden Ports für die CIDRs für alle Subnetze geöffnet sind, die von der VPC verwendet werden, die Ihr AWS verwaltetes Microsoft AD enthält. In diesem Tutorial lassen wir sowohl eingehenden als auch ausgehenden Datenverkehr von 10.0.0.0/16 (dem CIDR-Block unserer AWS verwalteten Microsoft AD-VPC) an den folgenden Ports zu:

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos-Authentifizierung
- TCP/UDP 389 — Lightweight Directory Access Protocol (LDAP)
- TCP 445 — Server-Nachrichtenblock (SMB)
- TCP 9389 — Active Directory Web Services (ADWS) (Optional — Dieser Port muss geöffnet sein, wenn Sie Ihren NetBIOS-Namen anstelle Ihres vollständigen Domainnamens für die Authentifizierung mit AWS Anwendungen wie Amazon WorkDocs oder Amazon verwenden möchten.) QuickSight

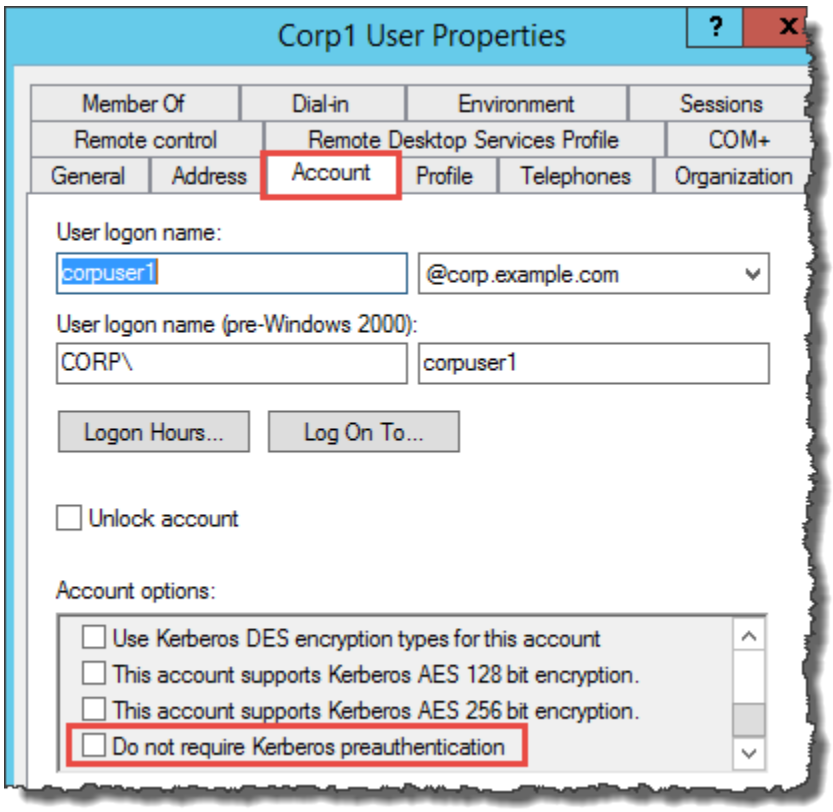
> **Note**
>
> SMBv1 wird nicht mehr unterstützt.
> Dies sind die minimalen Ports, die für die Verbindung der VPC mit dem selbstverwalteten Verzeichnis notwendig sind. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports.

Sicherstellen, dass Kerberos-Vorauthentifizierung aktiviert ist

Benutzerkonten in beiden Verzeichnissen müssen Kerberos Vorauthentifizierung aktiviert haben. Dies ist die Standardeinstellung. Wir überprüfen allerdings die Eigenschaften eines beliebigen Benutzers, um sicherzustellen, dass nichts geändert ist.

Um die Kerberos-Einstellungen eines Benutzers anzuzeigen

1. Öffnen Sie Server Manager auf Ihrem selbstverwalteten Domain-Controller.
2. Wählen Sie im Menü Tools den Eintrag Active Directory Users and Computers.
3. Wählen Sie den Ordner Users (Benutzer) und öffnen Sie das Kontextmenü (rechte Maustaste). Wählen Sie im rechten Bereich ein beliebiges Benutzerkonto aus. Wählen Sie Properties (Eigenschaften).
4. Wählen Sie die Registerkarte Account. Scrollen Sie in der Liste Account options nach unten und stellen Sie sicher, dass Do not require Kerberos preauthentication nicht ausgewählt ist.



DNS-bedingte Weiterleitungen für Ihre selbstverwaltete Domain konfigurieren

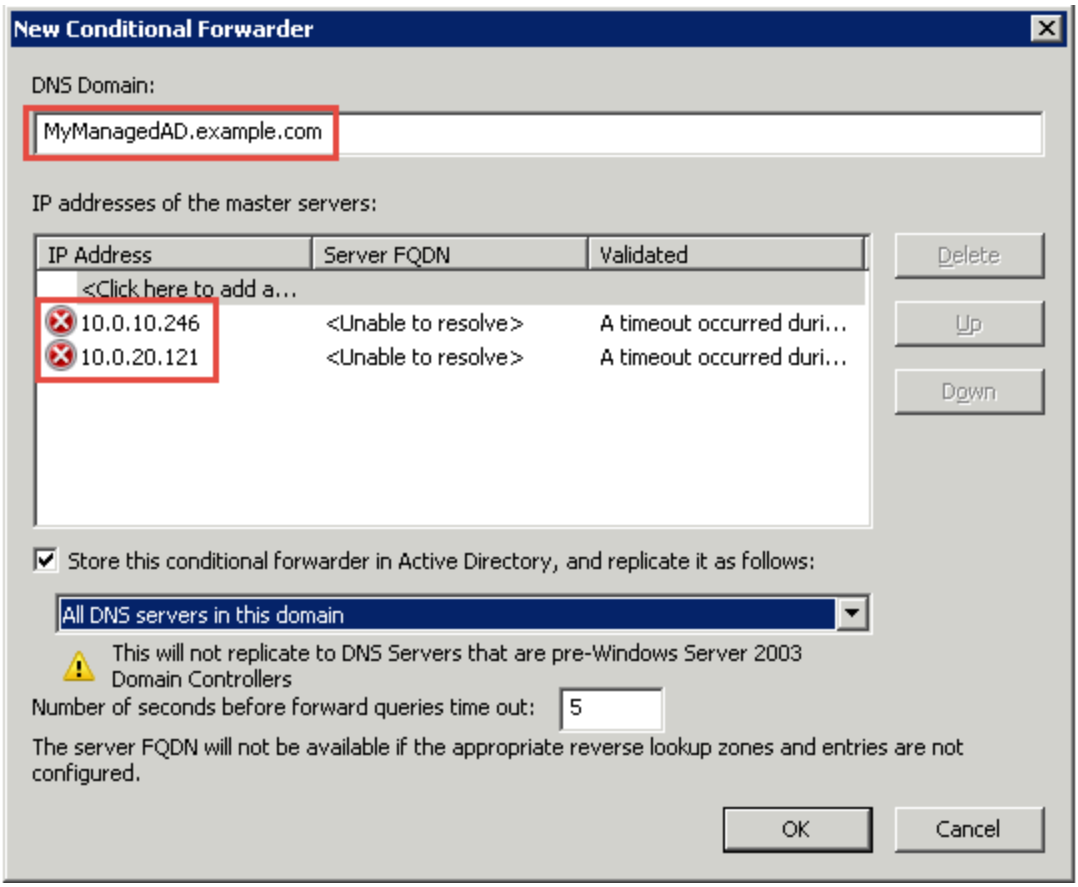
Sie müssen DNS-bedingte Weiterleitungen auf jeder Domain einrichten. Bevor Sie dies auf Ihrer selbstverwalteten Domain tun, erhalten Sie zunächst einige Informationen zu Ihrem AWS verwalteten Microsoft AD.

So konfigurieren Sie bedingte Weiterleitungen auf Ihre selbstverwaltete Domain

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Directory Service Konsole.
2. Wählen Sie im Navigationsbereich Directories aus.
3. Wählen Sie die Verzeichnis-ID Ihres AWS Managed Microsoft AD.
4. Notieren Sie sich auf der Seite Details die Werte in Directory name (Verzeichnisname) und die DNS address (DNS-Adresse) Ihres Verzeichnisses.
5. Kehren Sie jetzt zu Ihrem selbstverwalteten Domain-Controller zurück. Öffnen Sie Server Manager.
6. Wählen Sie im Menü Tools den Eintrag DNS.

7. Erweitern Sie in der Konsolenstruktur den DNS-Server der Domain, für die Sie die Vertrauensstellung einrichten. Unser Server ist WIN-5V70CN7VJ0.corp.example.com.
8. Wählen Sie in der Konsolenbaumstruktur Conditional Forwarders.
9. Wählen Sie im Menü Action den Eintrag New conditional forwarder.
10. Geben Sie unter DNS-Domäne den vollqualifizierten Domänennamen (FQDN) Ihres AWS verwalteten Microsoft AD ein, den Sie zuvor notiert haben. In diesem Beispiel lautet MyManaged der FQDN AD.Example.com.
11. Wählen Sie die IP-Adressen der Primärserver und geben Sie die DNS-Adressen Ihres AWS verwalteten Microsoft AD-Verzeichnisses ein, die Sie zuvor notiert haben. In diesem Beispiel sind dies: 10.0.10.246, 10.0.20.121

    Nach der Eingabe der DNS-Adressen ist es möglich, einen "Timeout" oder "nicht lösbar" Fehler zu erhalten. Sie können diese Fehler in der Regel ignorieren.



12. Markieren Sie das Kontrollkästchen Store this conditional forwarder in Active Directory, and replicate it as follows.
13. Wählen Sie All DNS servers in this domain und dann OK.

Nächster Schritt

Schritt 2: Ihr AWS Managed Microsoft AD vorbereiten

Schritt 2: Ihr AWS Managed Microsoft AD vorbereiten

Lassen Sie uns nun Ihr AWS Managed Microsoft AD für die Vertrauensbeziehung vorbereiten. Viele der folgenden Schritte sind fast identisch mit dem, was Sie gerade bei Ihrer selbstverwalteten Domain gemacht haben. Diesmal arbeiten Sie jedoch mit Ihrem AWS Managed Microsoft AD.

Ihre VPC-Subnetze und Sicherheitsgruppen konfigurieren

Sie müssen Datenverkehr von Ihrem selbstverwalteten Netzwerk zur VPC zulassen, die Ihr AWS verwaltetes Microsoft AD enthält. Dazu müssen Sie sicherstellen, dass die ACLs, die den Subnetzen zugeordnet sind, die für die Bereitstellung Ihres AWS verwalteten Microsoft AD verwendet werden, und die auf Ihren Domänencontrollern konfigurierten Sicherheitsgruppenregeln den erforderlichen Datenverkehr zur Unterstützung von Vertrauensstellungen zulassen.

Die Portanforderungen variieren je nach der Version von Windows Server, die von Ihren Domain-Controllern, den Services und den Anwendungen verwendet wird, die die Vertrauensstellung nutzen. Für dieses Tutorial müssen Sie folgende Ports öffnen:

Eingehend

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos-Authentifizierung
- UDP 123 – NTP
- TCP 135 – RPC
- TCP/UDP 389 – LDAP
- TCP/UDP 445 – SMB
- TCP/UDP 464 – Kerberos-Authentifizierung
- TCP 636 - LDAPS (LDAP über TLS/SSL)
- TCP 3268-3269 – Globaler Katalog
- TCP/UDP 49152-65535 – Flüchtige Ports für RPC

> **Note**
>
> SMBv1 wird nicht mehr unterstützt.

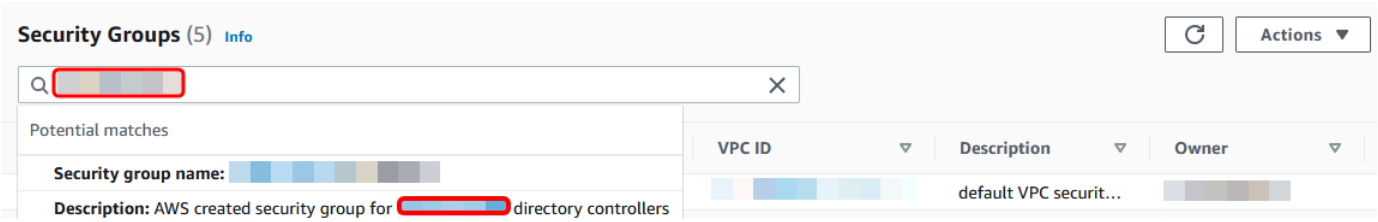
Ausgehend

- ALL

> **Note**
>
> Dies sind die minimalen Ports, die benötigt werden, um eine Verbindung zwischen der VPC und dem selbstverwalteten Verzeichnis herstellen zu können. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports.

So konfigurieren Sie ausgehende und eingehende Regeln für Ihren AWS verwalteten Microsoft AD-Domänencontroller

1. Kehren Sie zur AWS Directory Service -Konsole zurück. Notieren Sie sich in der Verzeichnisliste die Verzeichnis-ID für Ihr AWS verwaltetes Microsoft AD-Verzeichnis.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
3. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
4. Verwenden Sie das Suchfeld, um nach Ihrer AWS verwalteten Microsoft AD-Verzeichnis-ID zu suchen. Wählen Sie in den Suchergebnissen die Sicherheitsgruppe mit der Beschreibung aus**`AWS created security group for yourdirectoryID directory controllers`**.

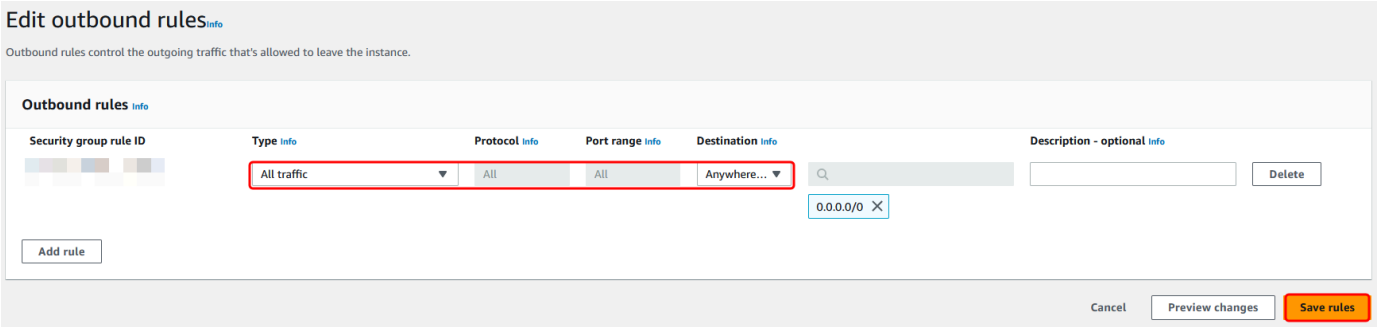


5. Wählen Sie die Registerkarte Outbound Rules dieser Sicherheitsgruppe. Wählen Sie Ausgehende Regeln bearbeiten und dann Regel hinzufügen. Geben Sie die folgenden Werte für die neue Regel ein:

   - Typ: ALL Traffic (GESAMTER Datenverkehr)

- Protocol: ALL (Alle)
- Destination bestimmt den Datenverkehr, der Ihre Domain-Controller verlassen kann, und wohin er gesendet werden kann. Geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich in CIDR-Notation an (z. B. 203.0.113.5/32). Sie können auch den Namen oder die ID einer anderen Sicherheitsgruppe in derselben Region angeben. Weitere Informationen finden Sie unter Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut.

6. Wählen Sie Regel speichern aus.



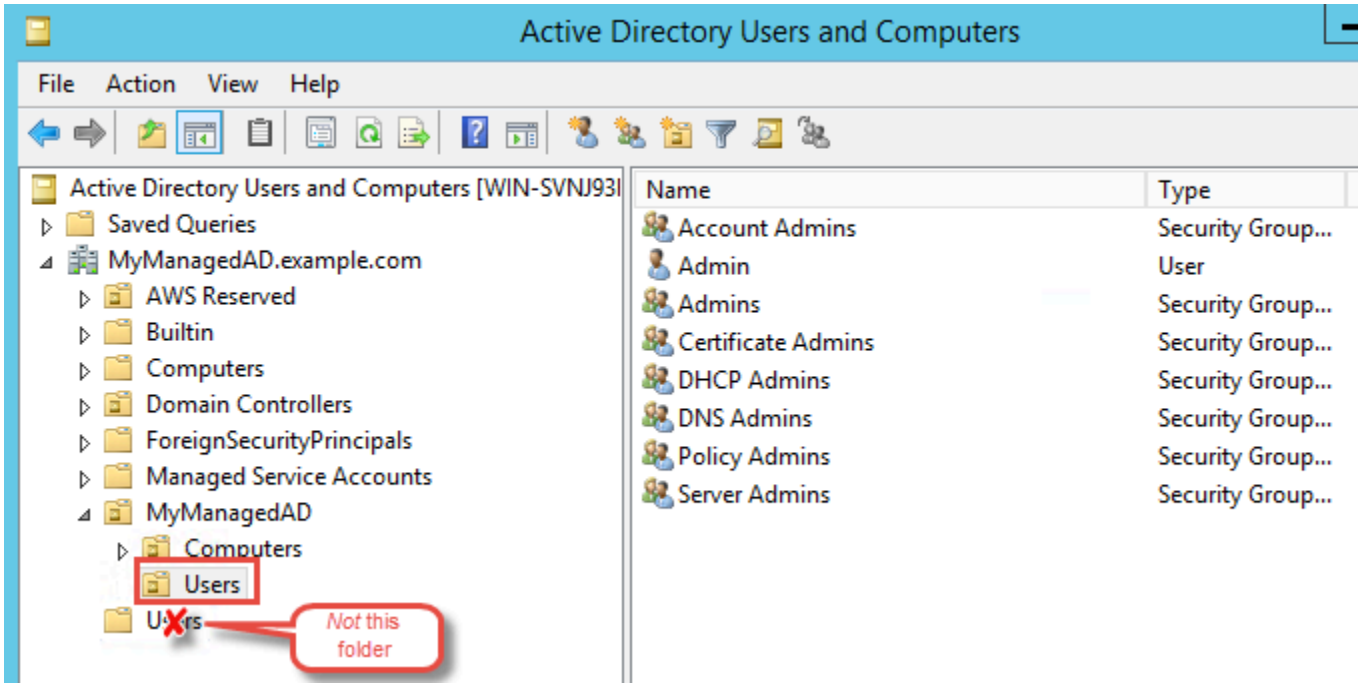
Sicherstellen, dass Kerberos-Vorauthentifizierung aktiviert ist

Jetzt möchten Sie sicherstellen, dass für Benutzer in Ihrem AWS Managed Microsoft AD auch die Kerberos-Vorauthentifizierung aktiviert ist. Dies ist derselbe Vorgang, den Sie für Ihr selbstverwaltetes Verzeichnis durchgeführt haben. Dies ist die Standardeinstellung, die jedoch noch einmal überprüft werden sollte, um sicherzustellen, dass nichts geändert ist.

So zeigen Sie Benutzer-Kerberos-Einstellungen an

1. Melden Sie sich bei einer Instanz an, die Mitglied Ihres AWS verwalteten Microsoft AD-Verzeichnisses ist, indem Sie entweder das Berechtigungen für das Administratorkonto für die Domäne oder ein Konto verwenden, dem Berechtigungen zur Verwaltung von Benutzern in der Domäne delegiert wurden.
2. Wenn sie nicht bereits installiert sind, installieren Sie das Active Directory-Benutzer- und -Computer-Tool und das DNS-Tool. Erfahren Sie, wie Sie diese Tools installieren, in Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD.
3. Öffnen Sie Server Manager. Wählen Sie im Menü Tools den Eintrag Active Directory Users and Computers.

4. Wählen Sie den Ordner Users in Ihrer Domain. Beachten Sie, dass es sich hierbei um den Ordner Users (Benutzer) unter Ihrem NetBIOS-Namen handelt, nicht um den Ordner Users (Benutzer) unter dem vollständig qualifizierten Domainnamen (FQDN).



5. Klicken Sie in der Liste der Benutzer mit der rechten Maustaste auf einen Benutzer, und klicken Sie dann auf Properties (Eigenschaften).
6. Wählen Sie die Registerkarte Account. Stellen Sie in der Liste Account options sicher, dass Do not require Kerberos preauthentication nicht ausgewählt ist.

Nächster Schritt

Schritt 3: Eine Vertrauensstellung einrichten

Schritt 3: Eine Vertrauensstellung einrichten

Da die Vorbereitungen jetzt abgeschlossen sind, können Sie die Vertrauensstellungen herstellen. Zuerst erstellen Sie die Vertrauensstellung in Ihrer selbstverwalteten Domain und dann schließlich in AWS Managed Microsoft AD. Wenn während der Erstellung von Vertrauensstellungen Probleme auftreten, finden Sie weitere Informationen unter Gründe für den Status der Vertrauensstellung.

Konfigurieren Sie die Vertrauensstellung in Ihrem selbstverwalteten Active Directory

Mithilfe dieses Tutorials können Sie eine bidirektionale Gesamtstruktur-Vertrauensstellung konfigurieren. Wenn Sie eine unidirektionale Gesamtstruktur-Vertrauensstellung nutzen möchten,

müssen Sie darauf achten, dass sich die Richtungen für die einzelnen Domains ergänzen. Wenn Sie beispielsweise auf Ihrer selbstverwalteten Domain eine ausgehende unidirektionale Vertrauensstellung erstellen, benötigen Sie auf AWS Managed Microsoft AD eine eingehende.

> **Note**
>
> AWS Managed Microsoft AD unterstützt auch externe Vertrauensstellungen. Für dieses Tutorial erstellen Sie jedoch eine bidirektionale Gesamtstruktur-Vertrauensstellung.

So konfigurieren Sie die Vertrauensstellung in Ihrem selbstverwalteten Active Directory

1. Öffnen Sie Server Manager und wählen Sie im Menü Tools die Option Active Directory Domains and Trusts.
2. Öffnen Sie mit einem Rechtsklick das Kontextmenü Ihrer Domain und wählen Sie Properties aus.
3. Wählen Sie die Registerkarte Trusts und dann New trust. Geben Sie den Namen von Ihrem AWS Managed Microsoft AD ein und wählen Sie Weiter aus.
4. Wählen Sie Forest trust. Wählen Sie Weiter.
5. Wählen Sie Two-way. Wählen Sie Weiter.
6. Wählen Sie This domain only. Wählen Sie Weiter.
7. Wählen Sie Forest-wide authentication. Wählen Sie Weiter.
8. Geben Sie ein Trust password ein. Merken Sie sich dieses Passwort gut, da Sie es beim Einrichten der Vertrauensstellung für Ihr AWS Managed Microsoft AD benötigen.
9. Bestätigen Sie im nächsten Dialogfeld Ihre Einstellungen und wählen Sie Next aus. Prüfen Sie, ob die Vertrauensstellung richtig erstellt wurde, und wählen Sie erneut Next aus.
10. Wählen Sie No, do not confirm the outgoing trust. Wählen Sie Weiter.
11. Wählen Sie No, do not confirm the incoming trust. Wählen Sie Weiter.

Konfigurieren Sie die Vertrauensstellung in Ihrem Verzeichnis in AWS Managed Microsoft AD

Zum Schluss konfigurieren Sie die Gesamtstruktur-Vertrauensstellung mit Ihrem Verzeichnis in AWS Managed Microsoft AD. Da Sie für die selbstverwaltete Domain eine bidirektionale Gesamtstruktur-Vertrauensstellung erstellt haben, müssen Sie mit Ihrem Verzeichnis in AWS Managed Microsoft AD ebenfalls eine bidirektionale Vertrauensstellung erstellen.

> **Note**
>
> Vertrauensbeziehungen sind ein globales Feature von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in Primäre -Region ausgeführt werden. Die Änderungen werden automatisch auf alle replizierten Regionen angewendet. Weitere Informationen finden Sie unter Globale und regionale Features.

So konfigurieren Sie die Vertrauensstellung in Ihrem Verzeichnis von AWS Managed Microsoft AD

1. Kehren Sie zur AWS Directory Service-Konsole zurück.
2. Wählen Sie auf der Seite Verzeichnisse Ihre ID von AWS Managed Microsoft AD aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Option Actions (Aktionen) und dann Add trust relationship (Vertrauensstellung hinzufügen aus.
5. Geben Sie auf der Seite Vertrauensstellung hinzufügen den Vertrauenstyp an. In diesem Fall wählen wir Gesamtstruktur-Vertrauensstellung. Geben Sie den FQDN Ihrer selbstverwalteten Domain ein (siehe **`corp.example.com`** in diesem Tutorial). Geben Sie das Passwort ein, das Sie beim Erstellen der Vertrauensstellung für Ihre selbstverwaltete Domain verwendet haben. Geben Sie die Richtung an. In unserem Beispiel wählen wir Zwei-Wege aus.
6. Geben Sie im Feld Bedingte Weiterleitung die IP-Adresse Ihres selbstverwalteten DNS-Servers ein. In unserem Beispiel lautet sie 172.16.10.153.
7. (Optional) Wählen Sie Weitere IP-Adresse hinzufügen aus und geben Sie eine zweite IP-Adresse für Ihren selbstverwalteten DNS-Server ein. Sie können insgesamt bis zu vier DNS-Server angeben.
8. Wählen Sie Add (Hinzufügen) aus.

Herzlichen Glückwunsch. Sie haben jetzt eine Vertrauensbeziehung zwischen Ihrer selbstverwalteten Domain (corp.example.com) und Ihrem AWS verwalteten Microsoft AD (AD.example.com).

MyManaged Zwischen diesen beiden Domains kann nur eine Vertrauensstellung eingerichtet werden. Wenn Sie beispielweise statt einer bidirektionalen eine unidirektionale Vertrauensstellung nutzen möchten, müssen Sie die bestehende Vertrauensstellung löschen und eine neue erstellen.

Weitere Informationen, etwa Anleitungen zum Bestätigen oder Löschen von Vertrauensstellungen, finden Sie unter Erstellen einer Vertrauensstellung.

Tutorial: Eine Vertrauensstellung zwischen zwei Domains von AWS Managed Microsoft AD erstellen

In diesem Tutorial erfahren Sie Schritt für Schritt, wie Sie zwischen zwei Domains von AWS Directory Service für Microsoft Active Directory eine Vertrauensstellung herstellen.

Themen

- Schritt 1: Ihr AWS Managed Microsoft AD vorbereiten
- Schritt 2: Die Vertrauensstellung mit einer anderen Domain von AWS Managed Microsoft AD erstellen

Weitere Informationen finden Sie auch unter:

Erstellen einer Vertrauensstellung

Schritt 1: Ihr AWS Managed Microsoft AD vorbereiten

In diesem Abschnitt bereiten Sie Ihr AWS verwaltetes Microsoft AD auf die Vertrauensbeziehung mit einem anderen AWS verwalteten Microsoft AD vor. Viele der folgenden Schritte sind fast identisch mit denen, die Sie in Tutorial: Eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD und Ihrer selbstverwalteten Active-Directory-Domain erstellen ausgeführt haben. Diesmal konfigurieren Sie Ihre AWS verwalteten Microsoft AD-Umgebungen jedoch so, dass sie miteinander funktionieren.

Ihre VPC-Subnetze und Sicherheitsgruppen konfigurieren

Sie müssen Datenverkehr von einem AWS verwalteten Microsoft AD-Netzwerk zur VPC zulassen, die Ihr anderes AWS verwaltetes Microsoft AD enthält. Dazu müssen Sie sicherstellen, dass die ACLs, die den Subnetzen zugeordnet sind, die für die Bereitstellung Ihres AWS verwalteten Microsoft AD verwendet werden, und die auf Ihren Domänencontrollern konfigurierten Sicherheitsgruppenregeln den erforderlichen Datenverkehr zur Unterstützung von Vertrauensstellungen zulassen.

Die Portanforderungen variieren je nach der Version von Windows Server, die von Ihren Domain-Controllern, den Services und den Anwendungen verwendet wird, die die Vertrauensstellung nutzen. Für dieses Tutorial müssen Sie folgende Ports öffnen:

Eingehend

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos-Authentifizierung
- UDP 123 – NTP
- TCP 135 – RPC
- TCP/UDP 389 – LDAP
- TCP/UDP 445 – SMB

> **Note**
>
> SMBv1 wird nicht mehr unterstützt.

- TCP/UDP 464 – Kerberos-Authentifizierung
- TCP 636 - LDAPS (LDAP über TLS/SSL)
- TCP 3268-3269 – Globaler Katalog
- TCP/UDP 1024-65535 – Flüchtige Ports für RPC

Ausgehend

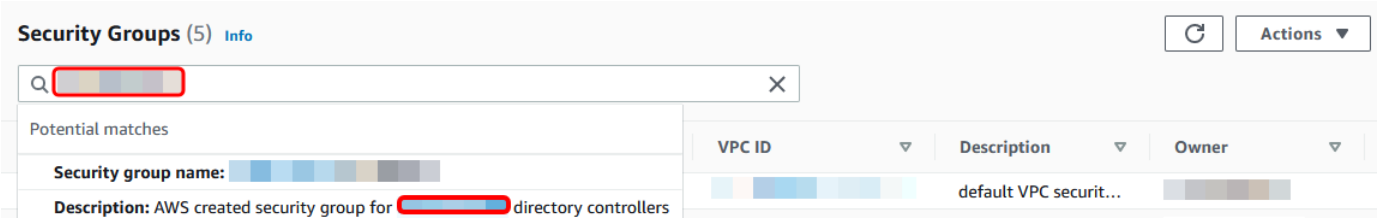
- ALL

> **Note**
>
> Dies sind die minimalen Ports, die benötigt werden, um die VPCs von beiden AWS Managed Microsoft ADs aus zu verbinden. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports. Weitere Informationen finden Sie unter Konfigurieren einer Firewall für Active-Directory-Domains und -Vertrauensstellungen auf der Website von Microsoft.

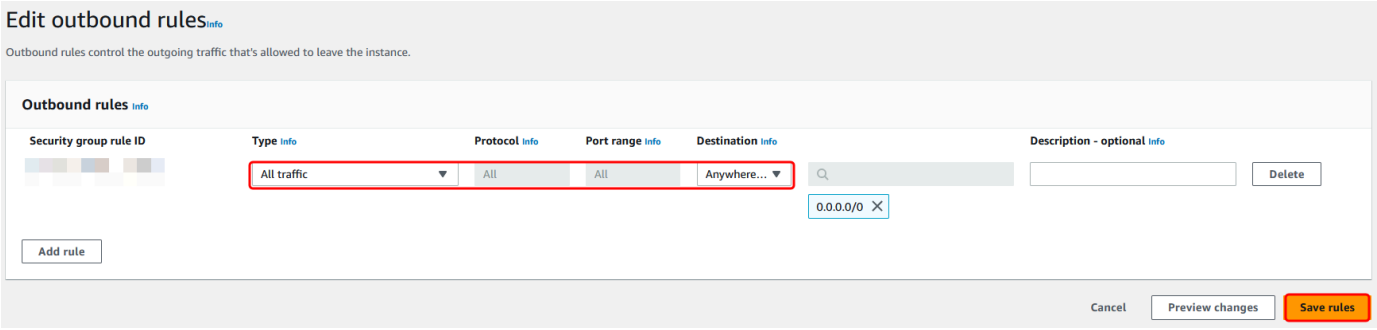
So konfigurieren Sie Ihre ausgehenden Regeln für den AWS verwalteten Microsoft AD-Domänencontroller

> **Note**
>
> Wiederholen Sie die nachfolgenden Schritte 1–6 für jedes Verzeichnis.

1. Rufen Sie die AWS Directory Service -Konsole auf. Notieren Sie sich in der Verzeichnisliste die Verzeichnis-ID für Ihr AWS verwaltetes Microsoft AD-Verzeichnis.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
3. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
4. Verwenden Sie das Suchfeld, um nach Ihrer AWS verwalteten Microsoft AD-Verzeichnis-ID zu suchen. Wählen Sie in den Suchergebnissen das Element mit der Beschreibung **`AWS created security group for yourdirectoryID directory controllers`**.



5. Wählen Sie die Registerkarte Outbound Rules dieser Sicherheitsgruppe. Wählen Sie Edit und dann Add another rule. Geben Sie die folgenden Werte für die neue Regel ein:
   - Typ: ALL Traffic (GESAMTER Datenverkehr)
   - Protocol: ALL (Alle)
   - Destination bestimmt den Datenverkehr, der Ihre Domain-Controller verlassen kann, und wohin er gesendet werden kann. Geben Sie eine einzelne IP-Adresse oder einen IP-Adressbereich in CIDR-Notation an (z. B. 203.0.113.5/32). Sie können auch den Namen oder die ID einer anderen Sicherheitsgruppe in derselben Region angeben. Weitere Informationen finden Sie unter Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut.
6. Wählen Sie Speichern.

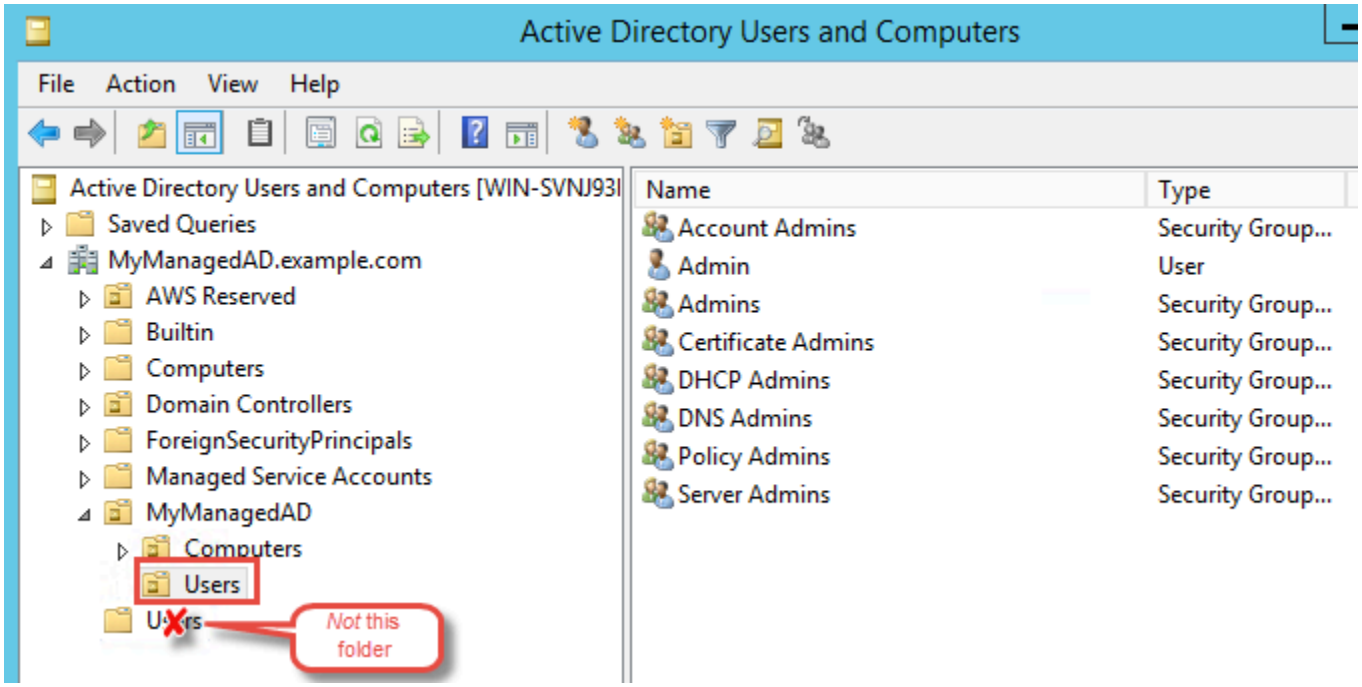


Sicherstellen, dass Kerberos-Vorauthentifizierung aktiviert ist

Jetzt möchten Sie sicherstellen, dass für Benutzer in Ihrem AWS Managed Microsoft AD auch die Kerberos-Vorauthentifizierung aktiviert ist. Dies ist das gleiche Verfahren wie für Ihr On-Premises-Verzeichnis. Dies ist die Standardeinstellung, die jedoch noch einmal überprüft werden sollte, um sicherzustellen, dass nichts geändert ist.

So zeigen Sie Benutzer-Kerberos-Einstellungen an

1. Melden Sie sich bei einer Instanz an, die Mitglied Ihres AWS verwalteten Microsoft AD-Verzeichnisses ist, indem Sie entweder das Berechtigungen für das Administratorkonto für die Domäne oder ein Konto verwenden, dem Berechtigungen zur Verwaltung von Benutzern in der Domäne delegiert wurden.
2. Wenn sie nicht bereits installiert sind, installieren Sie das Active Directory-Benutzer- und -Computer-Tool und das DNS-Tool. Erfahren Sie, wie Sie diese Tools installieren, in Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD.
3. Öffnen Sie Server Manager. Wählen Sie im Menü Tools den Eintrag Active Directory Users and Computers.
4. Wählen Sie den Ordner Users in Ihrer Domain. Beachten Sie, dass es sich hierbei um den Ordner Users (Benutzer) unter Ihrem NetBIOS-Namen handelt, nicht um den Ordner Users (Benutzer) unter dem vollständig qualifizierten Domainnamen (FQDN).



5. Klicken Sie in der Liste der Benutzer mit der rechten Maustaste auf einen Benutzer, und klicken Sie dann auf Properties (Eigenschaften).
6. Wählen Sie die Registerkarte Account. Stellen Sie in der Liste Account options sicher, dass Do not require Kerberos preauthentication nicht ausgewählt ist.

Nächster Schritt

Schritt 2: Die Vertrauensstellung mit einer anderen Domain von AWS Managed Microsoft AD erstellen

Schritt 2: Die Vertrauensstellung mit einer anderen Domain von AWS Managed Microsoft AD erstellen

Jetzt, da die Vorbereitungen abgeschlossen sind, müssen Sie nur noch die Vertrauensstellungen zwischen Ihren beiden Domains in AWS Managed Microsoft AD erstellen. Wenn während der Erstellung von Vertrauensstellungen Probleme auftreten, finden Sie weitere Informationen unter Gründe für den Status der Vertrauensstellung.

Die Vertrauensstellung in Ihrer ersten Domain von AWS Managed Microsoft AD konfigurieren

Mithilfe dieses Tutorials können Sie eine bidirektionale Gesamtstruktur-Vertrauensstellung konfigurieren. Wenn Sie eine unidirektionale Gesamtstruktur-Vertrauensstellung nutzen möchten, müssen Sie darauf achten, dass sich die Richtungen für die einzelnen Domains ergänzen. Wenn

Sie zum Beispiel eine einseitige, ausgehende Vertrauensstellung für diese erste Domain erstellen, müssen Sie eine einseitige, eingehende Vertrauensstellung für Ihre zweite Domain in AWS Managed Microsoft AD erstellen.

> **Note**
>
> AWS Managed Microsoft AD unterstützt auch externe Vertrauensstellungen. Für dieses Tutorial erstellen Sie jedoch eine bidirektionale Gesamtstruktur-Vertrauensstellung.

So konfigurieren Sie die Vertrauensstellung in Ihrer ersten Domain von AWS Managed Microsoft AD

1. Öffnen Sie die AWS Directory Service-Konsole.
2. Wählen Sie auf der Seite Verzeichnisse Ihre AWS Managed Microsoft AD ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Option Actions (Aktionen) und dann Add trust relationship (Vertrauensstellung hinzufügen aus.
5. Geben Sie auf der Seite Vertrauensstellung hinzufügen den FQDN Ihrer zweiten Domain von AWS Managed Microsoft AD ein. Merken Sie sich dieses Passwort gut, da Sie es beim Einrichten der Vertrauensstellung für Ihren zweiten AWS Managed Microsoft AD benötigen. Geben Sie die Richtung an. In diesem Fall wählen wir Zwei-Wege aus.
6. Geben Sie im Feld Bedingte Weiterleitung die IP-Adresse Ihres zweiten DNS-Servers für AWS Managed Microsoft AD ein.
7. (Optional) Wählen Sie Weitere IP-Adresse hinzufügen und geben Sie eine zweite IP-Adresse für Ihren zweiten DNS-Server für AWS Managed Microsoft AD ein. Sie können insgesamt bis zu vier DNS-Server angeben.
8. Wählen Sie Add (Hinzufügen) aus. Die Vertrauensstellung wird an dieser Stelle fehlschlagen, was zu erwarten ist, bis wir die andere Seite der Vertrauensstellung erstellen.

Konfigurieren der Vertrauensstellung in Ihrer zweiten Domain von AWS Managed Microsoft AD

Zum Schluss konfigurieren Sie die Gesamtstruktur-Vertrauensstellung mit Ihrem zweiten Verzeichnis für AWS Managed Microsoft AD. Da Sie eine zweiseitige Vertrauensstellung in der ersten Domain von AWS Managed Microsoft AD erstellt haben, erstellen Sie auch eine zweiseitige Vertrauensstellung mit dieser Domain von AWS Managed Microsoft AD.

So konfigurieren Sie die Vertrauensstellung in Ihrer zweiten Domain von AWS Managed Microsoft AD

1. Kehren Sie zur AWS Directory Service-Konsole zurück.
2. Wählen Sie auf der Seite Verzeichnisse Ihre zweite AWS Managed Microsoft AD ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Option Actions (Aktionen) und dann Add trust relationship (Vertrauensstellung hinzufügen aus.
5. Geben Sie auf der Seite Vertrauensstellung hinzufügen den FQDN Ihrer ersten Domain von AWS Managed Microsoft AD ein. Geben Sie das Passwort ein, das Sie beim Erstellen der Vertrauensstellung für Ihre On-Premises-Domain verwendet haben. Geben Sie die Richtung an. In diesem Fall wählen wir Zwei-Wege aus.
6. Geben Sie im Feld Bedingte Weiterleitung die IP-Adresse Ihres ersten DNS-Servers für AWS Managed Microsoft AD ein.
7. (Optional) Wählen Sie Weitere IP-Adresse hinzufügen und geben Sie eine zweite IP-Adresse für Ihren ersten DNS-Server für AWS Managed Microsoft AD ein. Sie können insgesamt bis zu vier DNS-Server angeben.
8. Wählen Sie Add (Hinzufügen) aus. Die Vertrauensstellung sollte kurz darauf verifiziert sein.
9. Gehen Sie nun zurück zu der Vertrauensstellung, die Sie in der ersten Domain erstellt haben, und verifizieren Sie die Vertrauensstellung erneut.

Herzlichen Glückwunsch. Sie haben jetzt eine Vertrauensstellung zwischen Ihren beiden Domains in AWS Managed Microsoft AD. Zwischen diesen beiden Domains kann nur eine Vertrauensstellung eingerichtet werden. Wenn Sie beispielweise statt einer bidirektionalen eine unidirektionale

Vertrauensstellung nutzen möchten, müssen Sie die bestehende Vertrauensstellung löschen und eine neue erstellen.

Connect Ihr AWS Managed Microsoft AD mit Microsoft Entra Connect Sync

Dieses Tutorial führt Sie durch die notwendigen Schritte zur Installation, Microsoft Entra Connect Syncum Ihr mit Ihrem AWS verwalteten Microsoft AD Microsoft Entra IDzu synchronisieren.

In diesem Tutorial führen Sie folgende Aufgaben aus:

1. Erstellen Sie einen AWS verwalteten Microsoft AD-Domänenbenutzer.
2. Laden Sie Entra Connect Sync herunter.
3. Wird verwendetWindows PowerShell, um ein Skript auszuführen, um die entsprechenden Berechtigungen für den neu erstellten Benutzer bereitzustellen.
4. Installieren Entra Connect Sync.

Voraussetzungen

Für dieses Tutorial benötigen Sie Folgendes:

- Ein AWS verwaltetes Microsoft AD. Weitere Informationen finden Sie unter the section called “Erstellen Sie Ihr AWS verwaltetes Microsoft AD”.
- Eine Amazon EC2 Windows Server-Instance, die mit Ihrem AWS Managed Microsoft AD verbunden ist. Weitere Informationen finden Sie unter Schließen Sie sich nahtlos einer Windows-Instance an.
- Ein Windows EC2-Server, der zur Verwaltung Ihres AWS verwalteten Microsoft AD Active Directory Administration Tools installiert ist. Weitere Informationen finden Sie unter the section called “Installieren Sie die AD-Verwaltungstools für AWS verwaltetes Microsoft AD”.

Schritt 1: Erstellen Sie einen Active Directory Domänenbenutzer

In diesem Tutorial wird davon ausgegangen, dass Sie bereits eine AWS verwaltete Microsoft AD- und eine Windows EC2-Server-Instanz Active Directory Administration Tools installiert haben. Weitere Informationen finden Sie unter the section called “Installieren Sie die AD-Verwaltungstools für AWS verwaltetes Microsoft AD”.

1. Connect zu der Instanz her, auf der Active Directory Administration Tools sie installiert wurden.

2. Erstellen Sie einen AWS verwalteten Microsoft AD-Domänenbenutzer. Dieser Benutzer wird der Active Directory Directory Service (AD DS) Connector account fürEntra Connect Sync. Eine ausführliche Anleitung zu diesem Vorgang finden Sie unterthe section called “Erstellen eines Benutzers”.

Schritt 2: Herunterladen Entra Connect Sync

- Laden Sie Entra Connect Sync von der MicrosoftWebsite auf die EC2-Instance herunter, die der AWS verwaltete Microsoft AD-Administrator ist.

> **Warning**
>
> Öffnen oder starten Sie das Programm Entra Connect Sync zu diesem Zeitpunkt nicht. In den nächsten Schritten werden die erforderlichen Berechtigungen für Ihren in Schritt 1 erstellten Domänenbenutzer bereitgestellt.

Schritt 3: Windows PowerShell Skript ausführen

- Öffnen Sie PowerShell als Administrator und führen Sie das folgende Skript aus. Während das Skript ausgeführt wird, werden Sie aufgefordert, das SaM AccountName für den neu erstellten Domänenbenutzer aus Schritt 1 einzugeben.

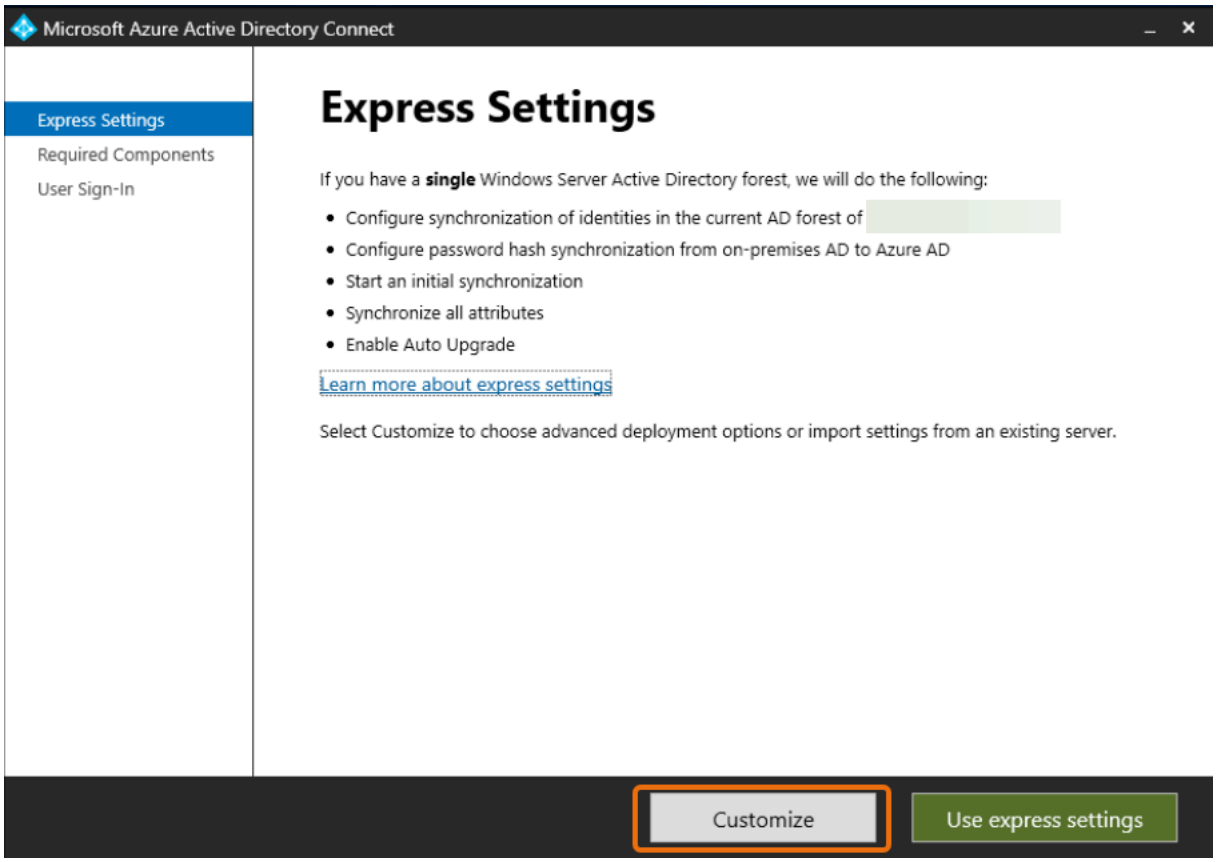
```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

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 {
```

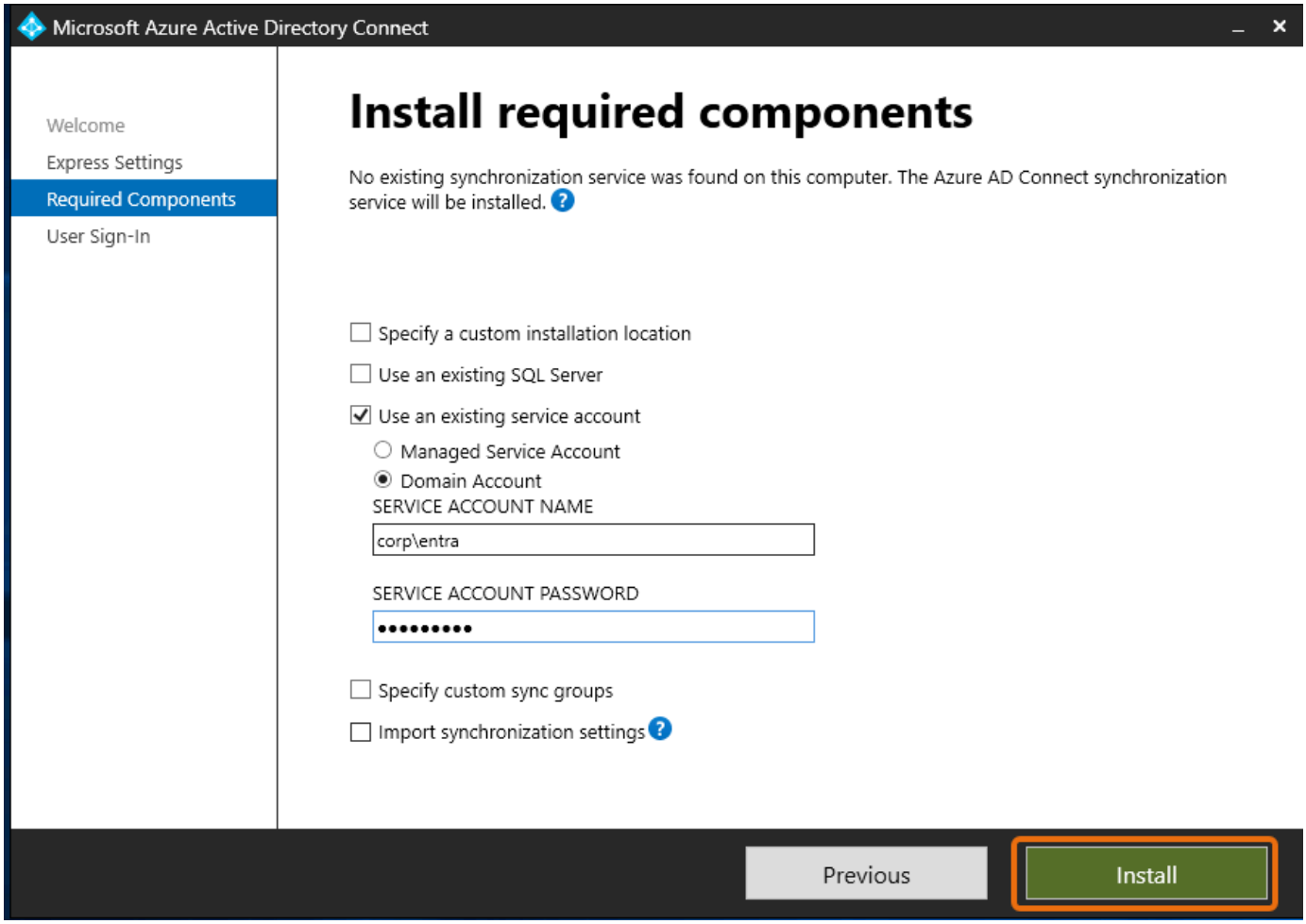
```
        Write-Host "An error occurred while setting permissions for
 $ADConnectorAccountDN on OU $OU : $_"
    }
    }
}
```

Schritt 4: Installieren Entra Connect Sync

1. Sobald das Skript abgeschlossen ist, können Sie die heruntergeladene Microsoft Entra Connect (früher bekannt alsAzure Active Directory Connect) Konfigurationsdatei ausführen.
2. Nach dem Ausführen der Konfigurationsdatei aus dem vorherigen Schritt wird ein Microsoft Azure Active Directory Connect Fenster geöffnet. Wählen Sie im Fenster Express-Einstellungen die Option Anpassen aus.



3. Aktivieren Sie im Fenster Erforderliche Komponenten installieren das Kontrollkästchen Bestehendes Dienstkonto verwenden. Geben Sie in den Feldern DIENSTKONTONAME und KENNWORT FÜR DAS DIENSTKONTO den AD DS Connector account Namen und das Passwort für den Benutzer ein, den Sie in Schritt 1 erstellt haben. Wenn Ihr AD DS Connector account Name beispielsweise lautet`entra`, wäre der Kontoname`corp\entra`. Wählen Sie dann Installieren aus.



4. Wählen Sie im Fenster für die Benutzeranmeldung eine der folgenden Optionen aus:

   a. Passthrough-Authentifizierung — Mit dieser Option können Sie sich mit Ihrem Benutzernamen und Passwort Active Directory bei Ihrem anmelden.

   b. Nicht konfigurieren — Auf diese Weise können Sie die Verbundanmeldung mit Microsoft Entra (früher bekannt als Azure Active Directory (AzureAD)) oder verwenden. Office 365

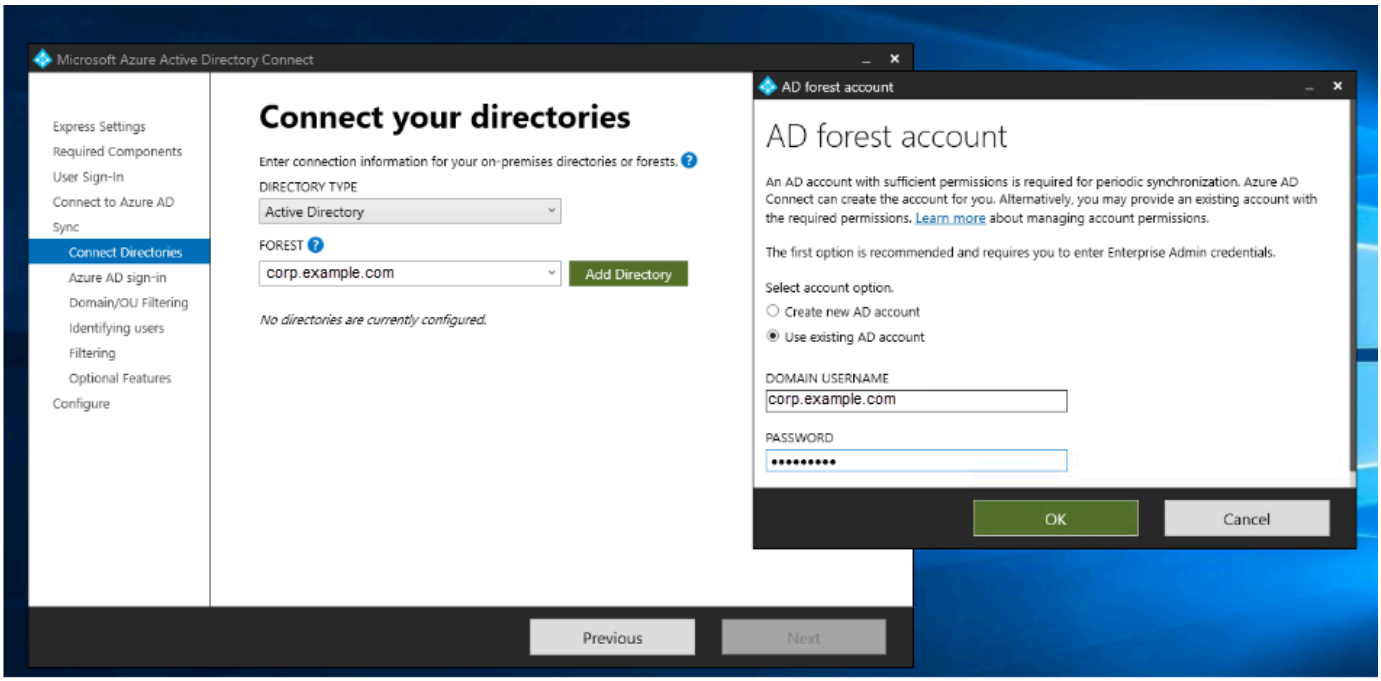
      Wählen Sie dann Weiter aus.

5. Geben Sie im Azure Fenster Connect to Ihren Global Administrator-Benutzernamen und Ihr Passwort für ein Entra ID und wählen Sie Weiter aus.

6. Wählen Active DirectorySie im Fenster Verbinden Sie Ihre Verzeichnisse als VERZEICHNISTYP aus. Wählen Sie die Gesamtstruktur für Ihr AWS verwaltetes Microsoft AD für FOREST aus. Wählen Sie dann Verzeichnis hinzufügen aus.

7. Es erscheint ein Popup-Fenster, in dem Sie nach Ihren Kontooptionen gefragt werden. Wählen Sie Bestehendes AD-Konto verwenden aus. Geben Sie den in Schritt 1 erstellten AD DS

Connector account Benutzernamen und das Passwort ein und wählen Sie dann OK aus. Wählen Sie dann Weiter.



8. Wählen Sie im Azure ADAnmeldefenster die Option Weiter aus, ohne alle UPN-Suffixe verifizierten Domänen zuzuordnen. Dies gilt nur, wenn Sie keine verifizierte Vanity-Domain hinzugefügt haben. Entra ID Wählen Sie dann Weiter aus.
9. Wählen Sie im Fenster zur Filterung von Domain/OU die Optionen aus, die Ihren Anforderungen entsprechen. Weitere Informationen finden Sie in Microsoft der Dokumentation Entra Connect Syncunter Filterung konfigurieren. Wählen Sie dann Weiter aus.
10. Behalten Sie im Fenster Identifizieren von Benutzern, Filtern und optionale Funktionen die Standardwerte bei und wählen Sie Weiter aus.
11. Überprüfen Sie im Fenster Konfigurieren die Konfigurationseinstellungen und wählen Sie Konfigurieren aus. Die Installation für Entra Connect Sync wird abgeschlossen und die Benutzer beginnen mit der Synchronisierung mitMicrosoft Entra ID.

Ihr Schema erweitern

AWS Managed Microsoft AD verwendet Schemas um zu organisieren und zu erzwingen, wie Verzeichnis-Daten gespeichert werden. Das Hinzufügen von Definitionen zu dem Schema wird als "Erweiterung des Schemas" bezeichnet. Schema-Erweiterungen ermöglichen Ihnen, das Schema Ihres Verzeichnisses in AWS Managed Microsoft AD über eine gültige LDAP Data Interchange

Format (LDIF) Datei zu ändern. Weitere Informationen über AD-Schemas und darüber, wie Sie Ihr Schema erweitern, finden Sie unter nachfolgenden Themen.

Themen

- Wann sollte das Schema von AWS Managed Microsoft AD erweitert werden?
- Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas

Wann sollte das Schema von AWS Managed Microsoft AD erweitert werden?

Sie können Ihr Schema von AWS Managed Microsoft AD durch das Hinzufügen neuer Objektklassen und Attribute erweitern. Tun Sie dies beispielsweise, wenn Sie eine Anwendung nutzen, für die Änderungen am Schema erforderlich sind, damit die Funktionen der Einmalanmeldung unterstützt werden.

Sie können Schemaerweiterungen auch verwenden, damit Anwendungen unterstützt werden, die auf bestimmten Active Directory-Objektklassen und -Attributen beruhen. Dies ist besonders dann nützlich, wenn Sie Firmenanwendungen in die AWS-Cloud migrieren müssen, die von AWS Managed Microsoft AD abhängen.

Jedes Attribut und jede Klasse, das bzw. die einem vorhandenen Active Directory-Schema hinzugefügt wird, muss mit einer eindeutigen ID definiert sein. Wenn Unternehmen dem Schema Erweiterungen hinzufügen, kann dadurch garantiert werden, dass das jeweilige neue Element nur einmal vorhanden ist und nicht in Konflikt mit einem anderen Element steht. Diese IDs werden als AD Object Identifiers (OIDs) bezeichnet und in AWS Managed Microsoft AD gespeichert.

Lesen Sie zum Einstieg Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas.

Verwandte Themen

- Ihr Schema erweitern
- Schemaelemente

Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas

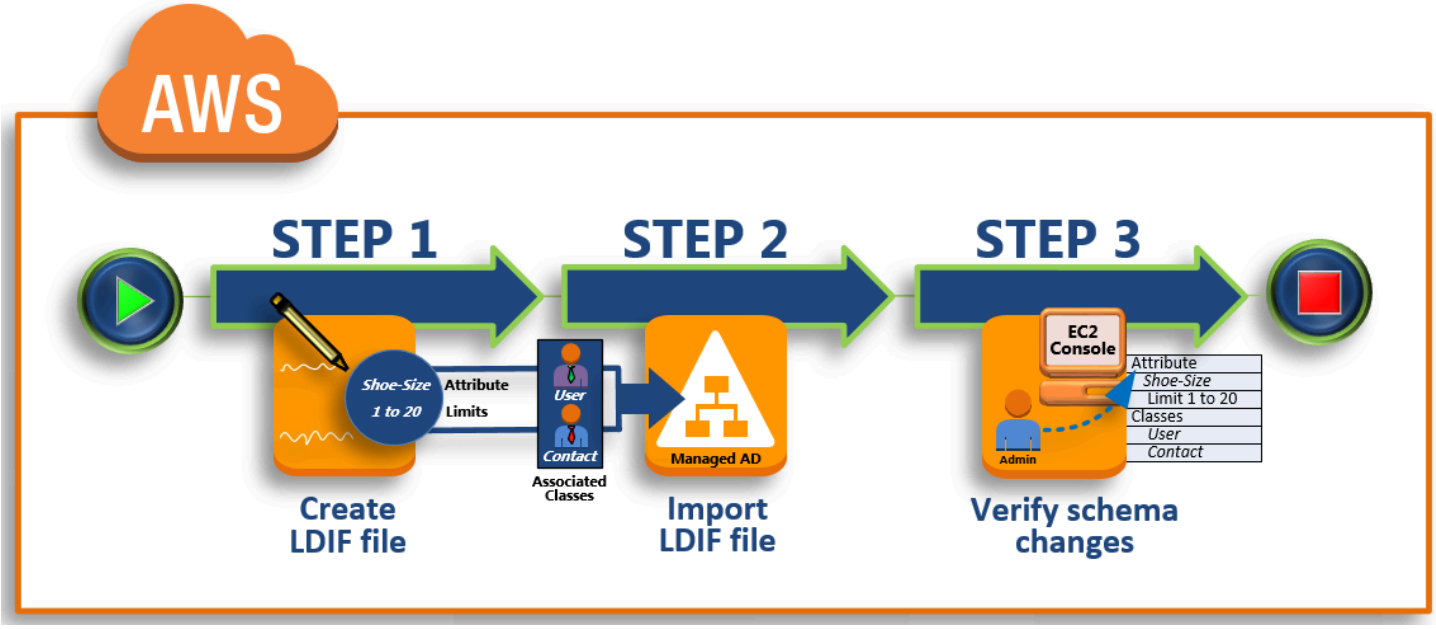
In diesem Tutorial erfahren Sie, wie Sie das Schema für Ihr AWS Verzeichnis Directory Service for Microsoft Active Directory, auch bekannt als AWS Managed Microsoft AD, erweitern können, indem Sie eindeutige Attribute und Klassen hinzufügen, die Ihren spezifischen Anforderungen entsprechen.

AWS Verwaltete Microsoft AD-Schemaerweiterungen können nur mit einer gültigen LDIF-Skriptdatei (Lightweight Directory Interchange Format) hochgeladen und angewendet werden.

Attribute (attributeSchema) definieren die Felder in der Datenbank, während Klassen (classSchema) die Tabellen in der Datenbank definieren. So werden beispielsweise alle Benutzerobjekte in Active Directory durch die Schemaklasse User definiert, während die einzelnen Eigenschaften eines Benutzers wie z. B. die E-Mail-Adresse oder Telefonnummer jeweils durch ein Attribut definiert werden.

Wenn Sie eine neue Eigenschaft wie z. B. „Shoe-Size" hinzufügen wollten, müssten Sie ein neues Attribut des Typs Integer definieren. Sie könnten auch Unter- und Obergrenzen definieren, beispielsweise 1 bis 20. Sobald das attributeSchema-Objekt für die Schuhgröße erstellt wurde, würden Sie dann das classSchema-Objekt User ändern, sodass dieses Attribut enthalten ist. Attribute können mit mehreren Klassen verknüpft werden. Shoe-Size könnte auch beispielsweise zur Klasse Contact hinzugefügt werden. Weitere Informationen zu den Active Directory-Schemas finden Sie unter Wann sollte das Schema von AWS Managed Microsoft AD erweitert werden?.

Dieser Workflow umfasst drei grundlegende Schritte.



Schritt 1: Ihre LDIF-Datei erstellen

Zunächst erstellen Sie eine LDIF-Datei und definieren die neuen Attribute sowie alle Klassen, denen die Attribute hinzugefügt werden sollen. Diese Datei verwenden Sie für die nächste Phase des Workflows.

Schritt 2: Ihre LDIF-Datei importieren

In diesem Schritt verwenden Sie die AWS Directory Service Konsole, um die LDIF-Datei in Ihre Microsoft Active Directory-Umgebung zu importieren.

Schritt 3: Prüfen, ob die Schemaerweiterung erfolgreich durchgeführt wurde

Schließlich prüfen Sie als Administrator über eine EC2 Instance, ob die neuen Erweiterungen im Active Directory-Schema-Snap-In aufgeführt sind.

Schritt 1: Ihre LDIF-Datei erstellen

Bei einer LDIF-Datei handelt es sich um ein standardmäßiges Klartext-Datenaustauschformat zur Darstellung von LDAP-Verzeichnisinhalten und Aktualisierungsanforderungen (LDAP = Lightweight Directory Access Protocol). LDIF übermittelt Verzeichnisinhalte als Datensatzgruppe mit einem Datensatz für jedes Objekt (oder jeden Eintrag). Auch Aktualisierungsanforderungen wie z. B. Hinzufügen, Ändern, Löschen und Umbenennen werden als Datensatzgruppe mit einem Datensatz für jede Aktualisierungsanforderung dargestellt.

Der AWS Directory Service importiert Ihre LDIF-Datei mit den Schemaänderungen, indem er die `ldifde.exe` Anwendung in Ihrem AWS verwalteten Microsoft AD-Verzeichnis ausführt. Daher werden Sie es hilfreich finden, wenn Sie die LDIF-Skriptsyntax verstehen. Weitere Informationen finden Sie unter LDIF Scripts.

Mehrere LDIF-Tools von Drittanbietern können Ihre Schemaaktualisierungen extrahieren, bereinigen und aktualisieren. Unabhängig davon, welches Tool Sie verwenden, ist es wichtig zu wissen, dass alle in Ihrer LDIF-Datei verwendeten Kennungen eindeutig sein müssen.

Wir empfehlen Ihnen dringend, sich die folgenden Konzepte und Tipps anzusehen, bevor Sie Ihre LDIF-Datei erstellen.

- Schemaelemente – Erfahren Sie mehr über Schemaelemente wie Attribute, Klassen, Objekt-IDs und verknüpfte Attribute. Weitere Informationen finden Sie unter Schemaelemente.

- Folge der Elemente – Stellen Sie sicher, dass die Reihenfolge, in der die Elemente in Ihrer LDIF-Datei angeordnet sind, von oben nach unten dem Directory Information Tree (DIT) folgt. In Bezug auf die Sequenzierung in einer LDIF-Datei gelten u. a. folgende allgemeine Regeln:

  - Trennen Sie die Elemente durch eine Leerzeile.
  - Listen Sie untergeordnete Elemente nach ihren übergeordneten Elementen auf.

  - Stellen Sie sicher, dass Elemente wie Attribute oder Objektklassen in dem Schema vorhanden sind. Falls dies nicht der Fall ist, müssen Sie sie zum Schema hinzufügen, bevor sie verwendet werden können. So muss beispielsweise ein Attribut erstellt werden, bevor Sie es einer Klasse zuweisen können.

- Format des DN – Definieren Sie für jede neue Anweisung in der LDIF-Datei den definierten Namen (DN) als erste Zeile der Anweisung. Der DN identifiziert ein Active Directory-Objekt innerhalb der Struktur des Active Directory-Objekts und muss die Domainkomponenten für Ihr Verzeichnis enthalten. Die Domainkomponenten für das Verzeichnis in diesem Tutorial lauten beispielsweise `DC=example,DC=com`.

  Der DN muss auch den allgemeinen Namen (CN) des Active Directory-Objekts enthalten. Der erste CN-Eintrag ist der Attribut- oder Klassenname. Als Nächstes müssen Sie `CN=Schema,CN=Configuration` verwenden. Dieser KN stellt sicher, dass Sie das Active Directory-Schema erweitern können. Wie bereits erwähnt, können Sie keine Inhalte von Active Directory-Objekten hinzufügen oder ändern. Im Folgenden sehen Sie das allgemeine Format für einen DN.

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  Für dieses Tutorial würde der DN für das neue Attribut „Shoe-Size” wie folgt aussehen:

  ```
  dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
  ```

- Warnungen – Beachten Sie die nachfolgenden Warnungen, bevor Sie Ihr Schema erweitern.
  - Bevor Sie Ihr Active Directory-Schema erweitern, ist es wichtig, die Microsoft-Warnungen bezüglich der Auswirkungen dieses Vorgangs zu beachten. Weitere Informationen finden Sie unter What You Must Know Before Extending the Schema.
  - Schemaattribute oder Klassen können nicht gelöscht werden. Wenn Ihnen ein Fehler unterläuft und Sie keine Wiederherstellung von einem Backup durchführen möchten, können Sie daher das Objekt nur deaktivieren. Weitere Informationen finden Sie unter Disabling Existing Classes and Attributes.
  - Änderungen an defaultSecurityDescriptor werden nicht unterstützt.

Weitere Informationen zum Aufbau von LDIF-Dateien und eine LDIF-Beispieldatei, die zum Testen AWS verwalteter Microsoft AD-Schemaerweiterungen verwendet werden kann, finden Sie im Artikel How to Extend your AWS Managed Microsoft AD Directory Schema im Security Blog. AWS

Nächster Schritt

Schritt 2: Ihre LDIF-Datei importieren

Schritt 2: Ihre LDIF-Datei importieren

Sie können Ihr Schema erweitern, indem Sie eine LDIF-Datei entweder von der AWS Directory Service Konsole oder mithilfe der API importieren. Weitere Informationen darüber, wie Sie dies mit den Schemaerweiterungs-APIs tun können, finden Sie in der AWS Directory Service -API-Referenz. Zurzeit unterstützt AWS keine externen Anwendungen wie Microsoft Exchange in Bezug auf die direkte Ausführung von Schemaaktualisierungen.

Important

Wenn Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnisschema aktualisieren, kann der Vorgang nicht rückgängig gemacht werden. Mit anderen Worten, wenn Sie eine neue Klasse oder ein neues Attribut erstellen, lässt Active Directory nicht zu, dass Sie diese(s) entfernen. Eine Deaktivierung ist jedoch möglich.
Wenn Sie die Schemaänderungen löschen müssen, besteht eine Möglichkeit darin, das Verzeichnis anhand eines früheren Snapshots wiederherzustellen. Beim Wiederherstellen eines Snapshots werden sowohl das Schema als auch die Verzeichnisdaten auf einen früheren Stand zurückgesetzt, nicht nur das Schema. Hinweis: Das maximal unterstützte Alter eines Snapshots beträgt 180 Tage. Weitere Informationen finden Sie unter Useful shelf life of a system-state backup of Active Directory auf der Microsoft-Website.

Bevor der Aktualisierungsvorgang beginnt, erstellt AWS Managed Microsoft AD einen Snapshot, um den aktuellen Status Ihres Verzeichnisses beizubehalten.

Note

Schemaerweiterungen sind eine globale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in Primäre -Region ausgeführt werden. Die Änderungen werden automatisch auf alle replizierten Regionen angewendet. Weitere Informationen finden Sie unter Globale und regionale Features.

So importieren Sie Ihre LDIF-Datei

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Wartung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Wartung.
4. Wählen Sie im Abschnitt Schema extensions (Schemaerweiterungen) die Option Actions (Aktionen) und dann Upload and update schema (Schema hochladen und aktualisieren) aus.
5. Klicken Sie im Dialogfeld auf Browse, wählen Sie eine gültige LDIF-Datei aus, geben Sie eine Beschreibung ein und wählen Sie dann Update Schema aus.

> **Important**
>
> Die Erweiterung des Schemas ist ein kritischer Vorgang. Wenden Sie keine Schemaaktualisierungen in Produktionsumgebungen an, ohne sie zuvor mit Ihrer Anwendung in einer Entwicklungs- oder Testumgebung zu testen.

Anwendung der LDIF-Datei

Nachdem Ihre LDIF-Datei hochgeladen wurde, ergreift AWS Managed Microsoft AD Maßnahmen, um Ihr Verzeichnis vor Fehlern zu schützen, indem es die Änderungen in der folgenden Reihenfolge anwendet.

1. Validierung der LDIF-Datei. Da LDIF-Skripts jedes Objekt in der Domäne manipulieren können, führt AWS Managed Microsoft AD direkt nach dem Upload Prüfungen durch, um sicherzustellen, dass der Importvorgang nicht fehlschlägt. Im Rahmen dieser Prüfungen wird u. a. Folgendes sichergestellt:
   - Die zu aktualisierenden Objekte befinden sich nur im Schema-Container.
   - Der DC-Teil (Domain-Controller) entspricht dem Namen der Domain, in der das LDIF-Skript ausgeführt wird.

2. Erstellen eines Snapshots Ihres Verzeichnisses. Mithilfe des Snapshots können Sie Ihr Verzeichnis wiederherstellen, falls nach der Schemaaktualisierung Probleme mit Ihrer Anwendung auftreten.
3. Wendet die Änderungen auf einen einzelnen DC an. AWS Managed Microsoft AD isoliert einen Ihrer DCs und wendet die Updates in der LDIF-Datei auf den isolierten DC an. Anschließend wählt es einen Ihrer DCs als primäres Schema aus, entfernt diesen DC aus der Verzeichnisreplikation und wendet Ihre LDIF-Datei mithilfe von an. `Ldifde.exe`
4. Die Replikation erfolgt auf allen DCs. AWS Managed Microsoft AD fügt den isolierten DC wieder der Replikation hinzu, um das Update abzuschließen. Währenddessen bietet Ihr Verzeichnis weiterhin ohne Unterbrechungen Active Directory-Service für Ihre Anwendungen.

Nächster Schritt

Schritt 3: Prüfen, ob die Schemaerweiterung erfolgreich durchgeführt wurde

Schritt 3: Prüfen, ob die Schemaerweiterung erfolgreich durchgeführt wurde

Nach Abschluss des Importprozesses ist es wichtig, sicherzustellen, dass die Schemaaktualisierungen auf Ihr Verzeichnis angewendet wurden. Dies ist besonders vor der Migration oder Aktualisierung von Anwendungen wichtig, die auf der Schemaaktualisierung beruhen. Sie können zu diesem Zweck verschiedene LDAP-Tools verwenden oder ein Test-Tool schreiben, das die entsprechenden LDAP-Befehle ausgibt.

Bei diesem Verfahren wird das Active Directory-Schema-Snap-In verwendet und/oder PowerShell um zu überprüfen, ob die Schemaaktualisierungen angewendet wurden. Sie müssen diese Tools auf einem Computer ausführen, der zu Ihrem AWS verwalteten Microsoft AD gehört. Hierbei kann es sich um einen Windows-Server handeln, der in Ihrem On-Premises-Netzwerk mit Zugriff auf Ihre Virtual Private Cloud (VPC) oder über eine Virtual Private Network (VPN)-Verbindung ausgeführt wird. Sie können diese Tools auch auf einer Windows-Instance von Amazon EC2 ausführen (siehe So starten Sie eine neue EC2-Instance mit nahtloser Domainverbindung).

Überprüfung mithilfe des Active Directory-Schema-Snap-Ins

1. Installieren Sie das Active Directory-Schema-Snap-In gemäß den Anweisungen auf der TechNetWebsite.
2. Öffnen Sie die Microsoft Management Console (MMC) und erweitern Sie die Struktur AD Schema für Ihr Verzeichnis.

3. Navigieren Sie durch die Ordner Classes und Attributes, bis Sie die zuvor vorgenommenen Schemaänderungen finden.

Um zu überprüfen, ob PowerShell

1. Öffnet ein PowerShell Fenster.
2. Verwenden Sie das nachfolgend dargestellte Cmdlet `Get-ADObject`, um die Schemaänderung zu prüfen. Beispielsweise:

   ```
   get-adobject -Identity 'CN=Shoe-
   Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
   ```

Optionaler Schritt

Fügen Sie dem neuen Attribut einen Wert hinzu — optional

Fügen Sie dem neuen Attribut einen Wert hinzu — optional

Verwenden Sie diesen optionalen Schritt, wenn Sie ein neues Attribut erstellt haben und dem Attribut in Ihrem AWS verwalteten Microsoft AD-Verzeichnis einen neuen Wert hinzufügen möchten.

So fügen Sie einen Wert zu einem Attribut hinzu

1. Öffnen Sie das Windows PowerShell Befehlszeilenprogramm und legen Sie das neue Attribut mit dem folgenden Befehl fest. In diesem Beispiel fügen wir dem Attribut für einen bestimmten Computer einen neuen Wert „EC2InstanceID” hinzu.

   ```
   PS C:\> set-adcomputer -Identity computer name -add @{example-
   EC2InstanceID = 'EC2 instance ID'}
   ```
2. Mit dem folgenden Befehl können Sie überprüfen, ob der Wert „EC2InstanceID” dem Computerobjekt hinzugefügt wurde:

   ```
   PS C:\> get-adcomputer -Identity computer name –Property example-
   EC2InstanceID
   ```

Zugehörige Ressourcen

Auf der Microsoft-Website sind folgende Links zu Ressourcen mit zugehörigen Informationen zu finden.

- Extending the Schema (Windows)
- Active Directory Schema (Windows)
- Active Directory Schema
- Windows-Verwaltung: Erweitern des Active Directory-Schemas
- Restrictions on Schema Extension (Windows)
- Ldifde

Ihr Verzeichnis in AWS Managed Microsoft AD verwalten

In diesem Abschnitt wird beschrieben, wie Sie allgemeine administrative Aufgaben für Ihre Umgebung in AWS Managed Microsoft AD verwalten.

Themen

- Alternative UPN-Suffixe hinzufügen
- Löschen Sie Ihr AWS verwaltetes Microsoft AD
- Den Standort Ihres Verzeichnisses umbenennen
- Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen
- Aktualisieren Sie Ihr AWS Managed Microsoft AD
- Verzeichnisinformationen anzeigen

Alternative UPN-Suffixe hinzufügen

Sie können die Verwaltung von Active Directory (AD)-Anmeldenamen vereinfachen und die Benutzeranmeldeerfahrung verbessern, indem Sie Suffixe von Benutzer-Prinzipalnamen (UPN) zu Ihrem Verzeichnis in AWS Managed Microsoft AD hinzufügen. Hierzu müssen Sie mit dem Admin-Konto oder einem Konto, das Mitglied der Gruppe AWS Delegated User Principal Name Suffix Administrators ist, angemeldet sein. Weitere Informationen zu dieser Gruppe finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.

So fügen Sie alternative UPN-Suffixe hinzu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Suchen Sie eine Amazon-EC2-Instance, die mit Ihrem Verzeichnis in AWS Managed Microsoft AD verbunden ist. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).

3. Wählen Sie im Fenster Server Manager die Option Tools aus. Wählen Sie dann den Eintrag Active Directory Domains and Trusts (Active-Directory-Domain und -Vertrauensbeziehungen) aus.
4. Klicken Sie im linken Bereich mit der rechten Maustaste auf Active-Directory-Domain und -Vertrauensstellungen und wählen Sie Eigenschaften aus.
5. Geben Sie auf der Registerkarte UPN Suffixes (UPN-Suffixe) ein alternatives UPN-Suffix ein (beispielsweise **`sales.example.com`**). Wählen Sie Add (Hinzufügen) und anschließend Apply (Anwenden) aus.
6. Wenn Sie weitere alternative UPN-Suffixe hinzufügen möchten, wiederholen Sie Schritt 5, bis die gewünschte Anzahl erreicht ist.

Löschen Sie Ihr AWS verwaltetes Microsoft AD

Wenn ein AWS verwaltetes Microsoft AD gelöscht wird, werden alle Verzeichnisdaten und Snapshots gelöscht und können nicht wiederhergestellt werden. Alle Instances, die dem Verzeichnis zugeordnet sind, bleiben erhalten, nachdem das Verzeichnis gelöscht wurde. Sie können sich jedoch nicht mit den Anmeldeinformationen Ihres Verzeichnisses bei diesen Instances anmelden. In dem Fall müssen Sie sich mit einem lokalen Benutzerkonto bei den jeweiligen Instances anmelden.

So löschen Sie ein Verzeichnis

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse. Stellen Sie sicher, dass Sie sich an dem AWS-Region Ort befinden, an dem Ihr Active Directory Gerät bereitgestellt wird. Weitere Informationen finden Sie unter Region auswählen.
2. Stellen Sie sicher, dass für das Verzeichnis, das Sie löschen möchten, keine AWS Anwendungen aktiviert sind. Aktivierte AWS Anwendungen verhindern, dass Sie Ihr AWS Managed Microsoft AD oder Simple AD löschen.

    a. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.

    b. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus. Im Bereich AWS Apps und Dienste sehen Sie, welche AWS Anwendungen für Ihr Verzeichnis aktiviert sind.

        - Deaktivieren Sie AWS Management Console den Zugriff. Weitere Informationen finden Sie unter AWS Management Console-Zugriff deaktivieren.

- Um Amazon zu deaktivieren WorkSpaces, müssen Sie den Service aus dem Verzeichnis in der WorkSpaces Konsole abmelden. Weitere Informationen finden Sie unter Abmeldung von einem Verzeichnis im WorkSpaces Amazon-Administratorhandbuch.
- Um Amazon zu deaktivieren WorkDocs, müssen Sie die WorkDocs Amazon-Website in der WorkDocs Amazon-Konsole löschen. Weitere Informationen finden Sie unter Löschen einer Site im WorkDocs Amazon-Administratorhandbuch.
- Um Amazon zu deaktivieren WorkMail, müssen Sie die WorkMail Amazon-Organisation in der WorkMail Amazon-Konsole entfernen. Weitere Informationen finden Sie unter Organisation entfernen im WorkMail Amazon-Administratorhandbuch.
- Um Amazon FSx für Windows File Server zu deaktivieren, müssen Sie das Amazon-FSx-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter Arbeiten mit Active Directory in FSx for Windows File Server im Amazon FSx for Windows File Server Server-Benutzerhandbuch.
- Um Amazon Relational Database Service zu deaktivieren, müssen Sie die Amazon-RDS-Instance aus der Domain entfernen. Weitere Informationen finden Sie unter Verwalten einer DB-Instance in einer Domain im Amazon-RDS-Benutzerhandbuch.
- Um den AWS Client VPN Dienst zu deaktivieren, müssen Sie den Verzeichnisdienst vom Client-VPN-Endpunkt entfernen. Weitere Informationen finden Sie unter Active DirectoryAuthentifizierung im AWS Client VPN Administratorhandbuch.
- Zur Deaktivierung von Amazon Connect müssen Sie die Amazon Connect-Instance löschen. Weitere Informationen finden Sie unter Löschen einer Amazon-Connect-Instance im Administrationshandbuch für Amazon Connect.
- Um Amazon zu deaktivieren QuickSight, müssen Sie sich von Amazon abmelden QuickSight. Weitere Informationen finden Sie unter Schließen Ihres Amazon QuickSight Kontos im QuickSight Amazon-Benutzerhandbuch.

> **Note**
>
> Wenn Sie es verwenden AWS IAM Identity Center und es zuvor mit dem AWS verwalteten Microsoft AD-Verzeichnis verbunden haben, das Sie löschen möchten, müssen Sie zuerst die Identitätsquelle ändern, bevor Sie es löschen können. Weitere Informationen finden Sie unter Identitätsquelle ändern im Benutzerhandbuch zu IAM Identity Center.

3. Wählen Sie im Navigationsbereich Verzeichnisse aus.

4. Wählen Sie nur das Verzeichnis, das gelöscht werden soll, und klicken Sie auf Löschen. Es dauert einige Minuten, bis das Verzeichnis gelöscht wird. Wenn dieser Vorgang abgeschlossen ist, wird es aus Ihrer Verzeichnisliste entfernt.

Den Standort Ihres Verzeichnisses umbenennen

Sie können den Namen des Standardstandorts Ihres Verzeichnisses von AWS Managed Microsoft AD umbenennen, sodass der Name mit bereits vorhandenen Microsoft Active Directory (AD)-Standortnamen übereinstimmt. Dadurch kann AWS Managed Microsoft AD vorhandene AD-Benutzer in Ihrem On-Premises-Verzeichnis schneller finden und authentifizieren. Dies führt zu einer besseren Benutzererfahrung, wenn sich Benutzer an AWS-Ressourcen wie Instances von Amazon EC2 und Amazon RDS für SQL Server anmelden, die Sie Ihrem Verzeichnis in AWS Managed Microsoft AD hinzugefügt haben.

Hierzu müssen Sie mit dem Admin-Konto oder einem Konto angemeldet sein, das Mitglied der Gruppe AWS Delegated Sites and Services Administrators ist. Weitere Informationen zu dieser Gruppe finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.

Weitere Informationen zur Umbenennung Ihres Standorts im Zusammenhang mit Vertrauensstellungen finden Sie unter Domain Locator Across a Forest Trust auf der Microsoft-Website.

So benennen Sie die Standorte von AWS Managed Microsoft AD um

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Suchen Sie eine Amazon-EC2-Instance, die mit Ihrem Verzeichnis in AWS Managed Microsoft AD verbunden ist. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
3. Wählen Sie im Fenster Server Manager die Option Tools aus. Wählen Sie dann Active Directory Sites and Services (Active Directory-Standorte und -Dienste) aus.
4. Erweitern Sie im linken Bereich den Ordner Sites (Standorte), klicken Sie mit der rechten Maustaste auf den Standortnamen (Standard: Default-Site-Names) und wählen Sie anschließend Rename (Umbenennen) aus.
5. Geben Sie den neuen Namen ein und wählen Sie Enter (Eingabe).

Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen

AWS Directory Service bietet automatische tägliche Snapshots und die Möglichkeit, manuelle Snapshots von Daten für Ihr AWS verwaltetes Microsoft AD Active Directory zu erstellen. Diese Snapshots können verwendet werden, um eine point-in-time Wiederherstellung für Ihr Active Directory durchzuführen. Sie sind auf fünf manuelle Snapshots für jedes AWS verwaltete Microsoft AD Active Directory beschränkt. Falls Sie diesen Maximalwert bereits erreicht haben, müssen Sie einen vorhandenen manuellen Snapshot löschen, bevor Sie einen neuen erstellen. Sie können keine Snapshots von AD-Connector-Verzeichnissen erstellen.

> **Note**
>
> Snapshot ist eine globale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in Primäre -Region ausgeführt werden. Die Änderungen werden automatisch auf alle replizierten Regionen angewendet. Weitere Informationen finden Sie unter Globale und regionale Features.

Themen

- Erstellen eines Snapshots Ihres Verzeichnisses
- Wiederherstellen Ihres Verzeichnisses mithilfe eines Snapshots
- Löschen eines Snapshots

Erstellen eines Snapshots Ihres Verzeichnisses

Mit einem Snapshot lässt sich Ihr Verzeichnis mit den Angaben wiederherstellen, die zum Zeitpunkt der Snapshot-Erstellung vorlagen. Gehen Sie zum Erstellen eines manuellen Snapshots Ihres Verzeichnisses folgendermaßen vor.

> **Note**
>
> Sie können maximal 5 manuelle Snapshots für jedes Verzeichnis erstellen. Falls Sie diesen Maximalwert bereits erreicht haben, müssen Sie einen vorhandenen manuellen Snapshot löschen, bevor Sie einen neuen erstellen.

So erstellen Sie einen manuellen Snapshot

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Verzeichnisdetails die Registerkarte Wartung aus.
4. Wählen Sie im Abschnitt Snapshots die Option Aktionen und dann Snapshot erstellen aus.
5. Geben Sie im Dialogfeld Verzeichnis-Snapshot erstellen einen Namen für den Snapshot ein, falls gewünscht. Wenn Sie fertig sind, wählen Sie Erstellen.

Je nach Größe des Verzeichnisses kann es einige Minuten dauern, bis der Snapshot erstellt wurde. Wenn der Snapshot fertig ist, ändert sich der Wert von Status in `Completed`.

Wiederherstellen Ihres Verzeichnisses mithilfe eines Snapshots

Das Wiederherstellen eines Verzeichnisses mithilfe eines Snapshots entspricht dem Zurücksetzen eines Verzeichnisses auf einen bestimmten vergangenen Zeitpunkt. Verzeichnis-Snapshots gelten nur für das Verzeichnis, in dem sie erstellt wurden. Ein Snapshot kann nur in dem Verzeichnis wiederhergestellt werden, in dem er erstellt wurde. Darüber hinaus beträgt das maximal unterstützte Alter eines manuellen Snapshots 180 Tage. Weitere Informationen finden Sie unter Useful shelf life of a system-state backup of Active Directory auf der Microsoft-Website.

> **Warning**
>
> Wir empfehlen, dass Sie sich vor einer Snapshot-Wiederherstellung an das AWS Support -Zentrum wenden. Möglicherweise können wir Ihnen helfen, eine Snapshot-Wiederherstellung zu vermeiden. Wiederherstellungen aus Snapshots können zu Datenverlust führen, da sie zeitpunktbezogen sind. Es ist wichtig, dass Sie sich darüber im Klaren sind, dass alle dem Verzeichnis zugeordneten DCs und DNS-Server offline sind, bis die Wiederherstellung abgeschlossen ist.

Gehen Sie folgendermaßen vor, um Ihr Verzeichnis mithilfe eines Snapshots wiederherzustellen.

So stellen Sie ein Verzeichnis mithilfe eines Snapshots wieder her

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.

3. Wählen Sie auf der Registerkarte Verzeichnisdetails die Registerkarte Wartung aus.
4. Wählen Sie im Abschnitt Snapshots einen Snapshot in der Liste aus, klicken Sie auf Aktionen und anschließend auf Snapshot wiederherstellen.
5. Überprüfen Sie im Dialogfeld Verzeichnis-Snapshot wiederherstellen die Informationen und wählen Sie dann Wiederherstellen aus.

Bei einem AWS verwalteten Microsoft AD-Verzeichnis kann es zwei bis drei Stunden dauern, bis das Verzeichnis wiederhergestellt ist. Nach einer erfolgreichen Wiederherstellung ändert sich der Wert Status für das Verzeichnis zu `Active`. Alle Änderungen, die nach dem Datum vorgenommen wurden, an dem der Snapshot erstellt wurde, werden überschrieben.

Löschen eines Snapshots

So löschen Sie einen Snapshot

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Verzeichnisdetails die Registerkarte Wartung aus.
4. Wählen Sie im Bereich Snapshots die Option Aktionen und anschließend die Option Snapshot löschen.
5. Überprüfen Sie, ob der Snapshot wirklich gelöscht werden soll, und wählen Sie dann Löschen aus.

Aktualisieren Sie Ihr AWS Managed Microsoft AD

Sie können Ihre Standard Edition AWS Managed Microsoft AD Active Directory auf die Enterprise Edition aktualisieren, indem Sie sich an AWS Support. Weitere Informationen finden Sie unter Erstellen von Supportanfragen und Fallmanagement im AWS Support Benutzerhandbuch.

> **Note**
>
> Die Replikation mehrerer Regionen ist nur in der AWS Managed Microsoft AD Enterprise Edition für die folgenden Regionen verfügbar:
>
> - US East (Ohio)
> - USA Ost (Nord-Virginia)

- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Hong Kong)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Kanada West (Calgary)
- China (Peking)
- China (Ningxia)
- Europa (Frankfurt)
- Europa (Zürich)
- Europa (Irland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Europa (Milan)
- Europa (Spain)
- Israel (Tel Aviv)
- Naher Osten (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)

- AWS GovCloud (USA West)

- AWS GovCloud (US-Ost)

Beim Upgrade Ihres AWS Managed Microsoft AD sind einige Einschränkungen zu beachten. Diese sind:

- Für das Upgrade fallen zusätzliche Kosten an. Weitere Informationen finden Sie unter AWS Directory Service -Preise.
- Sobald Ihr Active Directory aktualisiert wurde, kann es nicht mehr auf die vorherige Version zurückgesetzt werden.
- Frühere Snapshots können Active Directory nach dem Upgrade nicht zur Wiederherstellung verwendet werden.
- Upgrades erfolgen an einem vereinbarten Datum und zu einer vereinbarten Uhrzeit. AWS Support Upgrades finden von Montag bis Freitag von 9.00 Uhr bis 17.00 Uhr (PDT) statt.
- Der Upgrade-Vorgang dauert vier bis fünf Stunden.
- Während des Upgrade-Vorgangs werden die Domänencontroller Ihres AWS Managed Microsoft AD nacheinander aktualisiert. Dies kann sich negativ auf Ihre Leistung auswirken und zu Ausfallzeiten während Ihres Wartungsfensters führen.
- Wenn Ihre Anwendungen die Hostnamen oder IP-Adressen der Domänencontroller anstelle des Domänennamens Ihres Active Directory verwenden, müssen diese Anwendungen aktualisiert werden.
- Wenn Sie LDAPS (Lightweight Directory Access Protocol over SSL) verwenden, benötigen die Domänencontroller neue Zertifikate.

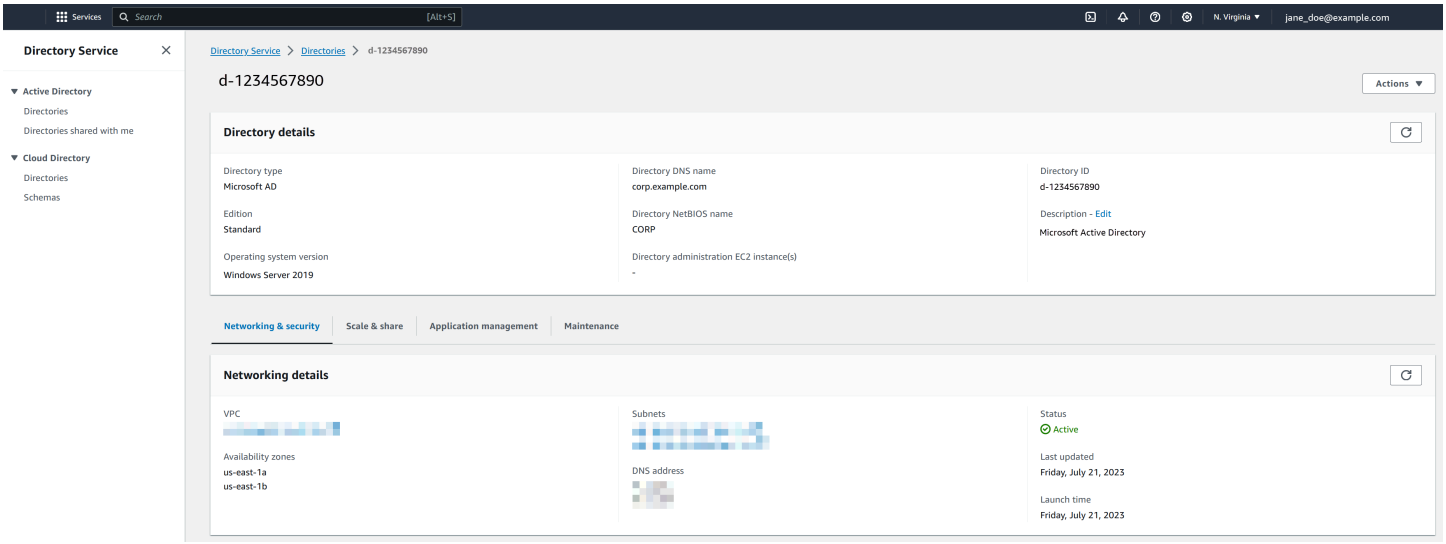
Verzeichnisinformationen anzeigen

Sie können detaillierte Informationen zu einem Verzeichnis einsehen.

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

1. Wählen Sie im Navigationsbereich der AWS Directory Service Konsole unter Active Directory Verzeichnisse aus.
2. Klicken Sie auf den Link der Verzeichnis-ID. Informationen über das Verzeichnis werden auf der Seite Verzeichnisdetails angezeigt.

Weitere Informationen zum Feld Status finden Sie unter Erläuterungen zum Verzeichnisstatus.



Benutzern und Gruppen den Zugriff auf AWS -Ressourcen gewähren

AWS Directory Service bietet die Möglichkeit, Ihren Verzeichnisbenutzern und -gruppen Zugriff auf AWS Dienste und Ressourcen zu gewähren, z. B. Zugriff auf die Amazon EC2 EC2-Konsole. Ähnlich wie Sie IAM-Benutzern Zugriff auf die Verwaltung von Verzeichnissen gewährenIdentitätsbasierte Richtlinien (IAM-Richtlinien), wie unter beschrieben, müssen Sie diesen Benutzern und Gruppen IAM-Rollen und -Richtlinien zuweisen, damit Benutzer in Ihrem Verzeichnis Zugriff auf andere AWS Ressourcen wie Amazon EC2 haben. Weitere Informationen finden Sie unter IAM-Rollen im IAM-Benutzerhandbuch.

Informationen darüber, wie Sie Benutzern Zugriff auf die gewähren, finden Sie unter AWS Management Console. Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren

Themen

- Erstellen einer neuen Rolle
- Bearbeiten der Vertrauensstellung für eine vorhandene Rolle
- Zuweisen von Benutzern oder Gruppen zu einer vorhandenen Rolle
- Anzeigen von Benutzern und Gruppen, die einer Rolle zugewiesen sind
- Entfernen eines Benutzers oder einer Gruppe aus einer Rolle
- Verwendung von AWS verwalteten Richtlinien mit AWS Directory Service

Erstellen einer neuen Rolle

Wenn Sie eine neue IAM-Rolle für die Verwendung mit erstellen müssen AWS Directory Service, müssen Sie sie mit der IAM-Konsole erstellen. Sobald die Rolle erstellt wurde, müssen Sie eine Vertrauensbeziehung mit dieser Rolle einrichten, bevor Sie diese Rolle in der AWS Directory Service Konsole sehen können. Weitere Informationen finden Sie unter Bearbeiten der Vertrauensstellung für eine vorhandene Rolle.

> **Note**
>
> Benutzer, die diese Aufgabe durchführen, müssen über die Berechtigung zur Ausführung der folgenden IAM-Aktionen verfügen. Weitere Informationen finden Sie unter Identitätsbasierte Richtlinien (IAM-Richtlinien).
>
> - ich bin: PassRole
> - ich bin: GetRole
> - ich bin: CreateRole
> - ich bin: PutRolePolicy

Um eine neue Rolle in der IAM-Konsole zu erstellen, gehen Sie wie folgt vor

1. Wählen Sie im Navigationsbereich der IAM Console Roles (Rollen) aus. Weitere Informationen finden Sie unter Erstellen einer Rolle (AWS Management Console) im IAM-Benutzerhandbuch.
2. Wählen Sie Rolle erstellen aus.
3. Wählen Sie unter Choose the service that will use this role (Wählen Sie den Service aus, der diese Rolle verwendet) die Option Directory Service und anschließend Next (Weiter) aus.
4. Aktivieren Sie das Kontrollkästchen neben der Richtlinie (z. B. AmazonEC2 FullAccess), die Sie auf Ihre Verzeichnisbenutzer anwenden möchten, und klicken Sie dann auf Weiter.
5. Fall erforderlich, fügen Sie ein Tag zur Rolle hinzu und klicken Sie dann auf Next (Weiter).
6. Geben Sie einen Role name (Rollennamen) und optional eine Description (Beschreibung) ein und wählen Sie dann Create role (Rolle erstellen) aus.

Beispiel: Eine Rolle für den Zugriff auf AWS Management Console erstellen

Die folgende Checkliste zeigt ein Beispiel der Aufgaben, die Sie zum Erstellen einer neuen Rolle ausführen müssen, die spezifischen Verzeichnisnutzer-Zugriff auf die Amazon-EC2-Konsole gewährt.

1. Erstellen Sie eine Rolle mit der IAM-Konsole mit dem oben beschriebenen Verfahren. Wenn Sie zur Eingabe einer Richtlinie aufgefordert werden, wählen Sie AmazonEC2 aus. FullAccess
2. Folgen Sie den Schritten unter Bearbeiten der Vertrauensstellung für eine vorhandene Rolle, um die soeben erstellte Rolle zu bearbeiten, und fügen Sie dann dem Richtliniendokument die erforderlichen Vertrauensstellungsinformationen hinzu. Dieser Schritt ist erforderlich, damit die Rolle sofort sichtbar ist, nachdem Sie AWS Management Console im nächsten Schritt den Zugriff auf die aktiviert haben.
3. Folgen Sie den Anweisungen unter Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren, um den allgemeinen Zugriff auf die AWS Management Console zu konfigurieren.
4. Folgen Sie den Anweisungen unter Zuweisen von Benutzern oder Gruppen zu einer vorhandenen Rolle, um der neuen Rolle Benutzer hinzuzufügen, die Vollzugriff auf EC2-Ressourcen benötigen.

Bearbeiten der Vertrauensstellung für eine vorhandene Rolle

Sie können Ihre vorhandenen IAM-Rollen Ihren AWS Directory Service Benutzern und Gruppen zuweisen. Dazu muss die Rolle jedoch eine Vertrauensbeziehung mit AWS Directory Service haben. Wenn Sie eine Rolle mithilfe des unter beschriebenen Verfahrens erstellenErstellen einer neuen Rolle, wird diese Vertrauensstellung automatisch eingerichtet. AWS Directory Service Sie müssen diese Vertrauensstellung nur für IAM-Rollen einrichten, die nicht von AWS Directory Service erstellt wurden.

Um eine Vertrauensbeziehung für eine bestehende Rolle einzurichten, AWS Directory Service

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich der IAM-Konsole unter Zugriffsverwaltung die Option Rollen.

   In der Konsole werden die Rollen für Ihr Konto angezeigt.
3. Wählen Sie den Namen der Rolle aus, die Sie ändern möchten, und öffnen Sie die Registerkarte Vertrauensstellungen auf der Rollenseite.
4. Wählen Sie Vertrauensrichtlinie bearbeiten aus.
5. Fügen Sie unter Vertrauensrichtlinie bearbeiten den folgenden Text ein und wählen Sie dann Richtlinie aktualisieren.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Sie können dieses Richtliniendokument auch mit der AWS CLI aktualisieren. Weitere Informationen finden Sie unter update-trust in der AWS CLI -Befehlsreferenz.

Zuweisen von Benutzern oder Gruppen zu einer vorhandenen Rolle

Sie können einem AWS Directory Service Benutzer oder einer Gruppe eine bestehende IAM-Rolle zuweisen. Stellen Sie dazu sicher, dass Sie die folgenden Schritte abgeschlossen haben.

Voraussetzungen

- Erstellen Sie ein AWS verwaltetes Microsoft AD.
- Erstellen Sie einen Benutzer oder eine Gruppe.
- Erstellen Sie eine Rolle, zu der eine Vertrauensbeziehung besteht AWS Directory Service. Sie können die Vertrauensbeziehung für eine bestehende Rolle bearbeiten.

> **Note**
>
> Der Zugriff für Benutzer in verschachtelten Gruppen innerhalb Ihres Verzeichnisses wird nicht unterstützt. Mitglieder übergeordneter Gruppen haben Konsolenzugriff, Mitglieder untergeordneter Gruppen nicht.

So weisen Sie einer vorhandenen IAM-Rolle Benutzer oder Gruppen zu

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole unter Active Directory die Option Verzeichnisse.

2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Ihre Zuweisungen vornehmen möchten, und wählen Sie dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
4. Scrollen Sie nach unten zum AWS Management ConsoleAbschnitt, wählen Sie Aktionen und Aktivieren aus.
5. Wählen Sie im Abschnitt Zugriff auf die Delegiertenkonsole den IAM-Rollennamen für die bestehende IAM-Rolle aus, der Sie Benutzer zuweisen möchten.
6. Wählen Sie auf der Seite Selected role (Rolle auswählen) unter Manage users and groups for this role (Benutzer und Gruppen für diese Rolle verwalten) die Option Add (Hinzufügen) aus.
7. Wählen Sie auf der Seite Benutzer und Gruppen zu Rollen hinzufügen unter SStruktur auswählen entweder die Struktur AWS Managed Microsoft AD (diese Struktur) oder die On-Premises-Struktur (vertrauenswürdige Struktur) aus, je nachdem, welche Struktur die Konten enthält, die Zugriff auf die AWS Management Console benötigen. Weitere Informationen zum Konfigurieren einer vertrauenswürdigen Gesamtstruktur finden Sie unter Tutorial: Eine Vertrauensstellung zwischen Ihrem AWS Managed Microsoft AD und Ihrer selbstverwalteten Active-Directory-Domain erstellen.
8. Wählen Sie unter Specify, which users or groups to add (Angeben, welche Benutzer oder Gruppen hinzugefügt werden sollen) entweder Find by user (Nach Benutzer suchen) oder Find by group (Nach Gruppe suchen) aus und geben Sie dann den Namen des Benutzers oder der Gruppe ein. Wählen Sie in der Liste der möglichen Treffer den Benutzer oder die Gruppe aus, den/die Sie hinzufügen möchten.
9. Wählen Sie Add (Hinzufügen) aus, um die Zuweisung der Benutzer und Gruppen zu der Rolle abzuschließen.

Anzeigen von Benutzern und Gruppen, die einer Rolle zugewiesen sind

Gehen Sie wie folgt vor, um die einer Rolle zugewiesenen Benutzer und Gruppen anzuzeigen.

Voraussetzungen

- Weisen Sie Ihre Benutzer oder Gruppen einer vorhandenen Rolle zu.

So zeigen Sie die einer Rolle zugewiesenen Benutzer und Gruppen an

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole unter Active Directory die Option Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Ihre Zuweisungen einsehen möchten, und wählen Sie dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.
4. Wählen Sie im Abschnitt Delegierter Konsolenzugriff die IAM-Rolle, die Sie anzeigen möchten.
5. Auf der Seite Ausgewählte Rolle können Sie unter dem Abschnitt Benutzer und Gruppen für diese Rolle verwalten die Benutzer und Gruppen einsehen, die der Rolle zugewiesen sind.

Entfernen eines Benutzers oder einer Gruppe aus einer Rolle

Gehen Sie wie folgt vor, um einen Benutzer oder eine Gruppe aus einer Rolle zu entfernen.

So entfernen Sie einen Benutzer oder eine Gruppe aus einer Rolle

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Ihre Zuweisungen entfernen möchten, und wählen Sie dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.

4. Wählen Sie im Abschnitt AWS Management Console die Rolle aus, die Sie anzeigen möchten.
5. Wählen Sie auf der Seite Selected role (Ausgewählte Rolle) unter Manage users and groups for this role (Benutzer und Gruppen für diese Rolle verwalten) die Benutzer oder Gruppen aus, aus denen die Rolle entfernt werden soll, und klicken Sie auf Remove (Entfernen). Die Rolle wird von den angegebenen Benutzern und Gruppen entfernt, nicht jedoch aus Ihrem Konto.

Verwendung von AWS verwalteten Richtlinien mit AWS Directory Service

AWS Directory Service bietet die folgenden verwalteten AWS-Richtlinien, um Ihren Benutzern und Gruppen Zugriff auf AWS-Services und -Ressourcen zu erteilen, beispielsweise Zugriff auf die Amazon-EC2-Konsole. Sie müssen sich an der AWS Management Console anmelden, bevor Sie diese Richtlinien anzeigen können.

- Schreibgeschützter Zugriff
- Power User Access
- Vollzugriff auf AWS Directory Service
- AWS Directory Service: schreibgeschützter Zugriff
- Vollzugriff auf Amazon Cloud Directory
- Amazon Cloud Directory: schreibgeschützter Zugriff
- Vollzugriff auf Amazon EC2
- Amazon EC2: schreibgeschützter Zugriff
- Vollzugriff auf Amazon VPC
- Amazon VPC: schreibgeschützter Zugriff
- Vollzugriff auf Amazon RDS
- Amazon RDS: schreibgeschützter Zugriff
- Vollzugriff auf Amazon DynamoDB
- Amazon DynamoDB: schreibgeschützter Zugriff
- Vollzugriff auf Amazon S3
- Amazon S3: schreibgeschützter Zugriff
- Vollzugriff auf AWS CloudTrail
- AWS CloudTrail: schreibgeschützter Zugriff
- Vollzugriff auf Amazon CloudWatch
- Amazon CloudWatch: schreibgeschützter Zugriff

- Vollzugriff auf Amazon CloudWatch Logs
- Amazon CloudWatch Logs: schreibgeschützter Zugriff

Weitere Informationen zum Erstellen eigener Richtlinien finden Sie unter Beispielrichtlinien für die Verwaltung von AWS-Ressourcen im IAM-Benutzerhandbuch.

Ermöglichen Sie den Zugriff auf AWS Anwendungen und Dienste

Benutzer können AWS Managed Microsoft AD autorisieren, AWS Anwendungen und Diensten wie Amazon WorkSpaces Zugriff auf Ihre Active Directory zu gewähren. Die folgenden AWS Anwendungen und Dienste können für die Verwendung mit AWS Managed Microsoft AD aktiviert oder deaktiviert werden.

AWS Anwendung/Dienst	Weitere Informationen …
Amazon Chime	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Chime.
Amazon Connect	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Connect.
Amazon FSx für Windows File Server	Weitere Informationen finden Sie unter Verwenden von Amazon FSx mit AWS Directory Service für Microsoft Active Directory.
Amazon QuickSight	Weitere Informationen finden Sie im QuickSight Amazon-Benutzerhandbuch.
Amazon Relational Database Service	Weitere Informationen finden Sie im Amazon RDS-Benutzerhandbuch.
Amazon WorkDocs	Weitere Informationen finden Sie im Amazon WorkDocs Administration Guide.
Amazon WorkMail	Weitere Informationen finden Sie im WorkMail Amazon-Administratorhandbuch.
Amazon WorkSpaces	Sie können ein Simple AD, AWS Managed Microsoft AD oder AD Connector direkt von

AWS Anwendung/Dienst	Weitere Informationen …
	aus erstellen WorkSpaces. Starten Sie einfach Advanced Setup bei der Erstellung Ihres Workspace. Weitere Informationen finden Sie im Amazon WorkSpaces Administration Guide.
AWS Client VPN	Weitere Informationen finden Sie im AWS Client VPN -Benutzerhandbuch.
AWS IAM Identity Center	Weitere Informationen finden Sie im AWS IAM Identity Center -Benutzerhandbuch.
AWS License Manager	Weitere Informationen finden Sie im License-Manager-Benutzerhandbuch.
AWS Management Console	Weitere Informationen finden Sie unter Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren.
AWS Private Certificate Authority	Weitere Informationen finden Sie unter AWS Private CA Connector für Active Directory.
AWS Transfer Family	Weitere Informationen finden Sie im AWS Transfer Family -Benutzerhandbuch.

Nach der Aktivierung verwalten Sie den Zugriff auf Ihre Verzeichnisse in der Konsole der Anwendung oder dem Service, denen Sie Zugriff auf Ihr Verzeichnis gewähren wollen. Gehen Sie wie folgt vor, um die oben beschriebenen Links zu AWS Anwendungen und Diensten in der AWS Directory Service Konsole zu finden.

Zum Anzeigen der Anwendungen und Services für ein Verzeichnis

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.

4. Sehen Sie sich die Liste im Abschnitt AWS -Anwendungen und -Services an.

Weitere Informationen zur Autorisierung oder Deautorisierung von AWS Anwendungen und Diensten mithilfe von AWS Directory ServiceAutorisierung für AWS Anwendungen und Dienste mit AWS Directory Service

Themen

- Erstellen einer Zugriffs-URL
- Single Sign-On

Erstellen einer Zugriffs-URL

Eine Zugriffs-URL wird bei AWS-Anwendungen und -Services wie Amazon WorkDocs verwendet, um eine Anmeldeseite zu erreichen, die mit Ihrem Verzeichnis verknüpft ist. Die URL muss global eindeutig sein. Folgen Sie der Anleitung unten, um eine Zugriffs-URL für Ihr Verzeichnis zu erstellen.

> **Warning**
>
> Nachdem die URL für den Anwendungszugriff für dieses Verzeichnis erstellt wurde, kann sie nicht mehr geändert werden. Nachdem eine Zugriffs-URL erstellt wurde, kann sie nicht mehr von anderen verwendet werden. Beim Löschen Ihres Verzeichnisses wird auch die Zugriffs-URL gelöscht. Dann kann sie in einem anderen Konto genutzt werden.

> **Note**
>
> Die Zugriffs-URL kann nur von der primären Region aus konfiguriert werden, wenn Verzeichnisse mit mehreren Regionen verwendet werden.

So erstellen Sie eine Zugriffs-URL

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

- Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, markieren Sie die primäre Region und wählen dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
- Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.

4. Wenn dem Verzeichnis keine Zugriffs-URL zugewiesen ist, wird im Bereich Application access URL (URL für den Anwendungszugriff) die Schaltfläche Create (Erstellen) angezeigt. Geben Sie einen Verzeichnisalias ein und wählen Sie Create (Erstellen) aus. Falls der Fehler Entity bereits vorhanden zurückgegeben wird, wurde das angegebene Alias bereits einem anderen Verzeichnis zugewiesen. Wählen Sie ein anderes Alias aus und wiederholen Sie die Schritte.

   Ihre Zugriffs-URL wird im Format *<alias>*.awsapps.com angegeben. Standardmäßig werden Sie über diese URL zur Anmeldeseite für Amazon WorkDocs weitergeleitet.

Single Sign-On

AWS Directory Service bietet die Möglichkeit, Ihren Benutzern den Zugriff auf Amazon WorkDocs von einem Computer aus zu ermöglichen, der mit dem Verzeichnis verbunden ist, ohne ihre Anmeldeinformationen separat eingeben zu müssen.

Bevor Sie Single Sign-On aktivieren, müssen Sie zusätzliche Schritte durchführen, um die Webbrowser Ihrer Benutzer zur Unterstützung von Single Sign-On vorzubereiten. Benutzer müssen eventuell ihre Web-Browser-Einstellungen ändern, um Single Sign-On zu ermöglichen.

> **Note**
>
> Single Sign-On funktioniert nur mit einem Computer, der dem AWS Directory Service - Verzeichnis beigetreten ist. Es kann nicht auf Computern verwendet werden, die nicht an das Verzeichnis angebunden sind.

Wenn es sich bei Ihrem Verzeichnis um ein AD Connector-Verzeichnis handelt und das AD Connector-Servicekonto nicht über die Berechtigung zum Hinzufügen oder Entfernen des Service-Prinzipalnamensattributs verfügt, stehen Ihnen für die folgenden Schritte 5 und 6 zwei Optionen zur Verfügung:

1. Sie können fortfahren und werden zur Eingabe des Benutzernamens und des Passworts für einen Verzeichnisbenutzer aufgefordert, der über diese Berechtigung zum Hinzufügen oder Entfernen des Service-Prinzipalnamensattributs für das AD Connector-Servicekonto verfügt. Diese Anmeldeinformationen werden nur verwendet, um Single Sign-On zu aktivieren, und werden nicht vom Service gespeichert. Die Berechtigungen des AD Connector-Servicekontos werden nicht geändert.
2. Sie können Berechtigungen delegieren, um es dem AD Connector Connector-Dienstkonto zu ermöglichen, das Dienstprinzipalnamenattribut für sich selbst hinzuzufügen oder zu entfernen. Sie können die folgenden PowerShell Befehle von einem Computer aus ausführen, der mit einer Domäne verbunden ist, und verwenden dabei ein Konto, das über die Berechtigungen für das AD Connector Connector-Dienstkonto verfügt. Der folgende Befehl gibt dem AD Connector-Servicekonto die Möglichkeit, ein Service-Prinzipalnamenattribut nur für sich selbst hinzuzufügen und zu entfernen.

```
$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"
```

Um Single Sign-On bei Amazon zu aktivieren oder zu deaktivieren WorkDocs

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Wählen Sie im Abschnitt URL für den Anwendungszugriff die Option Aktivieren aus, um Single Sign-On für Amazon WorkDocs zu aktivieren.

   Wenn die Schaltfläche Aktivieren nicht angezeigt wird, müssen Sie zuerst eine Access-URL erstellen, bevor diese Option angezeigt wird. Weitere Informationen zum Erstellen einer Zugriffs-URL finden Sie unter Erstellen einer Zugriffs-URL.
5. Wählen Sie im Dialogfeld Single Sign-On für dieses Verzeichnis aktivieren die Option Aktivieren. Single Sign-On ist für das Verzeichnis aktiviert.
6. Wenn Sie Single Sign-On mit Amazon später deaktivieren möchten WorkDocs, wählen Sie Deaktivieren und wählen Sie dann im Dialogfeld Single Sign-On für dieses Verzeichnis deaktivieren erneut Deaktivieren aus.

Themen

- Single Sign-On für IE und Chrome
- Single Sign-On für Firefox

Single Sign-On für IE und Chrome

Damit die Browser Microsoft Internet Explorer (IE) und Google Chrome Single Sign-On unterstützen, müssen auf dem Client-Computer die folgenden Aufgaben durchgeführt werden:

- Fügen Sie Ihre Zugriffs-URL (z. B. https://*<alias>*.awsapps.com) zur Liste der zulässigen Websites für Single Sign-On hinzu.
- Aktivieren Sie Active Scripting (). JavaScript
- Erlauben Sie die automatische Anmeldung.
- Aktivieren Sie die integrierte Authentifizierung.

Sie oder Ihre Benutzer können diese Aufgaben manuell ausführen, oder Sie können diese Einstellungen mithilfe von Gruppenrichtlinieneinstellungen ändern.

Themen

Manuelles Update für Single Sign-On in Windows

Um Single Sign-On in einem Windows-Computer manuell zu aktivieren, führen Sie die folgenden Schritte auf dem Client-Computer aus. Einige dieser Einstellungen können bereits korrekt eingestellt sein.

Single Sign-On für Internet Explorer und Chrome unter Windows manuell aktivieren

1. Um das Dialogfeld Internet Properties zu öffnen, wählen Sie das Start-Menü, geben `Internet Options` in das Suchfeld ein, und wählen Internet Options.
2. Fügen Sie Ihre Zugriffs-URL zur Liste der zulässigen Websites für Single Sign-On hinzu, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie im Dialogfeld Internet Properties die Registerkarte Security.
   b. Wählen Sie Local intranet und Sites.
   c. Wählen Sie im Dialogfeld Local intranet die Option Advanced.
   d. Fügen Sie Ihre Zugriffs-URL zur Liste der Websites hinzu und klicken Sie auf Close.
   e. Wählen Sie im Dialogfeld Local intranet OK.
3. Zum Aktivieren der aktiven Skripts, führen Sie die folgenden Schritte aus:
   a. Wählen Sie auf der Registerkarte Security im Dialogfeld Internet Properties die Option Custom level.
   b. Scrollen Sie im Dialogfeld Security Settings - Local Intranet Zone nach unten bis Scripting und wählen Sie Enable unter Active scripting.
   c. Wählen Sie im Dialogfeld Security Settings - Local Intranet Zone OK.
4. Zum Aktivieren der automatischen Anmeldung, führen Sie die folgenden Schritte aus:
   a. Wählen Sie auf der Registerkarte Security im Dialogfeld Internet Properties die Option Custom level.
   b. Scrollen Sie im Dialogfeld Security Settings - Local Intranet Zone nach unten bis User Authentication und wählen Sie Automatic logon only in Intranet zone unter Logon.

c. Wählen Sie im Dialogfeld Security Settings - Local Intranet Zone OK.

d. Wählen Sie im Dialogfeld Security Settings - Local Intranet Zone OK.

5. Zum Aktivieren der integrierten Authentifizierung, führen Sie die folgenden Schritte aus:

a. Wählen Sie im Dialogfeld Internet Properties die Registerkarte Advanced.

b. Scrollen Sie nach unten bis Security, und wählen Sie Enable Integrated Windows Authentication.

c. Wählen Sie im Dialogfeld Internet Properties OK.

6. Schließen Sie den Browser und öffnen Sie ihn erneut, damit diese Änderungen wirksam werden.

Manuelles Update für Single Sign-On in OS X

Um manuell Single Sign-On für Chrome in OS X zu aktivieren, führen Sie die folgenden Schritte aus. Sie benötigen Administratorrechte auf Ihrem Computer, um diese Schritte ausführen zu können.

Single Sign-On für Chrome auf OS X manuell aktivieren

1. Fügen Sie der AuthServerAllowlistRichtlinie Ihre Zugriffs-URL hinzu, indem Sie den folgenden Befehl ausführen:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Öffnen Sie System Preferences, wechseln Sie in den Bereich Profiles und löschen Sie das Profil `Chrome Kerberos Configuration`.

3. Starten Sie Chrome neu und öffnen Sie chrome://policy in Chrome, um zu bestätigen, dass die neuen Einstellungen vorhanden sind.

Gruppenrichtlinieneinstellungen für Single Sign-On

Der Domain-Administrator kann Gruppenrichtlinieneinstellungen implementieren, um die Single-Sign-On-Änderungen auf Client-Computern durchzuführen, die mit der Domain verbunden sind.

> **Note**
>
> Wenn Sie die Chrome-Webbrowser auf den Computern in Ihrer Domain mit Chrome-Richtlinien verwalten, müssen Sie Ihre Zugriffs-URL zur AuthServerAllowlistRichtlinie

hinzufügen. Weitere Informationen zum Einrichten von Chrome-Richtlinien finden Sie unter Policy-Einstellungen in Chrome.

Single Sign-On für Internet Explorer und Chrome mit Gruppenrichtlinieneinstellungen aktivieren

1. Erstellen Sie ein neues Gruppenrichtlinienobjekt, indem Sie die folgenden Schritte ausführen:
   a. Öffnen Sie das Tool für die Gruppenrichtlinienverwaltung, navigieren Sie zu Ihrer Domain und wählen Sie Group Policy Objects.
   b. Wählen Sie im Hauptmenü Action und dann New.
   c. Geben Sie in das Dialogfeld Neues GPO einen aussagekräftigen Namen für das Gruppenrichtlinienobjekt ein, wie beispielsweise `IAM Identity Center Policy`, und behalten Sie für Source Starter GPO den Eintrag (kein) bei. Klicken Sie auf OK.
2. Fügen Sie die Zugriffs-URL zur Liste der zulässigen Websites für Single Sign-On hinzu, indem Sie die folgenden Schritte ausführen:
   a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Gruppenrichtlinienobjekte, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre IAM-Identity-Center-Richtlinie und wählen Sie Bearbeiten.
   b. Navigieren Sie in der Richtlinien-Baumstruktur zu User Configuration > Preferences > Windows Settings.
   c. Öffnen Sie in der Liste Windows Settings das Kontextmenü (Rechtsklick) für Registry und wählen Sie New registry item.
   d. Geben Sie im Dialogfeld New Registry Properties die folgenden Einstellungen ein, und wählen Sie OK:

      Action (Aktion)

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      Pfad

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

Der Wert für den *<alias>* wird von Ihrer Zugriffs-URL abgeleitet. Wenn Ihre Zugriffs-URL `https://examplecorp.awsapps.com` ist, wird `examplecorp` der Alias und der Registrierungsschlüssel wird `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Wertname

`https`

Werttyp

`REG_DWORD`

Wertdaten

1

3. Zum Aktivieren der aktiven Skripts, führen Sie die folgenden Schritte aus:

   a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Gruppenrichtlinienobjekte, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre IAM-Identity-Center-Richtlinie und wählen Sie Bearbeiten.

   b. Navigieren Sie in der Richtlinien-Baumstrukturzu Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

   c. Öffnen Sie in der Liste Intranet Zone das Kontextmenü (Rechtsklick) für Allow active scripting und wählen Sie Edit.

   d. Geben Sie im Dialogfeld Allow active scripting die folgenden Einstellungen ein, und wählen Sie OK:

      - Wählen Sie das Optionsfeld Enabled.
      - Setzen Sie unter Options die Option Allow active scripting auf Enable.

4. Zum Aktivieren der automatischen Anmeldung, führen Sie die folgenden Schritte aus:

   a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Group Policy Objects, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre SSO-Richtlinie und wählen Sie Bearbeiten.

   b. Navigieren Sie in der Richtlinien-Baumstrukturzu Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. Öffnen Sie in der Liste Intranet Zone das Kontextmenü (Rechtsklick) für Logon options und wählen Sie Edit.

d. Geben Sie im Dialogfeld Logon options die folgenden Einstellungen ein, und wählen Sie OK:

- Wählen Sie das Optionsfeld Enabled.
- Setzen Sie unter Options die Logon options auf Automatic logon only in Intranet zone.

5. Zum Aktivieren der integrierten Authentifizierung, führen Sie die folgenden Schritte aus:

a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Gruppenrichtlinienobjekte, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre IAM-Identity-Center-Richtlinie und wählen Sie Bearbeiten.

b. Navigieren Sie in der Richtlinien-Baumstruktur zu User Configuration > Preferences > Windows Settings.

c. Öffnen Sie in der Liste Windows Settings das Kontextmenü (Rechtsklick) für Registry und wählen Sie New registry item.

d. Geben Sie im Dialogfeld New Registry Properties die folgenden Einstellungen ein, und wählen Sie OK:

Action (Aktion)

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

Pfad

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

Wertname

```
EnableNegotiate
```

Werttyp

```
REG_DWORD
```

Wertdaten

```
1
```

6. Schließen Sie das Fenster Group Policy Management Editor, falls es noch geöffnet ist.

7. Weisen Sie die neue Richtlinie Ihrer Domain zu, indem Sie die folgenden Schritte ausführen:

    a. Öffnen Sie im Gruppenrichtlinien-Baum das Kontextmenü (Rechtsklick) für Ihre Domain, und wählen Sie Link an Existing GPO.

    b. Wählen Sie in der Liste Gruppenrichtlinienobjekte Ihre IAM-Identity-Center-Richtlinie, und wählen Sie OK.

Diese Änderungen werden nach dem nächsten Gruppenrichtlinien-Update auf dem Client wirksam, oder wenn sich der Benutzer das nächste Mal anmeldet.

Single Sign-On für Firefox

Damit der Mozilla Firefox-Browser Single Sign-On unterstützt, fügen Sie Ihre Zugriffs-URL (z. B. https://*<alias>*.awsapps.com) der Liste der genehmigten Websites für Single Sign-On hinzu. Dies kann manuell oder automatisiert durch ein Skript erfolgen.

Themen

- Manuelles Update für Single Sign-On
- Automatisches Update für Single Sign-On

Manuelles Update für Single Sign-On

Um manuell Ihre Zugriffs-URL zur Liste der zulässigen Websites in Firefox hinzuzufügen, führen Sie die folgenden Schritte auf dem Client-Computer aus.

So fügen Sie manuell Ihre Zugriffs-URL zur Liste der zulässigen Websites in Firefox hinzu

1. Öffnen Sie Firefox und öffnen Sie die Seite `about:config`.
2. Öffnen Sie die Einstellung `network.negotiate-auth.trusted-uris` und fügen Sie Ihre Zugriffs-URL der Liste der Websites hinzu. Verwenden Sie ein Komma (,), um mehrere Einträge zu trennen.

Automatisches Update für Single Sign-On

Als Domainadministrator können Sie ein Skript hinzufügen, um Ihre Zugriffs-URL auf allen Computern in Ihrem Netzwerk der Firefox-Benutzereinstellung `network.negotiate-auth.trusted-uris` hinzuzufügen. Weitere Informationen finden Sie unter https://support.mozilla.org/en-US/questions/939037.

Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren

AWS Directory Service ermöglicht es Ihnen, Mitgliedern Ihres Verzeichnisses Zugriff auf AWS Management Console zu gewähren. Standardmäßig haben die Mitglieder Ihres Verzeichnisses keinen Zugriff auf AWS-Ressourcen. Sie weisen Ihren Verzeichnismitgliedern IAM-Rollen zu, um ihnen Zugriff auf die verschiedenen AWS-Services und Ressourcen zu geben. Die IAM-Rolle definiert die Services, Ressourcen und Zugriffsebenen, die für das Mitglied Ihres Verzeichnisses verfügbar sind.

Bevor Sie den Mitgliedern Ihres Verzeichnisses Konsolenzugriff gewähren können, muss das Verzeichnis über eine Zugriffs-URL verfügen. Weitere Informationen zum Abrufen von Verzeichnisdetails und der Zugriffs-URL finden Sie unter Verzeichnisinformationen anzeigen. Weitere Informationen zum Erstellen einer Zugriffs-URL finden Sie unter Erstellen einer Zugriffs-URL.

Weitere Informationen zum Erstellen von IAM-Rollen und zum Zuweisen dieser Rollen zu den Mitgliedern Ihres Verzeichnisses finden Sie unter Benutzern und Gruppen den Zugriff auf AWS - Ressourcen gewähren.

Themen

- AWS Management Console-Zugriff aktivieren
- AWS Management Console-Zugriff deaktivieren
- Die Dauer der Anmeldesitzung festlegen

Zugehöriger Blog-Artikel zur AWS-Sicherheit

- Wie Sie mit AWS Managed Microsoft AD und Ihren On-Premises-Anmeldeinformationen auf die AWS Management Console zugreifen

> **Note**
>
> Der Zugriff auf AWS Management Console ist ein regionales Feature von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.

AWS Management Console-Zugriff aktivieren

Standardmäßig ist der Konsolenzugriff für kein Verzeichnis aktiviert. Gehen Sie zum Aktivieren des Konsolenzugriffs für Benutzer und Gruppen in Ihrem Verzeichnis folgendermaßen vor:

So aktivieren Sie den Konsolenzugriff

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie den Zugriff auf die AWS Management Console aktivieren möchten, und wählen Sie dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.
4. Wählen Sie unter dem Abschnitt AWS Management Console die Option Aktivieren aus. Der Konsolenzugriff ist jetzt für Ihr Verzeichnis aktiviert.

   Bevor sich die Benutzer mit Ihrer Zugangs-URL bei der Konsole anmelden können, müssen Sie Ihre Benutzer zunächst der Rolle hinzufügen. Weitere Informationen zum Zuweisen von Benutzern zu IAM-Rollen finden Sie unter Zuweisen von Benutzern oder Gruppen zu einer vorhandenen Rolle. Nachdem die IAM-Rollen zugewiesen wurden, können die entsprechenden Benutzer über die Zugriffs-URL auf die Konsole zugreifen. Lautet die Zugriffs-URL Ihres Verzeichnisses zum Beispiel „example-corp.awsapps.com“, lautet die URL für den Zugriff auf die Konsole „https://example-corp.awsapps.com/console/“.

AWS Management Console-Zugriff deaktivieren

Gehen Sie zum Deaktivieren des Konsolenzugriffs für Benutzer und Gruppen in Ihrem Verzeichnis folgendermaßen vor:

So deaktivieren Sie den Konsolenzugriff

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

- Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie den Zugriff auf die AWS Management Console deaktivieren möchten, und wählen Sie dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
- Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.

4. Wählen Sie im Abschnitt AWS Management Console die Option Deaktivieren aus. Der Konsolenzugriff ist jetzt für Ihr Verzeichnis deaktiviert.
5. Nach dem Zuweisen von IAM-Rollen zu Benutzern oder Gruppen im Verzeichnis ist die Schaltfläche Deaktivieren möglicherweise nicht mehr verfügbar. In diesem Fall müssen Sie alle IAM-Rollenzuweisungen für das Verzeichnis entfernen, bevor Sie fortfahren, einschließlich der Zuweisungen für Benutzer oder Gruppen in Ihrem Verzeichnis, die gelöscht wurden, was als Gelöschter Benutzer oder Gelöschte Gruppe angezeigt wird.

   Nachdem alle IAM-Rollenzuweisungen entfernt wurden, wiederholen Sie die oben genannten Schritte.

Die Dauer der Anmeldesitzung festlegen

Standardmäßig haben die Benutzer 1 Stunde Zeit, um nach dem Anmelden in der Konsole eine Sitzung zu nutzen, bevor sie abgemeldet werden. Nach dieser Zeit müssen sich die Benutzer erneut anmelden, um eine weitere 1-stündige Sitzung zu starten, bevor sie erneut abgemeldet werden. Gehen Sie folgendermaßen vor, um die Dauer auf bis zu 12 Stunden pro Sitzung zu ändern.

So legen Sie die Dauer der Anmeldesitzung fest

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie die Login-Sitzungslänge einstellen möchten, und wählen Sie dann die Registerkarte Anwendungsverwaltung. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.

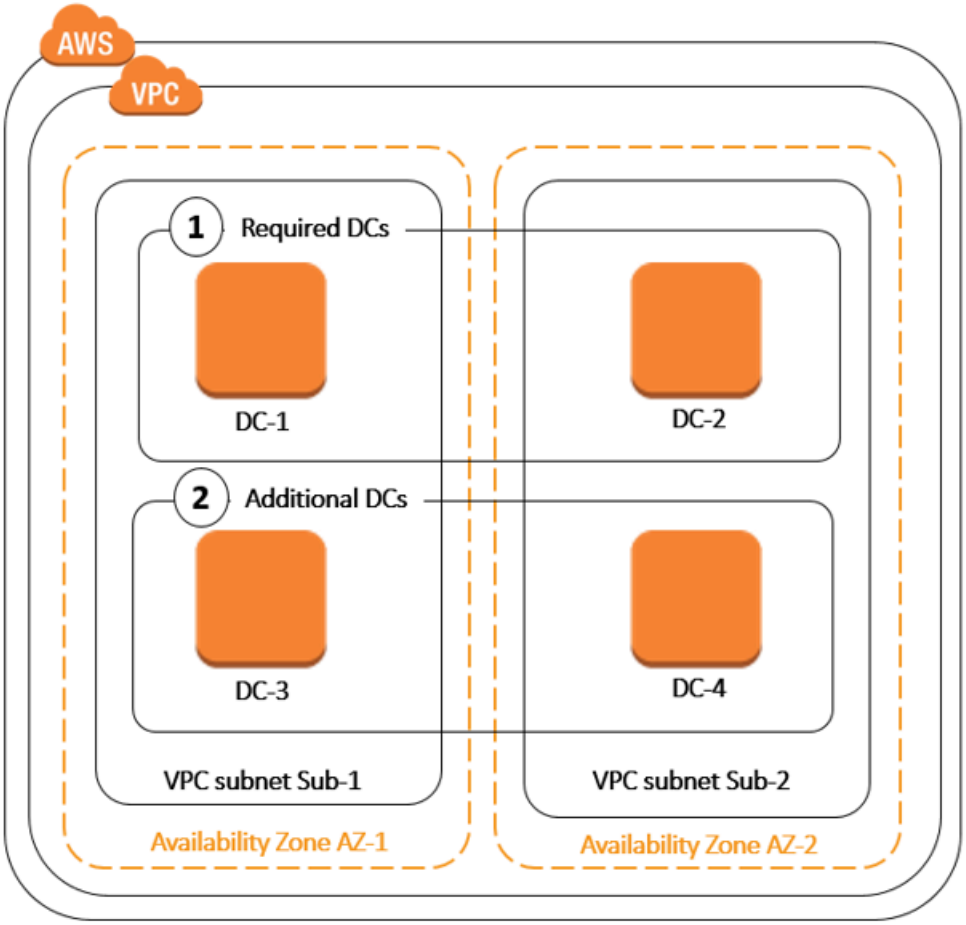
4. Wählen Sie unter dem Abschnitt AWS-Anwendungen und -Services die Option AWS-Managementkonsole.
5. Wählen Sie im Dialogfeld Zugriff auf AWS-Ressourcen verwalten die Option Fortfahren.
6. Bearbeiten Sie auf der Seite Assign users and groups to IAM roles unter Set login session length den Zahlenwert, und wählen Sie dann Save.

Bereitstellen zusätzlicher Domain-Controller

Die Bereitstellung zusätzlicher Domain-Controller erhöht die Redundanz. Dies führt zu einer noch größeren Ausfallsicherheit und höherer Verfügbarkeit. Dies verbessert auch die Leistung Ihres Verzeichnisses, weil mehr Active Directory-Anfragen unterstützt werden. Sie können jetzt beispielsweise AWS Managed Microsoft AD verwenden, um mehrere .NET-Anwendungen zu unterstützen, die auf großen Flotten von Amazon EC2- und Amazon RDS for SQL Server Server-Instances bereitgestellt werden.

Wenn Sie Ihr Verzeichnis zum ersten Mal erstellen, stellt AWS Managed Microsoft AD zwei Domänencontroller in mehreren Availability Zones bereit, was für Hochverfügbarkeitszwecke erforderlich ist. Später können Sie problemlos weitere Domänencontroller über die AWS Directory Service Konsole bereitstellen, indem Sie einfach die Gesamtzahl der gewünschten Domänencontroller angeben. AWS Managed Microsoft AD verteilt die zusätzlichen Domain-Controller auf die Availability Zones und Amazon VPC-Subnetze, auf denen Ihr Verzeichnis läuft.

In der folgenden Abbildung beispielsweise stellen DC-1 und DC-2 die beiden Domain-Controller dar, die ursprünglich mit Ihrem Verzeichnis erstellt wurden. In der AWS Directory Service Konsole werden diese Standard-Domänencontroller als Erforderlich bezeichnet. AWS Managed Microsoft AD lokalisiert jeden dieser Domänencontroller während der Verzeichniserstellung bewusst in separaten Availability Zones. Später können Sie zwei weitere Domain-Controller hinzufügen, um die Authentifizierungslast bei Spitzenanmeldezeiten zu verteilen. DC-3 und DC-4 und reflektieren den neuen Domain-Controller, die die Konsole jetzt als Additional angibt. Wie zuvor platziert AWS Managed Microsoft AD die neuen Domänencontroller wieder automatisch in verschiedenen Availability Zones, um die hohe Verfügbarkeit Ihrer Domain sicherzustellen.



Dank dieses Prozess müssen Sie die Verzeichnisdatenreplikation, die automatischen täglichen Snapshots oder die Überwachung für die zusätzlichen Domain-Controller nicht mehr manuell konfigurieren. Außerdem ist es für Sie einfacher, unternehmenskritische, in das Active Directory integrierte Workloads in die AWS -Cloud zu migrieren und auszuführen, ohne dass Sie Ihre eigene Active-Directory-Infrastruktur bereitstellen und warten müssen. Mithilfe der UpdateNumberOfDomainControllersAPI können Sie auch zusätzliche Domänencontroller für AWS Managed Microsoft AD bereitstellen oder entfernen.

> **Note**
>
> Zusätzliche Domänencontroller sind ein regionales Feature von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter Globale und regionale Features.

Zusätzliche Domain-Controller hinzufügen oder entfernen

Bevor Sie zusätzliche Domain-Controller hinzufügen oder entfernen, finden Sie hier weitere Informationen zu den Anforderungen an Domain-Controller:

- Nachdem Sie zusätzliche Domain-Controller bereitgestellt haben, können Sie die Anzahl der Domain-Controller auf zwei reduzieren, das Minimum für Fehlertoleranz und hohe Verfügbarkeit.
- Die gelöschten Domain-Controller werden aus der Liste der zusätzlichen Domain-Controller entfernt. Die primären und sekundären Domain-Controller sind erforderlich und können nicht gelöscht werden.
- Wenn Sie Ihr AWS verwaltetes Microsoft AD so konfiguriert haben, dass LDAPS aktiviert wird, wird LDAPS für alle zusätzlichen Domänencontroller, die Sie hinzufügen, ebenfalls automatisch aktiviert. Weitere Informationen finden Sie unter Sicheres LDAP oder LDAPS aktivieren.

Führen Sie die folgenden Schritte aus, um zusätzliche Domain-Controller in Ihrem Verzeichnis in AWS Managed Microsoft AD bereitzustellen oder daraus zu entfernen.

Zusätzliche Domain-Controller hinzufügen oder entfernen

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn unter Multi-Region-Replikation mehrere Regionen angezeigt werden, wählen Sie die Region aus, in der Sie Domain-Controller hinzufügen oder entfernen möchten, und wählen Sie dann die Registerkarte Skalieren und Freigeben. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Skalieren und Freigeben.
4. Wählen Sie im Abschnitt Domain-Controller die Option Bearbeiten.
5. Geben Sie die Anzahl der Domain-Controller an, die Ihrem Verzeichnis hinzugefügt oder daraus entfernt werden sollen, und wählen Sie dann Ändern.
6. Wenn AWS Managed Microsoft AD den Bereitstellungsprozess abgeschlossen hat, zeigen alle Domain-Controller den Status Aktiv an, und sowohl die zugewiesene Availability Zone als auch die Amazon VPC-Subnetze werden angezeigt. Neue Domain-Controller werden gleichmäßig auf die Availability Zones Subnetze verteilt, in denen Ihr Verzeichnis bereits bereitgestellt ist.

Verwandter Blogartikel zum Thema AWS Sicherheit

- So erhöhen Sie die Redundanz und Leistung Ihres AWS Directory Service for AWS Managed Microsoft AD durch Hinzufügen von Domänencontrollern

Benutzer von Active Directory zu AWS Managed Microsoft AD migrieren

Sie können das Active Directory Migration Toolkit (ADMT) zusammen mit dem Password Export Service (PES) verwenden, um Benutzer von Ihrem selbstverwalteten Active Directory in Ihr verwaltetes Microsoft AD-Verzeichnis zu migrieren. AWS Auf diese Weise können Sie Active Directory-Objekte und verschlüsselte Passwörter für Ihre Benutzer einfacher migrieren.

Eine ausführliche Anleitung finden Sie unter Migration Ihrer On-Premises-Domain zu AWS Managed Microsoft AD mit ADMT im AWS Security Blog.

AWS Verwaltete Microsoft AD-Kontingente

Im Folgenden sind die Standardkontingente für AWS Managed Microsoft AD aufgeführt. Jedes Kontingent gilt pro Region, sofern nicht anders angegeben.

AWS Verwaltete Microsoft AD-Kontingente

Ressource	Standardkontingent
AWS Verwaltete Microsoft AD-Verzeichnisse	20
Manuelle Snapshots*	5 pro AWS verwaltetem Microsoft AD
Alter manueller Snapshots **	180 Tage
Maximale Anzahl von Domain-Controllern pro Verzeichnis	20
Freigegebene Domains pro Standard Microsoft AD.***	5
Freigegebene Domains pro Enterprise Microsoft AD-***	125

Ressource	Standardkontingent
Maximale Anzahl registrierter Zertifizierungsstellenzertifikate (CA) pro Verzeichnis	5
Maximale Gesamtzahl der AWS Regionen in einem einzigen AWS verwalteten Microsoft AD (Enterprise Edition) -Verzeichnis ****	5

* Das Kontingent für manuelle Snapshots kann nicht geändert werden.

** Das maximal unterstützte Alter eines manuellen Snapshots beträgt 180 Tage und kann nicht geändert werden. Dies liegt an dem Tombstone-Lifetime-Attribut gelöschter Objekte, das die Nutzungsdauer einer Systemstatussicherung von Active Directory definiert. Eine Wiederherstellung von einem Snapshot, der älter als 180 Tage ist, ist nicht möglich. Weitere Informationen finden Sie unter Useful shelf life of a system-state backup of Active Directory auf der Microsoft-Website.

*** Das Standardkontingent für freigegebene Domains bezieht sich auf die Anzahl der Konten, für die ein einzelnes Verzeichnis freigegeben werden kann.

**** Dies umfasst eine primäre Region und bis zu 4 zusätzliche Regionen. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.

> **Note**
>
> Sie können Ihrem AWS elastic network interface (ENI) keine öffentliche IP-Adresse zuordnen.

Informationen zum Anwendungsdesign und der Lastverteilung finden Sie unter Programmieren Ihrer Anwendungen.

Informationen zu den Kontingenten für Speicher und Objekte finden Sie in der Vergleichstabelle auf der Seite zu AWS Directory Service-Preisen.

Anwendungskompatibilität für AWS Managed Microsoft AD

AWS Der Directory Service für Microsoft Active Directory (AWS Managed Microsoft AD) ist mit mehreren AWS Diensten und Drittanbieteranwendungen kompatibel.

Im Folgenden finden Sie eine Liste kompatibler AWS Anwendungen und Dienste:

- Amazon Chime – Detaillierte Anweisungen finden Sie unter Herstellen einer Verbindung mit Active Directory.
- Amazon Connect – Weitere Informationen finden Sie unter Wie Amazon Connect funktioniert.
- Amazon EC2 – Weitere Informationen finden Sie unter Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory.
- Amazon QuickSight — Weitere Informationen finden Sie unter Benutzerkonten in der Amazon QuickSight Enterprise Edition verwalten.
- Amazon RDS für MySQL – Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung für MySQL.
- Amazon RDS für Oracle – Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Amazon RDS für Oracle.
- Amazon RDS für PostgreSQL – Weitere Informationen finden Sie unter Verwenden der Kerberos-Authentifizierung mit Amazon RDS für PostgreSQL.
- Amazon RDS für SQL Server – Weitere Informationen finden Sie unter Verwenden der Windows-Authentifizierung mit einer DB-Instance für Amazon RDS Microsoft SQL Server.
- Amazon WorkDocs — Ausführliche Anweisungen finden Sie unter Herstellen einer Verbindung zu Ihrem lokalen Verzeichnis mit AWS Managed Microsoft AD.
- Amazon WorkMail — Eine ausführliche Anleitung finden Sie unter Amazon WorkMail in ein vorhandenes Verzeichnis integrieren (Standardkonfiguration).
- AWS Client VPN - Ausführliche Anweisungen finden Sie unter Client-Authentifizierung und Autorisierung.
- AWS IAM Identity Center — Ausführliche Anweisungen finden Sie unter Connect von IAM Identity Center mit einem lokalen Active Directory.
- AWS License Manager - Weitere Informationen finden Sie unter Benutzerbasierte Abonnements in. AWS License Manager
- AWS Management Console — Weitere Informationen finden Sie unterDen Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren.
- FSx für Windows File Server – Weitere Informationen finden Sie unter Was ist FSx für Windows File Server?.
- WorkSpaces - Ausführliche Anweisungen finden Sie unter Starten eines WorkSpace mithilfe von AWS Managed Microsoft AD.

Aufgrund der Vielzahl von kundenspezifischen und kommerziellen off-the-shelf Anwendungen, die Active Directory verwenden, kann und kann AWS es keine formelle oder umfassende Überprüfung der Kompatibilität von Drittanbieteranwendungen mit dem AWS Directory Service für Microsoft Active Directory (AWS Managed Microsoft AD) durchführen. Obwohl AWS wir mit Kunden zusammenarbeiten, um mögliche Probleme bei der Anwendungsinstallation zu lösen, können wir nicht garantieren, dass eine Anwendung mit AWS Managed Microsoft AD kompatibel ist oder weiterhin sein wird.

Die folgenden Drittanbieteranwendungen sind mit AWS Managed Microsoft AD kompatibel:

- Active Directory-basierte Aktivierung (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(früher bekannt als Azure Active Directory (AzureAD))
- Microsoft Entra Connect(früher bekannt alsAzure Active Directory Connect)
- DFS-Replikation (Distributed File System Replication, DFSR)
- DFS-Namespaces (Distributed File System Namespaces, DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(einschließlich SQL Server AlwaysOn-Verfügbarkeitsgruppen)
- Microsoft System Center Configuration Manager(SCCM) — Der Benutzer, der SCCM bereitstellt, muss Mitglied der Gruppe AWS Delegated System Management Administrators sein.
- Microsoft Windows and Windows Server OS
- Office 365

Beachten Sie, dass möglicherweise nicht alle Konfigurationen dieser Anwendungen unterstützt werden.

Richtlinien für die Kompatibilität

Bei Anwendungen mit einer nicht kompatiblen Konfiguration kann das Problem oftmals mit Anwendungsbereitstellungskonfigurationen behoben werden. Im Folgenden werden die häufigsten

Gründe für die Inkompatibilität einer Anwendung aufgeführt. Kunden können anhand dieser Informationen Kompatibilitätsmerkmale einer gewünschten Anwendung prüfen und mögliche Bereitstellungsänderungen identifizieren.

- Domain-Administrator oder andere privilegierte Berechtigungen – Bei manchen Anwendungen ist eine Installation als Domain-Administrator erforderlich. Da Sie die ausschließliche Kontrolle über diese Berechtigungsstufe behalten AWS müssen, um Active Directory als verwalteten Dienst bereitzustellen, können Sie solche Anwendungen nicht als Domänenadministrator installieren. Sie können solche Anwendungen jedoch häufig installieren, indem Sie bestimmte, weniger privilegierte und AWS unterstützte Berechtigungen an die Person delegieren, die die Installation durchführt. Weitere Informationen zu den Berechtigungen, die Ihre Anwendung benötigt, erhalten Sie von Ihrem Anwendungsanbieter. Weitere Informationen zu Berechtigungen, mit denen Sie delegieren AWS können, finden Sie unter. Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt
- Zugriff auf privilegierte Active Directory Container — In Ihrem Verzeichnis bietet AWS Managed Microsoft AD eine Organisationseinheit (OU), über die Sie die volle administrative Kontrolle haben. Sie haben keine Berechtigung zum Erstellen und Schreiben und möglicherweise nur eine eingeschränkte Leseberechtigung für Container, die in der Active Directory-Struktur höher stehen als Ihre OU. Anwendungen, die Container erstellen oder auf Container zugreifen, für die Sie keine Berechtigung haben, funktionieren möglicherweise nicht. Diese Anwendungen unterstützen jedoch oftmals das Verwenden eines Containers, den Sie alternativ in Ihrer OU erstellt haben. Erkundigen Sie sich bei Ihrem Anwendungsanbieter nach Möglichkeiten zum Erstellen und Verwenden eines Containers in Ihrer OU. Weitere Informationen zum Verwalten Ihrer OU finden Sie unter So verwalten Sie AWS Managed Microsoft AD.
- Schemaänderungen während des Installationsworkflows — Einige Active Directory Anwendungen erfordern Änderungen am Active Directory-Standardschema, und sie versuchen möglicherweise, diese Änderungen im Rahmen des Anwendungsinstallationsworkflows zu installieren. Aufgrund des privilegierten Charakters von Schemaerweiterungen AWS ist dies möglich, indem LDIF-Dateien (Lightweight Directory Interchange Format) nur über die AWS Directory Service Konsole, CLI oder SDK importiert werden. Solche Anwendungen werden häufig mit einer LDIF-Datei geliefert, die Sie im Rahmen der Schemaaktualisierung auf das Verzeichnis anwenden können. AWS Directory Service Weitere Informationen zur Funktionsweise des LDIF-Importprozesses finden Sie unter Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas. Sie können die Anwendung so installieren, dass die Schemainstallation während des Installationsprozesses umgangen wird.

Bekannte inkompatible Anwendungen

Im Folgenden sind häufig nachgefragte kommerzielle off-the-shelf Anwendungen aufgeführt, für die wir keine Konfiguration gefunden haben, die mit AWS Managed Microsoft AD funktioniert. AWS aktualisiert diese Liste von Zeit zu Zeit nach eigenem Ermessen aus Höflichkeit, um Ihnen zu helfen, unproduktive Bemühungen zu vermeiden. AWS stellen Sie diese Informationen ohne Garantie oder Ansprüche bezüglich der aktuellen oder future Kompatibilität zur Verfügung.

- 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 Testumgebungs-Tutorials für Managed Microsoft AD

Dieser Abschnitt enthält eine Reihe von geführten Tutorials, die Ihnen helfen, eine Testumgebung in einzurichten AWS , in der Sie mit AWS Managed Microsoft AD experimentieren können.

Themen

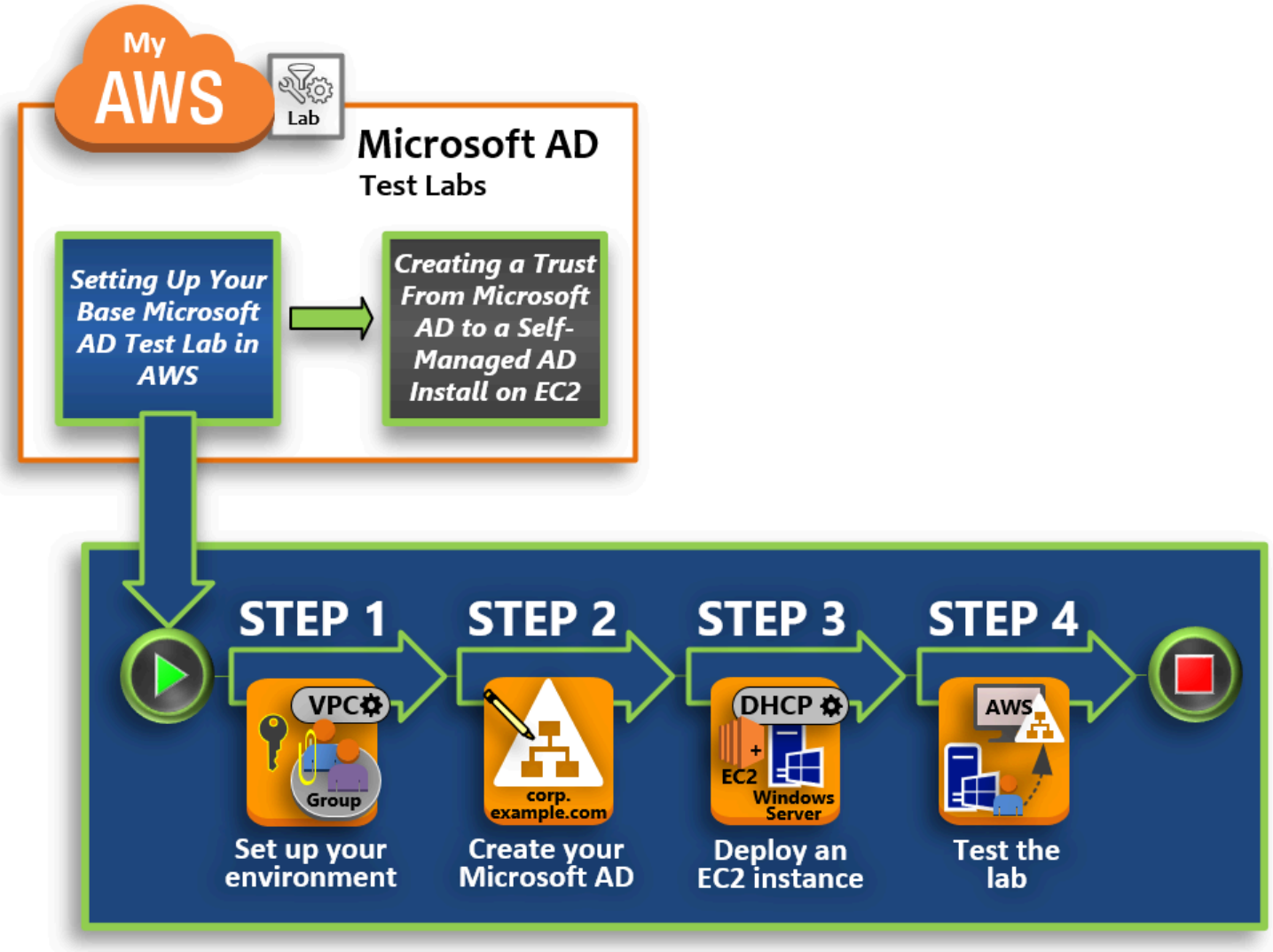
- Tutorial: Einrichten Ihres AWS Managed Microsoft AD-Basis-Testlabors in AWS
- Tutorial: Erstellen einer Vertrauensstellung von AWS Managed Microsoft AD zu einer selbstverwalteten Active Directory-Installation auf Amazon EC2

Tutorial: Einrichten Ihres AWS Managed Microsoft AD-Basis-Testlabors in AWS

In diesem Tutorial erfahren Sie, wie Sie Ihre AWS Umgebung einrichten, um sich auf eine neue AWS Managed Microsoft AD-Installation vorzubereiten, die eine neue Amazon EC2 EC2-Instance verwendet, auf der Windows Server 2019 ausgeführt wird. Anschließend lernen Sie, typische Active Directory-Verwaltungstools zu verwenden, um Ihre AWS verwaltete Microsoft AD-Umgebung von Ihrer EC2-Windows-Instance aus zu verwalten. Wenn Sie das Tutorial abgeschlossen haben, haben Sie die Netzwerkvoraussetzungen eingerichtet und eine neue AWS verwaltete Microsoft AD-Gesamtstruktur konfiguriert.

Wie in der folgenden Abbildung dargestellt, ist das Lab, das Sie anhand dieses Tutorials erstellen, die grundlegende Komponente für praktisches Lernen über AWS Managed Microsoft AD. Sie können

später optionale Tutorials hinzufügen, um weitere praktische Erfahrungen zu sammeln. Diese Tutorialreihe ist ideal für alle Personen geeignet, die bei AWS Managed Microsoft AD einsteigen und eine Testumgebung zu Evaluierungszwecken benötigen. Für dieses Tutorial brauchen Sie ungefähr 1 Stunde.



Schritt 1: Richten Sie Ihre AWS Umgebung für AWS Managed Microsoft AD Active Directory ein

Nachdem Sie Ihre vorausgesetzten Aufgaben abgeschlossen haben, erstellen und konfigurieren Sie eine Amazon VPC in Ihrer EC2-Instance.

Schritt 2: Erstellen Sie Ihr AWS verwaltetes Microsoft AD Active Directory

In diesem Schritt richten Sie AWS Managed Microsoft AD AWS zum ersten Mal ein.

Schritt 3: Stellen Sie eine Amazon EC2 EC2-Instance bereit, um Ihr AWS verwaltetes Microsoft AD Active Directory zu verwalten

Hier durchlaufen Sie die verschiedenen Aufgaben nach der Bereitstellung, die für Client-Computer erforderlich sind, um eine Verbindung mit Ihrer neuen Domain herzustellen und ein neues Windows Server-System in EC2 einzurichten.

Schritt 4: Sicherstellen, dass die grundlegende Testumgebung funktional ist

Schließlich überprüfen Sie als Administrator, ob Sie sich von Ihrem Windows-Server-System in EC2 aus bei AWS Managed Microsoft AD anmelden und verbinden können. Nachdem Sie erfolgreich getestet haben, ob die Testumgebung funktional ist, können Sie weitere Module zu der Testumgebung hinzufügen.

Voraussetzungen

Wenn Sie nur die UI-Schritte in diesem Tutorial nutzen wollen, um Ihre Testumgebung einzurichten, überspringen Sie diesen Abschnitt über die Voraussetzungen und fahren fort mit Schritt 1. Wenn Sie jedoch beabsichtigen, AWS CLI Befehle oder AWS Tools for Windows PowerShell Module zu verwenden, um Ihre Testlabumgebung zu erstellen, müssen Sie zunächst Folgendes konfigurieren:

- IAM-Benutzer mit dem Zugriffs- und geheimen Zugriffsschlüssel — Ein IAM-Benutzer mit einem Zugriffsschlüssel ist erforderlich, wenn Sie die Module AWS CLI oder AWS Tools for Windows PowerShell verwenden möchten. Wenn Sie noch keinen Zugriffsschlüssel haben, lesen Sie bitte den Abschnitt Erstellen, Ändern und Anzeigen von Zugriffsschlüsseln (AWS Management Console).
- AWS Command Line Interface (optional) — Laden Sie das herunter und installieren Sie es AWS CLI unter Windows. Öffnen Sie nach der Installation die Eingabeaufforderung oder das Windows PowerShell Fenster, und geben Sie dann Folgendes ein`aws configure`. Beachten Sie, dass Sie den Zugriffsschlüssels und den geheimen Schlüssel benötigen, um die Einrichtung abzuschließen. Weitere Informationen darüber finden Sie unter der ersten Voraussetzung für die Schritte. Die folgenden Informationen werden abgefragt:
  - AWS Zugriffsschlüssel-ID [Keine]: `AKIAIOSFODNN7EXAMPLE`
  - AWS geheimer Zugriffsschlüssel [Keine]: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - Standardregionsname [Keiner]: `us-west-2`
  - Standardausgabeformat [Keines]: `json`

- AWS Tools for Windows PowerShell (Optional) – Laden Sie die neuste Version von AWS Tools for Windows PowerShell unter https://aws.amazon.com/powershell/ herunter und führen Sie anschließend den folgenden Befehl aus. Beachten Sie, dass Sie Ihren Zugriffsschlüssels und den geheimen Schlüssel benötigen, um die Einrichtung abzuschließen. Weitere Informationen darüber finden Sie unter der ersten Voraussetzung für die Schritte.

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

Schritt 1: Richten Sie Ihre AWS Umgebung für AWS Managed Microsoft AD Active Directory ein

Bevor Sie AWS Managed Microsoft AD in Ihrem AWS Testlabor erstellen können, müssen Sie zunächst Ihr Amazon EC2 EC2-Schlüsselpaar so einrichten, dass alle Anmeldedaten verschlüsselt werden.

Erstellen eines Schlüsselpaares

Wenn Sie bereits ein Schlüsselpaar haben, können Sie diesen Schritt überspringen. Weitere Informationen zu Amazon EC2 EC2-Schlüsselpaaren finden Sie unter Schlüsselpaare erstellen.

So erstellen Sie ein Schlüsselpaar

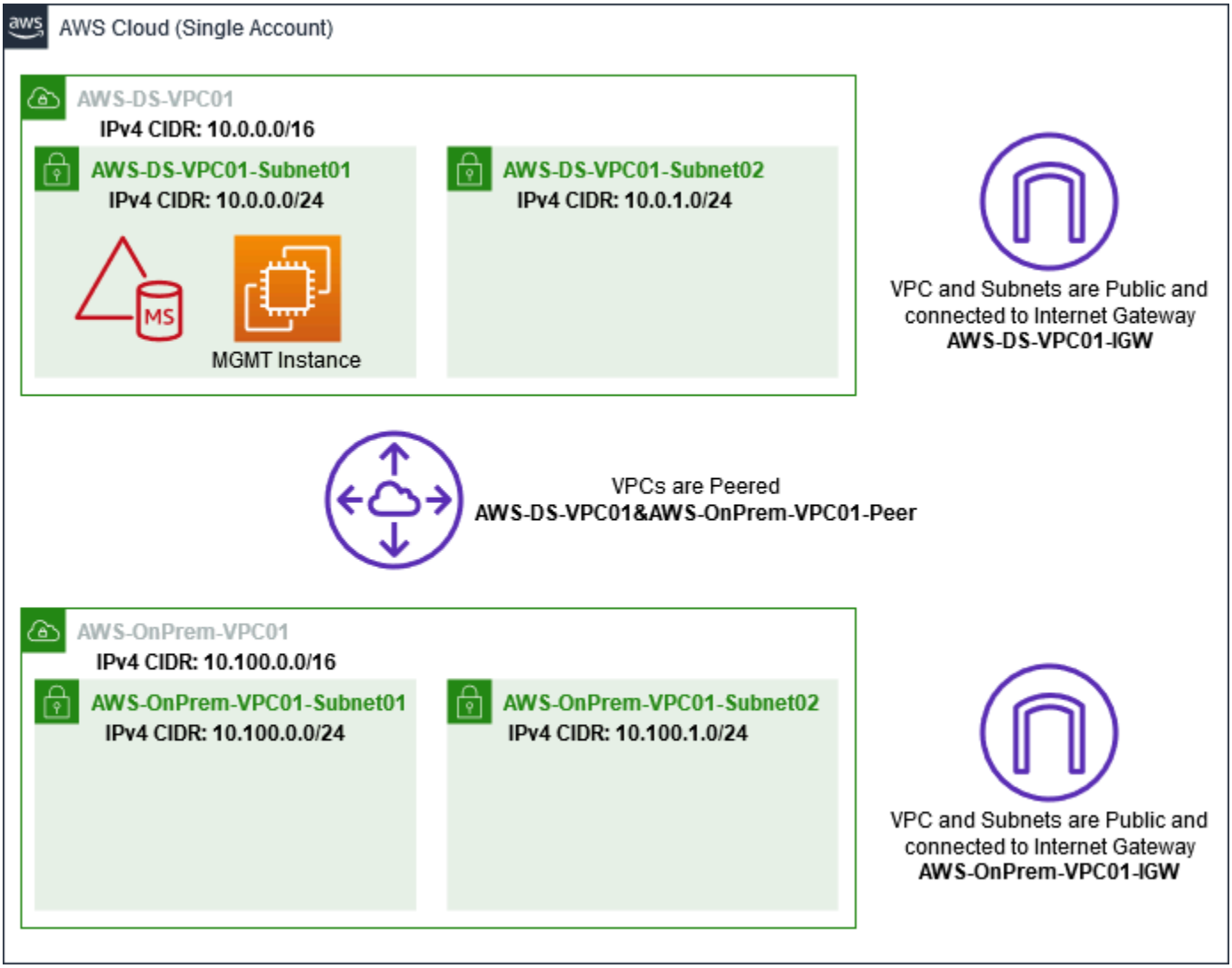
1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security Key Pairs, und wählen Sie dann Create Key Pair.
3. Geben Sie als Schlüsselpaar-Name **`AWS-DS-KP`** ein. Wählen Sie als Schlüsselpaar-Dateiformat die Option pem und dann Erstellen aus.
4. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Der Dateiname ist der Name, den Sie beim Erstellen Ihres Schlüsselpaars mit der Erweiterung `.pem` angegeben haben. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

> **Important**
>
> Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern. Sie müssen den Namen für Ihr Schlüsselpaar beim Starten einer Instance angeben. Der entsprechende

private Schlüssel muss jedes Mal angegeben werden, wenn Sie das Passwort für die Instance entschlüsseln.

Zwei Amazon-VPCs erstellen, konfigurieren und miteinander verbinden

Wie in der folgenden Abbildung zu sehen ist, haben Sie nach Abschluss dieses mehrstufigen Prozesses zwei öffentliche VPCs, zwei öffentliche Subnetze pro VPC, ein Internet-Gateway pro VPC und eine VPC-Peering-Verbindung zwischen den VPCs erstellt und konfiguriert. Wir haben uns aus Gründen der Einfachheit und der Kosten für die Verwendung öffentlicher VPCs und Subnetze entschieden. Für Produktions-Workloads empfehlen wir Ihnen, private VPCs zu verwenden. Weitere Informationen zur Verbesserung der VPC-Sicherheit finden Sie unter Sicherheit in Amazon Virtual Private Cloud.



Alle PowerShell Beispiele verwenden die AWS CLI VPC-Informationen von unten und sind in us-west-2 erstellt. Sie können jede unterstützte Region auswählen, in der Sie Ihre Umgebung erstellen möchten. Allgemeine Informationen finden Sie unter Was ist Amazon VPC?.

Schritt 1: Zwei VPCs erstellen

In diesem Schritt müssen Sie zwei VPCs in demselben Konto mithilfe der in der folgenden Tabelle angegebenen Parameter erstellen. AWS Managed Microsoft AD unterstützt die Verwendung separater Konten mit dieser Freigeben Ihres Verzeichnisses Funktion. Die erste VPC wird für AWS Managed Microsoft AD verwendet. Die zweite VPC wird für Ressourcen verwendet, die später in Tutorial: Erstellen einer Vertrauensstellung von AWS Managed Microsoft AD zu einer selbstverwalteten Active Directory-Installation auf Amazon EC2 verwendet werden können.

Verwaltete Active Directory-VPC-Informationen	On-Premises-VPC-Informationen
Namenskürzel: -DS-VPC01 AWS	Namenskürzel: - -VPC01 AWS OnPrem
IPv4-CIDR-Block: 10.0.0.0/16	IPv4-CIDR-Block: 10.100.0.0/16
IPv6-CIDR-Block: Kein IPv6-CIDR-Block	IPv6-CIDR-Block: Kein IPv6-CIDR-Block
Tenancy: Standard	Tenancy: Standard

Detaillierte Anweisungen finden Sie unter Erstellen einer VPC.

Schritt 2: Zwei Subnetzen pro VPC erstellen

Nachdem Sie die VPCs erstellt haben, müssen Sie zwei Subnetze pro VPC erstellen und dabei die in der folgenden Tabelle angegebenen Parameter verwenden. In dieser Testumgebung wird jedes Subnetz ein /24 sein. Dadurch können bis zu 256 Adressen pro Subnetz vergeben werden. Jedes Subnetz muss sich in einem separaten AZ befinden. Die Unterbringung jedes Subnetzes in einem separaten in AZ ist eine der AWS Voraussetzungen für verwaltetes Microsoft AD.

AWS-DS-VPC01-Subnetzinformationen:	AWS- -VPC01-Subnetzinformationen OnPrem
Namenskürzel: -DS-VPC01-Subnet01 AWS VPC: AWS vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 Availability Zone: us-west-2a	Namenskürzel: - -VPC01-Subnet01 AWS OnPrem

AWS-DS-VPC01-Subnetzinformationen:	AWS- -VPC01-Subnetzinformationen OnPrem
IPv4 CIDR Block: 10.0.0.0/24	VPC: AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem Availability Zone: us-west-2a IPv4 CIDR Block: 10.100.0.0/24
Namenskürzel: -DS-VPC01-Subnet02 AWS VPC: AWS vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 Availability Zone: us-west-2b IPv4 CIDR block: 10.0.1.0/24	Namenskürzel: - -VPC01-Subnet02 AWS OnPrem VPC: AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem Availability Zone: us-west-2b IPv4 CIDR Block: 10.100.1.0/24

Detaillierte Anweisungen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC.

Schritt 3 Ein Internet-Gateway erstellen und es an Ihre VPCs anhängen

Da wir öffentliche VPCs verwenden, müssen Sie ein Internet-Gateway erstellen und an Ihre VPCs anhängen, indem Sie die in der folgenden Tabelle angegebenen Parameter verwenden. Damit können Sie sich mit Ihren EC2-Instances verbinden und diese verwalten.

Informationen zu AWS-DS-VPC01-Internet-Gateway	AWS- OnPrem -VPC01 Internet-Gateway-Informationen
Namenskürzel: -DS-VPC01-IGW AWS	Namenskürzel: - -VPC01-IGW AWS OnPrem
VPC: AWS vpc-xxxxxxxxxxxxxxxxx -DS-VPC01	VPC: AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem

Detaillierte Anweisungen finden Sie unter Internet-Gateways.

Schritt 4: Konfigurieren Sie eine VPC-Peering-Verbindung zwischen AWS-DS-VPC01 und - -VPC01 AWS OnPrem

Da Sie zuvor bereits zwei VPCs erstellt haben, müssen Sie diese mithilfe von VPC-Peering unter Verwendung der in der folgenden Tabelle angegebenen Parameter miteinander vernetzen. Es gibt zwar viele Möglichkeiten, Ihre VPCs zu verbinden, aber in diesem Tutorial wird VPC Peering verwendet. AWS Managed Microsoft AD unterstützt viele Lösungen zur Verbindung Ihrer VPCs. Einige davon umfassen VPC-Peering, Transit Gateway und VPN.

Namensschild für die Peering-Verbindung: -DS-VPC01& - -VPC01-Peer AWSAWS OnPrem

VPC (Antragsteller): vpc-xxxxxxxxxxxxxxxxx -DS-VPC01 AWS

Konto: Mein Konto

Region: Diese Region

VPC (Akzeptierer): AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem

Anweisungen zum Erstellen einer VPC-Peering-Verbindung mit einer anderen VPC in Ihrem Konto finden Sie unter Erstellen einer VPC-Peering-Verbindung mit einer anderen VPC in Ihrem Konto.

Schritt 5: Der Haupt-Routing-Tabelle jeder VPC zwei Routen hinzufügen

Damit die in den vorherigen Schritten erstellten Internet-Gateways und VPC-Peering-Verbindungen funktionieren, müssen Sie die Haupt-Routing-Tabelle beider VPCs mit den in der folgenden Tabelle angegebenen Parametern aktualisieren. Sie fügen zwei Routen hinzu: 0.0.0.0/0, die zu allen Zielen führt, die der Routing-Tabelle nicht explizit bekannt sind, und 10.0.0.0/16 oder 10.100.0.0/16, die zu jeder VPC über die oben eingerichtete VPC-Peering-Verbindung führen.

Sie können ganz einfach die richtige Routentabelle für jede VPC finden, indem Sie nach dem VPC-Namensschild (AWS-DS-VPC01 oder - -VPC01) filtern. AWS OnPrem

AWS-DS-VPC01 Informationen zu Route 1	AWS-DS-VPC01-Informationen zu Route 2	AWS- Informationen zu Route 1 -VPC01 OnPrem	AWS- Informationen zu -VPC01 OnPrem Route 2
Ziel: 0.0.0.0/0	Ziel: 10.100.0.0/16 Ziel: pcx-xxxxx xxxxxxxxxxxx AWS-	Ziel: 0.0.0.0/0	Ziel: 10.0.0.0/16 Ziel: pcx-xxxxx xxxxxxxxxxxx -DS-

AWS-DS-VPC01 Informationen zu Route 1	AWS-DS-VPC01-Informationen zu Route 2	AWS- Informationen zu Route 1 -VPC01 OnPrem	AWS- Informationen zu -VPC01 OnPrem Route 2
Ziel: igw-xxxxx xxxxxxxxxxxx -DS-VPC01-IGW AWS	DS-VPC01& - - VPC01-Peer AWS OnPrem	Ziel: igw-xxxxx xxxxxxxxxxxx AWS-OnPrem-VPC01	VPC01& AWS- - VPC01-Peer AWS OnPrem

Anweisungen zum Hinzufügen von Routen zu einer VPC-Routing-Tabelle finden Sie unter Hinzufügen und Entfernen von Routen aus einer Routing-Tabelle.

Sicherheitsgruppen für Amazon EC2 EC2-Instances erstellen

Standardmäßig erstellt AWS Managed Microsoft AD eine Sicherheitsgruppe, um den Verkehr zwischen seinen Domänencontrollern zu verwalten. In diesem Abschnitt müssen Sie 2 Sicherheitsgruppen erstellen (eine für jede VPC), die zur Verwaltung des Datenverkehrs innerhalb Ihrer VPC für Ihre EC2-Instances verwendet werden, wobei Sie die in den folgenden Tabellen angegebenen Parameter verwenden. Außerdem fügen Sie eine Regel hinzu, die eingehenden RDP (3389)-Datenverkehr aus jeder beliebigen Quelle und für alle aus der lokalen VPC eingehenden Verkehrstypen zulässt. Weitere Informationen finden Sie unter Amazon-EC2-Sicherheitsgruppen für Windows-Instances.

AWS-DS-VPC01-Sicherheitsgruppeninformationen:
Name der Sicherheitsgruppe: AWS DS Test Lab Security Group
Beschreibung: AWS DS Test Lab Sicherheitsgruppe
VPC: AWS vpc-xxxxxxxxxxxxxxxxx -DS-VPC01

Regeln für eingehende Sicherheitsgruppen für -DS-VPC01 AWS

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp
Zielbereich	TCP	3389	Meine IP	Remotedesktop

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp
Gesamter Datenverkehr	Alle	Alle	10.0.0.0/16	Gesamter lokaler VPC-Verkehr

Regeln für ausgehende Sicherheitsgruppen für -DS-VPC01 AWS

Typ	Protocol (Protokoll)	Port-Bereich	Bestimmungsort	Datenverkehrstyp
Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	Gesamter Datenverkehr

AWS- Informationen zur Sicherheitsgruppe -VPC01: OnPrem
Name der Sicherheitsgruppe: AWS OnPrem Test Lab Security Group.
Beschreibung: AWS OnPrem Test Lab Security Group.
VPC: AWS vpc-xxxxxxxxxxxxxxxxx - -VPC01 OnPrem

Regeln für eingehende Sicherheitsgruppen für - AWS-VPC01 OnPrem

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp
Zielbereich	TCP	3389	Meine IP	Remotedesktop
Zielbereich	TCP	53	10.0.0.0/16	DNS
Zielbereich	TCP	88	10.0.0.0/16	Kerberos
Zielbereich	TCP	389	10.0.0.0/16	LDAP

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp
Zielbereich	TCP	464	10.0.0.0/16	Kerberos Passwort ändern/einrichten
Zielbereich	TCP	445	10.0.0.0/16	SMB/CIFS
Zielbereich	TCP	135	10.0.0.0/16	Replikation
Zielbereich	TCP	636	10.0.0.0/16	LDAP SSL
Zielbereich	TCP	49152–65535	10.0.0.0/16	RPC
Zielbereich	TCP	3268 - 3269	10.0.0.0/16	LDAP GC und LDAP GC SSL
Benutzerdefinierte UDP-Regel	UDP	53	10.0.0.0/16	DNS
Benutzerdefinierte UDP-Regel	UDP	88	10.0.0.0/16	Kerberos
Benutzerdefinierte UDP-Regel	UDP	123	10.0.0.0/16	Windows-Uhrzeit
Benutzerdefinierte UDP-Regel	UDP	389	10.0.0.0/16	LDAP
Benutzerdefinierte UDP-Regel	UDP	464	10.0.0.0/16	Kerberos Passwort ändern/einrichten

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp
Gesamter Datenverkehr	Alle	Alle	10.100.0.0/16	Gesamter lokaler VPC-Verkehr

Regeln für ausgehende Sicherheitsgruppen für - -VPC01 AWS OnPrem

Typ	Protocol (Protokoll)	Port-Bereich	Bestimmungsort	Datenverkehrstyp
Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	Gesamter Datenverkehr

Ausführliche Anweisungen zum Erstellen und Hinzufügen von Regeln zu Ihren Sicherheitsgruppen finden Sie unter Mit Sicherheitsgruppen arbeiten.

Schritt 2: Erstellen Sie Ihr AWS verwaltetes Microsoft AD Active Directory

Sie können Ihr Verzeichnis unter Verwendung von drei verschiedenen Methoden erstellen. Sie können das AWS Management Console Verfahren (für dieses Tutorial empfohlen) oder eines der AWS Tools for Windows PowerShell Verfahren AWS CLI oder verwenden, um Ihr Verzeichnis zu erstellen.

Methode 1: So erstellen Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnis (AWS Management Console)

1. Wählen Sie im Navigationsbereich AWS Directory Service -Konsole den Eintrag Verzeichnisse und wählen Sie Verzeichnis einrichten aus.
2. Wählen Sie auf der Seite Verzeichnistyp auswählen die Option AWS Managed Microsoft AD aus und klicken Sie dann auf Weiter.
3. Geben Sie auf der Seite Enter directory information (Verzeichnisinformationen eingeben) die folgenden Informationen ejn und wählen Sie dann Next (Weiter) aus.

   - Wählen Sie in Edition entweder Standard Edition oder Enterprise Edition aus. Weitere Informationen zu Editionen finden Sie unter AWS Directory Service für Microsoft Active Directory.

- Geben Sie in Directory DNS name (DNS-Name des Verzeichnisses) den Wert **`corp.example.com`** ein.
- Geben Sie in Directory NetBIOS name (Verzeichnis-NetBIOS-Name) den Wert **`corp`** ein.
- Geben Sie in Destination (Ziel) den Wert **`AWS DS Managed`** ein.
- Geben Sie für Admin password das Passwort ein, das Sie für dieses Konto verwenden wollen, und wiederholen Sie die Passworteingabe in Confirm password. Dieses Admin-Konto wird automatisch erstellt, wenn das Verzeichnis erstellt wird. Das Passwort darf das Wort admin nicht beinhalten. Das Verzeichnisadministrator-Passwort unterscheidet zwischen Groß-/Kleinschreibung und muss zwischen 8 und 64 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:
  - Kleinbuchstaben (a – z)
  - Großbuchstaben (A – Z)
  - Zahlen (0 – 9)
  - Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

4. Geben Sie auf der Seite Choose VPC and subnets (VPC und Subnetze wählen) die folgenden Informationen an und wählen Sie dann Next (Weiter).
   - Wählen Sie für VPC die Option, die mit AWS-DS-VPC01 beginnt und mit (10.0.0.0/16) endet.
   - Für Subnetze wählen Sie die öffentlichen Subnetze 10.0.0.0/24 and 10.0.1.0/24.
5. Überprüfen Sie auf der Seite Review & create (Überprüfen und erstellen) die Verzeichnisinformationen und nehmen Sie gegebenenfalls Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen). Das Erstellen des Verzeichnisses dauert 20 bis 40 Minuten. Sobald sie erstellt wurden, ändert sich der Status in Active.

Methode 2: So erstellen Sie Ihr AWS verwaltetes Microsoft AD (Windows PowerShell) (optional)

1. Öffnen Sie Windows PowerShell.
2. Geben Sie den folgenden Befehl ein: Stellen Sie sicher, dass Sie die in Schritt 4 des vorherigen AWS Management Console Verfahrens angegebenen Werte verwenden.

```
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
```

Methode 3: So erstellen Sie Ihr AWS verwaltetes Microsoft AD (AWS CLI) (optional)

1. Öffnen Sie das AWS CLI.
2. Geben Sie den folgenden Befehl ein: Stellen Sie sicher, dass Sie die in Schritt 4 des vorherigen AWS Management Console Verfahrens angegebenen Werte verwenden.

```
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
```

Schritt 3: Stellen Sie eine Amazon EC2 EC2-Instance bereit, um Ihr AWS verwaltetes Microsoft AD Active Directory zu verwalten

Für dieses Lab verwenden wir Amazon EC2 EC2-Instances mit öffentlichen IP-Adressen, um den Zugriff auf die Management-Instance von überall aus zu vereinfachen. In einer Produktionsumgebung können Sie Instances verwenden, die sich in einer privaten VPC befinden und auf die nur über ein VPN oder einen AWS Direct Connect Link zugegriffen werden kann. Es ist nicht notwendig, dass die Instance über eine öffentliche IP-Adresse verfügt.

In diesem Abschnitt durchlaufen Sie die verschiedenen Aufgaben nach der Bereitstellung, die für Client-Computer erforderlich sind, um unter Verwendung des Windows Servers auf Ihrer neuen EC2-Instance eine Verbindung mit Ihrer neuen Domain herzustellen. Sie verwenden die Windows Server im nächsten Schritt, um sicherzustellen, dass die Testumgebung funktional ist.

Optional: Erstellen Sie einen in AWS-DS-VPC01 festgelegten DHCP-Optionen für Ihr Verzeichnis

In diesem optionalen Verfahren richten Sie einen DHCP-Optionsbereich ein, sodass EC2-Instances in Ihrer VPC automatisch Ihr AWS verwaltetes Microsoft AD für die DNS-Auflösung verwenden. Weitere Informationen finden Sie unter DHCP-Optionssets.

So erstellen Sie eine DHCP-Optionsliste für Ihr Verzeichnis

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich DHCP Options Sets und anschließend Create DHCP Options Set aus.
3. Geben Sie auf der Seite Create DHCP options set (DHCP-Optionsliste erstellen) die folgenden Werte für Ihr Verzeichnis ein:

- Geben Sie bei Name **`AWS DS DHCP`** ein.
- Geben Sie für Domainname **`corp.example.com`** ein.
- Geben Sie für Domainnamen-Server die IP-Adressen der DNS-Server Ihres von AWS bereitgestellten Verzeichnisses ein.

> **Note**
>
> Um diese Adressen zu finden, rufen Sie die Seite AWS Directory Service Verzeichnisse auf und wählen Sie dann die entsprechende Verzeichnis-ID aus. Identifizieren und verwenden Sie auf der Seite Details die IP-Adressen, die in der DNS-Adresse angezeigt werden.
> Sie können diese Adressen auch finden, indem Sie die AWS Directory Service -Seite Verzeichnisse aufrufen und die entsprechende Verzeichnis-ID auswählen. Wählen Sie dann Skalieren und freigeben. Identifizieren und verwenden Sie unter Domain-Controller die IP-Adressen, die unter IP-Adresse angezeigt werden.

- Geben Sie nichts für die Einstellungen für NTP servers, NetBIOS name servers und NetBIOS node type an.

4. Wählen Sie Create DHCP options set (DHCP-Optionsliste erstellen) und anschließend Close (Schließen) aus. Die neue DHCP-Optionsliste wird in der Liste der DHCP-Optionen angezeigt.
5. Notieren Sie sich die ID der neuen DHCP-Optionsliste (dopt-***xxxxxxxx***). Sie brauchen sie zum Schluss dieses Verfahrens, wenn Sie die neue Optionsliste Ihrer VPC zuordnen.

> **Note**
>
> Die nahtlose Domainverbindung funktioniert, ohne dass ein DHCP-Optionssatz konfiguriert werden muss.

6. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
7. Wählen Sie in der VPC-Liste AWS DS VPC, dann Aktionen und anschließend DHCP-Optionsliste bearbeiten aus.
8. Wählen Sie auf der Seite Edit DHCP options set (DHCP-Optionsliste bearbeiten) die Optionsliste aus, die Sie sich in Schritt 5 notiert haben, und wählen Sie dann Save (Speichern) aus.

Erstellen Sie eine Rolle, um Windows-Instanzen mit Ihrer AWS verwalteten Microsoft AD-Domäne zu verbinden

Gehen Sie wie folgt vor, um eine Rolle zu konfigurieren, die eine Amazon EC2 EC2-Windows-Instance mit einer Domain verbindet. Weitere Informationen finden Sie unter Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory.

So konfigurieren Sie EC2, um Windows-Instances mit Ihrer Domain zu verbinden

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Klicken Sie im Navigationsbereich der IAM-Konsole auf Rollen, und wählen Sie dann Rolle erstellen.
3. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität auswählen) die Option AWS -Service aus.
4. Wählen Sie für Choose the service that will use this role (Wählen Sie den Service aus, der diese Rolle verwendet) die Option EC2 und danach Next: Permissions (Nächster Schritt: Berechtigungen) aus.
5. Führen Sie auf der Seite Attached permissions policy (Richtlinie für angefügte Berechtigungen) die folgenden Schritte aus:

   - Wählen Sie das Kästchen neben der von AmazonSSM ManagedInstanceCore verwalteten Richtlinie aus. Diese Richtlinie enthält die erforderlichen Mindestberechtigungen zum Verwenden des Systems-Managers-Dienstes.
   - Wählen Sie das Kästchen neben der von DirectoryServiceAccessAmazonSSM verwalteten Richtlinie aus. Die Richtlinie enthält die Berechtigungen zum Verbinden von Instances mit einem von AWS Directory Service verwalteten Active Directory.

   Weitere Informationen zu diesen verwalteten Richtlinien und anderen Richtlinien zum Anfügen an ein IAM-Instance-Profil für Systems Manager finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager -Benutzerhandbuch. Informationen über verwaltete Richtlinien finden Sie unter AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.
6. Wählen Sie Next: Tags (Weiter: Tags (Markierungen)) aus.
7. (Optional) Fügen Sie ein oder mehrere Tag (Markierung)-Schlüssel-Wert-Paare hinzu, um den Zugriff für diese Rolle zu organisieren, zu verfolgen oder zu steuern, und wählen Sie dann Next: Review (Weiter: Prüfen) aus.

8. Geben Sie unter Rollenname einen Namen für die Rolle ein, der beschreibt, dass sie verwendet wird, um Instances zu einer Domäne hinzuzufügen, z. B. EC2. DomainJoin
9. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein.
10. Wählen Sie Create role (Rolle erstellen) aus. Das System leitet Sie zur Seite Roles (Rollen) zurück.

Erstellen Sie eine Amazon EC2 EC2-Instance und treten Sie dem Verzeichnis automatisch bei

In diesem Verfahren richten Sie ein Windows Server-System in einer EC2-Instance ein, das später zur Verwaltung von Benutzern, Gruppen und Richtlinien in Active Directory verwendet werden kann.

So erstellen Sie eine EC2-Instance und verbinden automatisch das Verzeichnis

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance aus.
3. Wählen Sie auf der Seite Schritt 1 neben Microsoft Windows Server 2019 Base – ami-***xxxxxxxxxxxxxxxxx*** die Option Auswählen.
4. Wählen Sie auf der Seite Schritt 2 den Eintrag t3.micro (beachten Sie, dass Sie einen größeren Instance-Typ wählen können) und wählen Sie dann Weiter: Instance-Details konfigurieren aus.
5. Führen Sie auf der Seite Step 3 die folgenden Schritte aus:
   - Wählen Sie für Netzwerk die VPC, die in AWS-DS-VPC01 endet (z. B. vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01).
   - Wählen Sie für Subnetz das öffentliche Subnetz 1, das für Ihre bevorzugte Availability Zone vorkonfiguriert sein sollte (z. B. subnet-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01-Subnet01 | ***us-west-2a***).
   - Wählen Sie für Auto-assign Public IP die Option Enable (falls die Subnetz-Einstellung nicht standardmäßig auf Enable gesetzt ist).
   - Wählen Sie für Domain join directory den Eintrag corp.example.com (d-***xxxxxxxxxx***).
   - Wählen Sie für die IAM-Rolle den Namen aus, den Sie Ihrer Instance-Rolle gegeben habenErstellen Sie eine Rolle, um Windows-Instanzen mit Ihrer AWS verwalteten Microsoft AD-Domäne zu verbinden, z. B. EC2. DomainJoin
   - Übernehmen Sie für die anderen Einstellungen die Standardwerte.
   - Wählen Sie Next: Add Storage aus.

6. Behalten Sie auf der Seite Step 4 die Standardeinstellungen bei und wählen Sie dann Next: Add Tags.
7. Wählen Sie auf der Seite Step 5 die Option Add Tag aus. Geben Sie unter Key die Zeichenfolge **`corp.example.com-mgmt`** ein und wählen Sie dann Next: Configure Security Group.
8. Wählen Sie auf der Seite Schritt 6 die Option Bestehende Sicherheitsgruppe auswählen, wählen Sie die AWS -DS-Testumgebungs-Sicherheitsgruppe (die Sie zuvor im Base-Tutorial eingerichtet haben) und wählen Sie dann Überprüfen und starten, um Ihre Instance zu überprüfen.
9. Überprüfen Sie auf der Seite Step 7 die Seite und wählen Sie dann Launch.
10. Erledigen Sie im Dialogfeld Select an existing key pair or create a new key pair Folgendes:

    - Wählen Sie Vorhandenes Schlüsselpaar auswählen aus.

    - Wählen Sie unter Schlüsselpaar auswählen die Option AWS-DS-KP.
    - Markieren Sie das Kontrollkästchen I acknowledge....
    - Wählen Sie Instances starten aus.
11. Wählen Sie Instances anzeigen aus, um zur Amazon-EC2-Konsole zurückzukehren und den Status der Bereitstellung anzuzeigen.

Die Active-Directory-Tools in Ihrer EC2-Instance installieren

Sie haben die Wahl zwischen zwei Methoden zur Installation der Active Directory-Domain-Management-Tools für Ihre EC2-Instance. Sie können die Server Manager-Benutzeroberfläche (für dieses Tutorial empfohlen) oder verwenden. Windows PowerShell

So installieren Sie die Active-Directory-Tools in Ihrer EC2-Instance (Server Manager)

1. Wählen Sie in der Amazon-EC2-Konsole die Option Instances, wählen Sie die zuvor erstellte Instance und wählen Sie dann Verbinden.
2. Wählen Sie im Dialogfeld Connect To Your Instance (Herstellen einer Verbindung mit Ihrer Instance) die Option Get Password (Passwort abrufen) aus, um Ihr Passwort abzurufen (sofern noch nicht geschehen), und wählen Sie anschließend Download Remote Desktop File (Remote Desktop-Datei herunterladen) aus.
3. Geben Sie im Dialogfeld Windows Security Ihre lokalen Administrator-Anmeldeinformationen für den Windows Server-Computer ein, um sich anzumelden (z. B. **`administrator`**).
4. Wählen Sie im Menü Start die Option Server Manager.

5. Wählen Sie im Dashboard Add Roles and Features.
6. Wählen Sie im Add Roles and Features Wizard Next.
7. Wählen Sie auf der Seite Select installation type die Option Role-based or feature-based installation und wählen Sie Next.
8. Stellen Sie sicher, dass auf der Seite Select destination server der lokale Server ausgewählt ist, und wählen Sie dann Next.
9. Wählen Sie auf der Seite Select server roles Next.
10. Führen Sie auf der Seite Select features die folgenden Schritte aus:
    - Wählen Sie das Kontrollkästchen Group Policy Management.
    - Erweitern Sie Remote Server Administration Tools und erweitern Sie dann Role Administration Tools.
    - Wählen Sie das Kontrollkästchen AD DS and AD LDS Tools.
    - Wählen Sie das Kontrollkästchen DNS Server Tools .
    - Wählen Sie Weiter aus.
11. Überprüfen Sie auf der Seite Confirm installation selections die Informationen und wählen Sie dann Install. Wenn die Installation des Features abgeschlossen ist, stehen die folgenden neuen Tools oder Snap-Ins über den Ordner Windows Administrative Tools im Start-Menü zur Verfügung.
    - Active Directory Administrative Center
    - Active-Directory-Domain und -Vertrauensbeziehungen
    - Active Directory-Modul für Windows PowerShell
    - Active Directory-Standorte und -Dienste
    - Active Directory-Benutzer und -Computer
    - ADSI bearbeiten
    - DNS
    - Gruppenrichtlinienverwaltung

Um die Active Directory-Tools auf Ihrer EC2-Instance zu installieren (Windows PowerShell) (optional)

1. Starten Windows PowerShell.
2. Geben Sie den folgenden Befehl ein:

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-
Tools,RSAT-DNS-Server
```

Schritt 4: Sicherstellen, dass die grundlegende Testumgebung funktional ist

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass die Testumgebung erfolgreich eingerichtet wurde, bevor Sie der Testumgebung weitere Module hinzufügen. Mit diesem Verfahren wird überprüft, ob Ihr Windows Server ordnungsgemäß konfiguriert ist, eine Verbindung zur Domäne corp.example.com herstellen kann und zur Verwaltung Ihrer AWS verwalteten Microsoft AD-Gesamtstruktur verwendet werden kann.

So stellen Sie sicher, dass die Testumgebung funktional ist

1. Melden Sie sich von der EC2-Instance ab, bei der Sie als lokaler Administrator angemeldet waren.
2. Wenn Sie wieder in der Amazon-EC2-Konsole sind, wählen Sie im Navigationsbereich Instances aus. Anschließend wählen Sie die Instance aus, die Sie erstellt haben. Wählen Sie Connect aus.
3. Wählen Sie im Dialogfeld Connect To Your Instance Download Remote Desktop File aus.
4. Geben Sie im Dialogfeld Windows Security Ihre Administrator-Anmeldeinformationen für die CORP-Domain ein, um sich anzumelden (z. B. **`corp\admin`**).
5. Sobald Sie angemeldet sind, wählen Sie im Start-Menü unter Windows Administrative Tools den Eintrag Active Directory Users and Computers.
6. Jetzt sollte corp.example.com angezeigt werden, mit allen Standard-OUs und Konten, die der neuen Domain zugeordnet sind. Beachten Sie unter Domänencontroller die Namen der Domänencontroller, die automatisch erstellt wurden, als Sie Ihr AWS verwaltetes Microsoft AD in Schritt 2 dieses Tutorials erstellt haben.

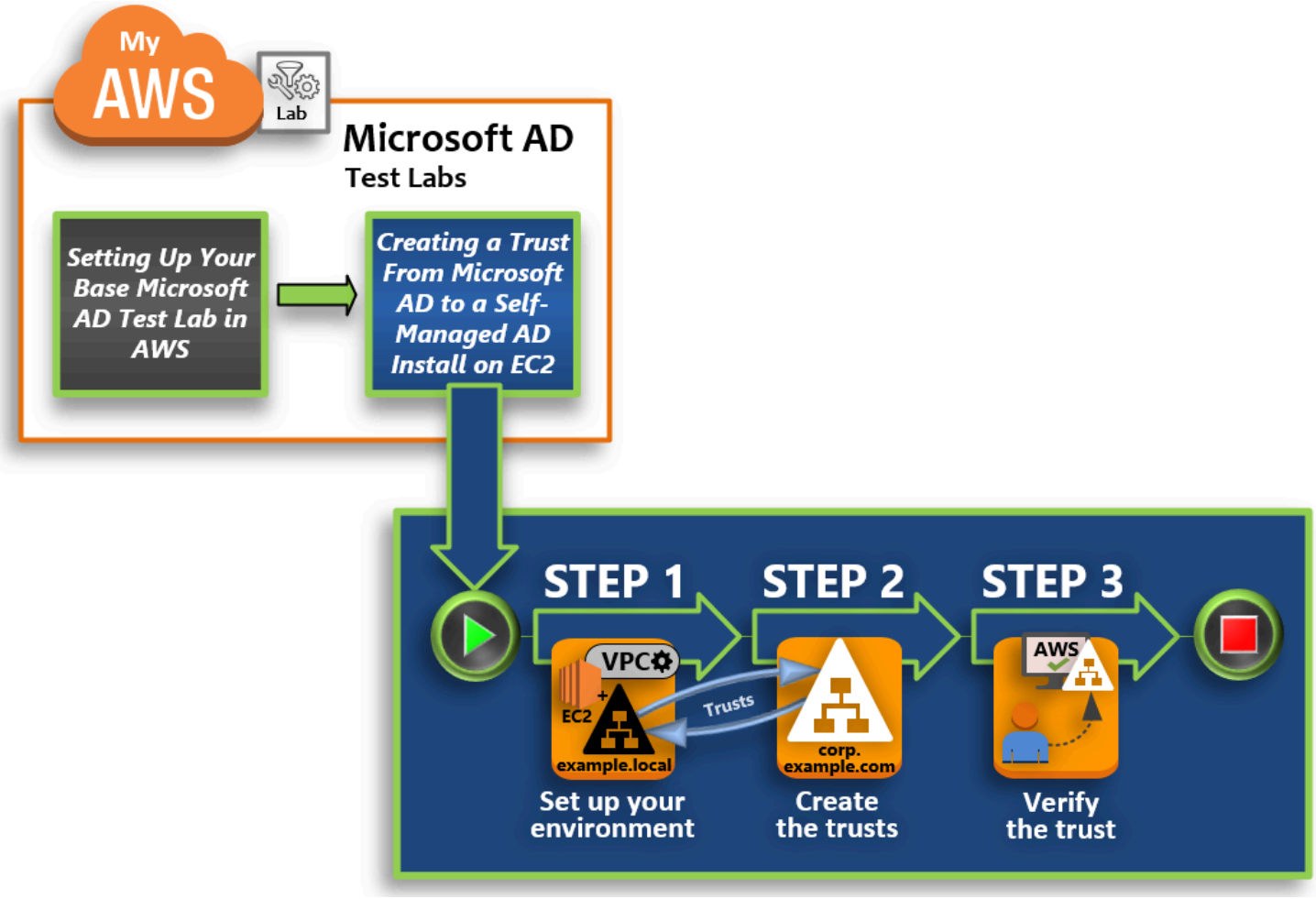
Herzlichen Glückwunsch! Ihre AWS verwaltete Microsoft AD-Basis-Testlabumgebung wurde jetzt konfiguriert. Sie können jetzt die nächsten Testumgebungen der Serie hinzufügen.

Nächstes Tutorial: Tutorial: Erstellen einer Vertrauensstellung von AWS Managed Microsoft AD zu einer selbstverwalteten Active Directory-Installation auf Amazon EC2

Tutorial: Erstellen einer Vertrauensstellung von AWS Managed Microsoft AD zu einer selbstverwalteten Active Directory-Installation auf Amazon EC2

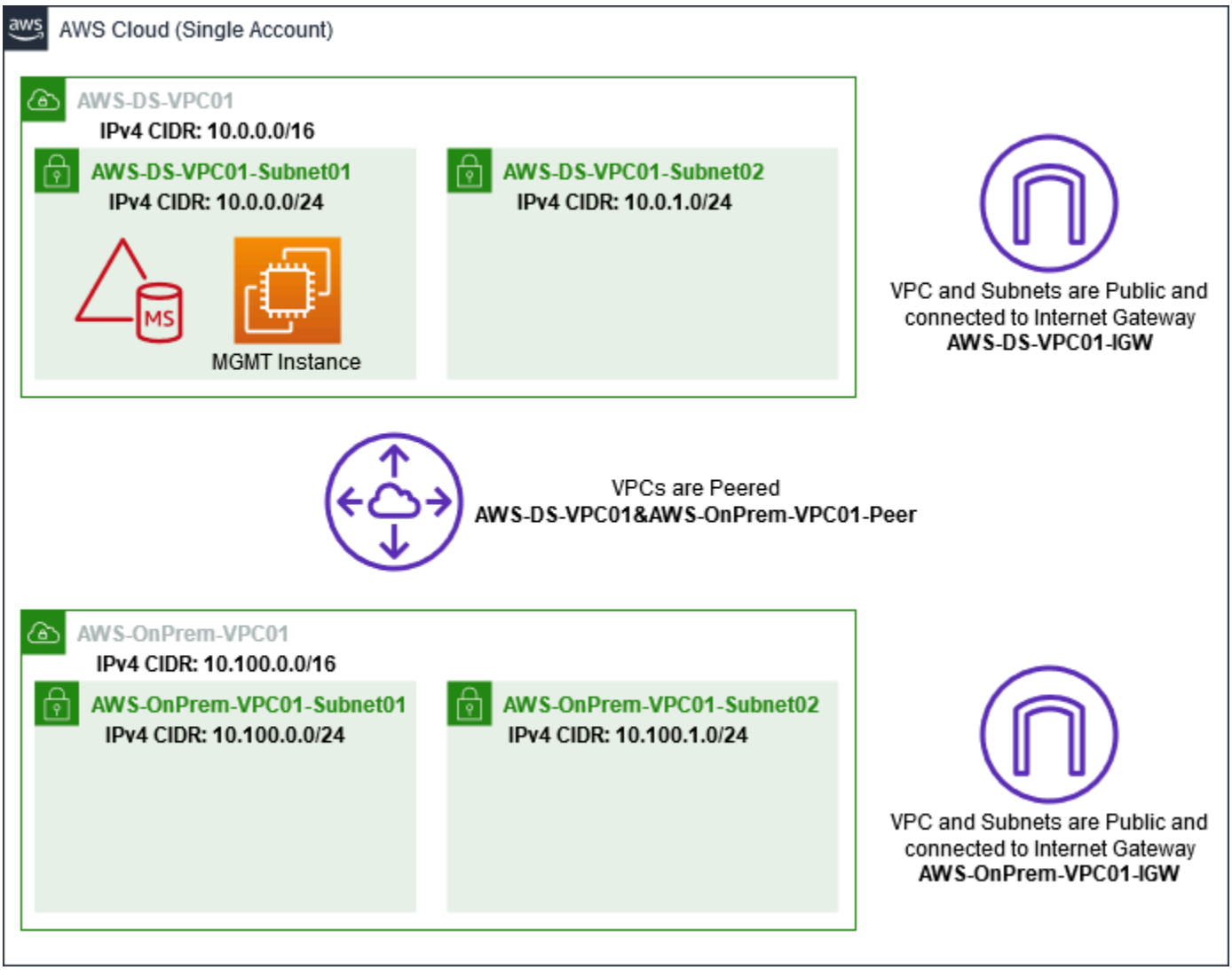
In diesem Tutorial erfahren Sie, wie Sie eine Vertrauensstellung zwischen der AWS Verzeichnisdienst-Gesamtstruktur für Microsoft Active Directory einrichten, die Sie im Basis-Tutorial erstellt haben. Sie erfahren außerdem, wie Sie einen neuen nativen Active-Directory-Forest auf einem Windows-Server in Amazon EC2 erstellen. Wie in der folgenden Abbildung dargestellt, ist das Lab, das Sie anhand dieses Tutorials erstellen, der zweite Baustein, der für die Einrichtung eines vollständigen AWS Managed Microsoft AD-Testlabors erforderlich ist. Sie können das Testlabor verwenden, um Ihre reinen Cloud- oder Hybrid-Cloud-basierten AWS Lösungen zu testen.

Es sollte nur einmal erforderlich sein, dieses Tutorial zu erstellen. Anschließend können Sie bei Bedarf weitere optionale Tutorials hinzufügen.



Schritt 1: Ihre Umgebung für Vertrauensstellungen einrichten

In diesem Abschnitt richten Sie Ihre Amazon EC2 EC2-Umgebung ein, stellen Ihre neue Gesamtstruktur bereit und bereiten Ihre VPC auf Vertrauensstellungen mit vor. AWS



Eine EC2-Instance für Windows Server 2019 erstellen

Gehen Sie wie folgt vor, um einen Mitgliedsserver für Windows Server 2019 in Amazon EC2 zu erstellen.

So erstellen Sie eine EC2-Instance für Windows Server 2019

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Amazon-EC2-Konsole Instance starten aus.
3. Suchen Sie auf der Seite Schritt 1 in der Liste nach Microsoft Windows Server 2019 Base – ami-***xxxxxxxxxxxxxxxx***. Wählen Sie anschließend Select aus.
4. Wählen Sie auf der Seite Step 2 die Option t2.large und wählen Sie dann Next: Configure Instance Details.

5. Führen Sie auf der Seite Step 3 die folgenden Schritte aus:

   - Wählen Sie für Netzwerk die Option vpc- ***xxxxxxxxxxxx*** AWS- OnPrem -VPC01 aus (das Sie zuvor im Basis-Tutorial eingerichtet haben).
   - *Wählen Sie für* ***Subnetz subnet*** *- xxxxxxxxxxxx | - **-VPC01-Subnet01** | - -VPC01 aus.* AWS OnPrem AWS OnPrem
   - Wählen Sie für Auto-assign Public IP die Option Enable (falls die Subnetz-Einstellung nicht standardmäßig auf Enable gesetzt ist).
   - Übernehmen Sie für die anderen Einstellungen die Standardwerte.
   - Wählen Sie Next: Add Storage aus.
6. Behalten Sie auf der Seite Step 4 die Standardeinstellungen bei und wählen Sie dann Next: Add Tags.
7. Wählen Sie auf der Seite Step 5 die Option Add Tag aus. Geben Sie unter Key die Zeichenfolge **`example.local-DC01`** ein und wählen Sie dann Next: Configure Security Group.
8. Wählen Sie auf der Seite Schritt 6 die Option Bestehende Sicherheitsgruppe auswählen, wählen Sie die AWS -On-Premises-Testumgebungs-Sicherheitsgruppe (die Sie zuvor im Base-Tutorial eingerichtet haben) und wählen Sie dann Überprüfen und starten, um Ihre Instance zu überprüfen.
9. Überprüfen Sie auf der Seite Step 7 die Seite und wählen Sie dann Launch.
10. Erledigen Sie im Dialogfeld Select an existing key pair or create a new key pair Folgendes:

    - Wählen Sie Vorhandenes Schlüsselpaar auswählen aus.
    - Wählen Sie unter Schlüsselpaar auswählen die Option AWS-DS-KP (die Sie zuvor im Base-Tutorial eingerichtet haben).
    - Markieren Sie das Kontrollkästchen I acknowledge....
    - Wählen Sie Instances starten aus.
11. Wählen Sie Instances anzeigen aus, um zur Amazon-EC2-Konsole zurückzukehren und den Status der Bereitstellung anzuzeigen.

Ihren Server zu einem Domain-Controller ernennen

Bevor Sie Vertrauensbeziehungen erstellen können, müssen Sie den ersten Domain-Controller für einen neuen Forest erstellen und bereitstellen. Während dieses Prozesses konfigurieren Sie einen neuen Active Directory-Forest, installieren DNS und richten Sie diesen Server so ein, dass er den

lokalen DNS-Server für die Namensauflösung verwendet. Nach Abschluss dieses Verfahrens müssen Sie den Server neu starten.

> **Note**
>
> Wenn Sie einen Domänencontroller erstellen möchten, der sich mit Ihrem lokalen Netzwerk repliziert AWS , müssen Sie die EC2-Instance zunächst manuell mit Ihrer lokalen Domäne verbinden. Anschließend können Sie den Server einem Domain-Controller bekanntgeben.

Ihren Server einem Domain-Controller bekanntgeben

1. Wählen Sie in der Amazon-EC2-Konsole die Option Instances, wählen Sie die zuvor erstellte Instance und wählen Sie dann Verbinden.
2. Wählen Sie im Dialogfeld Connect To Your Instance Download Remote Desktop File aus.
3. Geben Sie im Dialogfeld Windows Security Ihre lokalen Administrator-Anmeldeinformationen für den Windows Server-Computer ein, um sich anzumelden (z. B. **`administrator`**). Wenn Sie das lokale Administratorpasswort noch nicht haben, gehen Sie zurück zur Amazon-EC2-Konsole, klicken Sie mit der rechten Maustaste auf die Instance und wählen Sie Windows-Passwort abrufen. Navigieren Sie zu Ihrer `AWS DS KP.pem` Datei oder Ihren persönlichen `.pem` Schlüssel, und wählen Sie dann Decrypt Password.
4. Wählen Sie im Menü Start die Option Server Manager.
5. Wählen Sie im Dashboard Add Roles and Features.
6. Wählen Sie im Add Roles and Features Wizard Next.
7. Wählen Sie auf der Seite Select installation type die Option Role-based or feature-based installation und wählen Sie Next.
8. Stellen Sie sicher, dass auf der Seite Select destination server der lokale Server ausgewählt ist, und wählen Sie dann Next.
9. Wählen Sie auf der Seite Select server roles die Option Active Directory Domain Services. Überprüfen Sie im Dialogfeld Add Roles and Features Wizard, ob das Kontrollkästchen Include management tools (if applicable) ausgewählt ist. Wählen Sie Add Features und anschließend Next aus.
10. Wählen Sie auf der Seite Features auswählen die Option Weiter aus.
11. Wählen Sie auf der Seite Active Directory Domain Services Next.
12. Wählen Sie auf der Seite Confirm installation selections Install.

13. Nachdem die Active Directory-Binärdateien installiert wurden, wählen Sie Close.
14. Wenn Server Manager geöffnet wird, suchen Sie nach einem Flag oben neben dem Wort Manage. Wenn dieses Flag gelb wird, kann der Server bekanntgegeben werden.
15. Wählen Sie das gelbe Flag und wählen Sie dann Promote this server to a domain controller.
16. Wählen Sie auf der Seite Deployment Configuration Add a new forest. Geben Sie in Root domain name die Zeichenfolge **`example.local`** ein und wählen Sie Next.
17. Erledigen Sie auf der Seite Domain Controller Options Folgendes:
    - Wählen Sie in Forest functional level und Domain functional level die Option Windows Server 2016.
    - Vergewissern Sie sich, dass unter Domänencontroller-Funktionen angeben sowohl DNS-Server als auch Global Catalog (GC) ausgewählt sind.
    - Geben Sie ein DSRM-Passwort (Directory Services Restore Mode) ein und bestätigen Sie es. Wählen Sie anschließend Weiter.
18. Ignorieren Sie auf der Seite DNS Options die Warnung über die Delegation und wählen Sie Next.
19. Vergewissern Sie sich, dass auf der Seite Zusätzliche Optionen EXAMPLE als NetBios Domainname aufgeführt ist.
20. Behalten Sie auf der Seite Paths die Standardwerte bei, und wählen Sie dann Next.
21. Wählen Sie auf der Seite Review Options Weiter. Der Server prüft jetzt, ob alle Voraussetzungen für den Domain-Controller erfüllt sind. Möglicherweise werden einige Warnungen angezeigt, Sie können sie jedoch einfach ignorieren.
22. Wählen Sie Installieren aus. Nachdem die Installation abgeschlossen ist, wird der Server neu gestartet und wird dann zu einem funktionalen Domain-Controller.

Konfigurieren Ihrer VPC

Die folgenden drei Verfahren führen Sie durch die Schritte zum Konfigurieren Ihrer VPC für die Anbindung an AWS.

Konfigurieren Ihrer ausgehenden VPC-Regeln

1. Notieren Sie sich in der AWS Directory Service Konsole die AWS verwaltete Microsoft AD-Verzeichnis-ID für corp.example.com, die Sie zuvor im Base-Tutorial erstellt haben.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
3. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.

4. Suchen Sie nach Ihrer AWS Managed Microsoft AD-Verzeichnis-ID. Wählen Sie in den Suchergebnissen das Element mit der Beschreibung AWS hat Sicherheitsgruppe für d-***xxxxxx***-Verzeichnis-Controller erstellt aus.

   > **Note**
   >
   > Diese Sicherheitsgruppe wurde automatisch erstellt, als Sie Ihr Verzeichnis erstellt haben.

5. Wählen Sie die Registerkarte Outbound Rules unter dieser Sicherheitsgruppe. Wählen Sie Edit, Add another rule und fügen Sie die folgenden Werte hinzu:

   - Wählen Sie für Type die Option All Traffic aus.
   - Geben Sie für Destination den Wert **`0.0.0.0/0`** ein.
   - Übernehmen Sie für die anderen Einstellungen die Standardwerte.
   - Wählen Sie Speichern.

So überprüfen Sie, ob die Kerberos-Vorauthentifizierung aktiviert ist

1. Öffnen Sie auf dem Domain-Controller example.local Server Manager.
2. Wählen Sie im Menü Tools den Eintrag Active Directory Users and Computers.
3. Gehen Sie in das Verzeichnis Users (Benutzer), klicken Sie mit der rechten Maustaste auf einen Benutzer und wählen Sie Properties (Eigenschaften). Wählen Sie dann die Registerkarte Account (Konto). Scrollen Sie in der Liste Account options nach unten und stellen Sie sicher, dass Do not require Kerberos preauthentication nicht ausgewählt ist.
4. Führen Sie dieselben Schritte für die Domain corp.example.com aus der Instance corp.example.com-mgmt aus.

So konfigurieren Sie DNS-bedingte Weiterleitungen

> **Note**
>
> Eine bedingte Weiterleitung ist ein DNS-Server in einem Netzwerk, der DNS-Abfragen entsprechend dem DNS-Domainnamen in der Anfrage weiterleitet. Ein DNS-Server kann beispielsweise so konfiguriert werden, dass er alle Anfragen, die er für Namen mit der

Endung widgets.example.com erhält, an die IP-Adresse eines bestimmten DNS-Servers oder an die IP-Adressen mehrerer DNS-Server weiterleitet.

1. Öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie im Navigationsbereich Verzeichnisse aus.
3. Wählen Sie die Verzeichnis-ID Ihres AWS Managed Microsoft AD aus.
4. Notieren Sie sich den vollqualifizierten Domainnamen (FQDN), corp.example.com, und die DNS-Adressen Ihres Verzeichnisses.
5. Jetzt kehren Sie zurück zu Ihrem Domain-Controller example.local und öffnen dann Server Manager.
6. Wählen Sie im Menü Tools den Eintrag DNS.
7. Erweitern Sie in der Konsolenstruktur den DNS-Server der Domain, für die Sie die Vertrauensbeziehung einrichten, und gehen Sie zu Conditional Forwarders.
8. Klicken Sie mit der rechten Maustaste auf Conditional Forwarders, und wählen Sie dann New Conditional Forwarder.
9. Geben Sie als DNS-Domain **`corp.example.com`** ein.
10. Wählen Sie unter IP-Adressen der Primärserver die Option <Klicken Sie hier, um hinzuzufügen... >, geben Sie die erste DNS-Adresse Ihres AWS verwalteten Microsoft AD-Verzeichnisses ein (die Sie im vorherigen Verfahren notiert haben), und drücken Sie dann die EINGABETASTE. Wiederholen Sie diesen Schritt für die zweite DNS-Adresse. Nach der Eingabe der DNS-Adressen können ein „Timeout“- oder ein „unable to resolve“-Fehler auftreten. Sie können diese Fehler in der Regel ignorieren.
11. Markieren Sie das Kontrollkästchen Store this conditional forwarder in Active Directory, and replicate as follows. Wählen Sie im Dropdown-Menü den Eintrag All DNS servers in this Forest und wählen Sie dann OK.

Schritt 2: Vertrauensstellungen erstellen

In diesem Abschnitt erstellen Sie zwei separate Forest-Vertrauensbeziehungen. Eine Vertrauensstellung wird von der Active Directory-Domäne auf Ihrer EC2-Instance und die andere von Ihrem AWS verwalteten Microsoft AD in AWS erstellt.

So stellen Sie das Vertrauen zwischen Ihrer EC2-Domain und Ihrem AWS verwalteten Microsoft AD her

1. Melden Sie sich bei example.local an.
2. Öffnen Sie Server Manager und wählen Sie in der Konsolenstruktur DNS. Notieren Sie die IPv4-Adresse für den Server. Sie benötigen diese im nächsten Verfahren, wenn Sie eine bedingte Weiterleitung von corp.example.com zum Verzeichnis example.local erstellen.
3. Wählen Sie im Menü Tools den Eintrag Active Directory Domains and Trusts.
4. Klicken Sie in der Konsolenstruktur mit der rechten Maustaste auf example.local und wählen Sie dann Properties.
5. Wählen Sie auf der Registerkarte Trusts die Option New Trust und dann Next.
6. Geben Sie auf der Seite Trust Name den Namen **`corp.example.com`** ein und wählen Sie dann Next.
7. Wählen Sie auf der Seite Trust Type die Option Forest trust und wählen Sie dann Next.

   > **Note**
   >
   > AWS Managed Microsoft AD unterstützt auch externe Vertrauensstellungen. Für dieses Tutorial erstellen Sie jedoch eine bidirektionale Gesamtstruktur-Vertrauensstellung.

8. Wählen Sie auf der Seite Direction of Trust die Option Two-way und wählen Sie dann Next.

   > **Note**
   >
   > Wenn Sie sich später entscheiden, dies stattdessen mit einer einseitigen Vertrauensstellung zu versuchen, vergewissern Sie sich, dass die Richtungen der Vertrauensstellung korrekt eingerichtet sind (ausgehend von der Trusting Domain, eingehend auf der Trusted Domain). Allgemeine Informationen finden Sie auf der Website von Microsoft unter Verstehen der Vertrauensstellungs-Richtung.

9. Wählen Sie auf der Seite Sides of Trust die Option This domain only und dann Next.
10. Wählen Sie auf der Seite Outgoing Trust Authentication Level die Option Forest-wide authentication und dann Next.

> **Note**
>
> Die selektive Authentifizierung ist zwar eine Option, aber der Einfachheit halber empfehlen wir, sie hier nicht zu aktivieren. Wenn diese Funktion konfiguriert ist, beschränkt sie den Zugriff über eine externe oder Gesamtstruktur-Vertrauensstellung auf diejenigen Benutzer in einer Trusted Domain oder Gesamtstruktur, denen explizit die Berechtigung zur Authentifizierung für Computerobjekte (Ressourcencomputer) in der Trusting Domain oder Gesamtstruktur erteilt wurde. Weitere Informationen finden Sie unter Konfigurieren der Einstellungen für die selektive Authentifizierung.

11. Geben Sie auf der Seite Trust Password zweimal das Passwort für die Vertrauensbeziehung ein, und wählen Sie dann Next. Im nächsten Verfahren verwenden Sie dasselbe Passwort.
12. Sehen Sie sich auf der Seite Trust Selections Complete die Ergebnisse an, und wählen Sie dann Next.
13. Sehen Sie sich auf der Seite Trust Creation Complete die Ergebnisse an, und wählen Sie dann Next.
14. Wählen Sie auf der Seite Confirm Outgoing Trust die Option No, do not confirm the outgoing trust. Wählen Sie anschließend Weiter.
15. Wählen Sie auf der Seite Confirm Incoming Trust die Option No, do not confirm the incoming trust. Wählen Sie anschließend Weiter.
16. Wählen Sie auf der Seite Completing the New Trust Wizard die Option Finish.

> **Note**
>
> Vertrauensbeziehungen sind eine globale Funktion von AWS Managed Microsoft AD. Wenn Sie Multi-Region-Replikation verwenden, müssen die folgenden Verfahren in Primäre -Region ausgeführt werden. Die Änderungen werden automatisch auf alle replizierten Regionen angewendet. Weitere Informationen finden Sie unter Globale und regionale Features.

So stellen Sie das Vertrauen zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer EC2-Domain her

1. Öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie das Verzeichnis corp.example.com.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:
   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.
   - Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die Option Actions (Aktionen) und dann Add trust relationship (Vertrauensstellung hinzufügen aus.
5. Führen Sie im Dialogfeld Add a trust relationship die folgenden Schritte aus:
   - Wählen Sie unter Vertrauenstyp die Option Gesamtstruktur-Vertrauenstellung aus.

     > **Note**
     >
     > Stellen Sie sicher, dass der Vertrauenstyp, den Sie hier auswählen, mit dem gleichen Vertrauenstyp übereinstimmt, der im vorherigen Verfahren konfiguriert wurde (Um die Vertrauensstellung zwischen Ihrer EC2-Domäne und Ihrem AWS verwalteten Microsoft AD zu erstellen).

   - Geben Sie für Bestehender oder neuer Name der Remote Domain example.local ein.
   - Geben Sie für Trust password dasselbe Passwort ein, das Sie im vorigen Verfahren verwendet haben.
   - Wählen Sie für Vertrauensstellungs-Richtung die Option Bidirektional.

     > **Note**
     >
     > - Wenn Sie sich später entscheiden, dies stattdessen mit einer einseitigen Vertrauensstellung zu versuchen, vergewissern Sie sich, dass die Richtungen der Vertrauensstellung korrekt eingerichtet sind (ausgehend von der Trusting Domain, eingehend auf der Trusted Domain). Allgemeine Informationen finden Sie auf der Website von Microsoft unter Verstehen der Vertrauensstellungs-Richtung.

- Die selektive Authentifizierung ist zwar eine Option, aber der Einfachheit halber empfehlen wir, sie hier nicht zu aktivieren. Wenn diese Funktion konfiguriert ist, beschränkt sie den Zugriff über eine externe oder Gesamtstruktur-Vertrauensstellung auf diejenigen Benutzer in einer Trusted Domain oder Gesamtstruktur, denen explizit die Berechtigung zur Authentifizierung für Computerobjekte (Ressourcencomputer) in der Trusting Domain oder Gesamtstruktur erteilt wurde. Weitere Informationen finden Sie unter Konfigurieren der Einstellungen für die selektive Authentifizierung.

- Geben Sie für Conditional forwarder die IP-Adresse Ihres DNS-Servers in der example.local-Gesamtstruktur ein (die Sie im vorigen Verfahren notiert haben).

> **Note**
>
> Eine bedingte Weiterleitung ist ein DNS-Server in einem Netzwerk, der DNS-Abfragen entsprechend dem DNS-Domainnamen in der Anfrage weiterleitet. Ein DNS-Server kann beispielsweise so konfiguriert werden, dass er alle Anfragen, die er für Namen mit der Endung widgets.example.com erhält, an die IP-Adresse eines bestimmten DNS-Servers oder an die IP-Adressen mehrerer DNS-Server weiterleitet.

6. Wählen Sie Hinzufügen aus.

Schritt 3: Die Vertrauensstellung überprüfen

In diesem Abschnitt testen Sie, ob die Vertrauensstellungen zwischen AWS und Active Directory auf Amazon EC2 erfolgreich eingerichtet wurden.

So überprüfen Sie die Vertrauensbeziehung

1. Öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie das Verzeichnis corp.example.com.
3. Führen Sie auf der Seite Verzeichnisdetails einen der folgenden Schritte aus:

   - Wenn Sie unter Multi-Region-Replikation mehrere Regionen angezeigt bekommen, wählen Sie die primäre Region aus und wählen dann die Registerkarte Netzwerk und Sicherheit. Weitere Informationen finden Sie unter Primäre Regionen im Vergleich zu zusätzlichen Regionen.

- Wenn unter Multi-Region-Replikation keine Regionen angezeigt werden, wählen Sie die Registerkarte Netzwerk und Sicherheit.

4. Wählen Sie im Abschnitt Trust relationships (Vertrauensstellungen) die gerade erstellte Vertrauensstellung aus.
5. Wählen Sie Actions und dann Verify trust relationship.

Nachdem die Überprüfung abgeschlossen ist, sollte Verified in der Spalte Status angezeigt werden.

Herzlichen Glückwunsch! Sie haben dieses Tutorial abgeschlossen! Sie verfügen jetzt über eine voll funktionsfähige Active Directory-Multiforest-Umgebung, in der Sie verschiedene Szenarien testen können. Zusätzliche Testlabor-Tutorials sind für 2018 geplant. Sehen Sie deshalb gelegentlich nach, ob es Neuigkeiten gibt.

Problembehandlung bei AWS verwaltetem Microsoft AD

Die folgenden Informationen können Ihnen beim Beheben von ein paar gängigen Problemen behilflich sein, die beim Erstellen oder Benutzen Ihres Verzeichnisses auftreten können.

Probleme mit Ihrem AWS verwalteten Microsoft AD

Einige Aufgaben zur Problembehandlung können nur bis abgeschlossen werden AWS Support. Hier sind einige der Aufgaben:

- Starten Sie Ihre von Ihnen AWS Directory Service bereitgestellten Domänencontroller neu.
- Aktualisieren Sie Ihr AWS Managed Microsoft AD.

Informationen zum Erstellen eines Supportfalls finden Sie unter Supportanfragen erstellen und Fallmanagement.

Probleme mit Netlogon und Secure-Channel-Kommunikation

Als Gegenmaßnahme gegen CVE-2020-1472 hat Microsoft Patches veröffentlicht, die die Art und Weise ändern, wie die Netlogon-Secure-Channel-Kommunikation von Domain-Controllern verarbeitet wird. Seit der Einführung dieser sicheren Netlogon-Änderungen werden einige Netlogon-Verbindungen (Server, Workstations und Vertrauensüberprüfungen) möglicherweise nicht von Ihrem Managed Microsoft AD akzeptiert. AWS

Um zu überprüfen, ob Ihr Problem mit Netlogon oder sicherer Kanalkommunikation zusammenhängt, durchsuchen Sie Ihre CloudWatch Amazon-Logs nach den Ereignis-IDs 5827 (für Probleme im Zusammenhang mit der Geräteauthentifizierung) oder 5828 (für Probleme mit der AD-Vertrauensvalidierung). Informationen zu CloudWatch in AWS Managed Microsoft AD finden Sie unterProtokollweiterleitung aktivieren.

Weitere Informationen über die Schadensbegrenzung für CVE-2020-1472 finden Sie auf der Microsoft-Website unter Verwaltung von Änderungen in Netlogon Secure Channel-Verbindungen im Zusammenhang mit CVE-2020-1472.

Probleme beim Zurücksetzen des Benutzerkennworts

Sie erhalten eine Fehlermeldung ähnlich der folgenden, wenn Sie versuchen, das Passwort eines Benutzers zurückzusetzen:

```
Response Status: 400 Bad Request
```

Dieses Problem kann auftreten, wenn es in Ihrer AWS verwalteten Microsoft AD-Organisationseinheit (OU) doppelte Objekte mit identischen Benutzeranmeldenamen gibt. Benutzeranmeldenamen müssen eindeutig sein. Weitere Informationen finden Sie in der Microsoft Dokumentation zur Behebung von Problemen mit Verzeichnisdaten.

Wiederherstellen des Passworts

Wenn ein Benutzer ein Passwort vergisst oder Probleme hat, sich in Ihrem Simple AD- oder AWS Managed Microsoft AD-Verzeichnis anzumelden, können Sie sein Passwort entweder mit dem AWS Management Console, Windows PowerShell oder dem AWS CLI zurücksetzen.

Weitere Informationen finden Sie unter Ein Benutzerpasswort zurücksetzen.

Weitere Ressourcen

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit AWS helfen.

- AWS Knowledge Center — Hier finden Sie häufig gestellte Fragen und Links zu anderen Ressourcen, die Ihnen bei der Behebung von Problemen helfen.
- AWS Support Center — Holen Sie sich technischen Support.
- AWS Premium Support Center — Holen Sie sich erstklassigen technischen Support.

Die folgenden Ressourcen können Ihnen bei der Behebung häufig auftretender Active Directory Probleme helfen.

- Active Directory-Dokumentation:
- AD DS Fehlerbehebung

Themen

Überwachen des DNS-Servers mit Microsoft Event Viewer

Sie können Ihre DNS-Ereignisse in AWS Managed Microsoft AD überwachen, sodass Sie DNS-Probleme schneller erkennen und beheben können. Wenn beispielsweise ein DNS-Datensatz fehlt, können Sie mit dem DNS Audit-Ereignisprotokoll die Ursache des Problems identifizieren und den Fehler beheben. Sie können DNS Audit-Ereignisprotokolle auch zur Verbesserung der Sicherheit einsetzen, sodass Anforderungen, die von verdächtigen IP-Adressen stammen, erkannt und blockiert werden.

Hierzu müssen Sie mit dem Admin-Konto oder einem Konto, das Mitglied der Gruppe AWS Domain Name System Administrators ist, angemeldet sein. Weitere Informationen zu dieser Gruppe finden Sie unter Was wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.

So greifen Sie auf Event Viewer für Ihr DNS in AWS Managed Microsoft AD zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Suchen Sie eine Amazon-EC2-Instance, die mit Ihrem Verzeichnis in AWS Managed Microsoft AD verbunden ist. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Sobald Sie mit der Amazon-EC2-Instance verbunden sind, öffnen Sie das Startmenü und wählen Sie den Ordner Windows Administrative Tools aus. Wählen Sie im Ordner Administrative Tools die Option Event Viewer aus.

5. Wählen Sie im Fenster der Ereignisanzeige Action (Aktion) und dann Connect to Another Computer (Verbindung zu einem anderen Computer) aus.
6. Wählen Sie Anderer Computer aus, geben Sie einen Ihrer DNS-Servernamen von AWS Managed Microsoft AD oder eine entsprechende IP-Adresse ein und klicken Sie dann auf OK.
7. Navigieren Sie im linken Fensterbereich zu Applications and Services Logs (Anwendungs- und Serviceprotokolle)>Microsoft>Windows>DNS-Server und wählen Sie Audit (Überwachen) aus.

Linux-Domain-Verbindungsfehler

Die folgenden Informationen können Ihnen beim Beheben einiger Fehlermeldungen helfen, die beim Verbinden einer EC2-Instance mit Ihrem Verzeichnis in AWS Managed Microsoft AD auftreten können.

Linux-Instances können nicht in die Domain eingebunden oder authentifiziert werden

Ubuntu 14.04-, 16.04- und 18.04-Instanzen müssen im DNS rückwärts auflösbar sein, bevor ein Bereich mit Microsoft Active Directory funktionieren kann. Andernfalls könnte eines der beiden folgenden Szenarien eintreten:

Szenario 1: Ubuntu-Instances, die noch keinem Bereich beigetreten sind

Für Ubuntu-Instances, die versuchen, einem Bereich beizutreten, könnte der `sudo realm join`-Befehl nicht die erforderlichen Berechtigungen für die Verbindung mit der Domain liefern und den folgenden Fehler ausgeben:

! Authentifizierung bei Active Directory ist fehlgeschlagen: SASL(-1): allgemeiner Fehler: GSSAPI-Fehler: Es wurde ein ungültiger Name angegeben (Erfolg) adcli: konnte keine Verbindung zur Domain EXAMPLE.COM herstellen: Authentifizierung bei Active Directory ist fehlgeschlagen: SASL(-1): allgemeiner Fehler: GSSAPI-Fehler: Es wurde ein ungültiger Name angegeben (Success) ! Unzureichende Berechtigungen, um den Domainbereich zu verbinden: Der Bereich konnte nicht verbunden werden: Unzureichende Berechtigungen, um die Domain zu verbinden

Szenario 2: Ubuntu-Instances, die einem Bereich beigetreten sind

Bei Ubuntu-Instanzen, die bereits mit einer Microsoft Active Directory-Domäne verknüpft sind, schlagen Versuche, mithilfe der Domänenanmeldedaten per SSH auf die Instanz zuzugreifen, möglicherweise mit folgenden Fehlern fehl:

$ 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:

Wenn Sie sich mit einem öffentlichen Schlüssel bei der Instance anmelden und `/var/log/auth.log` prüfen, werden möglicherweise die folgenden Fehlermeldungen in Bezug auf den nicht gefundenen Benutzer angezeigt:

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]

`kinit` funktioniert für den Benutzer jedoch. Hier ein Beispiel:

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

Workaround

Der aktuell empfohlene Workaround für beide dieser Szenarien ist, wie nachstehend beschrieben, die Deaktivierung von Reverse DNS in `/etc/krb5.conf` im Abschnitt [libdefaults]:

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

Probleme bei der einseitigen Vertrauensauthentifizierung mit nahtloser Domainverbindung

Wenn Sie eine unidirektionale ausgehende Vertrauensstellung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrem lokalen Active Directory eingerichtet haben, tritt möglicherweise ein Authentifizierungsproblem auf, wenn Sie versuchen, sich mit Ihren vertrauenswürdigen Active Directory-Anmeldeinformationen mit Winbind für die zur Domäne gehörende Linux-Instanz zu authentifizieren.

Fehler

31. Juli 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Falsches Passwort von user@corp.example.com von xxx.xxx.xxx.xxx Port 18309 ssh2

31. Juli 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): Passwort wird abgerufen (0x00000390)

31. Juli 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item hat ein Passwort zurückgegeben

31. Juli 00:05:00 EC2Amaz-LSMWQT sshd [23832]: pam_winbind (sshd:auth): Anfrage wbcLogonUser fehlgeschlagen: WBC_ERR_AUTH_ERROR, PAM-Fehler: PAM_SYSTEM_ERR (4), NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**, Fehlermeldung lautete: Der Objektname wurde nicht gefunden.

31. Juli 00:05:00 EC2Amaz-LSMWQT sshd [23832]: pam_winbind (sshd:auth): interner Modulfehler (retval = PAM_SYSTEM_ERR (4), user = 'CORP\ user')

Workaround

Um dieses Problem zu beheben, müssen Sie eine Anweisung in der Konfigurationsdatei des PAM-Moduls auskommentieren oder entfernen (`/etc/security/pam_winbind.conf`). Gehen Sie dazu wie folgt vor.

1. Öffnen Sie die Datei `/etc/security/pam_winbind.conf` in einem Text-Editor.

   ```
   sudo vim /etc/security/pam_winbind.conf
   ```

2. Kommentieren Sie die folgende Anweisung aus oder entfernen Sie sie: krb5_auth = yes.

   ```
   [global]
   ```

```
cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Stoppen Sie den Winbind-Service und starten Sie ihn dann erneut.

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

Active Directory – Geringer verfügbarer Speicherplatz

Wenn Ihr AWS verwaltetes Microsoft AD aufgrund des geringen verfügbaren Speicherplatzes in Active Directory beeinträchtigt ist, sind sofortige Maßnahmen erforderlich, um das Verzeichnis wieder in den aktiven Zustand zu versetzen. Die beiden häufigsten Ursachen für diese Beeinträchtigung werden in den folgenden Abschnitten behandelt:

1. SYSVOL-Ordner speichert nicht nur wesentliche Gruppenrichtlinienobjekte
2. Die Active-Directory-Datenbank hat das Volume ausgefüllt

Preisinformationen zu AWS verwaltetem Microsoft AD-Speicher finden Sie unter AWS Directory Service Preise.

SYSVOL-Ordner speichert nicht nur wesentliche Gruppenrichtlinienobjekte

Eine häufige Ursache für diese Beeinträchtigung ist das Speichern nicht wesentlicher Dateien für die Verarbeitung von Gruppenrichtlinien im SYSVOL-Ordner. Diese nicht wesentlichen Dateien können EXE, MSIs oder andere Dateien sein, die für die Verarbeitung von Gruppenrichtlinien nicht wesentlich sind. Die wesentlichen Objekte für die Verarbeitung von Gruppenrichtlinien sind Gruppenrichtlinienobjekte, An-/Abmeldeskripts und der zentrale Speicher für Gruppenrichtlinienobjekte. Alle nicht benötigten Dateien sollten auf einem oder mehreren Dateiservern als Ihren AWS verwalteten Microsoft AD-Domänencontrollern gespeichert werden.

Wenn Dateien für die Gruppenrichtlinien-Softwareinstallation benötigt werden, sollten Sie einen Dateiserver verwenden, um diese Installationsdateien zu speichern. Wenn Sie einen Dateiserver nicht selbst verwalten möchten, AWS bietet Amazon FSx eine verwaltete Dateiserveroption an.

Um nicht erforderliche Dateien zu entfernen, können Sie über den UNC-Pfad (Universal Naming Convention) auf die SYSVOL-Freigabe zugreifen. Wenn der vollqualifizierte Domainname (FQDN) Ihrer Domain beispielsweise example.com ist, lautet der UNC-Pfad für SYSVOL „\\example.local\SYSVOL\example.local\“. Sobald Sie Objekte, die für die Verarbeitung des Verzeichnisses von Gruppenrichtlinien nicht erforderlich sind, gefunden und entfernt haben, sollte das Verzeichnis innerhalb von 30 Minuten zum Status „Aktiv“ zurückkehren. Wenn das Verzeichnis nach 30 Minuten nicht aktiv ist, wenden Sie sich bitte an den AWS Support.

Wenn Sie nur wesentliche Gruppenrichtliniendateien in Ihrer SYSVOL-Freigabe speichern, wird sichergestellt, dass Sie Ihr Verzeichnis durch Aufblähen des SYSVOL-Ordners nicht beeinträchtigen.

Die Active-Directory-Datenbank hat das Volume ausgefüllt

Eine häufige Ursache für diese Beeinträchtigung ist darauf zurückzuführen, dass die Active Directory-Datenbank das Volume füllt. Um festzustellen, ob dies der Fall ist, können Sie die Gesamtzahl der Objekte in Ihrem Verzeichnis überprüfen. Das Wort Gesamtzahl ist fett formatiert, um sicherzustellen, dass Sie verstehen, dass gelöschte Objekte zur Gesamtzahl der Objekte in einem Verzeichnis zählen.

Standardmäßig bewahrt AWS Managed Microsoft AD Elemente 180 Tage lang im AD-Papierkorb auf, bevor sie zu einem recycelten Objekt werden. Sobald ein Element zu einem Recycled-Objekt (veraltet) wird, wird es für weitere 180 Tage aufbewahrt. Anschließend wird es dauerhaft aus dem Verzeichnis gelöscht. Wenn also ein Objekt gelöscht wird, war es vor dem Löschen noch 360 Tage in der Verzeichnisdatenbank vorhanden. Aus diesem Grund muss die Gesamtzahl der Objekte berücksichtigt werden.

Weitere Informationen zur Anzahl von Objekten, die von AWS Managed Microsoft AD unterstützt werden, finden Sie unter AWS Directory Service Preise.

Um die Gesamtzahl der Objekte in einem Verzeichnis abzurufen, das die gelöschten Objekte enthält, können Sie den folgenden PowerShell Befehl von einer Windows-Instanz aus ausführen, die der Domäne angehört. Anweisungen zum Einrichten einer Verwaltungs-Instance finden Sie unter Benutzer und Gruppen in AWS Managed Microsoft AD verwalten.

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |
 Select-Object -Property 'Count'
```

Nachfolgend ist eine Beispielausgabe für den obigen Befehl aufgeführt:

```
Count
10000
```

Wenn die Gesamtzahl über der unterstützten Objektanzahl für die in der obigen Anmerkung aufgeführten Verzeichnisgröße liegt, haben Sie die Kapazität Ihres Verzeichnisses überschritten.

Im Folgenden sind die Optionen aufgeführt, um diese Beeinträchtigung zu beheben:

1. AD bereinigen
   a. Löschen Sie alle unerwünschten AD-Objekte.
   b. Entfernen Sie alle Objekte, die nicht erforderlich sind, aus dem AD-Papierkorb. Beachten Sie, dass dieser Vorgang destruktiv ist. Die einzige Möglichkeit, diese gelöschten Objekte wiederherzustellen, besteht in der Wiederherstellung des Verzeichnisses.
   c. Mit dem folgenden Befehl werden alle gelöschten Objekte aus dem AD-Papierkorb entfernt.

   > **Important**
   >
   > Verwenden Sie diesen Befehl mit äußerster Vorsicht, da dies ein destruktiver Befehl ist, und die einzige Möglichkeit, diese gelöschten Objekte wiederherzustellen, besteht in der Wiederherstellung des Verzeichnisses.

   ```
   $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. Eröffnen Sie einen Fall beim AWS Support, um die AWS Directory Service Rückforderung des freien Speicherplatzes zu beantragen.
2. Wenn Ihr Verzeichnistyp Standard Edition ist, wenden Sie sich an den AWS Support und fordern Sie ein Upgrade Ihres Verzeichnisses auf Enterprise Edition an. Dadurch erhöhen sich auch die Kosten für Ihr Verzeichnis. Preisinformationen finden Sie unter AWS Directory Service – Preise.

In AWS Managed Microsoft AD haben Mitglieder der Administratorgruppe AWS Delegated Deleted Object Lifetime die Möglichkeit, das `msDS-DeletedObjectLifetime` Attribut zu ändern, das festlegt, wie lange (in Tagen) gelöschte Objekte im AD-Papierkorb aufbewahrt werden, bevor sie zu recycelten Objekten werden.

> **Note**
>
> Dies ist ein Thema für Fortgeschrittene. Bei unsachgemäßer Konfiguration können Datenverluste die Folge sein. Es wird dringend empfohlen, zuerst The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting zu lesen, um diese Prozesse besser zu verstehen.

Die Möglichkeit, den Wert des Attributs `msDS-DeletedObjectLifetime` in eine niedrigere Zahl zu ändern, kann dazu beitragen, dass die Anzahl der Objekte die unterstützten Grenzwerte nicht überschreitet. Der niedrigste gültige Wert, auf den dieses Attribut eingestellt werden kann, ist 2 Tage. Sobald dieser Wert überschritten wird, können Sie das gelöschte Objekt mit dem AD-Papierkorb nicht mehr wiederherstellen. Zum Wiederherstellen gelöschter Objekte müssen Sie Ihr Verzeichnis mithilfe eines Snapshots wiederherstellen. Weitere Informationen finden Sie unter Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen. Wiederherstellungen aus Snapshots können zu Datenverlust führen, da sie zeitpunktbezogen sind.

Führen Sie den folgenden Befehl aus, um die Lebensdauer der gelöschten Objekte Ihres Verzeichnisses zu ändern:

> **Note**
>
> Wenn Sie den Befehl so ausführen, wie er ist, wird der Attributwert für die Lebensdauer der gelöschten Objekte auf 30 Tage festgelegt. Wenn Sie die Lebensdauer verlängern oder verkürzen möchten, ersetzen Sie „30“ durch die gewünschte Zahl. Wir empfehlen jedoch, keinen höheren Wert als die Standardanzahl 180 zu verwenden.

```
$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}
```

Fehler in Zusammenhang mit Schemaerweiterungen

Die folgenden Informationen können Ihnen beim Beheben einiger Fehlermeldungen helfen, die bei einer Schemaerweiterung für Ihr Verzeichnis in AWS Managed Microsoft AD auftreten können.

Weiterleitungen

Fehler

> Fügen Sie dem Eintrag ab Zeile 1 einen Fehler hinzu: Verweis Der serverseitige Fehler lautet: 0x202b Ein Verweis wurde vom Server zurückgegeben. Der erweiterte Serverfehler lautet: 0000202B: RefErr: DSID-0310082F, data 0, 1 access points \tref 1: „example.com“ Anzahl der geänderten Objekte: 0

Fehlerbehebung

> Stellen Sie sicher, dass in allen Feldern für definierte Namen der richtige Domainname angegeben ist. In dem Beispiel oben sollte `DC=example,dc=com` durch den `DistinguishedName` ersetzt werden, der vom Cmdlet `Get-ADDomain` angezeigt wird.

Lesen der Importdatei nicht möglich

Fehler

> Lesen der Importdatei nicht möglich. Anzahl der geänderten Objekte: 0

Fehlerbehebung

> Die importierte LDIF-Datei ist leer (0 Byte). Stellen Sie sicher, dass die richtige Datei hochgeladen wurde.

Syntaxfehler

Fehler

> Es gibt einen Syntaxfehler in der Eingabedatei Fehlgeschlagen in Zeile 21. The last token starts with 'q'. Anzahl der geänderten Objekte: 0

Fehlerbehebung

Der Text in Zeile 21 ist nicht ordnungsgemäß formatiert. Der erste Buchstabe des ungültigen Texts lautet A. Aktualisieren Sie Zeile 21 mit gültiger LDIF-Syntax. Weitere Informationen zum Formatieren der LDIF-Datei finden Sie unter Schritt 1: Ihre LDIF-Datei erstellen.

Attribut oder Wert vorhanden

Fehler

Fehler beim Eintrag ab Zeile 1 hinzufügen: Attribut oder Wert existiert Der serverseitige Fehler lautet: 0x2083 Der angegebene Wert existiert bereits. Der erweiterte Serverfehler lautet: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain):len 4 Anzahl der geänderten Objekte: 0

Fehlerbehebung

Die Schemaänderung wurde bereits angewendet.

Kein solches Attribut vorhanden

Fehler

Fehler beim Eintrag ab Zeile 1 hinzufügen: Kein solches Attribut Der serverseitige Fehler lautet: 0x2085 Der Attributwert kann nicht entfernt werden, da er im Objekt nicht vorhanden ist. Der erweiterte Serverfehler lautet: 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problem 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (mayContain):len 4 Anzahl der geänderten Objekte: 0

Fehlerbehebung

Die LDIF-Datei versucht, ein Attribut aus einer Klasse zu entfernen, das betreffende Attribut ist der Klasse zurzeit jedoch nicht angefügt. Die Schemaänderung wurde wahrscheinlich bereits angewendet.

Fehler

Fehler beim Eintrag ab Zeile 41 hinzufügen: Kein solches Attribut 0x57 Der Parameter ist falsch. The extended server error is: 0x208d Directory object not found. Der erweiterte

Serverfehler lautet: „00000057: LdapErr: DSID-0C090D8A, Kommentar: Fehler bei Attributkonvertierungsvorgang, Daten 0, v2580“ Anzahl der geänderten Objekte: 0

Fehlerbehebung

Das Attribut in Zeile 41 ist nicht korrekt. Überprüfen Sie die Schreibweise erneut.

Kein solches Objekt vorhanden

Fehler

Fehler beim Eintrag ab Zeile 1 hinzufügen: Kein solches Objekt Der serverseitige Fehler lautet: 0x208d Verzeichnisobjekt nicht gefunden. Der erweiterte Serverfehler lautet: 0000208D: NameErr: DSID-03100238, Problem 2001 (NO_OBJECT), Daten 0, beste Übereinstimmung von: „CN=Schema,CN=Konfiguration,DC=example,DC=com“ Anzahl der geänderten Objekte: 0

Fehlerbehebung

Das Objekt, auf das von dem definierten Namen (DN) verwiesen wird, ist nicht vorhanden.

Gründe für den Status der Vertrauensstellung

Wenn Erstellung von Vertrauensstellungen nicht erfolgreich ist, enthält die Statusmeldung weitere Informationen. Hier finden Sie Hilfe zu verstehen, was diese Nachrichten bedeuten.

Zugriff verweigert

Der Zugriff wurde verweigert, wenn Sie versuchen, die Vertrauensstellung zu erstellen. Entweder das Vertrauensstellungspasswort ist falsch, oder die Sicherheitseinstellungen der Remote-Domain ermöglichen keine Konfiguration der Vertrauensstellung. Versuchen Sie Folgendes, um dieses Problem zu beheben:

- Das AWS Managed Microsoft AD Active Directory und die selbstverwaltete , mit der Active Directory Sie eine Vertrauensstellung erstellen möchten, müssen denselben Namen für die erste Website haben. Der Name des ersten Standorts ist auf festgelegt`Default-First-Site-Name`. Ein Fehler aufgrund Zugriffsverweigerung tritt auf, wenn diese Namen zwischen Domänen variieren.
- Stellen Sie sicher, dass Sie das gleiche Vertrauensstellungspasswort verwenden wie beim Erstellen der entsprechenden Vertrauensstellung in der Remote-Domain.

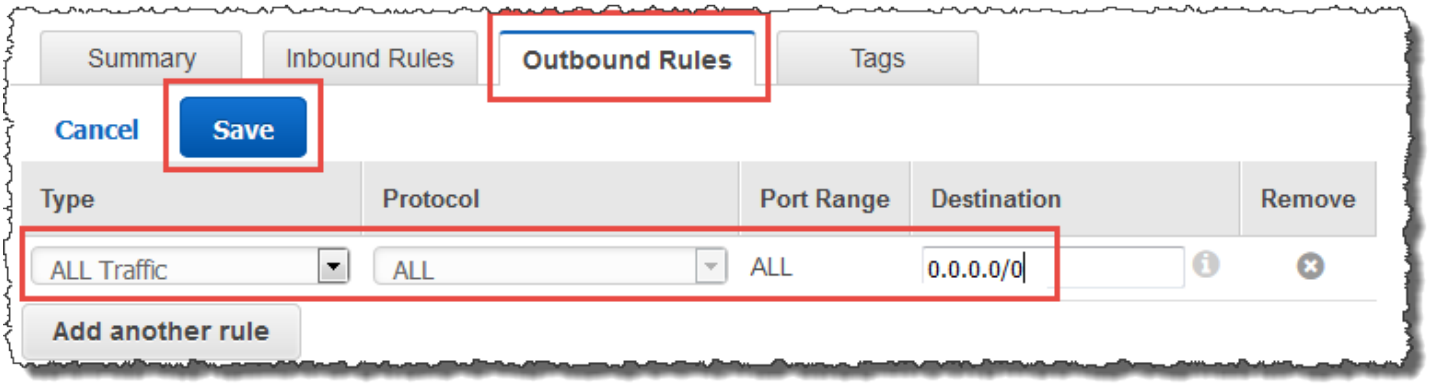
- Vergewissern Sie sich außerdem, dass Ihre Domain-Sicherheitseinstellungen die Erstellung von Vertrauensstellungen ermöglichen.
- Überprüfen Sie, ob Ihre lokale Sicherheitsrichtlinie korrekt eingerichtet ist. Überprüfen Sie insbesondere `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` und stellen Sie sicher, dass sie mindestens die drei folgenden benannten Pipes enthält:
  - netlogon
  - samr
  - lsarpc
- Stellen Sie sicher, dass die oben genannten Pipes als Wert(e) auf dem NullSessionPipes Registrierungsschlüssel vorhanden sind, der sich im Registrierungspfad HKLM\SYSTEM \CurrentControlSet\servicesLanmanServer\Parameter befindet. Diese Werte müssen in getrennten Zeilen eingefügt werden.

  > **Note**
  >
  > Standardmäßig ist `Network access: Named Pipes that can be accessed anonymously` nicht festgelegt und zeigt `Not Defined` an. Das ist normal, weil die effektiven Standardeinstellungen für `Network access: Named Pipes that can be accessed anonymously` des Domain-Controllers gleich `netlogon`, `samr`, `lsarpc` sind.

- Überprüfen Sie die folgende Einstellung für Server Message Block (SMB) Signing in der Standardrichtlinie für Domain-Controller. Diese Einstellungen finden Sie unter Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien/ Sicherheitsoptionen. Sie sollten den folgenden Einstellungen entsprechen:
  - Microsoft Netzwerkclient: Digital signieren Sie die Kommunikation (als immer): Standard: Aktiviert
  - Microsoft Network Client: Digitale Signierung der Kommunikation (wenn der Server zustimmt): Standard: Aktiviert
  - Microsoft Netzwerkserver: Digitale Sign-Kommunikation (als immer): Aktiviert
  - Microsoft Netzwerkserver: Digital signieren Sie die Kommunikation (wenn der Client zustimmt): Standard: Aktiviert

Der angegebene Domain-Name ist nicht vorhanden oder konnte nicht hergestellt werden

Um dieses Problem zu beheben, vergewissern Sie sich, dass die Einstellungen der Sicherheitsgruppe für Ihre Domain und die Zugriffssteuerungsliste (ACL) für Ihre VPC korrekt sind und Sie die Informationen für Ihre bedingte Weiterleitung richtig eingegeben haben. AWS konfiguriert die Sicherheitsgruppe so, dass sie nur die Ports öffnet, die für die Active-Directory-Kommunikation erforderlich sind. In der Standard-Konfiguration akzeptiert die Sicherheitsgruppe Datenverkehr zu diesen Ports von jeder beliebigen IP-Adresse aus. Ausgehender Verkehr ist auf die Sicherheitsgruppe beschränkt. Sie müssen die Regel für ausgehenden Datenverkehr in der Sicherheitsgruppe aktualisieren, um den Datenverkehr in Ihr On-Premises-Netzwerk zuzulassen. Weitere Informationen zu Sicherheitsanforderungen finden Sie unter Schritt 2: Ihr AWS Managed Microsoft AD vorbereiten.



Wenn die DNS-Server für die Netzwerke der anderen Verzeichnisse öffentliche (nicht RFC 1918) IP-Adressen verwenden, müssen Sie eine IP-Route auf dem Verzeichnis von der Directory Services Console zu den DNS-Servern hinzufügen. Weitere Informationen finden Sie unter Eine Vertrauensbeziehung erstellen, überprüfen oder löschen und Voraussetzungen.

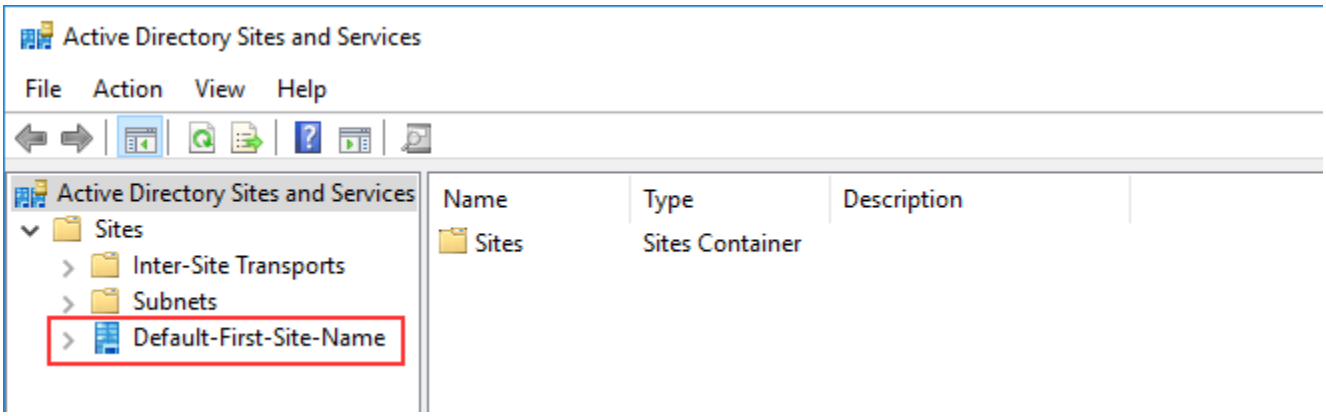
Die Internet Assigned Numbers Authority (IANA) hat die folgenden drei Blöcke der IP-Adressumgebung für private Internetdienste reserviert:

- 10.0.0.0 - 10.255.255.255 (10/8 Präfix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 Präfix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 Präfix)

Weitere Informationen finden Sie unter https://tools.ietf.org/html/rfc1918.

Stellen Sie sicher, dass der Standard-AD-Standortname für Ihr AWS Managed Microsoft AD mit dem Standard-AD-Standortnamen in Ihrer On-Premises-Infrastruktur übereinstimmt. Der Computer bestimmt den Namen des Standorts anhand einer Domain, in der der Computer Mitglied ist, und nicht anhand der Domain des Benutzers. Die Umbenennung des Standorts in den nächstgelegenen On-Premises-Standort stellt sicher, dass der DC Locator einen Domain-Controller vom nächstgelegenen Standort verwendet. Wenn dies das Problem nicht behebt, ist es möglich, dass Informationen aus einer zuvor erstellten bedingten Weiterleitung zwischengespeichert wurden und die Erstellung einer neuen Vertrauensstellung verhindern. Warten Sie einige Minuten und versuchen Sie dann erneut, die Vertrauensstellung und die bedingte Weiterleitung zu erstellen.

Weitere Informationen darüber, wie dies funktioniert, finden Sie unter Domain Locator incross a Forest Trust auf der -MicrosoftWebsite.



Der Vorgang konnte in dieser Domain nicht ausgeführt werden

Um dieses Problem zu lösen, stellen Sie sicher, dass beide Domains bzw. Verzeichnisse keine überlappenden NETBIOS-Namen haben. Falls die Domains/Verzeichnisse sich überschneidende NETBIOS-Namen haben, erstellen Sie eines davon mit einem anderen NETBIOS-Namen neu und versuchen Sie es dann erneut.

Die Erstellung einer Vertrauensstellung schlägt aufgrund des Fehlers „Erforderlicher und gültiger Domainname“ fehl

DNS-Namen dürfen nur alphabetische Zeichen (A–Z), Ziffern (0–9), das Minuszeichen (-) und Punkte (.) enthalten. Punkte sind nur zulässig, wenn sie zur Abgrenzung der Bestandteile von Namen im Domain-Stil verwendet werden. Berücksichtigen Sie dabei auch Folgendes:

- AWS Managed Microsoft AD unterstützt keine Vertrauensstellungen mit Single Label Domains. Weitere Informationen finden Sie unter -MicrosoftUnterstützung für Single Label Domains.

- Laut RFC 1123 (https://tools.ietf.org/html/rfc1123) sind die einzigen Zeichen, die in DNS-Bezeichnungen verwendet werden können, „A“ bis „Z“, „a“ bis „z“, „0" bis „9" und ein Bindestrich („-“). Ein Punkt [.] wird auch in DNS-Namen verwendet, jedoch nur zwischen DNS-Labels und am Ende eines FQDN.
- Gemäß RFC 952 (https://tools.ietf.org/html/rfc952) ist ein „Name“ (Netz-, Host-, Gateway- oder Domainname) eine Textkette mit bis zu 24 Zeichen aus dem Alphabet (A–Z), Ziffern (0–9), dem Minuszeichen (-) und dem Punkt (.). Beachten Sie, dass Punkte nur zulässig sind, wenn sie der Abgrenzung von Komponenten von Namen im „Domain-Stil“ dienen.

Weitere Informationen finden Sie unter Einhaltung von Namensbeschränkungen für Hosts und Domains auf der -MicrosoftWebsite.

Standard-Tools für das Testen von Vertrauensstellungen

Im Folgenden finden Sie Tools, mit denen Sie verschiedene Probleme im Zusammenhang mit Vertrauensstellungen beheben können.

AWS Tools zur Fehlerbehebung bei Systems Manager Automation

Support Automation Workflows (SAW) nutzen AWS Systems Manager Automation, um Ihnen ein vordefiniertes Runbook für bereitzustellen AWS Directory Service. Das AWSSupport-TroubleshootDirectoryTrustRunbook-Tool hilft Ihnen bei der Diagnose häufiger Probleme mit der Vertrauensstellung zwischen AWS Managed Microsoft AD und einem On-PremisesMicrosoft-Active Directory.

DirectoryServicePortTest -Tool

Das DirectoryServicePortTest Testtool kann bei der Behebung von Problemen mit der Vertrauensstellung zwischen AWS Managed Microsoft AD und On-Premises-Active-Directory hilfreich sein. Ein Beispiel, wie das Tool verwendet werden kann, finden Sie unter Testen Sie Ihren AD Connector.

NETDOM- und NLTEST-Tool

Administratoren können sowohl die Befehlszeilentools Netdom als auch Nltest verwenden, um Vertrauensstellungen zu finden, anzuzeigen, zu erstellen, zu entfernen und zu verwalten. Diese Tools kommunizieren direkt mit der LSA-Stelle auf einem Domain-Controller. Ein Beispiel für die Verwendung dieser Tools finden Sie unter Netdom und NLTEST auf der -MicrosoftWebsite.

Tool zur Paketerfassung

Sie können das integrierte Windows-Hilfsprogramm zur Paketerfassung verwenden, um ein potenzielles Netzwerkproblem zu untersuchen und zu beheben. Weitere Informationen finden Sie unter Eine Netzwerkverfolgung erfassen, ohne etwas zu installieren.

AD Connector

AD Connector ist ein Verzeichnisgateway, mit dem Sie Verzeichnisanfragen an Ihre lokalen Standorte umleiten können, Microsoft Active Directory ohne Informationen in der Cloud zwischenzuspeichern. AD Connector ist in zwei Größen verfügbar, klein und groß. Ein kleiner AD Connector ist für kleinere Organisationen und eine geringe Anzahl von Operationen pro Sekunde vorgesehen. Ein großer AD Connector ist für größere Organisationen und eine mäßige bis hohe Anzahl von Operationen pro Sekunde vorgesehen. Sie können Anwendungslasten über mehrere AD Connectors verteilen, um gemäß Ihren Leistungsanforderungen zu skalieren. Es gibt keine erzwungenen Benutzer- oder Verbindungslimits.

AD Connector unterstützt keine transitiven Active Directory-Vertrauensstellungen. AD Connectors und Ihre lokalen Active Directory-Domänen haben eine 1:1 -Beziehung. Das heißt, Sie müssen für jede lokale Domäne, einschließlich untergeordneter Domänen in einer Active Directory-Gesamtstruktur, für die Sie sich authentifizieren möchten, einen eindeutigen AD Connector erstellen.

> **Note**
>
> AD Connector kann nicht mit anderen AWS Konten geteilt werden. Wenn dies eine Anforderung ist, sollten Sie die Verwendung von AWS Managed Microsoft AD in Betracht ziehenFreigeben Ihres Verzeichnisses. AD Connector ist auch nicht Multi-VPC-fähig, was bedeutet, dass AWS Anwendungen wie in derselben VPC wie Ihr AD Connector bereitgestellt WorkSpaceswerden müssen.

Nach der Einrichtung von AD Connector profitieren Sie von folgenden Vorteilen:

- Ihre Endbenutzer und IT-Administratoren können ihre vorhandenen Unternehmensanmeldedaten verwenden WorkSpaces, um sich bei AWS Anwendungen wie Amazon WorkDocs oder Amazon anzumelden WorkMail.
- Sie können AWS Ressourcen wie Amazon EC2 EC2-Instances oder Amazon S3 S3-Buckets über den rollenbasierten IAM-Zugriff auf die verwalten. AWS Management Console
- Sie können bestehende Sicherheitsrichtlinien (wie Ablauf von Kennwörtern, Kennwortverlauf und Kontosperrungen) konsistent durchsetzen, unabhängig davon, ob Benutzer oder IT-Administratoren auf Ressourcen in Ihrer lokalen Infrastruktur oder in der Cloud zugreifen. AWS

- Sie können AD Connector verwenden, um die Multi-Faktor-Authentifizierung zu aktivieren, indem Sie es in Ihre bestehende RADIUS-basierte MFA-Infrastruktur integrieren und so eine zusätzliche Sicherheitsebene bieten, wenn Benutzer auf Anwendungen zugreifen. AWS

Lesen Sie die Themen in diesem Abschnitt, um zu erfahren, wie Sie eine Verbindung zu einem Verzeichnis herstellen und die AD-Connector-Features optimal nutzen.

Themen

Erste Schritte mit AD Connector

Mit AD Connector können Sie eine Verbindung AWS Directory Service zu Ihrem bestehenden Unternehmen herstellenActive Directory. Wenn Sie mit Ihrem vorhandenen Verzeichnis verbunden sind, verbleiben alle Ihre Verzeichnisdaten auf Ihren Domänencontrollern. AWS Directory Service repliziert keine Ihrer Verzeichnisdaten.

Themen

AD-Connector-Voraussetzungen

Zum Herstellen einer Verbindung mit Ihrem vorhandenen Verzeichnis über AD Connector benötigen Sie Folgendes:

Amazon VPC

Richten Sie eine VPC mit Folgendem ein:

- Mindestens zwei Subnetze. Jedes dieser Subnetze muss sich in einer anderen Availability Zone befinden.
- Die VPC muss mit Ihrem vorhandenen Netzwerk über ein VPN (Virtual Private Network) oder AWS Direct Connect verbunden sein.
- Die VPC muss über Standard-Hardware-Tenancy verfügen.

AWS Directory Service verwendet eine Struktur mit zwei VPCs. Die EC2-Instances, aus denen Ihr Verzeichnis besteht, laufen außerhalb Ihres AWS Kontos und werden von verwaltet. AWS Sie haben zwei Netzwerkadapter `ETH0` und `ETH1`. `ETH0` ist der Verwaltungsadapter und existiert außerhalb Ihres Kontos. `ETH1` wird in Ihrem Konto erstellt.

Der Management-IP-Bereich des `ETH0`-Netzwerks Ihres Verzeichnisses wird programmatisch ausgewählt, um sicherzustellen, dass er nicht mit der VPC kollidiert, in der Ihr Verzeichnis bereitgestellt wird. Dieser IP-Bereich kann sich in einem der folgenden Paare befinden (da Verzeichnisse in zwei Subnetzen ausgeführt werden):

- 10.0.1.0/24 und 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 und 192.168.2.0/24

Wir vermeiden Konflikte, indem wir das erste Oktett des `ETH1`-CIDR überprüfen. Wenn es mit einer 10 beginnt, dann wählen wir eine 192.168.0.0/16 VPC mit den Subnetzen 192.168.1.0/24 und 192.168.2.0/24. Wenn das erste Oktett etwas anderes als eine 10 ist, wählen wir eine 10.0.0.0/16 VPC mit den Subnetzen 10.0.1.0/24 und 10.0.2.0/24.

Der Auswahlalgorithmus berücksichtigt nicht die Routen auf Ihrer VPC. Es ist daher möglich, dass dieses Szenario zu einem IP-Routing-Konflikt führt.

Weitere Informationen finden Sie unter den folgenden Themen im Amazon VPC Benutzerhandbuch:

- Was ist Amazon VPC?
- Subnetze in Ihrer VPC
- Hinzufügen eines Hardware Virtual Private Gateway zu Ihrer VPC

Weitere Informationen AWS Direct Connect zu finden Sie im Benutzerhandbuch.AWS Direct Connect

Besteht Active Directory

Sie müssen eine Verbindung zu einem bestehenden Netzwerk mit einer Active Directory Domain herstellen.

> **Note**
>
> AD Connector unterstützt Single Label Domains nicht.

Die Funktionsebene dieser Active Directory Domain muss mindestens so hoch sein`Windows Server 2003`. AD Connector unterstützt auch das Herstellen einer Verbindung mit einer auf einer Amazon-EC2-Instance gehosteten Domain.

> **Note**
>
> AD Connector unterstützt keine schreibgeschützten Domain-Controller (RODC), wenn es in Verbindung mit dem Amazon-EC2-Feature zur Domainverbindung verwendet wird.

Servicekonto

Sie müssen über Anmeldeinformationen für ein Servicekonto im vorhandenen Verzeichnis verfügen, dem die folgenden Berechtigungen zugewiesen sind:

- Lesen von Benutzern und Gruppen – erforderlich
- Computer mit der Domäne verbinden — Nur erforderlich, wenn Seamless Domain Join verwendet wird und WorkSpaces
- Computerobjekte erstellen — Nur erforderlich, wenn Seamless Domain Join verwendet wird und WorkSpaces
- Das Kennwort für das Dienstkonto sollte den AWS Kennwortanforderungen entsprechen. AWS Die Passwörter sollten wie folgt lauten:
  - Zwischen 8 und 128 Zeichen lang, einschließlich.
  - Enthält mindestens ein Zeichen aus drei der folgenden vier Kategorien:
    - Kleinbuchstaben (a – z)
    - Großbuchstaben (A – Z)
    - Zahlen (0 – 9)

- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

Weitere Informationen finden Sie unter Zuweisen von Berechtigungen zu Ihrem Servicekonto.

> **Note**
>
> AD Connector verwendet Kerberos für die Authentifizierung und Autorisierung von AWS -Anwendungen. LDAP wird nur für die Suche nach Benutzer- und Gruppenobjekten (Lesevorgänge) verwendet. Bei den LDAP-Transaktionen ist nichts veränderbar und Anmeldeinformationen werden nicht im Klartext übergeben. Die Authentifizierung erfolgt durch einen AWS internen Dienst, der Kerberos-Tickets verwendet, um LDAP-Operationen als Benutzer auszuführen.

Benutzerberechtigungen

Alle Active Directory-Benutzer müssen die Berechtigung haben, ihre eigenen Attribute zu lesen. Insbesondere die folgenden Attribute:

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

Standardmäßig haben Active Directory-Benutzer Leseberechtigungen für diese Attribute. Administratoren können jedoch diese Berechtigungen im Laufe der Zeit ändern. Daher sollten Sie vor der ersten Einrichtung von AD Connector überprüfen, ob Ihre Benutzer über diese Leseberechtigungen verfügen.

IP-Adressen

Holen Sie sich die IP-Adressen von zwei DNS-Servern oder Domain-Controllern in Ihrem vorhandenen Verzeichnis.

AD Connector ermittelt `_ldap._tcp.<DnsDomainName>` und `_kerberos._tcp.<DnsDomainName>` SRV-Datensätze von diesen Servern bei der Verbindung

zu Ihrem Verzeichnis, daher müssen diese Server diese SRV-Datensätze enthalten. Der AD Connector versucht, einen gemeinsamen Domain-Controller zu finden, der LDAP und Kerberos-Services bietet, sodass diese SRV-Datensätze mindestens einen gemeinsamen Domain-Controller enthalten müssen. Weitere Informationen zu SRV-Datensätzen finden Sie unter SRV Resource Records auf Microsoft. TechNet

Ports für Subnetze

Damit AD Connector Verzeichnisanfragen an Ihre vorhandenen Active Directory Domain-Controller weiterleiten kann, muss die Firewall für Ihr vorhandenes Netzwerk die folgenden Ports für die CIDRs für beide Subnetze in Ihrer Amazon VPC geöffnet haben.

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos-Authentifizierung
- TCP/UDP 389 – LDAP

Das ist das Minimum an notwendigen Ports, damit AD Connector eine Verbindung mit Ihrem Verzeichnis herstellen kann. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports.

Wenn Sie AD Connector und Amazon verwenden möchten WorkSpaces, muss das Attribut disableVlvSupportLDAP für Ihre Domain-Controller auf 0 gesetzt werden. Dies ist die Standardeinstellung für die Domain-Controller. AD Connector kann Benutzer im Verzeichnis nicht abfragen, wenn das DisableVLVSupportLDAP-Attribut aktiviert ist. Dadurch wird verhindert, dass AD Connector mit arbeitet Amazon WorkSpaces.

> **Note**
>
> Wenn sich die DNS-Server oder Domain-Controller-Server für Ihre bestehende Active Directory Domain innerhalb der VPC befinden, müssen die mit diesen Servern verknüpften Sicherheitsgruppen die oben genannten Ports für die CIDRs für beide Subnetze in der VPC geöffnet haben.

Weitere Portanforderungen finden Sie in der Dokumentation unter AD- und AD DS-Portanforderungen. Microsoft

Kerberos-Vorabauthentifizierung

Für Ihre Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Detaillierte Anweisungen dazu, wie Sie diese Einstellung aktivieren, finden Sie unter Sicherstellen, dass

Kerberos-Vorauthentifizierung aktiviert ist. Allgemeine Informationen zu dieser Einstellung finden Sie unter Vorauthentifizierung ein. Microsoft TechNet

Verschlüsselungstypen

AD Connector unterstützt die folgenden Verschlüsselungstypen bei der Authentifizierung Ihrer Active-Directory-Domain-Controller über Kerberos:

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center Voraussetzungen

Wenn Sie IAM Identity Center mit AD Connector verwenden möchten, müssen Sie sicherstellen, dass Folgendes zutrifft:

- Ihr AD Connector ist im Verwaltungskonto Ihrer AWS Organisation eingerichtet.
- Ihre Instance von IAM Identity Center befindet sich in der gleichen Region, in der Ihr AD Connector eingerichtet ist.

Weitere Informationen finden Sie unter Voraussetzungen für IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

Voraussetzungen für Multifaktor-Authentifizierung

Für die Unterstützung von Multi-Faktor-Authentifizierung in Ihrem AD-Connector-Verzeichnis benötigen Sie Folgendes:

- Ein Remote Authentication Dial-In User Service (RADIUS)-Server in Ihrem vorhandenen Netzwerk, der zwei Client-Endpunkte hat. Die RADIUS-Client-Endpunkte müssen folgende Anforderungen erfüllen:
  - Für die Erstellung der Endpunkte benötigen Sie die IP-Adressen der AWS Directory Service -Server. Diese IP-Adressen finden Sie im Directory IP Address-Feld Ihres Verzeichnisses.
  - Beide RADIUS-Endpunkte müssen denselben geheimen Code verwenden.
- Ihr vorhandenes Netzwerk muss eingehenden Datenverkehr über den standardmäßigen RADIUS-Serverport (1812) von den Servern zulassen. AWS Directory Service

- Die Benutzernamen für Ihren RADIUS-Server und Ihr vorhandenes Verzeichnis müssen identisch sein.

Weitere Informationen zum Verwenden von AD Connector mit MFA finden Sie unter Multifaktor-Authentifizierung für AD Connector aktivieren.

Zuweisen von Berechtigungen zu Ihrem Servicekonto

Für die Verbindung mit Ihrem vorhandenen Verzeichnis benötigen Sie die Anmeldeinformationen für ein AD-Connector-Servicekonto im vorhandenen Verzeichnis, dem bestimmte Berechtigungen zugewiesen wurden. Obwohl Mitglieder der Gruppe Domain-Administratoren über ausreichende Berechtigungen verfügen, um das Verzeichnis aufzurufen, ist es eine bewährte Methode, ein Servicekonto zu verwenden, das nur über die Berechtigungen verfügt, die zum Aufrufen des Verzeichnisses mindestens notwendig sind. Das folgende Verfahren zeigt, wie Sie eine neue Gruppe mit dem Namen erstellen`Connectors`, die erforderlichen Rechte delegieren, die für die Verbindung mit AWS Directory Service dieser Gruppe erforderlich sind, und anschließend ein neues Dienstkonto zu dieser Gruppe hinzufügen.

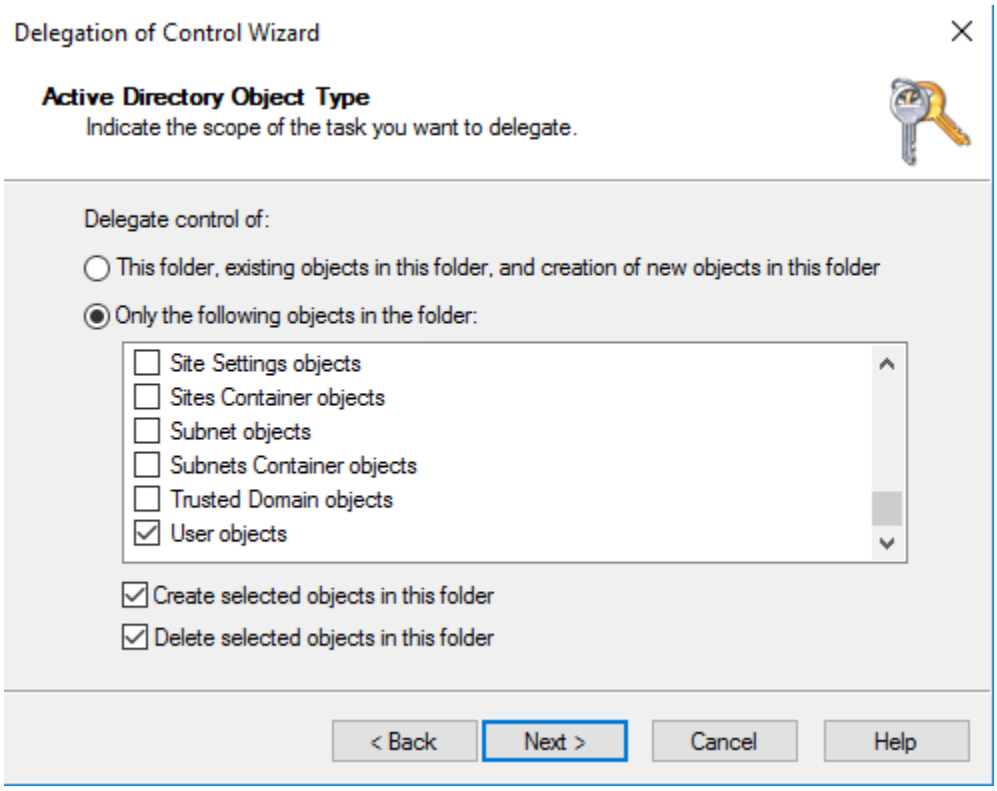
Dieser Vorgang muss auf einem Computer durchgeführt werden, der Ihrem Verzeichnis hinzugefügt ist und auf dem das MMC-Snap-In Active Directory User and Computers installiert ist. Außerdem müssen Sie als Domain-Administrator angemeldet sein.

So weisen Sie Ihrem Servicekonto Berechtigungen zu

1. Öffnen Sie Active Directory User und Computer und wählen Sie in der Navigationsbaumstruktur Ihre Domain-Root aus.
2. Klicken Sie in der Liste im linken Bereich mit der rechten Maustaste auf Users, wählen Sie New und dann Group.
3. Geben Sie im Dialogfeld New Object - Group Folgendes ein und klicken Sie auf OK.

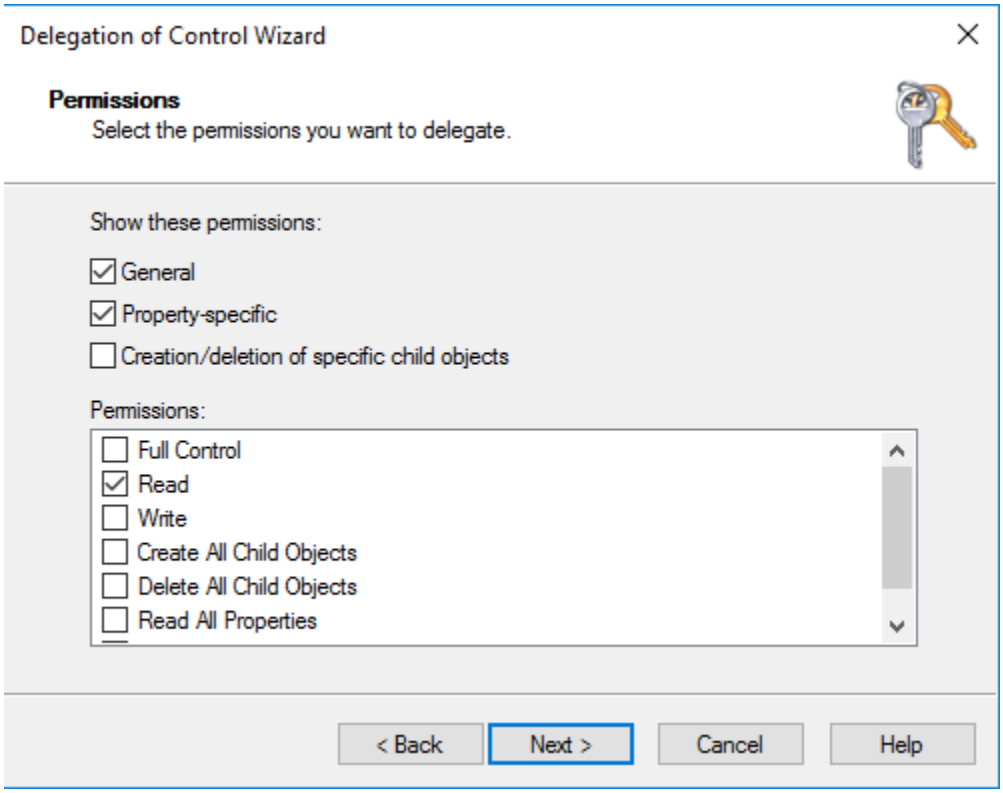
Feld	Wert/Auswahl
Group name (Gruppenname)	`Connectors`
Group scope (Gruppenumfang)	Global
Group type (Gruppentyp)	Sicherheit

4. Wählen Sie in der Navigationsstruktur Active Directory User und Computer Ihre Domain-Root aus. Wählen Sie im Menü Action und dann Delegate Control. Wenn Ihr AD Connector mit AWS Managed Microsoft AD verbunden ist, haben Sie keinen Zugriff auf die Delegiertensteuerung auf Domänenstammebene. Um die Steuerung zu delegieren, wählen Sie in diesem Fall die Organisationseinheit unter Ihrer Verzeichnis-Organisationseinheit aus, in der Ihre Computerobjekte erstellt werden.
5. Klicken Sie auf der Seite Delegation of Control Wizard auf Next und dann auf Add.
6. Geben Sie in das Dialogfeld Select Users, Computers, or Groups `Connectors` ein und klicken Sie auf OK. Wenn mehr als ein Objekt gefunden wurde, wählen Sie die oben erstellte Gruppe `Connectors`. Klicken Sie auf Weiter.
7. Wählen Sie auf der Seite Tasks to Delegate Create a custom task to delegate und dann Next.
8. Wählen Sie Only the following objects in the folder und dann Computer objects und User objects.
9. Wählen Sie Create selected objects in this folder und Delete selected objects in this folder. Wählen Sie anschließend Weiter.



10. Wählen Sie Read und dann Next.

> **Note**
>
> Wenn Sie Seamless Domain Join oder verwenden WorkSpaces, müssen Sie auch Schreibberechtigungen aktivieren, damit Active Directory Computerobjekte erstellen kann.



11. Überprüfen Sie die Informationen auf der Seite Completing the Delegation of Control Wizard und klicken Sie auf Finish.
12. Erstellen Sie ein Benutzerkonto mit einem sicheren Passwort und fügen Sie diesen Benutzer zur Gruppe `Connectors` hinzu. Dieser Benutzer wird als Ihr AD Connector Connector-Dienstkonto bezeichnet. Da er jetzt Mitglied der `Connectors` Gruppe ist, verfügt er jetzt über ausreichende Rechte, um eine Verbindung mit AWS Directory Service dem Verzeichnis herzustellen.

Testen Sie Ihren AD Connector

Damit AD Connector eine Verbindung zu Ihrem vorhandenen Verzeichnis herstellen kann, muss die Firewall für Ihr vorhandenes Netzwerk bestimmte Ports für die CIDRs für beide Subnetze in der VPC geöffnet haben. Um zu prüfen, ob das der Fall ist, führen Sie die folgenden Schritte aus:

Testen der Verbindung

1. Starten Sie eine Windows-Instance in der VPC und stellen Sie eine VPC-Verbindung über RDP her. Die Instance muss Mitglied Ihrer vorhandenen Domain sein. Die weiteren Schritte werden in dieser VPC-Instance ausgeführt.
2. Laden Sie die DirectoryServicePortTestTestanwendung herunter und entpacken Sie sie. Der Quellcode und die Visual Studio-Projektdateien sind enthalten, sodass Sie die Testanwendung bei Bedarf ändern können.

   > **Note**
   >
   > Dieses Skript wird auf Windows Server 2003 oder älteren Betriebssystemen nicht unterstützt.

3. Führen Sie die Testanwendung DirectoryServicePortTest in einer Windows-Eingabeaufforderung mit den folgenden Optionen aus:

   > **Note**
   >
   > Die DirectoryServicePortTest Testanwendung kann nur verwendet werden, wenn die Domänen- und Gesamtstrukturfunktionsebenen auf Windows Server 2012 R2 oder niedriger eingestellt sind.

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp
 "53,88,389" -udp "53,88,389"
```

<domain_name>

Der vollqualifizierte Domainname. Dieser wird verwendet, um die Gesamtstruktur- und Funktionsebenen der Domain zu prüfen. Wenn Sie den Domainnamen nicht angeben, werden die Funktionsebenen nicht getestet.

<server_IP_address>

Die IP-Adresse eines Domain-Controllers in Ihrer vorhandenen Domain. Die Ports werden mit dieser IP-Adresse getestet. Wenn Sie die IP-Adresse nicht angeben, werden die Ports nicht getestet.

Diese Test-App bestimmt, ob die erforderlichen Ports von der VPC zu Ihrer Domain geöffnet sind und überprüft auch die minimale Gesamtstruktur und Domain-Funktionsebenen.

Die Ausgabe sieht folgendermaßen oder ähnlich aus:

```
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
```

Nachfolgend der Quellcode für die Anwendung 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;
        }
    }
}
```

Einen AD Connector erstellen

Führen Sie die folgenden Schritte aus, um mit AD Connector eine Verbindung zu einem vorhandenen Verzeichnis herzustellen. Bevor Sie dieses Verfahren beginnen, stellen Sie sicher, dass Sie die in AD-Connector-Voraussetzungen angegebenen Voraussetzungen erfüllt haben.

> **Note**
>
> Sie können keinen AD Connector mit einer Cloud-Formation-Vorlage erstellen.

So stellen Sie eine Verbindung mit AD Connector her

1. Wählen Sie im Navigationsbereich AWS Directory Service -Konsole den Eintrag Verzeichnisse und wählen Sie Verzeichnis einrichten aus.
2. Wählen Sie auf der Seite Verzeichnistyp auswählen die Option AD Connector aus und klicken Sie dann auf Weiter.
3. Geben Sie auf der Seite Enter AD Connector information (AD Connector-Informationen eingeben) die folgenden Informationen ein:

   Verzeichnisgröße

   Wählen Sie die Größenoption Small (Klein) oder Large (Groß). Weitere Informationen über Größen finden Sie unter AD Connector.

   Verzeichnisbeschreibung

   Eine optionale Beschreibung des Verzeichnisses.
4. Geben Sie auf der Seite Choose VPC and subnets (VPC und Subnetze wählen) die folgenden Informationen an und wählen Sie dann Next (Weiter).

   VPC

   Die VPC für das Verzeichnis.

   Subnets

   Wählen Sie Subnetze für die Domain-Controller aus. Die beiden Subnetze müssen zu verschiedenen Availability-Zonen gehören.
5. Geben Sie auf der Seite Connect to AD (Mit AD verbinden) die folgenden Informationen ein:

   DNS-Name des Verzeichnisses

   Den vollständig qualifizierten Namen Ihres vorhandenen Verzeichnisses, z. B `corp.example.com`.

NetBIOS-Name des Verzeichnisses

Den Kurznamen Ihres vorhandenen Verzeichnisses, z. B `CORP`.

DNS-IP-Adressen

Die IP-Adresse von mindestens einem DNS-Server in Ihrem vorhandenen Verzeichnis. Diese Server müssen von jedem in Schritt 4 angegebenen Subnetz aus erreichbar sein. Diese Server können sich außerhalb von befinden AWS, sofern Netzwerkkonnektivität zwischen den angegebenen Subnetzen und den IP-Adressen des DNS-Servers besteht.

Benutzername für Service-Konto

Den Benutzernamen eines Benutzers im vorhandenen Verzeichnis. Weitere Informationen zu diesem Konto finden Sie im Abschnitt AD-Connector-Voraussetzungen.

Passwort des Service-Kontos

Das Passwort für das vorhandene Benutzerkonto. Bei diesem Passwort wird zwischen Groß- und Kleinschreibung unterschieden und es muss zwischen 8 und 128 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:

- Kleinbuchstaben (a – z)
- Großbuchstaben (A – Z)
- Zahlen (0 – 9)
- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password (Passwort bestätigen)

Geben Sie das Passwort für das vorhandene Benutzerkonto erneut ein.

6. Überprüfen Sie auf der Seite Review & create (Überprüfen und erstellen) die Verzeichnisinformationen und nehmen Sie gegebenenfalls Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen). Es dauert einige Minuten, bis das Verzeichnis erstellt wurde. Sobald sie erstellt wurden, ändert sich der Status in Active.

Was wird mit Ihrem AD Connector erstellt

Wenn Sie einen AD Connector erstellen, erstellt er AWS Directory Service automatisch ein elastic network interface (ENI) und ordnet es jeder Ihrer AD Connector-Instanzen zu. Jede dieser ENIs ist für die Konnektivität zwischen Ihrer VPC und AWS Directory Service AD Connector

unerlässlich und sollte niemals gelöscht werden. Sie können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, AWS Directory Service anhand der Beschreibung identifizieren: "Die Netzwerkschnittstelle wurde für die Verzeichnis-ID AWS erstellt“. Weitere Informationen finden Sie unter Elastic Network-Schnittstellen im Amazon EC2 Benutzerhandbuch.

> **Note**
>
> AD-Connector-Instances werden standardmäßig in zwei Availability Zones in einer Region bereitgestellt und mit Ihrer Amazon Virtual Private Cloud (VPC) verbunden. AD-Connector-Instances, die ausfallen, werden automatisch in derselben Availability Zone mit derselben IP-Adresse ersetzt.

Wenn Sie sich bei einer AWS Anwendung oder einem Dienst anmelden, der in einen AD Connector (AWS IAM Identity Center im Lieferumfang enthalten) integriert ist, leitet die App oder der Dienst Ihre Authentifizierungsanfrage an AD Connector weiter, der die Anfrage dann zur Authentifizierung an einen Domänencontroller in Ihrem selbstverwalteten Active Directory weiterleitet. Wenn Sie erfolgreich bei Ihrem selbstverwalteten Active Directory authentifiziert wurden, gibt AD Connector dann ein Authentifizierungstoken an die App oder den Dienst zurück (ähnlich einem Kerberos-Token). Zu diesem Zeitpunkt können Sie jetzt auf die App oder den AWS Dienst zugreifen.

So verwalten Sie AD Connector

In diesem Abschnitt werden alle Verfahren für die Ausführungen und Verwaltung einer AD-Connector-Umgebung aufgeführt.

Themen

- Ihr AD-Connector-Verzeichnis sichern
- Ihr AD-Connector-Verzeichnis überwachen
- Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem Active Directory
- Ihr AD-Connector-Verzeichnis verwalten
- Aktivieren des Zugriffs auf AWS Anwendungen und Services
- Die DNS-Adresse für AD Connector aktualisieren

Ihr AD-Connector-Verzeichnis sichern

In diesem Abschnitt wird beschrieben, wie Sie Ihre AD-Connector-Umgebung sichern.

Themen

Ihre Anmeldeinformationen für Ihr AD-Connector-Servicekonto in AWS Directory Service aktualisieren

Die AD-Connector-Anmeldeinformationen, die Sie in AWS Directory Service angeben, stellen das Servicekonto dar, das für den Zugriff auf Ihr bestehendes On-Premises-Verzeichnis verwendet wird. Sie können die Anmeldeinformationen des Service-Kontos in AWS Directory Service ändern, indem Sie die folgenden Schritte ausführen.

> **Note**
>
> Wenn AWS IAM Identity Center für das Verzeichnis aktiviert ist, muss AWS Directory Service den Service-Prinzipalnamen (SPN) vom aktuellen Servicekonto auf das neue Servicekonto übertragen. Falls das aktuelle Servicekonto nicht zum Löschen des SPN oder das neue Servicekonto nicht zum Hinzufügen des SPN berechtigt ist, werden Sie nach den Anmeldeinformationen eines Verzeichniskontos gefragt, das die Berechtigungen zum Ausführen beider Aktionen hat. Diese Anmeldeinformationen werden nur für die Übertragung des SPN verwendet. Sie werden nicht vom Service gespeichert.

So aktualisieren Sie die Anmeldeinformationen Ihres AD-Connector-Servicekontos in AWS Directory Service

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole unter Active Directory die Option Verzeichnisse.

2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Scrollen Sie auf der Seite mit den Verzeichnisdetails nach unten zum Abschnitt mit den Anmeldeinformationen für das Servicekonto.
4. Wählen Sie im Abschnitt Service account credentials (Servicekonto-Anmeldeinformationen) die Option Update (Aktualisieren) aus.
5. Geben Sie im Dialogfeld Anmeldeinformationen für das Servicekonto aktualisieren den Benutzernamen und das Passwort für das Servicekonto ein. Geben Sie das Passwort erneut ein, um es zu bestätigen, und wählen Sie dann Aktualisieren.

Multifaktor-Authentifizierung für AD Connector aktivieren

Die Multifaktor-Authentifizierung kann für AD Connector aktiviert werden, wenn Active Directory On-Premises- oder in EC2-Instances ausgeführt wird. Weitere Informationen zur Verwendung der Multifaktor-Authentifizierung mit AWS Directory Service finden Sie unter AD-Connector-Voraussetzungen.

> **Note**
>
> Die Multifaktor-Authentifizierung ist für Simple AD nicht verfügbar. MFA kann jedoch für Ihr Verzeichnis in AWS Managed Microsoft AD aktiviert werden. Weitere Informationen finden Sie unter Aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD.

So aktivieren Sie die Multifaktor-Authentifizierung für AD Connector

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Wählen Sie den Verzeichnis-ID-Link für Ihr AD Connector-Verzeichnis aus.
3. Wählen Sie auf der Registerkarte Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk und Sicherheit) aus.
4. Wählen Sie im Abschnitt Multi-factor authentication (Mehrfaktoren-Authentifizierung) die Option Actions (Aktionen) und dann Enable (Aktivieren) aus.
5. Geben Sie auf der Seite Multi-Faktor-Authentifizierung (MFA) aktivieren die folgenden Werte ein:

   Label anzeigen

   Geben Sie einen Labelnamen an.

DNS-Name oder IP-Adressen des RADIUS-Servers

Die IP-Adressen Ihrer RADIUS-Server-Endpunkte oder die IP-Adresse Ihres RADIUS-Server-Load Balancer. Sie können mehrere IP-Adressen getrennt durch ein Komma eingeben (z. B. `192.0.0.0,192.0.0.12`).

> **Note**
>
> RADIUS MFA gilt nur für die Authentifizierung des Zugriffs auf die AWS Management Console oder auf Amazon Enterprise-Anwendungen und -Services wie WorkSpaces Amazon oder Amazon QuickSight Chime. Es bietet keine MFA für Windows Workloads, die auf EC2-Instances laufen, oder für die Anmeldung bei einer EC2-Instance. AWS Directory Service unterstützt keine RADIUS-Challenge/Response-Authentifizierung.
>
> Benutzer müssen zum Zeitpunkt der Eingabe ihres Benutzernamens und Passworts ihren MFA-Code haben. Alternativ müssen Sie eine Lösung verwenden, die MFA out-of-band wie die SMS-Textverifizierung für den Benutzer durchführt. In out-of-band MFA-Lösungen müssen Sie sicherstellen, dass Sie den RADIUS-Timeoutwert entsprechend Ihrer Lösung festlegen. Wenn Sie eine out-of-band MFA-Lösung verwenden, fordert die Anmeldeseite den Benutzer auf, einen MFA-Code einzugeben. In diesem Fall besteht die bewährte Methode darin, dass die Benutzer ihr Passwort sowohl in das Passwortfeld als auch in das MFA-Feld eingeben.

Port

Der Port, den Ihr RADIUS-Server für die Kommunikation verwendet. Ihr On-Premises-Netzwerk muss eingehenden Datenverkehr über den Standard-RADIUS-Server-Port (UDP:1812) von den AWS Directory Service-Servern zulassen.

Shared secret code (Gemeinsamer geheimer Code)

Der gemeinsame geheime Code, der bei der Erstellung Ihrer RADIUS-Endpunkte angegeben wurde.

Confirm shared secret code (Gemeinsamen geheimen Code bestätigen)

Bestätigen Sie den gemeinsamen geheimen Code für Ihre RADIUS-Endpunkte.

Protocol (Protokoll)

Wählen Sie das Protokoll aus, das bei der Erstellung Ihrer RADIUS-Endpunkte angegeben wurde.

Server-Timeout (in Sekunden)

Die Zeit in Sekunden, die gewartet werden muss, bis der RADIUS-Server antwortet. Dies muss ein Wert zwischen 1 und 50 sein.

Maximale Wiederholungen von RADIUS-Anfragen

Die Anzahl der Kommunikationsversuche mit dem RADIUS-Server. Dies muss ein Wert zwischen 0 und 10 sein.

Die Multifaktor-Authentifizierung ist verfügbar, wenn sich der RADIUS-Status in Enabled ändert.

6. Wählen Sie Enable (Aktivieren) aus.

Clientseitiges LDAPS mit AD Connector aktivieren

Über die clientseitige LDAPS-Unterstützung in AD Connector wird die Kommunikation zwischen Microsoft Active Directory (AD) und AWS-Anwendungen verschlüsselt. Beispiele für solche Anwendungen sind WorkSpaces, AWS IAM Identity Center, Amazon QuickSight und Amazon Chime. Diese Verschlüsselung hilft Ihnen, die Identitätsdaten Ihrer Organisation besser zu schützen und Ihre Sicherheitsanforderungen zu erfüllen.

Themen

Voraussetzungen

Bevor Sie clientseitiges LDAPS aktivieren, müssen Sie die folgenden Anforderungen erfüllen.

Themen

- Netzwerkanforderungen

Serverzertifikate in Active Directory bereitstellen

Um clientseitiges LDAPS aktivieren zu können, müssen Sie Serverzertifikate für jeden Domain-Controller in Ihrem Active Directory abrufen und installieren. Diese Zertifikate werden vom LDAP-Service verwendet, um SSL-Verbindungen von LDAP-Clients zu überwachen und automatisch zu akzeptieren. Sie können SSL-Zertifikate verwenden, die entweder von einer internen Active Directory Certificate Services (ADCS)-Bereitstellung ausgestellt oder von einem kommerziellen Aussteller erworben werden. Weitere Informationen zu Active Directory-Serverzertifikatanforderungen finden Sie unter LDAP over SSL (LDAPS) Certificate auf der Microsoft-Website.

CA-Zertifikat-Anforderungen

Ein Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das den Aussteller Ihrer Serverzertifikate darstellt, ist für den clientseitigen LDAPS-Betrieb erforderlich. Zertifizierungsstellenzertifikate (CA-Zertifikate) werden mit den Serverzertifikaten abgeglichen, die von den Active-Directory-Domain-Controllern zur Verschlüsselung der LDAP-Kommunikation bereitgestellt werden. Beachten Sie die folgenden Zertifizierungsstellenzertifikat-Anforderungen:

- Es können nur Zertifikate registriert werden, die noch mehr als 90 Tage lang gültig sind.
- Zertifikate müssen im PEM-Format (Privacy-Enhanced Mail) vorliegen. Wenn Sie Zertifizierungsstellenzertifikate aus Active Directory exportieren, wählen Sie base64-codiertes X.509 (.CER) als Exportdateiformat aus.
- Es können maximal fünf (5) CA-Zertifikate pro AD-Connector-Verzeichnis gespeichert werden.
- Zertifikate, die den RSASSA-PSS-Signaturalgorithmus verwenden, werden nicht unterstützt.

Netzwerkanforderungen

LDAP-Datenverkehr der AWS-Anwendung wird ausschließlich auf TCP-Port 636 ausgeführt, ohne Rückgriff auf LDAP-Port 389. Für die Windows LDAP-Kommunikation, die Replikation, Vertrauensstellungen und mehr unterstützt, wird jedoch weiterhin LDAP-Port 389 mit Windows-nativer Sicherheit verwendet. Konfigurieren Sie AWS-Sicherheitsgruppen und -Netzwerk-Firewalls, um TCP-Kommunikation an Port 636 in AD Connector (ausgehend) und am selbstverwalteten Active Directory (eingehend) zu ermöglichen.

Clientseitiges LDAPS aktivieren

Um clientseitiges LDAPS zu aktivieren, importieren Sie das Zertifikat Ihrer Zertifizierungsstelle (CA) in AD Connector und aktivieren dann LDAPS für Ihr Verzeichnis. Nach der Aktivierung fließt der gesamte LDAP-Verkehr zwischen AWS-Anwendungen und Ihrem selbstverwalteten Active Directory mit SSL-Kanalverschlüsselung (Secure Sockets Layer).

Sie können zwei verschiedene Verfahren nutzen, um client-seitiges LDAPS für Ihr Verzeichnis zu aktivieren. Sie können entweder die AWS Management Console-Methode oder die AWS CLI-Methode verwenden.

Themen

Schritt 1: Ein Zertifikat in AWS Directory Service registrieren

Nutzen Sie eines der folgenden Verfahren, um ein Zertifikat in AWS Directory Service zu registrieren.

Verfahren 1: So registrieren Sie Ihr Zertifikat in AWS Directory Service (AWS Management Console)

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Wählen Sie im Abschnitt Client-side LDAPS (clientseitiges LDAPS) das Menü Actions (Aktionen) aus und klicken Sie dann auf Register certificate (Zertifikat registrieren).
5. Klicken Sie im Dialogfeld Register a CA certificate (Registrieren eines CA-Zertifikats) auf die Option Browse (Durchsuchen), wählen Sie dann das Zertifikat aus und klicken Sie anschließend auf die Option Open (Öffnen).
6. Wählen Sie die Option Register certificate (Zertifikat registrieren) aus.

Verfahren 2: So registrieren Sie Ihr Zertifikat in AWS Directory Service (AWS CLI)

- Führen Sie den folgenden Befehl aus. Zeigen Sie für die Zertifikatdaten auf den Speicherort der Zertifizierungsstellen-Zertifikatdatei. In der Antwort wird eine Zertifikat-ID angegeben.

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

Schritt 2: Den Registrierungsstatus überprüfen

Um sich den Status einer Zertifikatsregistrierung oder eine Liste der registrierten Zertifikate anzeigen zu lassen, nutzen Sie eines der folgenden Verfahren.

Verfahren 1: So überprüfen Sie den Zertifikatregistrierungsstatus in AWS Directory Service (AWS Management Console)

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Überprüfen Sie den aktuellen Status der Zertifikatregistrierung, der in der Spalte Registration status (Registrierungsstatus) angezeigt wird. Wenn sich der Wert des Registrierungsstatus in Registered (Registriert) ändert, ist Ihr Zertifikat erfolgreich registriert worden.

Verfahren 2: So überprüfen Sie den Status der Zertifikatregistrierung in AWS Directory Service (AWS CLI)

- Führen Sie den folgenden Befehl aus. Wenn der Statuswert `Registered` zurückgegeben wird, wurde Ihr Zertifikat erfolgreich registriert.

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

Schritt 3: Clientseitiges LDAPS aktivieren

Verwenden Sie eine der folgenden Methoden, um clientseitiges LDAPS in AWS Directory Service zu aktivieren.

> **Note**
>
> Sie müssen mindestens ein Zertifikat erfolgreich registriert haben, bevor Sie das clientseitige LDAPS aktivieren können.

Verfahren 1: So aktivieren Sie clientseitiges LDAPS in AWS Directory Service (AWS Management Console)

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Wählen Sie Enable (Aktivieren) aus. Steht diese Option nicht zur Verfügung, überprüfen Sie, ob ein gültiges Zertifikat erfolgreich registriert wurde, und versuchen Sie es dann erneut.
3. Wählen Sie im Dialogfeld Enable client-side LDAPS (Client-seitiges LDAPS aktivieren) die Option Enable (Aktivieren).

Verfahren 2: So aktivieren Sie clientseitiges LDAPS in AWS Directory Service (AWS CLI)

- Führen Sie den folgenden Befehl aus.

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

Schritt 4: Den LDAPS-Status überprüfen

Verwenden Sie eine der folgenden Methoden, um den LDAPS-Status in AWS Directory Service zu überprüfen.

Verfahren 1: So überprüfen Sie den LDAPS-Status in AWS Directory Service (AWS Management Console)

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Wenn der Statuswert als Enabled (Aktiviert) angezeigt wird, wurde das LDAPS erfolgreich konfiguriert.

Verfahren 2: So überprüfen Sie den LDAPS-Status in AWS Directory Service (AWS CLI)

- Führen Sie den folgenden Befehl aus. Wenn der Statuswert `Enabled` zurückgibt, wurde das LDAPS erfolgreich konfiguriert.

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

Clientseitiges LDAPS überprüfen

Verwenden Sie diese Befehle, um Ihre LDAPS-Konfiguration zu verwalten.

Sie können zwei verschiedene Verfahren nutzen, um client-seitige LDAPS-Einstellungen zu verwalten. Sie können entweder die AWS Management Console-Methode oder die AWS CLI-Methode verwenden.

Zertifikatsdetails anzeigen

Nutzen Sie eines der folgenden Verfahren, um zu sehen, wann ein Zertifikat abläuft.

Verfahren 1: So lassen Sie sich Zertifikatdetails in AWS Directory Service (AWS Management Console) anzeigen

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) werden unter CA certificates (CA-Zertifikate) Informationen zum Zertifikat angezeigt.

Verfahren 2: So lassen Sie sich Zertifikatdetails in AWS Directory Service (AWS CLI) anzeigen

- Führen Sie den folgenden Befehl aus. Verwenden Sie für die Zertifikat-ID den von `register-certificate` oder `list-certificates` zurückgegebenen Bezeichner.

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

Ein Zertifikat abmelden

Nutzen Sie eines der folgenden Verfahren, um ein Zertifikat abzumelden.

> **Note**
>
> Wenn nur ein Zertifikat registriert ist, müssen Sie zuerst LDAPS deaktivieren, bevor Sie das Zertifikat abmelden können.

Verfahren 1: So melden Sie ein Zertifikat in AWS Directory Service (AWS Management Console) ab

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Wählen Sie im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) die Option Actions (Aktionen) und klicken Sie dann auf Deregister certificate (Zertifikat abmelden).
5. Wählen Sie im Dialogfeld Deregister a CA certificate (Ein CA-Zertifikat abmelden) die Option Deregister (Abmelden).

Verfahren 2: So melden Sie ein Zertifikat in AWS Directory Service (AWS CLI) ab

- Führen Sie den folgenden Befehl aus. Verwenden Sie für die Zertifikat-ID den von `register-certificate` oder `list-certificates` zurückgegebenen Bezeichner.

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

Clientseitiges LDAPS deaktivieren

Nutzen Sie eines der folgenden Verfahren, um clientseitiges LDAPS zu deaktivieren.

Verfahren 1: So deaktivieren Sie clientseitiges LDAPS in AWS Directory Service (AWS Management Console)

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.

4. Wählen Sie im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) die Option Disable (Deaktivieren) aus.
5. Klicken Sie im Dialogfeld Disable client-side LDAPS (Clientseitiges LDAPS deaktivieren) auf Disable (Deaktivieren).

Verfahren 2: So deaktivieren Sie clientseitiges LDAPS in AWS Directory Service (AWS CLI)

- Führen Sie den folgenden Befehl aus.

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

Die mTLS-Authentifizierung in AD Connector für die Verwendung mit Smartcards aktivieren

Sie können die zertifikatsbasierte Mutual Transport Layer Security (mTLS) -Authentifizierung mit Smartcards verwenden, um Benutzer WorkSpaces über Ihr selbstverwaltetes Active Directory (AD) und AD Connector bei Amazon zu authentifizieren. Wenn diese Option aktiviert ist, wählen Benutzer ihre Smartcard auf dem WorkSpaces Anmeldebildschirm aus und geben zur Authentifizierung eine PIN ein, anstatt einen Benutzernamen und ein Passwort zu verwenden. Von dort aus verwendet der virtuelle Desktop von Windows oder Linux die Smartcard, um sich über das native Desktop-Betriebssystem bei AD zu authentifizieren.

> **Note**
>
> Die Smartcard-Authentifizierung in AD Connector ist nur im Folgenden AWS-Regionen und nur mit verfügbar WorkSpaces. Andere AWS Anwendungen werden derzeit nicht unterstützt.
>
> - USA Ost (Nord-Virginia)
> - USA West (Oregon)
> - Asien-Pazifik (Sydney)
> - Asien-Pazifik (Tokio)
> - Europa (Irland)
> - AWS GovCloud (US-West)

Themen

Voraussetzungen

Um die zertifikatsbasierte MTLS-Authentifizierung (Mutual Transport Layer Security) mithilfe von Smartcards für den WorkSpaces Amazon-Client zu aktivieren, benötigen Sie eine funktionsfähige Smartcard-Infrastruktur, die in Ihre selbstverwaltete Smartcard-Infrastruktur integriert ist. Active Directory Weitere Informationen zur Einrichtung der Smartcard-Authentifizierung bei Amazon WorkSpaces und Active Directory finden Sie im WorkSpaces Amazon-Administratorhandbuch.

Bevor Sie die Smartcard-Authentifizierung für aktivieren WorkSpaces, überprüfen Sie bitte die folgenden Überlegungen:

CA-Zertifikat-Anforderungen

AD Connector benötigt für die Smartcard-Authentifizierung ein Zertifikat der Zertifizierungsstelle (CA), das den Aussteller Ihrer Benutzerzertifikate darstellt. AD Connector ordnet CA-Zertifikate den Zertifikaten zu, die von Ihren Benutzern mit ihren Smartcards vorgelegt wurden. Beachten Sie die folgenden Zertifizierungsstellenzertifikat-Anforderungen:

- Bevor Sie ein CA-Zertifikat registrieren können, müssen noch mehr als 90 Tage vor dem Ablaufdatum liegen.
- CA-Zertifikate müssen im PEM-Format (Privacy-Enhanced Mail) vorliegen. Wenn Sie CA-Zertifikate aus Active Directory exportieren, wählen Sie Base64-encoded X.509 (.CER) als Exportdateiformat.
- Alle Root- und Zwischen-CA-Zertifikate, die von einer ausstellenden Zertifizierungsstelle zu Benutzerzertifikaten verkettet sind, müssen hochgeladen werden, damit die Smartcard-Authentifizierung erfolgreich ist.
- Es können maximal 100 CA-Zertifikate pro AD-Connector-Verzeichnis gespeichert werden
- AD Connector unterstützt den RSASSA-PSS-Signaturalgorithmus für CA-Zertifikate nicht.

- Stellen Sie sicher, dass der Certificate Propagation Service auf Automatisch eingestellt ist und läuft.

Voraussetzungen für ein Benutzer-Zertifikat

Im Folgenden sind einige der Anforderungen für das Benutzerzertifikat aufgeführt:

- Das Smartcard-Zertifikat des Benutzers hat den Subject Alternative Name (SAN) des Benutzers userPrincipalName (UPN).
- Das Smartcard-Zertifikat des Benutzers verfügt über Enhanced Key Usage als Clientauthentifizierung für die Smartcard-Anmeldung (1.3.6.1.4.1.311.20.2.2) (1.3.6.1.5.5.7.3.2).
- Die Informationen zum Online Certificate Status Protocol (OCSP) für das Smartcard-Zertifikat des Benutzers sollten Access Method=On-Line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) im Authority Information Access lauten.

Weitere Informationen zu AD Connector- und Smartcard-Authentifizierungsanforderungen finden Sie unter Anforderungen im Amazon WorkSpaces Administration Guide. Hilfe zur Behebung von WorkSpaces Amazon-Problemen, wie z. B. beim Einloggen WorkSpaces, Zurücksetzen des Passworts oder Herstellen einer Verbindung zu WorkSpaces, finden Sie unter Problembehandlung bei WorkSpaces Kundenproblemen im WorkSpaces Amazon-Benutzerhandbuch.

Prozess zur Überprüfung des Zertifikatswiderrufs

Um die Smartcard-Authentifizierung durchführen zu können, muss AD Connector den Widerrufsstatus von Benutzerzertifikaten mithilfe des Online Certificate Status Protocol (OCSP) überprüfen. Um die Überprüfung von Zertifikaten durchzuführen, muss die URL eines OCSP-Responders über das Internet zugänglich sein. Wenn Sie einen DNS-Namen verwenden, muss die URL eines OCSP-Responders eine Top-Level-Domain verwenden, die in der Root-Zone-Datenbank der Internet Assigned Numbers Authority (IANA) zu finden ist.

Die Überprüfung des Widerrufs von AD-Connector-Zertifikaten erfolgt nach dem folgenden Verfahren:

- AD Connector muss die AIA-Erweiterung (Authority Information Access) im Benutzerzertifikat auf eine OCSP-Responder-URL prüfen und verwendet dann die URL, um auf Widerruf zu prüfen.
- Wenn AD Connector die URL in der AIA-Erweiterung des Benutzerzertifikats nicht auflösen oder keine OCSP-Responder-URL im Benutzerzertifikat finden kann, verwendet AD Connector die optionale OCSP-URL, die bei der Registrierung des Root-CA-Zertifikats angegeben wurde.

Wenn die URL in der AIA-Erweiterung für das Benutzerzertifikat zwar aufgelöst wird, aber nicht reagiert, schlägt die Benutzerauthentifizierung fehl.

- Wenn die bei der Registrierung des Root-CA-Zertifikats angegebene OCSP-Responder-URL nicht aufgelöst werden kann, nicht antwortet oder keine OCSP-Responder-URL angegeben wurde, schlägt die Benutzerauthentifizierung fehl.
- Der OCSP-Server muss RFC 6960 entsprechen. Darüber hinaus muss der OCSP-Server Anfragen mit der GET-Methode für Anfragen unterstützen, die insgesamt weniger als oder gleich 255 Byte sind.

> **Note**
>
> AD Connector benötigt eine HTTP-URL für die OCSP-Responder-URL.

Weitere Überlegungen

Bevor Sie die Smartcard-Authentifizierung in AD Connector aktivieren, sollten Sie die folgenden Punkte berücksichtigen:

- AD Connector verwendet die zertifikatsbasierte gegenseitige Transport-Layer-Security-Authentifizierung (mutual TLS), um Benutzer mit hardware- oder softwarebasierten Smartcard-Zertifikaten bei Active Directory zu authentifizieren. Derzeit werden nur Karten der Typen Common Access Cards (CAC) und Personal Identity Verification (PIV) unterstützt. Andere Arten von hardware- oder softwarebasierten Smartcards funktionieren möglicherweise, wurden aber nicht für die Verwendung mit dem WorkSpaces Streaming-Protokoll getestet.
- Die Smartcard-Authentifizierung ersetzt die Authentifizierung mit Benutzername und Passwort für WorkSpaces.

  Wenn Sie in Ihrem AD Connector Connector-Verzeichnis andere AWS Anwendungen mit aktivierter Smartcard-Authentifizierung konfiguriert haben, zeigen diese Anwendungen weiterhin den Eingabebildschirm für Benutzername und Passwort an.
- Durch die Aktivierung der Smartcard-Authentifizierung wird die Länge der Benutzersitzung auf die maximale Gültigkeitsdauer für Kerberos-Servicetickets begrenzt. Sie können diese Einstellung mithilfe einer Gruppenrichtlinie konfigurieren. Sie ist standardmäßig auf 10 Stunden festgelegt. Weitere Informationen zu dieser Einstellung finden Sie in der Microsoft-Dokumentation.

- Der unterstützte Kerberos-Verschlüsselungstyp des AD-Connector-Servicekontos sollte mit jedem der unterstützten Kerberos-Verschlüsselungstypen des Domain-Controllers übereinstimmen.

Die Smartcard-Authentifizierung aktivieren

Um die Smartcard-Authentifizierung für WorkSpaces auf Ihrem AD Connector zu aktivieren, müssen Sie zunächst Ihre Zertifizierungsstellenzertifikate (CA) in AD Connector importieren. Sie können Ihre CA-Zertifikate mithilfe der AWS Directory Service Konsole, API oder CLI in AD Connector importieren. Gehen Sie wie folgt vor, um Ihre CA-Zertifikate zu importieren und anschließend die Smartcard-Authentifizierung zu aktivieren.

Themen

Schritt 1: Die eingeschränkte Kerberos-Delegierung für das AD-Connector-Servicekonto aktivieren

Um die Smartcard-Authentifizierung mit AD Connector zu verwenden, müssen Sie Kerberos Constrained Delegation (KCD) für das AD-Connector-Servicekonto für den LDAP-Service im selbstverwalteten AD-Verzeichnis aktivieren.

Kerberos Constrained Delegation ist ein Feature in Windows Server. Mit diesem Feature können Administratoren die Vertrauensstellung von Anwendungen festlegen und durchsetzen, indem sie den Bereich begrenzen, in dem Anwendungsservices im Namen eines Benutzers handeln können. Weitere Informationen finden Sie unter Kerberos Constrained Delegation.

> **Note**
>
> Kerberos Constrained Delegation (KCD) erfordert, dass der Benutzernamenteil des AD Connector Connector-Dienstkontos mit dem sAM AccountName desselben Benutzers übereinstimmt. Das SaM AccountName ist auf 20 Zeichen beschränkt. sAM AccountName ist ein Microsoft Active Directory-Attribut, das als Anmeldename für frühere Versionen von Windows-Clients und -Servern verwendet wurde.

1. Verwenden Sie den Befehl `SetSpn`, um einen Service-Prinzipalnamen (SPN) für das AD-Connector-Servicekonto im selbstverwalteten AD festzulegen. Dadurch wird das Servicekonto für die Delegierungskonfiguration aktiviert.

   Der SPN kann eine beliebige Service- oder Namenskombination sein, jedoch kein Duplikat eines vorhandenen SPN. `-s` sucht nach Duplikaten.

   ```
   setspn -s my/spn service_account
   ```

2. Öffnen Sie mit der rechten Maustaste in AD-Benutzer und -Computer das Kontextmenü und wählen Sie Eigenschaften aus.
3. Wählen Sie die Registerkarte Delegierung.
4. Wählen Sie die Optionen Diesem Benutzer nur für die Delegierung an den angegebenen Service vertrauen und Alle Authentifizierungsprotokolloptionen verwenden.
5. Wählen Sie Hinzufügen und dann Benutzer oder Computer, um den Domain-Controller zu finden.
6. Wählen Sie OK, um eine Liste der verfügbaren Services anzuzeigen, die für die Delegierung verwendet werden.
7. Wählen Sie den Servicetyp ldap und wählen Sie OK.
8. Wählen Sie OK aus, um die Konfiguration zu speichern.
9. Wiederholen Sie diesen Vorgang für andere Domänencontroller im Active Directory. Alternativ können Sie den Vorgang automatisieren mit PowerShell.

Schritt 2: Das CA-Zertifikat in AD Connector registrieren

Verwenden Sie eine der folgenden Methoden, um ein CA-Zertifikat für Ihr AD-Connector-Verzeichnis zu registrieren.

Methode 1: So registrieren Sie Ihr CA-Zertifikat in AD Connector (AWS Management Console)

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Wählen Sie im Abschnitt Smartcard-Authentifizierung die Option Aktionen und dann Zertifikat registrieren aus.

5. Wählen Sie im Dialogfeld Zertifikat registrieren die Option Datei auswählen, wählen Sie ein Zertifikat und wählen Sie dann Öffnen. Sie können optional eine Widerrufsprüfung für dieses Zertifikat durchführen, indem Sie die URL eines OCSP-Responders (Online Certificate Status Protocol) angeben. Weitere Informationen zu OCSP finden Sie unter Prozess zur Überprüfung des Zertifikatswiderrufs.
6. Wählen Sie die Option Register certificate (Zertifikat registrieren) aus. Wenn Sie sehen, dass sich der Status des Zertifikats in Registriert ändert, wurde der Registrierungsvorgang erfolgreich abgeschlossen.

Methode 2: So registrieren Sie Ihr CA-Zertifikat in AD Connector (AWS CLI)

- Führen Sie den folgenden Befehl aus. Zeigen Sie für die Zertifikatdaten auf den Speicherort der Zertifizierungsstellen-Zertifikatdatei. Verwenden Sie das optionale `ClientCertAuthSettings` Objekt, um eine sekundäre OCSP-Responder-Adresse anzugeben.

  ```
  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
  ```

  Bei Erfolg liefert die Antwort eine Zertifikat-ID. Sie können auch überprüfen, ob Ihr CA-Zertifikat erfolgreich registriert wurde, indem Sie den folgenden CLI-Befehl ausführen:

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

  Wenn der Statuswert `Registered` zurückgegeben wird, haben Sie Ihr Zertifikat erfolgreich registriert.

Schritt 3: Die Smartcard-Authentifizierung für unterstützte AWS -Anwendungen und -Services aktivieren

Verwenden Sie eine der folgenden Methoden, um ein CA-Zertifikat für Ihr AD-Connector-Verzeichnis zu registrieren.

Methode 1: So aktivieren Sie die Smartcard-Authentifizierung in AD Connector (AWS Management Console)

1. Navigieren Sie auf der Seite mit den Verzeichnisdetails zum Abschnitt Smartcard-Authentifizierung und wählen Sie Aktivieren aus. Steht diese Option nicht zur Verfügung, überprüfen Sie, ob ein gültiges Zertifikat erfolgreich registriert wurde, und versuchen Sie es dann erneut.
2. Wählen Sie im Dialogfeld Smartcard-Authentifizierung aktivieren die Option Aktivieren aus.

Methode 2: So aktivieren Sie die Smartcard-Authentifizierung in AD Connector (AWS CLI)

- Führen Sie den folgenden Befehl aus.

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

  Bei Erfolg gibt AD Connector eine `HTTP 200`-Antwort mit leerem HTTP-Textkörper zurück.

Die Einstellungen für die Smartcard-Authentifizierung verwalten

Sie können zwei verschiedene Methoden zur Verwaltung der Smartcard-Einstellungen verwenden. Sie können entweder die AWS Management Console Methode oder die AWS CLI Methode verwenden.

Themen

- Zertifikatsdetails anzeigen
- Ein Zertifikat abmelden
- Die Smartcard-Authentifizierung deaktivieren

Zertifikatsdetails anzeigen

Nutzen Sie eines der folgenden Verfahren, um zu sehen, wann ein Zertifikat abläuft.

Methode 1: Um die Zertifikatsdetails in AWS Directory Service (AWS Management Console) anzuzeigen

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.

2. Wählen Sie den Verzeichnis-ID-Link für Ihr AD Connector-Verzeichnis aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Wählen Sie im Abschnitt Smartcard-Authentifizierung unter CA-Zertifikate die Zertifikat-ID aus, um Details zu diesem Zertifikat anzuzeigen.

Methode 2: So zeigen Sie die Zertifikatsdetails in AWS Directory Service (AWS CLI) an

- Führen Sie den folgenden Befehl aus. Verwenden Sie für die Zertifikat-ID den von `register-certificate` oder `list-certificates` zurückgegebenen Bezeichner.

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

Ein Zertifikat abmelden

Nutzen Sie eines der folgenden Verfahren, um ein Zertifikat abzumelden.

> **Note**
>
> Wenn nur ein Zertifikat registriert ist, müssen Sie zunächst die Smartcard-Authentifizierung deaktivieren, bevor Sie das Zertifikat deregistrieren können.

Methode 1: Um die Registrierung eines Zertifikats in AWS Directory Service () aufzuheben AWS Management Console

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie den Verzeichnis-ID-Link für Ihr AD Connector-Verzeichnis aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Wählen Sie im Abschnitt Smartcard-Authentifizierung unter CA-Zertifikate das Zertifikat aus, für das Sie die Registrierung aufheben möchten, wählen Sie Aktionen und dann Registrierung für Zertifikat aufheben aus.

> **Important**
>
> Stellen Sie sicher, dass das Zertifikat, das Sie deregistrieren möchten, nicht aktiv ist oder derzeit als Teil einer CA-Zertifikatskette für die Smartcard-Authentifizierung verwendet wird.

5. Wählen Sie im Dialogfeld Deregister a CA certificate (Ein CA-Zertifikat abmelden) die Option Deregister (Abmelden).

Methode 2: Um die Registrierung eines Zertifikats in () aufzuheben AWS Directory ServiceAWS CLI

- Führen Sie den folgenden Befehl aus. Verwenden Sie für die Zertifikat-ID den von `register-certificate` oder `list-certificates` zurückgegebenen Bezeichner.

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

Die Smartcard-Authentifizierung deaktivieren

Verwenden Sie eine der folgenden Methoden, um die Smartcard-Authentifizierung zu deaktivieren.

Methode 1: Um die Smartcard-Authentifizierung in AWS Directory Service () zu deaktivieren AWS Management Console

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie den Verzeichnis-ID-Link für Ihr AD Connector-Verzeichnis aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
4. Wählen Sie im Abschnitt Smartcard-Authentifizierung die Option Deaktivieren aus.
5. Wählen Sie im Dialogfeld Smartcard-Authentifizierung deaktivieren die Option Deaktivieren aus.

Methode 2: Um die Smartcard-Authentifizierung in AWS Directory Service (AWS CLI) zu deaktivieren

- Führen Sie den folgenden Befehl aus.

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

Einrichten von AWS Private CA Connector für AD

Sie können Ihr selbstverwaltetes Active Directory (AD) in AWS Private Certificate Authority (CA) mit AD Connector integrieren, um Zertifikate für Ihre mit der AD-Domain verbundenen Benutzer, Gruppen und Maschinen auszustellen und zu verwalten. AWS Private CA Mit Connector für AD können Sie einen vollständig verwalteten AWS Private CA Drop-In-Ersatz für Ihre selbstverwalteten CAs verwenden, ohne lokale Agenten oder Proxyserver bereitstellen, patchen oder aktualisieren zu müssen.

Sie können die AWS Private CA Integration mit Ihrem Verzeichnis über die Directory-Service-Konsole, die AWS Private CA Connector-for-AD-Konsole oder durch Aufrufen der `CreateTemplate`-API einrichten. Informationen zum Einrichten der Private-CA-Integration über die - AWS Private CA Connector-für-Active-Directory-Konsole finden Sie unter AWS Private CA Connector für Active Directory. Im Folgenden finden Sie Schritte zum Einrichten dieser Integration über die AWS Directory Service Konsole.

Voraussetzungen

Wenn Sie AD Connector verwenden, müssen Sie zusätzliche Berechtigungen an das Servicekonto delegieren. Richten Sie die Zugriffssteuerungsliste (ACL) in Ihrem Servicekonto ein, damit Sie Folgendes tun können.

- Fügen Sie einen Service-Prinzipalnamen (SPN) hinzu oder entfernen sie ihn zu sich selbst.
- Erstellen und aktualisieren Sie Zertifizierungsstellen in den folgenden Containern:

```
#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
```

- Erstellen und aktualisieren Sie ein NT AuthCertificates Certification Authority-Objekt wie im folgenden Beispiel. Wenn das NT AuthCertificates Certification Authority-Objekt vorhanden ist, müssen Sie Berechtigungen dafür delegieren. Wenn das Objekt nicht existiert, müssen Sie die Fähigkeit, untergeordnete Objekte zu erstellen, an den Public-Key-Services-Container delegieren.

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

> **Note**
>
> Wenn Sie AWS Managed Microsoft AD verwenden, werden die zusätzlichen Berechtigungen automatisch delegiert, wenn Sie den AWS Private CA Connector for AD-Service mit Ihrem Verzeichnis autorisieren.

Sie können das folgende PowerShell Skript verwenden, um die zusätzlichen Berechtigungen zu delegieren und das NT-AuthCertifiates Zertifizierungsstellenobjekt zu erstellen. Ersetzen Sie „myconnectoraccount“ durch den Namen des Servicekontos.

```
$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"
```

So richten Sie AWS Private CA Connector für AD ein

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die - AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit unter AWS Private CA Connector für AD die Option AWS Private CA Connector für AD einrichten aus. Die Seite Private CA-Zertifikat erstellen für Active Directory wird angezeigt. Führen Sie die Schritte in der -Konsole aus, um Ihre Private CA für den Active DirectoryKonnektor zu erstellen, um sich bei Ihrer Private CA zu registrieren. Weitere Informationen finden Sie unter Einen Konnektor erstellen.
4. Nachdem Sie Ihren Connector erstellt haben, folgen Sie den nachstehenden Schritten, um Details anzuzeigen, darunter den Status des Connectors und den Status der zugehörigen Private CA.

So zeigen Sie AWS Private CA Connector für AD an

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die - AWS Directory Service Konsole unter https://console.aws.amazon.com/directoryservicev2/.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Unter Netzwerk und Sicherheit können Sie unter AWS Private CA Connector für AD Ihre Private-CA-Konnektoren und zugehörige Private CA einsehen. Standardmäßig sehen Sie die folgenden Felder:

    a. AWS Private CA Konnektor-ID – Die eindeutige Kennung für einen AWS Private CA Konnektor. Wenn Sie darauf klicken, wird die Detailseite dieses AWS Private CA Konnektors angezeigt.

    b. AWS Private CA Betreff – Informationen über den definierten Namen für die CA. Wenn Sie darauf klicken, gelangen Sie zur Detailseite dieses AWS Private CA.

    c. Status – Basierend auf einer Statusprüfung für den AWS Private CA Connector und die AWS Private CA. Wenn beide Prüfungen erfolgreich sind, wird Aktiv angezeigt. Wenn eine der Prüfungen fehlschlägt, wird 1/2 Prüfungen fehlgeschlagen angezeigt. Wenn beide Prüfungen fehlschlagen, wird Fehlgeschlagen angezeigt. Weitere Informationen über den Status „fehlgeschlagen“ erhalten Sie, wenn Sie den Mauszeiger über den Hyperlink

bewegen, um zu erfahren, welche Prüfung fehlgeschlagen ist. Folgen Sie den Anweisungen in der Konsole, um das Problem zu beheben.

d. Erstellungsdatum – Der Tag, an dem der AWS Private CA Connector erstellt wurde.

Weitere Informationen finden Sie unter Konnektor-Details anzeigen.

Ihr AD-Connector-Verzeichnis überwachen

Sie können Ihr AD-Connector-Verzeichnis mit folgenden Methoden überwachen:

Themen

- Erläuterungen zum Verzeichnisstatus
- Konfigurieren von Verzeichnisstatusbenachrichtigungen mit Amazon SNS

Erläuterungen zum Verzeichnisstatus

Im Folgenden sind die verschiedenen Zustandsangaben für ein Verzeichnis aufgeführt.

Aktiv

Das Verzeichnis funktioniert normal. AWS Directory Service hat keine Probleme für Ihr Verzeichnis erkannt.

Erstellen

Das Verzeichnis wird gerade erstellt. Die Verzeichniserstellung nimmt in der Regel 20 bis 45 Minuten in Anspruch, kann jedoch je nach Systemauslastung abweichen.

Deleted (Gelöscht)

Das Verzeichnis wurde gelöscht. Alle Ressourcen für das Verzeichnis wurden freigegeben. Ein Verzeichnis, das diesen Zustand erreicht hat, kann nicht wiederhergestellt werden.

Wird gelöscht

Das Verzeichnis wird gerade gelöscht. Das Verzeichnis bleibt in diesem Zustand, bis es vollständig gelöscht ist. Sobald ein Verzeichnis diesen Zustand erreicht, kann der Löschvorgang nicht mehr abgebrochen werden und das Verzeichnis ist nicht wiederherstellbar.

Fehlgeschlagen

Das Verzeichnis konnte nicht erstellt werden. Löschen Sie dieses Verzeichnis. Falls das Problem weiterhin besteht, kontaktieren Sie das AWS Support -Zentrum.

Beeinträchtigt

Das Verzeichnis wird nicht fehlerfrei ausgeführt. Mindestens ein Problem wurde erkannt und vermutlich wird nicht bei allen Verzeichnisvorgängen die volle Leistungskapazität erreicht. Es gibt viele mögliche Gründe dafür, dass sich das Verzeichnis in diesem Zustand befindet. Darunter fallen normale betriebliche Wartungsaktivitäten wie das Patchen oder die EC2-Instance-Rotation, das temporäre Hot-Spotting durch eine Anwendung auf einem Ihrer Domain-Controller oder Änderungen, die Sie an Ihrem Netzwerk vorgenommen haben und die versehentlich die Verzeichniskommunikation stören. Weitere Informationen finden Sie unter Problembehandlung bei AWS verwaltetem Microsoft AD, Fehlerbehebung in AD Connector, Beheben von Fehlern in Simple AD. AWS Behebt Probleme im Zusammenhang mit normalen Wartungsarbeiten innerhalb von 40 Minuten. Falls das Verzeichnis nach der Konsultation des Themas Fehlerbehebung länger als 40 Minuten den Status Beeinträchtigt aufweist, sollten Sie das AWS Support -Zentrum kontaktieren.

> **Important**
>
> Stellen Sie keinen Snapshot für ein Verzeichnis mit dem Status „Impaired“ (Beeinträchtigt) wieder her. Nur selten ist eine Snapshot-Wiederherstellung nötig, um Beeinträchtigungen zu beheben. Weitere Informationen finden Sie unter Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen.

Inoperable (Funktionsunfähig)

Das Verzeichnis ist nicht funktionsfähig. Alle Verzeichnisendpunkte haben Probleme gemeldet.

Angefragt

Eine Anforderung zum Erstellen Ihres Verzeichnisses steht zurzeit an.

Konfigurieren von Verzeichnisstatusbenachrichtigungen mit Amazon SNS

Mit Amazon Simple Notification Service (Amazon SNS) können Sie E-Mail- oder Textnachrichten (SMS) erhalten, wenn sich der Status Ihres Verzeichnisses ändert. Sie werden benachrichtigt, wenn

das Verzeichnis vom Status Aktiv zu Beeinträchtigt oder Funktionsunfähig wechselt. Außerdem erhalten Sie eine Benachrichtigung, wenn das Verzeichnis in einen aktiven Status zurückkehrt.

Funktionsweise

Amazon SNS verwendet „Themen“ zum Sammeln und Verteilen von Nachrichten. Jedes Thema hat einen oder mehrere Subscriber, die zu diesem Thema veröffentlichte Nachrichten empfangen. Mit den folgenden Schritten können Sie AWS Directory Service als Herausgeber zu einem Amazon SNS-Thema hinzufügen. Wenn eine Änderung des Status Ihres Verzeichnisses AWS Directory Service erkennt, veröffentlicht es eine Nachricht zu diesem Thema, die dann an die Abonnenten des Themas gesendet wird.

Sie können mehrere Verzeichnisse als Publisher zu einem einzelnen Thema zuordnen. Sie können auch Verzeichnis-Statusmeldungen zu Themen hinzufügen, die Sie zuvor in Amazon SNS erstellt haben. Sie haben umfassende Kontrolle, wer ein Thema veröffentlichen und abonnieren kann. Umfassende Informationen zu Amazon SNS finden Sie unter Was ist Amazon SNS?.

So aktivieren Sie SNS Messaging für Ihr Verzeichnis

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie die Registerkarte Wartung aus.
4. Wählen Sie im Abschnitt Verzeichnisüberwachung die Option Aktionen und dann Benachrichtigung erstellen aus.
5. Wählen Sie auf der Seite Benachrichtigung erstellen die Option Benachrichtigungstyp auswählen und dann Neue Benachrichtigung erstellen aus. Wenn Sie bereits über ein SNS-Thema verfügen, können Sie Vorhandenes SNS-Thema zuordnen wählen, um Status-Nachrichten aus diesem Verzeichnis zu diesem Thema zu senden.

> **Note**
>
> Wenn Sie Neue Benachrichtigung erstellen wählen, jedoch denselben Themen-Namen für ein SNS-Thema wählen, das bereits vorhanden ist, erstellt Amazon SNS kein neues Thema, sondern fügt die neue Abonnement-Information zum vorhandenen Thema hinzu. Wenn Sie Vorhandenes SNS-Thema zuordnen wählen, können Sie immer nur ein SNS-Thema wählen, das sich in derselben Region wie das Verzeichnis befindet.

6. Wählen Sie Empfängertyp und geben Sie die Kontaktinformationen für den Empfänger ein. Wenn Sie eine Telefonnummer für SMS eingeben, verwenden Sie nur Zahlen. Geben Sie keine Gedankenstriche, Leerzeichen oder Klammern ein.
7. (Optional) Geben Sie einen Namen für Ihr Thema und einen SNS-Anzeigenamen ein. Der Anzeigename ist ein kurzer Name von bis zu 10 Zeichen, der in alle SMS-Nachrichten zu diesem Thema aufgenommen wird. Bei der Verwendung der SMS-Option ist der Anzeigename erforderlich.

   > **Note**
   >
   > Wenn Sie mit einem IAM-Benutzer oder einer IAM-Rolle angemeldet sind, die nur über die DirectoryServiceFullAccess verwaltete Richtlinie verfügt, muss Ihr Themenname mit „“ beginnenDirectoryMonitoring. Wenn Sie Ihren Themennamen anpassen möchten, benötigen Sie zusätzliche Berechtigungen für SNS.

8. Wählen Sie Erstellen.

Wenn Sie zusätzliche SNS-Abonnenten festlegen möchten, z. B. eine zusätzliche E-Mail-Adresse, Amazon SQS-Warteschlangen oder AWS Lambda, können Sie dies über die Amazon SNS-Konsole tun.

Verzeichnis-Status-Nachrichten aus einem Thema entfernen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie die Registerkarte Wartung aus.
4. Wählen Sie im Abschnitt Verzeichnisüberwachung einen SNS-Themennamen in der Liste aus, klicken Sie auf Aktionen und dann auf Entfernen.
5. Wählen Sie Remove (Entfernen) aus.

Dadurch wird Ihr Verzeichnis als Publisher für das ausgewählte SNS-Thema entfernt. Wenn Sie das gesamte Thema löschen möchten, können Sie dies über die Amazon SNS-Konsole tun.

> **Note**
>
> Stellen Sie vor dem Löschen eines Amazon-SNS-Themas mithilfe der SNS-Konsole sicher, dass kein Verzeichnis Status-Nachrichten zu diesem Thema sendet.
> Wenn Sie ein Amazon-SNS-Thema mithilfe der SNS-Konsole löschen, wird diese Änderung nicht sofort in der Directory-Services-Konsole sichtbar. Sie würden nur benachrichtigt werden, wenn das nächste Mal ein Verzeichnis eine Nachricht zu diesem gelöschten Thema veröffentlicht. In diesem Fall würden Sie einen aktualisierten Status auf der Registerkarte Monitoring sehen, der angibt, dass das Thema nicht gefunden wurde.
> Um zu vermeiden, dass wichtige Verzeichnisstatusmeldungen fehlen, ordnen Sie daher Ihr Verzeichnis vor dem Löschen eines Themas, das Nachrichten von empfängt AWS Directory Service, einem anderen Amazon SNS-Thema zu.

Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem Active Directory

AD Connector ist ein Verzeichnisgateway, mit dem Sie Verzeichnisanfragen an Ihre lokalen Standorte umleiten können, Microsoft Active Directory ohne Informationen in der Cloud zwischenzuspeichern. Hier finden Sie weitere Informationen darüber, wie Sie Amazon EC2 mit einer Active-Directory-Domain verbinden können:

- Sie können eine Amazon EC2 EC2-Instance nahtlos mit Ihrer Active Directory Domain verbinden, wenn die Instance gestartet wird. Weitere Informationen finden Sie unter Nahtloses Verbinden einer Amazon EC2 Windows EC2-Instance mit Ihrem AWS Managed Microsoft AD mit AD Connector.
- Wenn Sie eine EC2-Instance manuell mit Ihrer Active Directory Domain verbinden müssen, müssen Sie die Instance in der richtigen Sicherheitsgruppe oder im Subnetz starten AWS-Region und dann die Instance mit der Domain verbinden. Active Directory
- Um eine Remote-Verbindung zu diesen Instances herstellen zu können, benötigen Sie eine IP-Verbindung zu den Instances von dem Netzwerk aus, von dem aus Sie sich verbinden. In den meisten Fällen muss hierfür Ihrer Amazon VPC ein Internet-Gateway zugeordnet sein und die Instance muss eine öffentliche IP-Adresse haben. Weitere Informationen zur Internetverbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet durch einen Internet-Gateway im Amazon-VPC-Benutzerhandbuch.

> **Note**
>
> Sobald Sie eine Instanz zu Ihrer selbstverwalteten Active Directory (lokalen) Instanz hinzufügen, kommuniziert die Instanz direkt mit Ihrer Instanz Active Directory und umgeht AD Connector.

Themen

Nahtloses Verbinden einer Amazon EC2 Windows EC2-Instance mit Ihrem AWS Managed Microsoft AD mit AD Connector

Durch dieses Verfahren wird eine Amazon EC2 Windows EC2-Instance nahtlos mit Ihrem AWS Managed Microsoft AD Active Directory verbunden.

Um einer Windows EC2-Instance nahtlos beizutreten

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste dasselbe Verzeichnis AWS-Region wie das bestehende Verzeichnis aus.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.
4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Windows-EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.
6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) Windows im Schnellstartbereich aus. Sie können das Windows Amazon Machine Image (AMI) in der Dropdown-Liste Amazon Machine Image (AMI) ändern.

7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen.

   a. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen.

   b. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels.

   c. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk.

   d. Wählen Sie Schlüsselpaar erstellen aus.

   e. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

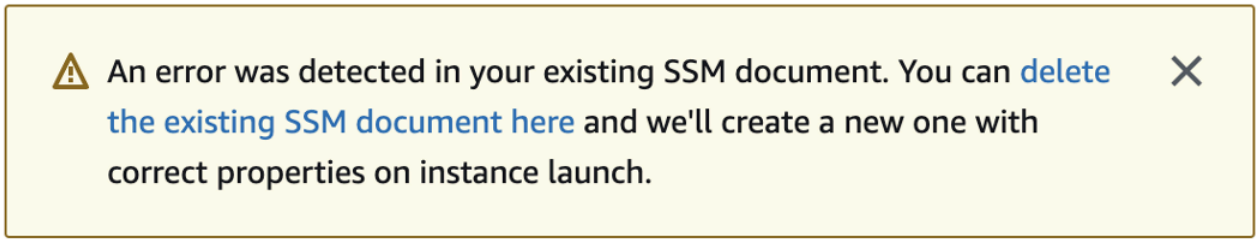
   > **Important**
   >
   > Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

    Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.
12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.

13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>
>
> Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:
>
> - Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
> - Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Für das IAM-Instance-Profil können Sie ein vorhandenes IAM-Instance-Profil auswählen oder ein neues erstellen. Wählen Sie aus der Dropdownliste für das IAM-Instanzprofil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM DirectoryServiceAccess angehängt sind. Um ein neues zu erstellen, wählen Sie den Link Neues IAM-Profil erstellen und gehen Sie dann wie folgt vor:

    1. Wählen Sie Rolle erstellen aus.
    2. Wählen Sie unter Vertrauenswürdige Entität auswählen die Option AWS -Service aus.
    3. Wählen Sie unter Use case (Anwendungsfall) die Option EC2 aus.

4. Wählen Sie in der Liste der Richtlinien unter Berechtigungen hinzufügen die Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM aus. DirectoryServiceAccess Geben Sie im Suchfeld **SSM** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess stellt die Berechtigungen zum Hinzufügen von Instances zu einer Gruppe bereit, die von verwaltet wird. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager -Benutzerhandbuch.

5. Geben Sie auf der Seite Benennen, überprüfen und erstellen einen Rollennamen ein. Sie benötigen diesen Rollennamen, um mit der EC2-Instance verbunden zu werden.
6. (Optional) Sie können im Feld Beschreibung eine Beschreibung des IAM-Instance-Profils angeben.
7. Wählen Sie Rolle erstellen aus.
8. Kehren Sie zur Seite Eine Instance starten zurück und wählen Sie das Aktualisierungssymbol neben dem IAM-Instance-Profil. Ihr neues IAM-Instance-Profil sollte in der Dropdown-Liste IAM-Instance-Profil sichtbar sein. Wählen Sie das neue Profil und belassen Sie die restlichen Einstellungen auf den Standardwerten.

16. Wählen Sie Launch Instance (Instance starten) aus.

Nahtloses Verbinden einer Amazon EC2 EC2-Linux-Instance mit Ihrem AWS verwalteten Microsoft AD mit AD Connector

Durch dieses Verfahren wird eine Amazon EC2 EC2-Linux-Instance nahtlos mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis verbunden.

Die folgenden Linux-Instance-Distributionen und -Versionen werden unterstützt:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-Bit x86)

- Red Hat Enterprise Linux 8 (HVM) (64-Bit x86)
- Ubuntu Server 18.04 LTS und Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Versionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 unterstützen das Feature der nahtlosen Domainverbindung nicht.

Voraussetzungen

Bevor Sie einen nahtlosen Domänenbeitritt zu einer EC2-Linux-Instance einrichten können, müssen Sie die Verfahren in diesem Abschnitt abschließen.

Ihr Servicekonto für die nahtlose Domainverbindung auswählen

Sie können Linux-Computer über AD Connector nahtlos mit Ihrer lokalen Active Directory Domäne verbinden. Dazu müssen Sie ein Benutzerkonto mit der Berechtigung zum Erstellen eines Computerkontos erstellen, um die Computer mit der Domain zu verbinden. Sie können Ihr AD-Connector-Servicekonto verwenden, wenn Sie möchten. Sie können auch jedes andere Konto verwenden, das über ausreichende Rechte verfügt, um Computer mit der Domain zu verbinden. Mitglieder der Domain-Admins oder anderer Gruppen verfügen möglicherweise über ausreichende Rechte, um Computer mit der Domain zu verbinden, wir empfehlen diese jedoch nicht. Als bewährte Methode empfehlen wir Ihnen, ein Servicekonto zu verwenden, das über die erforderlichen Mindestberechtigungen verfügt, um Computer mit der Domain zu verbinden.

Um ein Konto mit den Mindestberechtigungen zu delegieren, die für den Beitritt von Computern zur Domäne erforderlich sind, können Sie die folgenden PowerShell Befehle ausführen. Sie müssen diese Befehle von einem Windows Computer aus ausführen, auf dem die Domäne installiert ist. Installieren Sie die Active Directory-Verwaltungstools für AWS Managed Microsoft AD Darüber hinaus müssen Sie ein Konto verwenden, das die Berechtigung hat, die Berechtigungen für Ihre Computer-OU oder Ihren Container zu ändern. Der PowerShell Befehl legt Berechtigungen fest, die es dem Dienstkonto ermöglichen, Computerobjekte im Standardcomputercontainer Ihrer Domäne zu erstellen. Wenn Sie eine grafische Benutzeroberfläche (GUI) bevorzugen, können Sie den manuellen Prozess verwenden, der unter Zuweisen von Berechtigungen zu Ihrem Servicekonto beschrieben wird.

```
$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"
```

Wenn Sie eine grafische Benutzeroberfläche (GUI) bevorzugen, können Sie den manuellen Prozess verwenden, der unter Zuweisen von Berechtigungen zu Ihrem Servicekonto beschrieben wird.

Die Secrets zum Speichern des Domain-Servicekontos erstellen

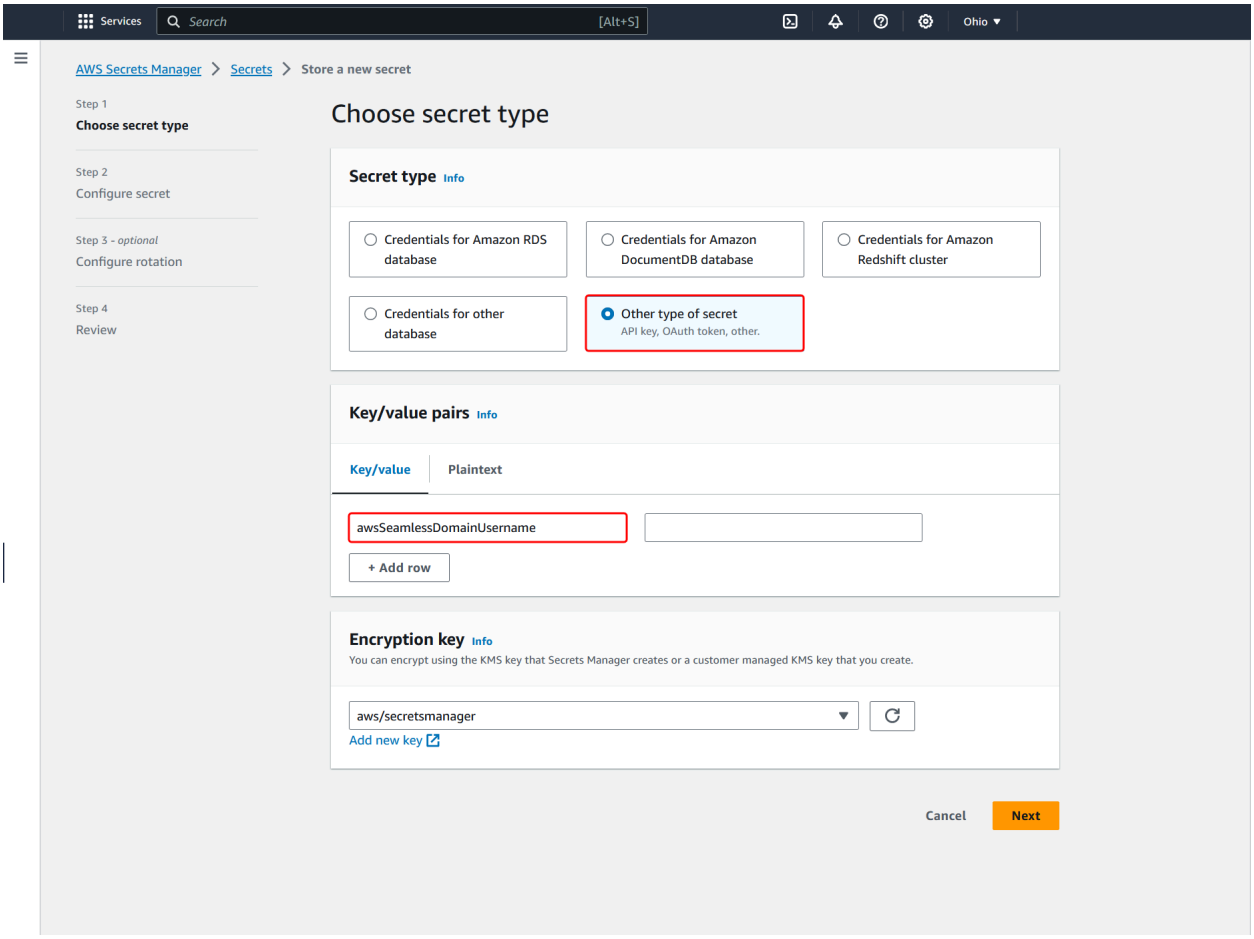
Sie können AWS Secrets Manager es zum Speichern des Domänendienstkontos verwenden.

So erstellen Sie Secrets und speichern die Kontoinformationen des Domainservices

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Secrets Manager Konsole unter https://console.aws.amazon.com/secretsmanager/.
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Gehen Sie auf der Seite Neues Geheimnis speichern wie folgt vor:
    a. Wählen Sie unter Geheimtyp die Option Andere Art von Geheimnissen aus.
    b. Gehen Sie unter Schlüssel/Wert-Paare wie folgt vor:

i. Geben Sie im ersten Feld **`awsSeamlessDomainUsername`** ein. Geben Sie in derselben Zeile im nächsten Feld den Benutzernamen für Ihr Dienstkonto ein. Wenn Sie den PowerShell Befehl beispielsweise zuvor verwendet haben, wäre der Name des Dienstkontos**`awsSeamlessDomain`**.

> **Note**
>
> Sie müssen **`awsSeamlessDomainUsername`** genau so eingeben, wie er lautet. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.



ii. Wählen Sie Zeile hinzufügen.

iii. Geben Sie in der neuen Zeile im ersten Feld **`awsSeamlessDomainPassword`** ein. Geben Sie in derselben Zeile im nächsten Feld das Passwort für Ihr Servicekonto ein.

> **Note**
>
> Sie müssen **`awsSeamlessDomainPassword`** genau so eingeben, wie er lautet. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.

iv. Behalten Sie unter Verschlüsselungsschlüssel den Standardwert bei`aws/secretsmanager`. AWS Secrets Manager verschlüsselt das Geheimnis immer, wenn Sie diese Option wählen. Sie können auch einen von Ihnen erstellten Schlüssel auswählen.

> **Note**
>
> Je nachdem AWS Secrets Manager, welches Geheimnis Sie verwenden, fallen Gebühren an. Die aktuelle vollständige Preisliste finden Sie unter AWS Secrets Manager – Preise.
> Sie können den AWS verwalteten Schlüssel`aws/secretsmanager`, den Secrets Manager erstellt, verwenden, um Ihre Geheimnisse kostenlos zu verschlüsseln. Wenn Sie Ihre eigenen KMS-Schlüssel zur Verschlüsselung Ihrer Geheimnisse erstellen, wird Ihnen der aktuelle AWS KMS Tarif AWS berechnet. Weitere Informationen finden Sie unter AWS Key Management Service -Preisgestaltung.

v. Wählen Sie Weiter aus.

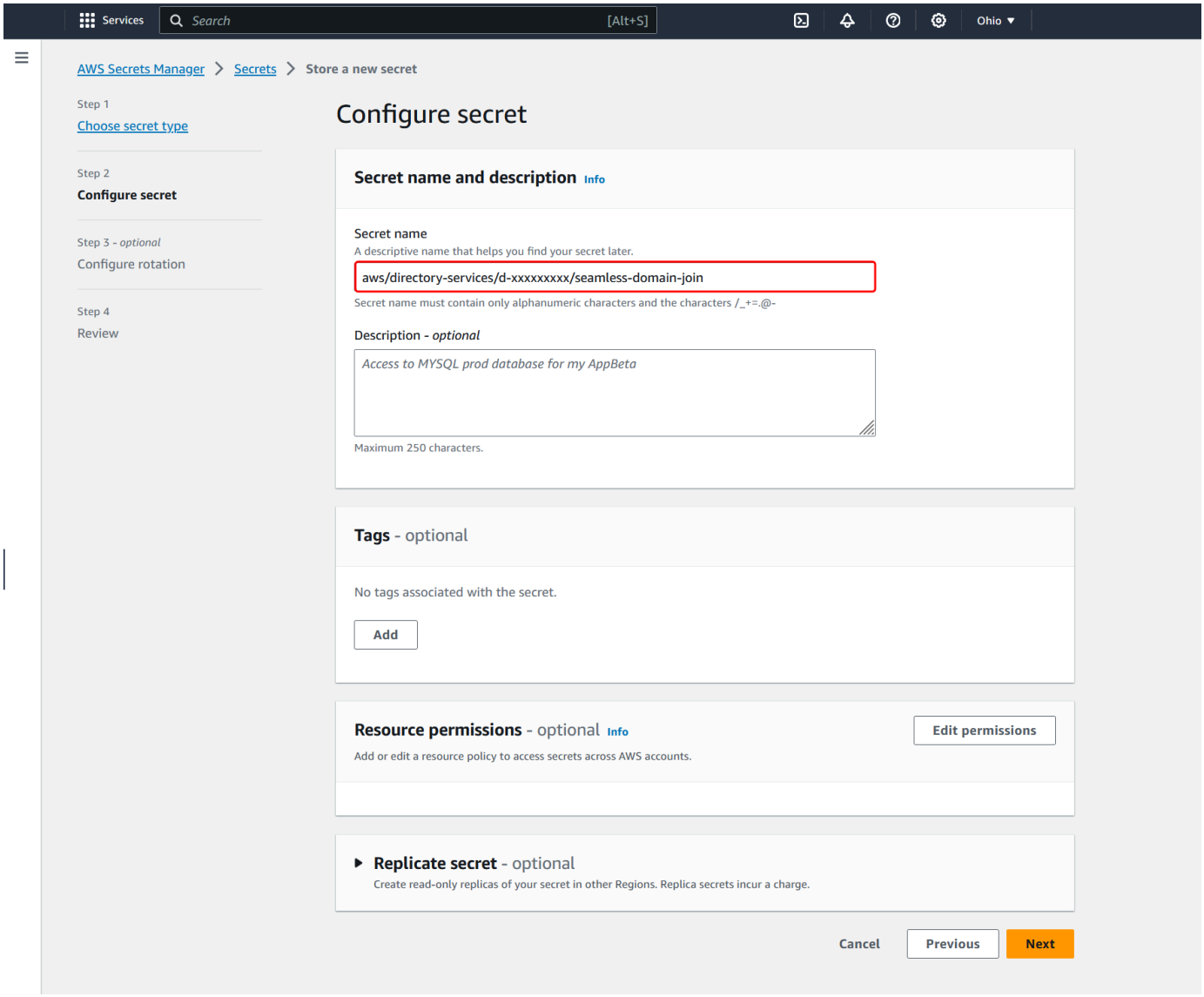
4. Geben Sie unter Geheimer Name einen geheimen Namen ein, der Ihre Verzeichnis-ID enthält. Verwenden Sie dabei das folgende Format und ersetzen Sie *`d-xxxxxxxxx`* durch Ihre Verzeichnis-ID:

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

Dies wird verwendet, um Secrets in der Anwendung abzurufen.

> **Note**
>
> Sie müssen **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** genau so eingeben, wie es ist, aber *`d-xxxxxxxxx`* durch Ihre Verzeichnis-ID ersetzen.

Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.



5. Belassen Sie alles andere auf den eingestellten Standardwerte und wählen Sie dann Weiter.
6. Wählen Sie unter Automatische Rotation konfigurieren die Option Automatische Rotation deaktivieren und wählen Sie dann Weiter.

   Sie können die Rotation für dieses Geheimnis aktivieren, nachdem Sie es gespeichert haben.
7. Überprüfen Sie die Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen zu speichern. Die Secrets-Manager-Konsole zeigt Ihnen wieder die Liste der Secrets in Ihrem Konto an, in der Ihr neues Secret nun enthalten ist.

8. Wählen Sie Ihren neu erstellten Secret-Namen aus der Liste und notieren Sie sich den Wert des Secret-ARN. Sie brauchen diesen im nächsten Abschnitt.

Schalten Sie die Rotation für das geheime Domänendienstkonto ein

Wir empfehlen, dass Sie die geheimen Daten regelmäßig wechseln, um Ihre Sicherheitslage zu verbessern.

So aktivieren Sie die Rotation für das geheime Domänendienstkonto

- Folgen Sie den Anweisungen unter Automatische Rotation für AWS Secrets Manager geheime Daten einrichten im AWS Secrets Manager Benutzerhandbuch.

  Verwenden Sie für Schritt 5 die Rotationsvorlage Microsoft Active Directory-Anmeldeinformationen im AWS Secrets Manager Benutzerhandbuch.

  Hilfe finden Sie im AWS Secrets Manager Benutzerhandbuch unter Problembehandlung bei der AWS Secrets Manager Rotation.

Die erforderliche IAM-Richtlinie und -Rolle erstellen

Gehen Sie wie folgt vor, um eine benutzerdefinierte Richtlinie zu erstellen, die nur Lesezugriff auf Ihren Secrets Manager Seamless Domain Join Secret (den Sie zuvor erstellt haben) ermöglicht, und um eine neue DomainJoin LinuxEC2 IAM-Rolle zu erstellen.

Die IAM-Leserichtlinie zu Secrets Manager erstellen

Sie verwenden die IAM-Konsole, um eine Richtlinie zu erstellen, die schreibgeschützten Zugriff auf Ihr Secrets-Manager-Secret gewährt.

So erstellen Sie die IAM-Leserichtlinie zu Secrets Manager

1. Melden Sie sich AWS Management Console als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Dann öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Access Management die Option Richtlinien aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie die Registerkarte JSON aus und kopieren Sie den Text aus dem folgenden JSON-Richtliniendokument. Fügen Sie ihn dann in das JSON-Textfeld ein.

> **Note**
>
> Stellen Sie sicher, dass Sie die Region und den Ressourcen-ARN durch die tatsächliche Region und den ARN des Secrets ersetzen, den Sie zuvor erstellt haben.

```
{
    "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. Wählen Sie danach Next aus. Die Richtlinienvalidierung meldet mögliche Syntaxfehler. Weitere Informationen finden Sie unter Validierung von IAM-Richtlinien.
6. Geben Sie auf der Seite Richtlinie überprüfen einen Namen für die Richtlinie ein, z. B. **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. Überprüfen Sie den Abschnitt Zusammenfassung, um die Berechtigungen einzusehen, die Ihre Richtlinie gewährt. Wählen Sie dann Richtlinie erstellen aus, um Ihre Änderungen zu speichern. Die neue Richtlinie erscheint in der Liste der verwalteten Richtlinien und ist nun bereit, einer Identität zugeordnet zu werden.

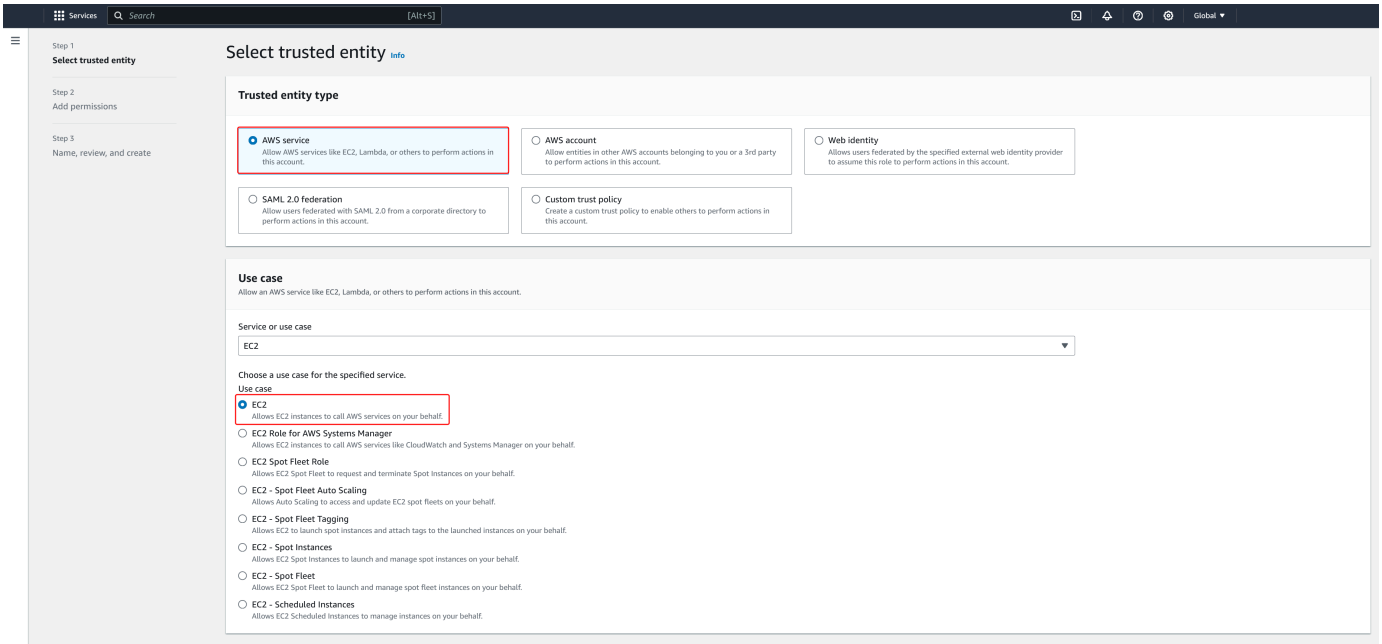
> **Note**
>
> Wir empfehlen Ihnen, eine Richtlinie pro Secret zu erstellen. Auf diese Weise wird sichergestellt, dass Instances nur auf das entsprechende Secret zugreifen können und die Auswirkungen einer Kompromittierung einer Instance minimiert werden.

Erstellen Sie die LinuxEC2-Rolle DomainJoin

Sie verwenden die IAM-Konsole, um die Rolle zu erstellen, die Sie für die Domainverbindung Ihrer Linux-EC2-Instance verwenden werden.

Um die LinuxEC2-Rolle zu erstellen DomainJoin

1. Melden Sie sich AWS Management Console als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Dann öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich unter Access Management die Option Rollen aus.
3. Wählen Sie im Inhaltsbereich die Option Rolle erstellen.
4. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität auswählen) die Option AWS -Service aus.
5. Wählen Sie unter Anwendungsfall die Option EC2 und dann Weiter aus.



6. Gehen Sie für Filterrichtlinien wie folgt vor:

   a. Geben Sie **`AmazonSSMManagedInstanceCore`** ein. Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

   b. Geben Sie **`AmazonSSMDirectoryServiceAccess`** ein. Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

   c. Geben Sie **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** ein (oder den Namen der Richtlinie, die Sie im vorherigen Verfahren erstellt haben). Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

d. Nachdem Sie die drei oben aufgeführten Richtlinien hinzugefügt haben, wählen Sie Rolle erstellen aus.

> **Note**
>
> AmazonSSM DirectoryServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einer Datei, die von Active Directory verwaltet wird. AWS Directory Service AmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager - Benutzerhandbuch.

7. Geben Sie im Feld Rollenname einen Namen für Ihre neue Rolle ein, z. B. **`LinuxEC2DomainJoin`** oder einen anderen Namen, den Sie bevorzugen.
8. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein.
9. (Optional) Wählen Sie unter Schritt 3: Stichwörter hinzufügen die Option Neues Tag hinzufügen aus, um Stichwörter hinzuzufügen. Tag-Schlüssel-Wert-Paare werden verwendet, um den Zugriff für diese Rolle zu organisieren, nachzuverfolgen oder zu kontrollieren.
10. Wählen Sie Rolle erstellen aus.

Verbinden Sie Ihre Amazon EC2 Linux-Instance nahtlos mit Ihrem AWS Managed Microsoft AD Active Directory

Nachdem Sie nun alle erforderlichen Aufgaben konfiguriert haben, können Sie das folgende Verfahren verwenden, um Ihre EC2-Linux-Instance nahtlos hinzuzufügen.

Um Ihrer Linux-Instance nahtlos beizutreten

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Regionsauswahl in der Navigationsleiste dasselbe Verzeichnis aus AWS-Region wie das bestehende Verzeichnis.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.

4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Linux EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.
6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) ein Linux-AMI aus, das Sie starten möchten.

> **Note**
>
> Das verwendete AMI muss AWS Systems Manager (SSM Agent) Version 2.3.1644.0 oder höher haben. Um die installierte SSM-Agent-Version in Ihrem AMI zu überprüfen, indem Sie eine Instance von diesem AMI aus starten, lesen Sie den Abschnitt Ermittlung der aktuell installierten SSM-Agent-Version. Wenn Sie den SSM Agent aktualisieren müssen, lesen Sie den Abschnitt Installieren und Konfigurieren von SSM Agent in EC2-Instances für Linux.
> SSM verwendet das `aws:domainJoin` Plugin, wenn eine Linux-Instance mit einer Domain verknüpft wird. Active Directory *`Das Plugin ändert den Hostnamen für die Linux-Instances in das Format EC2AMAZ- XXXXXXX.`* Weitere Informationen *`aws:domainJoin`* dazu finden Sie in der Plugin-Referenz zum AWS Systems Manager Befehlsdokument im Benutzerhandbuch.AWS Systems Manager

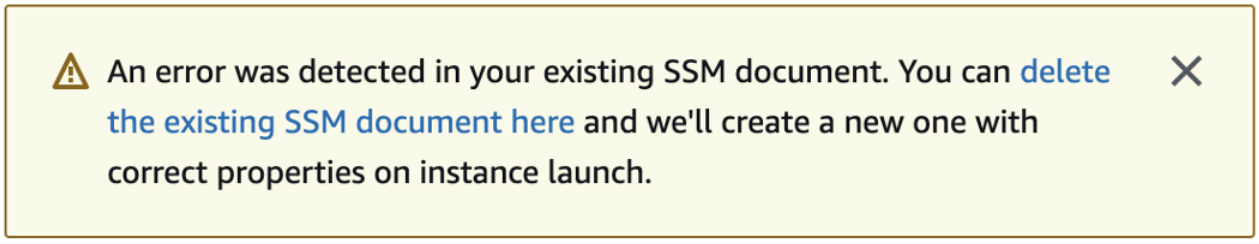
7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk. Wählen Sie Schlüsselpaar erstellen aus. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

> **Important**
>
> Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

    Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.
12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>

Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:

- Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
- Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Wählen Sie für das IAM-Instanzprofil die IAM-Rolle aus, die Sie zuvor im Abschnitt Voraussetzungen erstellt haben. Schritt 2: LinuxEC2-Rolle erstellen. DomainJoin
16. Wählen Sie Launch Instance (Instance starten) aus.

> **Note**
>
> Wenn Sie eine nahtlose Domainverbindung mit SUSE Linux durchführen, ist ein Neustart erforderlich, bevor die Authentifizierungen funktionieren. Um SUSE vom Linux-Terminal aus neu zu starten, geben Sie sudo reboot ein.

Ihr AD-Connector-Verzeichnis verwalten

In diesem Abschnitt wird die Verwaltung allgemeiner Administrationsaufgaben für Ihre AD-Connector-Umgebung beschrieben.

Themen

Ihr AD Connector löschen

Wenn ein AD Connector gelöscht wird, bleibt Ihr On-Premises-Verzeichnis intakt. Alle zugeordneten Instances bleiben ebenfalls erhalten und sind weiterhin mit Ihrem On-Premises-Verzeichnis verknüpft.

Sie können sich nach wie vor mit den Anmeldeinformationen Ihres Verzeichnisses bei diesen Instances anmelden.

So löschen Sie AD Connector

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse. Stellen Sie sicher, dass Sie sich dort befinden AWS-Region , wo Ihr AD Connector bereitgestellt wird. Weitere Informationen finden Sie unter Region auswählen.
2. Stellen Sie sicher, dass keine AWS Anwendungen für den AD Connector aktiviert sind, den Sie löschen möchten. Aktivierte AWS Anwendungen verhindern, dass Sie Ihren AD Connector löschen.

   a. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.

   b. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus. Im Bereich AWS Apps und Dienste sehen Sie, welche AWS Anwendungen für Ihren AD Connector aktiviert sind.

      - AWS Management Console Zugriff deaktivieren. Weitere Informationen finden Sie unter AWS Management Console-Zugriff deaktivieren.
      - Um Amazon zu deaktivieren WorkSpaces, müssen Sie den Service aus dem Verzeichnis in der WorkSpaces Konsole abmelden. Weitere Informationen finden Sie unter Abmeldung von einem Verzeichnis im WorkSpaces Amazon-Administratorhandbuch.
      - Um Amazon zu deaktivieren WorkDocs, müssen Sie die WorkDocs Amazon-Website in der WorkDocs Amazon-Konsole löschen. Weitere Informationen finden Sie unter Löschen einer Site im WorkDocs Amazon-Administratorhandbuch.
      - Um Amazon zu deaktivieren WorkMail, müssen Sie die WorkMail Amazon-Organisation in der WorkMail Amazon-Konsole entfernen. Weitere Informationen finden Sie unter Organisation entfernen im WorkMail Amazon-Administratorhandbuch.
      - Um Amazon FSx für Windows File Server zu deaktivieren, müssen Sie das Amazon-FSx-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter Arbeiten mit Active Directory in FSx for Windows File Server im Amazon FSx for Windows File Server Server-Benutzerhandbuch.
      - Um Amazon Relational Database Service zu deaktivieren, müssen Sie die Amazon-RDS-Instance aus der Domain entfernen. Weitere Informationen finden Sie unter Verwalten einer DB-Instance in einer Domain im Amazon-RDS-Benutzerhandbuch.

- Um den AWS Client VPN Dienst zu deaktivieren, müssen Sie den Verzeichnisdienst vom Client-VPN-Endpunkt entfernen. Weitere Informationen finden Sie unter Active DirectoryAuthentifizierung im AWS Client VPN Administratorhandbuch.
- Zur Deaktivierung von Amazon Connect müssen Sie die Amazon Connect-Instance löschen. Weitere Informationen finden Sie unter Löschen einer Amazon-Connect-Instance im Administrationshandbuch für Amazon Connect.
- Um Amazon zu deaktivieren QuickSight, müssen Sie sich von Amazon abmelden QuickSight. Weitere Informationen finden Sie unter Schließen Ihres Amazon QuickSight Kontos im QuickSight Amazon-Benutzerhandbuch.

> **Note**
>
> Wenn Sie es verwenden AWS IAM Identity Center und es zuvor mit dem AWS verwalteten Microsoft AD-Verzeichnis verbunden haben, das Sie löschen möchten, müssen Sie zuerst die Identitätsquelle ändern, bevor Sie es löschen können. Weitere Informationen finden Sie unter Identitätsquelle ändern im Benutzerhandbuch zu IAM Identity Center.

3. Wählen Sie im Navigationsbereich Verzeichnisse aus.
4. Wählen Sie nur den AD Collector, der gelöscht werden soll, und klicken Sie auf Löschen. Es dauert einige Minuten, bis der AD Connector gelöscht ist. Wenn der AD Connector gelöscht wurde, wird er aus Ihrer Verzeichnisliste entfernt.

Verzeichnisinformationen anzeigen

Sie können detaillierte Informationen zu einem Verzeichnis einsehen.

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

1. Wählen Sie im Navigationsbereich der AWS Directory Service Konsole unter Active Directory Verzeichnisse aus.
2. Klicken Sie auf den Link der Verzeichnis-ID. Informationen über das Verzeichnis werden auf der Seite Verzeichnisdetails angezeigt.

Weitere Informationen zum Feld Status finden Sie unter Erläuterungen zum Verzeichnisstatus.

Aktivieren des Zugriffs auf AWS Anwendungen und Services

Benutzer können AD Connector autorisieren, AWS Anwendungen und Services wie Amazon WorkSpacesZugriff auf Ihr zu gewährenActive Directory. Die folgenden AWS Anwendungen und Services können für die Arbeit mit AD Connector aktiviert oder deaktiviert werden.

AWS Anwendung/Service	Weitere Informationen …
Amazon Chime	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Chime.
Amazon Connect	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Connect.
Amazon WorkDocs	Weitere Informationen finden Sie im Amazon-WorkDocs Administratorhandbuch.
Amazon WorkMail	Weitere Informationen finden Sie im Amazon-WorkMail Administratorhandbuch.
Amazon WorkSpaces	Sie können Simple AD, AWS Managed Microsoft AD oder AD Connector direkt aus erstellen WorkSpaces. Starten Sie einfach Advanced Setup bei der Erstellung Ihres Workspace. Weitere Informationen finden Sie im Amazon-WorkSpaces Administratorhandbuch.
AWS Client VPN	Weitere Informationen finden Sie im AWS Client VPN -Benutzerhandbuch.
AWS IAM Identity Center	Weitere Informationen finden Sie im AWS IAM Identity Center -Benutzerhandbuch.
AWS Management Console	Weitere Informationen finden Sie unter Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren.

AWS Anwendung/Service	Weitere Informationen …
AWS Transfer Family	Weitere Informationen finden Sie im AWS Transfer Family -Benutzerhandbuch.

Nach der Aktivierung verwalten Sie den Zugriff auf Ihre Verzeichnisse in der Konsole der Anwendung oder dem Service, denen Sie Zugriff auf Ihr Verzeichnis gewähren wollen. Führen Sie die folgenden Schritte aus, um die oben beschriebenen AWS Anwendungs- und Servicelinks in der AWS Directory Service Konsole zu finden.

Zum Anzeigen der Anwendungen und Services für ein Verzeichnis

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Sehen Sie sich die Liste im Abschnitt AWS -Anwendungen und -Services an.

Weitere Informationen zum Autorisieren oder Aufheben der Autorisierung von AWS Anwendungen und Services mit finden Sie AWS Directory Serviceunter Autorisierung für AWS Anwendungen und Dienste mit AWS Directory Service.

Die DNS-Adresse für AD Connector aktualisieren

Gehen Sie bei der Aktualisierung der DNS-Adressen, auf die AD Connector verweist, folgendermaßen vor.

> **Note**
>
> Wenn derzeit eine Aktualisierung ausgeführt wird, müssen Sie vor dem Übermitteln einer weiteren Aktualisierung warten, bis der aktuelle Vorgang abgeschlossen ist.
> Wenn Sie WorkSpaces mit Ihrem AD Connector verwenden, stellen Sie sicher, dass auch die DNS-Adressen Ihres WorkSpace aktualisiert werden. Weitere Informationen finden Sie unter DNS-Server für WorkSpaces aktualisieren.

So aktualisieren Sie die DNS-Einstellungen für AD Connector

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole unter Active Directory die Option Verzeichnisse.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
3. Wählen Sie auf der Seite Verzeichnisdetails die Registerkarte Netzwerk und Sicherheit aus.
4. Scrollen Sie nach unten zum Abschnitt Vorhandene DNS-Einstellungen und wählen Sie Aktualisieren.
5. Geben Sie im Dialogfeld Update existing DNS addresses (Vorhandene DNS-Adressen aktualisieren) die aktualisierten DNS-IP-Adressen ein und wählen Sie dann Update (Aktualisieren) aus.

Weitere Informationen zur Problembehandlung bei AD Connector finden Sie unter Problembehandlung bei AD Connector.

Bewährte Methoden für AD Connector

Hier finden Sie einige Vorschläge und Richtlinien, die Sie in Betracht ziehen sollten, um Probleme zu vermeiden und AD Connector bestmöglich zu nutzen.

Einrichten: Voraussetzungen

Beachten Sie die folgenden Richtlinien, bevor Sie Ihr Verzeichnis erstellen.

Sicherstellen, dass Sie den richtigen Verzeichnistyp verwenden

AWS Directory Service bietet mehrere Möglichkeiten zur Verwendung Microsoft Active Directory mit anderen AWS Diensten. Sie können den Verzeichnisdienst mit den Funktionen wählen, die Sie benötigen, ohne Ihr Budget zu überlasten:

- AWS Der Directory Service für Microsoft Active Directory ist ein funktionsreicher, verwalteter Dienst, der in der Microsoft Active Directory AWS Cloud gehostet wird. AWS Managed Microsoft AD ist die beste Wahl, wenn Sie mehr als 5.000 Benutzer haben und eine Vertrauensbeziehung zwischen einem AWS gehosteten Verzeichnis und Ihren lokalen Verzeichnissen einrichten möchten.

- AD Connector verbindet einfach Ihr vorhandenes lokales System Active Directory mit AWS. AD Connector ist die beste Wahl, wenn Sie Ihr vorhandenes On-Premises-Verzeichnis mit AWS - Services verwenden möchten.
- Simple AD ist ein niedriges, kostengünstiges Verzeichnis mit grundlegender Active Directory Kompatibilität. Es unterstützt 5 000 oder weniger Benutzer, Samba-4-kompatible Anwendungen und LDAP-Kompatibilität für LDAP-fähige Anwendungen.

Einen detaillierteren Vergleich der AWS Directory Service Optionen finden Sie unterWelche sollte man auswählen.

Sicherstellen, dass Ihre VPCs und Instances korrekt konfiguriert sind

Um eine Verbindung zu Ihren Verzeichnissen herzustellen, sie zu verwalten und zu nutzen, müssen Sie die VPCs, denen die Verzeichnisse zugeordnet sind, ordnungsgemäß konfigurieren. Weitere Informationen über die Anforderungen zur VPC-Sicherheit und Netzwerken finden Sie unter AWS Voraussetzungen für verwaltetes Microsoft AD, AD-Connector-Voraussetzungen oder Simple-AD-Voraussetzungen.

Wenn Sie Ihrer Domain eine Instance hinzufügen, stellen Sie sicher, dass Sie eine Verbindung und Remote-Zugriff auf Ihre Instance haben, wie in Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory beschrieben.

Sich der eigenen Grenzen bewusst sein

Erfahren Sie mehr über die verschiedenen Beschränkungen für Ihren spezifischen Verzeichnistyp. Der verfügbare Speicherplatz und die Gesamtgröße Ihrer Objekte sind die einzigen Einschränkungen in Bezug auf die Anzahl der Objekte, die Sie in Ihrem Verzeichnis speichern können. Einzelheiten zu dem von Ihnen ausgewählten Verzeichnis finden Sie unter AWS Verwaltete Microsoft AD-Kontingente, Kontingente für AD Connector oder Kontingente für Simple AD.

Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut

AWS erstellt eine Sicherheitsgruppe und fügt sie den elastischen Netzwerkschnittstellen Ihres Verzeichnisses hinzu, auf die von Ihren Peering-VPCs aus zugegriffen werden kann oder deren Größe geändert wurde. AWS konfiguriert die Sicherheitsgruppe so, dass unnötiger Datenverkehr zum Verzeichnis blockiert wird, und lässt den erforderlichen Datenverkehr zu.

Ändern der Verzeichnissicherheitsgruppe

Wenn Sie die Sicherheit der Sicherheitsgruppen Ihrer Verzeichnisse ändern möchten, können Sie dies tun. Nehmen Sie diese Änderungen nur vor, wenn Sie verstehen, wie Sicherheitsgruppenfilter funktionieren. Weitere Informationen finden Sie unter Amazon-EC2-Sicherheitsgruppen für Linux-Instances im Amazon-EC2-Benutzerhandbuch. Unsachgemäße Änderungen können zum Verlust der Kommunikation mit den vorgesehenen Computern und Instanzen führen. AWS empfiehlt, nicht zu versuchen, zusätzliche Ports für Ihr Verzeichnis zu öffnen, da dies die Sicherheit Ihres Verzeichnisses beeinträchtigt. Sehen Sie sich das AWS -Modell übergreifender Verantwortlichkeit genau an.

> **Warning**
>
> Es ist technisch möglich, dass Sie die Sicherheitsgruppe des Verzeichnisses anderen von Ihnen erstellten EC2-Instances zuordnen. AWS Empfiehlt jedoch, von dieser Vorgehensweise abzuraten. AWS kann Gründe haben, die Sicherheitsgruppe ohne vorherige Ankündigung zu ändern, um den Funktions- oder Sicherheitsanforderungen des verwalteten Verzeichnisses gerecht zu werden. Solche Änderungen wirken sich auf alle Instances aus, denen Sie die Verzeichnis-Sicherheitsgruppe zuordnen, und können den Betrieb der dazugehörigen Instances stören. Außerdem entsteht durch die Zuordnung der Verzeichnis-Sicherheitsgruppe zu Ihren EC2-Instances möglicherweise ein potenzielles Sicherheitsrisiko für Ihre EC2-Instances.

On-Premises-Standorte und Subnetze korrekt konfigurieren, wenn AD Connector verwendet wird

Wenn Ihr On-Premises-Netzwerk Active-Directory-Standorte definiert hat, müssen Sie sicherstellen, dass die Subnetze in der VPC, in der sich Ihr AD Connector befindet, in einem Active-Directory-Standort definiert sind, und dass es keine Konflikte zwischen den Subnetzen in Ihrer VPC und den Subnetzen in Ihren anderen Standorten gibt.

Um Domain-Controller zu entdecken, verwendet AD Connector den Active-Directory-Standort, dessen Subnetz-IP-Adressbereiche in der Nähe derjenigen in der VPC liegen, die AD Connector enthalten. Wenn Sie einen Standort haben, dessen Subnetze die gleichen IP-Adressbereiche haben wie die in Ihrer VPC, erkennt AD Connector die Domain-Controller in diesem Standort, die sich möglicherweise nicht in der Nähe Ihrer Region befinden.

Machen Sie sich mit Benutzernamenbeschränkungen für AWS Anwendungen vertraut

AWS Directory Service unterstützt die meisten Zeichenformate, die bei der Erstellung von Benutzernamen verwendet werden können. Es gibt jedoch Zeichenbeschränkungen, die für Benutzernamen gelten, die für die Anmeldung bei AWS Anwendungen wie WorkSpaces Amazon, Amazon oder Amazon WorkDocs verwendet werden. WorkMail QuickSight Diese Einschränkungen verlangen, dass die folgenden Zeichen nicht verwendet werden:

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

> **Note**
>
> Das Symbol @ ist zulässig, wenn es einem UPN-Suffix vorausgeht.

Programmieren Ihrer Anwendungen

Stellen Sie folgende Überlegungen an, ehe Sie Ihre Anwendungen programmieren:

Auslastungstests vor der Inbetriebnahme

Führen Sie Labortests mit Anwendungen und Anforderungen durch, die Ihren Produktions-Workload darstellen, um sicherzustellen, dass das Verzeichnis entsprechend der Arbeitslast Ihrer Anwendung skaliert wird. Wenn Sie zusätzliche Kapazitäten benötigen, verteilen Sie Ihre Ladevorgänge über mehrere AD Connector-Verzeichnisse.

Verwenden Ihres Verzeichnisses

Hier finden Sie einige Vorschläge zur Verwendung Ihres Verzeichnisses.

Regelmäßig die Administrator-Anmeldeinformationen wechseln

Ändern Sie das AD-Connector-Administratorpasswort Ihres Servicekontos regelmäßig und stellen Sie sicher, dass das Passwort Ihren vorhandenen Active-Directory-Passwortrichtlinien entspricht. Anleitungen zum Ändern des Servicekonto-Passworts finden Sie unter Ihre Anmeldeinformationen für Ihr AD-Connector-Servicekonto in AWS Directory Service aktualisieren.

Eindeutige AD-Connectors für jede Domain verwenden

AD Connectors und Ihre On-Premises-AD-Domains haben eine 1-zu-1-Beziehung. Das bedeutet, dass für jede On-Premises-Domain, einschließlich untergeordneter Domains in AD-Gesamtstrukturen, die Sie authentifizieren möchten, ein eindeutiger AD Connector erstellt werden muss. Für jeden AD Connector, den Sie erstellen, müssen Sie ein anderes Service-Konto verwenden, auch wenn sie mit dem gleichen Verzeichnis verbunden sind.

Überprüfen der Kompatibilität

Wenn Sie AD Connector verwenden, müssen Sie sicherstellen, dass Ihr lokales Verzeichnis mit AWS Directory Service s kompatibel ist und bleibt. Weitere Informationen zu Ihren Verantwortlichkeiten finden Sie in unserem Modell für übergreifende Verantwortlichkeit.

Kontingente für AD Connector

Im Folgenden finden Sie die Standardkontingente für AD Connector. Jedes Kontingent gilt pro Region, sofern nicht anders angegeben.

Kontingente für AD Connector

Ressource	Standardkontingent
Verzeichnisse in AD Connector	10
Maximale Anzahl registrierter Zertifizierungsstellenzertifikate (CA) pro Verzeichnis	5

Richtlinie zur Anwendungskompatibilität für AD-Connector

Als Alternative zum AWS Directory Service für Microsoft Active Directory (AWS Verwaltetes Microsoft AD) ist AD Connector ausschließlich ein Active-Directory-Proxy für AWS-erstellte Anwendungen und Services. Sie konfigurieren den Proxy für die Verwendung einer angegebenen Active Directory-Domain. Wenn die Anwendung in Active Directory nach einem Benutzer oder einer Gruppe suchen muss, leitet AD Connector die Anforderungen an das Verzeichnis weiter. Wenn sich ein Benutzer bei der Anwendung anmeldet, leitet AD Connector die Authentifizierungsanforderung ebenfalls an das Verzeichnis weiter. Es gibt keine Anwendungen von Drittanbietern, die mit AD Connector kompatibel sind.

Die folgende Liste enthält die kompatiblen AWS-Anwendungen und -Services:

- Amazon Chime – Detaillierte Anweisungen finden Sie unter Herstellen einer Verbindung mit Active Directory.
- Amazon Connect – Weitere Informationen finden Sie unter Wie Amazon Connect funktioniert.
- Amazon EC2 für Windows oder Linux — Sie können die nahtlose Active Directory-Domain-Join-Funktion von Amazon EC2 Windows oder Linux verwenden, um Ihre Instance mit Ihrem selbstverwalteten Active Directory (lokal) zu verbinden. Nach dem Herstellen der Verbindung kommuniziert die Instance direkt mit Ihrem Active Directory und umgeht AD Connector. Weitere Informationen finden Sie unter Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem Active Directory.
- AWS Management Console – Sie können AD Connector verwenden, um AWS Management Console-Benutzer über ihre Active-Directory-Anmeldeinformationen zu authentifizieren, ohne eine SAML-Infrastruktur einrichten zu müssen. Weitere Informationen finden Sie unter Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren.
- Amazon QuickSight — Weitere Informationen finden Sie unter Benutzerkonten in der Amazon QuickSight Enterprise Edition verwalten.
- AWS IAM Identity Center – Ausführliche Anweisungen finden Sie unter IAM Identity Center mit einem On-Premises-Active-Directory verbinden.
- AWS Transfer Family – Eine ausführliche Anleitung finden Sie unter Arbeiten mit AWS Directory Service für Microsoft Active Directory.
- AWS Client VPN – Detaillierte Anweisungen finden Sie unter Client-Authentifizierung und -Autorisierung.
- Amazon WorkDocs — Ausführliche Anweisungen finden Sie unter Herstellen einer Verbindung zu Ihrem lokalen Verzeichnis mit AD Connector.
- Amazon WorkMail — Eine ausführliche Anleitung finden Sie unter Amazon WorkMail in ein vorhandenes Verzeichnis integrieren (Standardkonfiguration).
- WorkSpaces — Ausführliche Anweisungen finden Sie unter Starten eines WorkSpace mit AD Connector.

> **Note**
>
> Amazon RDS ist nur mit AWS Managed Microsoft AD kompatibel und nicht mit AD Connector. Weitere Informationen finden Sie im Abschnitt AWS Managed Microsoft AD auf der AWS Directory ServiceFAQ-Seite.

Fehlerbehebung in AD Connector

Im Folgenden können Sie einige häufig auftretende Probleme beheben, die bei der Erstellung oder Verwendung Ihres AD Connector auftreten können.

Themen

Probleme bei der Erstellung

Im Folgenden sind häufig auftretende Probleme bei der Erstellung von AD Connector aufgeführt

Der Fehler „Beschränktes AZ” wird angezeigt, wenn ich ein Verzeichnis erstellen will.

Einige AWS Konten, die vor 2012 erstellt wurden, haben möglicherweise Zugriff auf Availability Zones in den Regionen USA Ost (Nord-Virginia), USA West (Nordkalifornien) oder Asien-Pazifik (Tokio), die keine AWS Directory Service Verzeichnisse unterstützen. Wenn Sie beim Erstellen eines eine solche Fehlermeldung erhaltenActive Directory, wählen Sie ein Subnetz in einer anderen Availability Zone und versuchen Sie erneut, das Verzeichnis zu erstellen.

Ich erhalte die Fehlermeldung „Verbindungsprobleme erkannt“, wenn ich versuche, AD Connector zu erstellen

Wenn Sie beim Versuch, einen AD Connector zu erstellen, die Fehlermeldung „Verbindungsproblem erkannt“ erhalten, kann der Fehler auf die Portverfügbarkeit oder die Komplexität des AD Connector-Passworts zurückzuführen sein. Sie können die Verbindung Ihres AD Connectors testen, um festzustellen, ob die folgenden Anschlüsse verfügbar sind:

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

Informationen zum Testen Ihrer Verbindung finden Sie unterTesten Sie Ihren AD Connector. Der Verbindungstest sollte für die Instanz durchgeführt werden, die mit beiden Subnetzen verbunden ist, denen die IP-Adressen des AD Connectors zugeordnet sind.

Wenn der Verbindungstest erfolgreich ist und die Instanz der Domäne beitritt, überprüfen Sie das Passwort Ihres AD Connectors. AD Connector muss die Anforderungen an die AWS Passwortkomplexität erfüllen. Weitere Informationen finden Sie unter Dienstkonto unterAD-Connector-Voraussetzungen.

Wenn Ihr AD Connector diese Anforderungen nicht erfüllt, erstellen Sie Ihren AD Connector mit einem Passwort, das diesen Anforderungen entspricht, neu.

Probleme mit der Verbindung

Im Folgenden sind häufig auftretende Verbindungsprobleme für AD Connector aufgeführt

- Ich erhalte die Fehlermeldung „Connectivity issues detected“, wenn ich eine Verbindung zu meinem On-Premises-Verzeichnis herstellen möchte
- Ich erhalte die Fehlermeldung „DNS unavailable“, wenn ich eine Verbindung zu meinem On-Premises-Verzeichnis herstellen möchte
- Ich erhalte die Fehlermeldung „SRV record“, wenn ich eine Verbindung zu meinem On-Premises-Verzeichnis herstellen möchte

Ich erhalte die Fehlermeldung „Connectivity issues detected“, wenn ich eine Verbindung zu meinem On-Premises-Verzeichnis herstellen möchte

Sie erhalten eine Fehlermeldung ähnlich der Folgenden, wenn Sie eine Verbindung zu Ihrem On-Premises-Verzeichnis herstellen möchten:

```
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 muss mit Ihren On-Premises-Domain-Controllern via TCP und UDP über folgende Ports kommunizieren können. Überprüfen Sie, ob Ihre Sicherheitsgruppen und On-Premises-Firewalls die TCP- und UDP-Kommunikation über diese Ports erlauben. Weitere Informationen finden Sie unter AD-Connector-Voraussetzungen.

- 88 (Kerberos)
- 389 (LDAP)

Je nach Bedarf benötigen Sie möglicherweise zusätzliche TCP/UDP-Ports. In der folgenden Liste finden Sie einige dieser Ports. Weitere Informationen zu den von Active Directory verwendeten Ports finden Sie in der Microsoft Dokumentation So konfigurieren Sie eine Firewall für Active Directory Domänen und Vertrauensstellungen.

- 135 (RPC Endpoint Mapper)
- 646 (LDAP-SSL)
- 3268 (LDAP-GC)
- 3269 (LDAP-GC-SSL)

Ich erhalte die Fehlermeldung „DNS unavailable“, wenn ich eine Verbindung zu meinem On-Premises-Verzeichnis herstellen möchte

Sie erhalten eine Fehlermeldung ähnlich der Folgenden, wenn Sie eine Verbindung zu Ihrem On-Premises-Verzeichnis herstellen möchten:

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector muss über TCP und UDP über Port 53 mit Ihrem On-Premises-DNS-Server kommunizieren können. Stellen Sie sicher, dass Ihre Sicherheitsgruppen und On-Premises-Firewalls die TCP- und UDP-Kommunikation über diesen Port erlauben. Weitere Informationen finden Sie unter AD-Connector-Voraussetzungen.

Ich erhalte die Fehlermeldung „SRV record“, wenn ich eine Verbindung zu meinem On-Premises-Verzeichnis herstellen möchte

Sie erhalten eine Fehlermeldung ähnlich einer oder mehr der Folgenden, wenn Sie eine Verbindung zu Ihrem On-Premises-Verzeichnis herstellen möchten:

```
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 muss beim Aufbau einer Verbindung zu Ihrem Verzeichnis SRV-Datensätze für `_ldap._tcp.<DnsDomainName>` und `_kerberos._tcp.<DnsDomainName>` abrufen. Sie erhalten diese Fehlermeldung, wenn der Service diese Datensätze nicht von den DNS-Servern abrufen kann, die Sie beim Aufbau einer Verbindung zu ihrem Verzeichnis angegeben haben. Weitere Informationen zu diesen SRV-Datensätzen finden Sie unter SRV record requirements.

Probleme mit der Authentifizierung

Hier sind einige häufig auftretende Authentifizierungsprobleme mit AD Connector:

- Ich erhalte die Fehlermeldung „Die Zertifikatsüberprüfung ist fehlgeschlagen“, wenn ich versuche, mich Amazon WorkSpaces mit einer Smartcard anzumelden
- Der Fehler „Ungültige Anmeldeinformationen” wird angezeigt, wenn das von AD Connector verwendete Servicekonto versucht, sich zu authentifizieren
- Ich erhalte die Fehlermeldung „Authentifizierung nicht möglich“, wenn ich AWS Anwendungen für die Suche nach Benutzern oder Gruppen verwende
- Ich erhalte eine Fehlermeldung zu meinen Verzeichnisanmeldedaten, wenn ich versuche, das AD Connector Connector-Dienstkonto zu aktualisieren
- Einige meiner Benutzer können sich in meinem Verzeichnis nicht authentifizieren.

Ich erhalte die Fehlermeldung „Die Zertifikatsüberprüfung ist fehlgeschlagen“, wenn ich versuche, mich Amazon WorkSpaces mit einer Smartcard anzumelden

Sie erhalten eine Fehlermeldung ähnlich der folgenden, wenn Sie versuchen, sich WorkSpaces mit einer Smartcard bei Ihrem anzumelden:

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

Der Fehler tritt auf, wenn das Zertifikat der Smartcard nicht ordnungsgemäß auf dem Client gespeichert ist, der die Zertifikate verwendet. Weitere Informationen zu AD Connector- und Smartcard-Anforderungen finden Sie unterVoraussetzungen.

Gehen Sie wie folgt vor, um Probleme mit der Smartcard zu beheben, Zertifikate im Zertifikatsspeicher des Benutzers zu speichern:

1. Greifen Sie auf dem Gerät, das Probleme beim Zugriff auf die Zertifikate hat, auf die Microsoft Management Console (MMC) zu.

   > **Important**
   >
   > Bevor Sie fortfahren, erstellen Sie eine Kopie des Smartcard-Zertifikats.

2. Navigieren Sie zum Zertifikatsspeicher in der MMC. Löschen Sie das Smartcard-Zertifikat des Benutzers aus dem Zertifikatsspeicher. Weitere Informationen zum Anzeigen des Zertifikatsspeichers in der MMC finden Sie in der Dokumentation unter Vorgehensweise: Anzeigen von Zertifikaten mit dem MMC-Snap-In. Microsoft
3. Entfernen Sie die Smartcard.
4. Setzen Sie die Smartcard erneut ein, damit sie das Smartcard-Zertifikat im Zertifikatsspeicher des Benutzers erneut auffüllen kann.

   > **Warning**
   >
   > Wenn die Smartcard das Zertifikat nicht erneut im Benutzerspeicher auffüllt, kann sie nicht für die Smartcard-Authentifizierung verwendet werden. WorkSpaces

Das Dienstkonto des AD Connectors sollte über Folgendes verfügen:

- `my/spn`zum Namen des Dienstprinzips hinzugefügt
- Delegiert für den LDAP-Dienst

Nach dem erneuten Auffüllen des Zertifikats auf der Smartcard sollte der lokale Domänencontroller daraufhin überprüft werden, ob die Zuordnung des Benutzerprinzipalnamens (UPN) für den alternativen Betreffnamen gesperrt ist. Weitere Informationen zu dieser Änderung finden Sie in der Dokumentation unter So deaktivieren Sie den alternativen Betreffnamen für die UPN-Zuordnung. Microsoft

Gehen Sie wie folgt vor, um den Registrierungsschlüssel Ihres Domänencontrollers zu überprüfen:

1. Navigieren Sie im Registrierungseditor zum folgenden Hive-Schlüssel

   HKEY_LOCAL_MACHINE\ SYSTEM\\ Services\ Kdc\ CurrentControlSet UseSubjectAltName
2. Select UseSubjectAltName. Stellen Sie sicher, dass der Wert auf 0 gesetzt ist.

> **Note**
>
> Wenn der Registrierungsschlüssel auf den lokalen Domänencontrollern festgelegt ist, kann der AD Connector die Benutzer nicht finden Active Directory und es wird die obige Fehlermeldung angezeigt.

Die Zertifikate der Zertifizierungsstelle (CA) sollten auf das AD Connector-Smartcard-Zertifikat hochgeladen werden. Das Zertifikat sollte OCSP-Informationen enthalten. Im Folgenden sind zusätzliche Anforderungen für die CA aufgeführt:

- Das Zertifikat sollte sich in der vertrauenswürdigen Stammzertifizierungsstelle des Domänencontrollers, des Zertifizierungsstellenservers und des befinden WorkSpaces.
- Offline- und Root-CA-Zertifikate enthalten keine OSCP-Informationen. Diese Zertifikate enthalten Informationen über ihren Widerruf.
- Wenn Sie ein Zertifizierungsstellenzertifikat eines Drittanbieters für die Smartcard-Authentifizierung verwenden, müssen die Zertifizierungsstelle und die Zwischenzertifikate im Active Directory NTAuth Store veröffentlicht werden. Sie müssen in der vertrauenswürdigen Stammzertifizierungsstelle für alle Domänencontroller, Zertifizierungsstellenserver und installiert sein. WorkSpaces

- Sie können den folgenden Befehl verwenden, um Zertifikate im Active Directory NTAuth Store zu veröffentlichen:

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

Weitere Informationen zum Veröffentlichen von Zertifikaten im NTauth-Speicher finden Sie unter Import des ausstellenden CA-Zertifikats in den Enterprise NTauth-Speicher im Access Amazon WorkSpaces with Common Access Cards Installation Guide.

Gehen Sie wie folgt vor, um zu überprüfen, ob das Benutzerzertifikat oder die CA-Kettenzertifikate von OCSP verifiziert wurden:

1. Exportieren Sie das Smartcard-Zertifikat an einen Speicherort auf dem lokalen Computer, z. B. auf Laufwerk C:.
2. Öffnen Sie eine Befehlszeilenaufforderung und navigieren Sie zu dem Speicherort, an dem das exportierte Smartcard-Zertifikat gespeichert ist.
3. Geben Sie den folgenden Befehl ein:

```
certutil -URL Certficate_name.cer
```

4. Nach dem Befehl sollte ein Popup-Fenster angezeigt werden. Wählen Sie die Option OCSP in der rechten Ecke und wählen Sie Abrufen. Der Status sollte wieder als verifiziert angezeigt werden.

Weitere Informationen zum Befehl certutil finden Sie in der Dokumentation unter certutil Microsoft

Der Fehler „Ungültige Anmeldeinformationen” wird angezeigt, wenn das von AD Connector verwendete Servicekonto versucht, sich zu authentifizieren

Das kann passieren, wenn die Festplatte auf Ihrem Domain-Controller nicht mehr über genügend Speicherplatz verfügt. Stellen Sie sicher, dass Ihre Domain-Controller-Festplatten nicht voll sind.

Ich erhalte die Fehlermeldung „Authentifizierung nicht möglich“, wenn ich AWS Anwendungen für die Suche nach Benutzern oder Gruppen verwende

Bei der Suche nach Benutzern während der Verwendung von AWS Anwendungen wie Amazon WorkSpaces oder Amazon können Fehler auftreten QuickSight, auch wenn der AD Connector

Connector-Status aktiv war. Abgelaufene Anmeldeinformationen können AD Connector daran hindern, Abfragen von Objekten in Ihrem Active Directory durchzuführen. Aktualisieren Sie das Passwort für das Servicekonto anhand der unter angegebenen SchritteDer nahtlose Domänenbeitritt für Amazon EC2 EC2-Instances funktioniert nicht mehr.

Ich erhalte eine Fehlermeldung zu meinen Verzeichnisanmeldedaten, wenn ich versuche, das AD Connector Connector-Dienstkonto zu aktualisieren

Sie erhalten eine Fehlermeldung, die einer oder mehreren der folgenden ähnelt, wenn Sie versuchen, das AD Connector Connector-Dienstkonto zu aktualisieren:

```
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
```

Möglicherweise liegt ein Problem mit der Zeitsynchronisierung und Kerberos vor. AD Connector sendet Kerberos-Authentifizierungsanforderungen an. Active Directory Diese Anfragen sind zeitkritisch, und wenn die Anfragen verzögert werden, schlagen sie fehl. Informationen zur Behebung dieses Problems finden Sie in der Dokumentation Empfehlung — Konfiguration des Root-PDC mit einer autoritativen Zeitquelle und Vermeidung von weit verbreitetem Zeitversatz. Microsoft Weitere Informationen zu Zeitdienst und Synchronisation finden Sie unten:

- Wie funktioniert der Windows Time Service
- Maximale Toleranz für die Synchronisation der Computeruhr
- WindowsTools und Einstellungen für den Zeitservice

Einige meiner Benutzer können sich in meinem Verzeichnis nicht authentifizieren.

Für Ihre Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Dies ist die Standardeinstellung für neue Benutzerkonten und sie sollte nicht geändert werden. Weitere Informationen zu dieser Einstellung finden Sie unter Vorauthentifizierung auf Microsoft TechNet.

Probleme mit der Wartung

Im Folgenden sind häufig auftretende Wartungsprobleme für AD Connector aufgeführt

- Mein Verzeichnis bleibt dauerhaft im Status „Angefragt”.
- Der nahtlose Domänenbeitritt für Amazon EC2 EC2-Instances funktioniert nicht mehr

Mein Verzeichnis bleibt dauerhaft im Status „Angefragt”.

Wenn sich Ihr Verzeichnis länger als fünf Minuten im „Angefragt”-Status befindet, löschen Sie das Verzeichnis und erstellen es neu. Wenn dieses Problem weiterhin besteht, wenden Sie sich an den AWS Support.

Der nahtlose Domänenbeitritt für Amazon EC2 EC2-Instances funktioniert nicht mehr

Wenn eine zuvor funktionierende nahtlose Domainverbindung für EC2-Instances bei aktivem AD Connector nicht mehr funktioniert, sind die Anmeldeinformationen für Ihr AD-Connector-Servicekonto möglicherweise abgelaufen. Abgelaufene Anmeldeinformationen können verhindern, dass AD Connector Computerobjekte in Ihrem erstelltActive Directory.

Um dieses Problem zu beheben, aktualisieren Sie die Passwörter des Service-Kontos in der folgenden Reihenfolge, damit die Passwörter übereinstimmen:

1. Aktualisieren Sie das Passwort für das Dienstkonto in IhremActive Directory.
2. Aktualisieren Sie das Passwort für das Dienstkonto in Ihrem AD Connector in AWS Directory Service. Weitere Informationen finden Sie unter Ihre Anmeldeinformationen für Ihr AD-Connector-Servicekonto in AWS Directory Service aktualisieren.

> **Important**
>
> Wenn Sie das Passwort nur in aktualisieren, wird die Passwortänderung AWS Directory Service nicht auf Ihr vorhandenes lokales System übertragen. Active Directory Daher ist es

wichtig, dass Sie die Änderung in der Reihenfolge vornehmen, die im vorherigen Verfahren angegeben wurde.

Ich kann meinen AD Connector nicht löschen

Wenn Ihr AD Connector in einen funktionsunfähigen Zustand wechselt, haben Sie keinen Zugriff mehr auf Ihre Domain-Controller. Wir blockieren das Löschen eines AD Connector, wenn noch Anwendungen damit verknüpft sind, da eine dieser Anwendungen das Verzeichnis möglicherweise immer noch verwendet. Eine Liste der Anwendungen, die Sie deaktivieren müssen, um Ihren AD Connector zu löschen, finden Sie unterIhr AD Connector löschen. Wenn Sie Ihren AD Connector immer noch nicht löschen können, können Sie hier Hilfe anfordern AWS Support.

Simple AD

Simple AD ist ein eigenständig verwaltetes Verzeichnis auf einem Samba 4 Active Directory kompatiblen Server. Es ist in zwei Größen erhältlich.

- Klein – Unterstützt bis zu 500 Benutzer (ungefähr 2.000 Objekte einschließlich Benutzern, Gruppen und Computern).
- Groß – Unterstützt bis zu 5.000 Benutzer (ungefähr 20.000 Objekte einschließlich Benutzern, Gruppen und Computern).

Simple AD bietet einen Teil der Funktionen von AWS Managed Microsoft AD, darunter die Möglichkeit, Benutzerkonten und Gruppenmitgliedschaften zu verwalten, Gruppenrichtlinien zu erstellen und anzuwenden, eine sichere Verbindung zu Amazon EC2 EC2-Instances herzustellen und Kerberos-basiertes Single Sign-On (SSO) bereitzustellen. Beachten Sie jedoch, dass Simple AD Funktionen wie Multi-Faktor-Authentifizierung (MFA), Vertrauensstellungen mit anderen Domänen, Active Directory-Verwaltungscenter, PowerShell Support, Active Directory-Papierkorb, gruppenverwaltete Dienstkonten und Schemaerweiterungen für POSIX- und Microsoft-Anwendungen nicht unterstützt.

Simple AD bietet viele Vorteile:

- Simple AD erleichtert die Verwaltung von Amazon EC2-Instances, auf denen Linux und Windows ausgeführt werden, und die Bereitstellung von Windows-Anwendungen in der AWS Cloud.
- Viele der Anwendungen und Tools, die Sie heutzutage benutzen und die den Microsoft Active Directory-Support erfordern, können mit Simple AD verwendet werden.
- Benutzerkonten in Simple AD ermöglichen den Zugriff auf AWS Anwendungen wie WorkSpaces Amazon WorkDocs oder Amazon WorkMail.
- Sie können AWS Ressourcen über den rollenbasierten IAM-Zugriff auf die verwalten. AWS Management Console
- Tägliche automatische Snapshots ermöglichen die Wiederherstellung. point-in-time

Simple AD unterstützt Folgendes nicht:

- Amazon AppStream 2.0
- Amazon Chime

- Amazon RDS für SQL Server
- Amazon RDS für Oracle
- AWS IAM Identity Center
- Vertrauensstellungen mit anderen Domain
- Active Directory Administrative Center
- PowerShell
- Active Directory-Papierkorb
- Gruppenverwaltete Service-Konten
- Schemaerweiterungen für POSIX und Microsoft-Anwendungen

Lesen Sie die Themen in diesem Abschnitt, um zu erfahren, wie Sie Ihr eigenes Simple AD erstellen.

Themen

Erste Schritte mit Simple AD

Simple AD erstellt ein vollständig verwaltetes, Samba-basiertes Verzeichnis in der AWS Cloud. Wenn Sie ein Verzeichnis mit Simple AD erstellen, AWS Directory Service erstellt in Ihrem Namen zwei Domänencontroller und DNS-Server. Die Domain-Controller werden in verschiedenen Subnetzen in einer Amazon VPC erstellt. Durch diese Redundanz wird sichergestellt, dass Ihr Verzeichnis auch bei einem Ausfall zugänglich bleibt.

Themen

- DNS für Simple AD konfigurieren

Simple-AD-Voraussetzungen

Um ein Simple AD zu erstellenActive Directory, benötigen Sie eine Amazon-VPC mit den folgenden Komponenten:

- Die VPC muss über Standard-Hardware-Tenancy verfügen.
- Die VPC darf nicht mit den folgenden VPC-Endpunkten konfiguriert sein:
  - Route53-VPC-Endpunkte, die bedingte DNS-Überschreibungen für *.amazonaws.com enthalten, die in nicht öffentliche IP-Adressen aufgelöst werden AWS
  - CloudWatch VPC-Endpunkt
  - Systems-Manager-VPC-Endpunkt
  - VPC-Endpunkt des Security Token Service
- Mindestens zwei Subnetze in zwei verschiedenen Availability Zones. Die Subnetze müssen sich im gleichen CIDR-Bereich (Classless Inter-Domain Routing) befinden. Wenn Sie die VPC für Ihr Verzeichnis erweitern oder die Größe ändern wollen, stellen Sie sicher, dass beide Domain-Controller-Subnetze für den erweiterten VPC CIDR-Bereich ausgewählt sind. Wenn Sie ein Simple AD erstellen, AWS Directory Service erstellt es in Ihrem Namen zwei Domänencontroller und DNS-Server.
  - Weitere Informationen zum CIDR-Bereich finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze im Amazon VPC-Benutzerhandbuch.
- Wenn Sie LDAPS-Unterstützung mit Simple AD benötigen, empfehlen wir Ihnen, diese über einen Network Load Balancer zu konfigurieren, der mit Port 389 verbunden ist. Dieses Modell ermöglicht es Ihnen, ein leistungsstarkes Zertifikat für die LDAPS-Verbindung zu verwenden, den Zugriff auf LDAPS über eine einzelne NLB-IP-Adresse zu vereinfachen und einen automatischen Failover über den NLB durchzuführen. Simple AD unterstützt die Verwendung von selbstsignierten Zertifikaten an Port 636 nicht. Weitere Informationen zum Konfigurieren von LDAPS mit Simple AD finden Sie unter So konfigurieren Sie einen LDAPS-Endpunkt für Simple AD im AWS -Blog zur Sicherheit.
- Die folgenden Verschlüsselungstypen müssen in dem Verzeichnis aktiviert werden:
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1
  - AES256_HMAC_SHA1

- Zukünftige Verschlüsselungstypen

> **Note**
>
> Wenn diese Verschlüsselungstypen deaktiviert werden, kann dies zu Kommunikationsproblemen mit RSAT (Remote Server Administration Tools) und zu Auswirkungen auf die Verfügbarkeit oder Ihr Verzeichnis führen.

- Weitere Informationen finden Sie unter Was ist Amazon VPC? im Amazon VPC-Benutzerhandbuch.

AWS Directory Service verwendet eine Struktur mit zwei VPCs. Die EC2-Instances, aus denen Ihr Verzeichnis besteht, laufen außerhalb Ihres AWS Kontos und werden von verwaltet. AWS Sie haben zwei Netzwerkadapter `ETH0` und `ETH1`. `ETH0` ist der Verwaltungsadapter und existiert außerhalb Ihres Kontos. `ETH1` wird in Ihrem Konto erstellt.

Der Management-IP-Bereich des `ETH0`-Netzwerks Ihres Verzeichnisses wird programmatisch ausgewählt, um sicherzustellen, dass er nicht mit der VPC kollidiert, in der Ihr Verzeichnis bereitgestellt wird. Dieser IP-Bereich kann sich in einem der folgenden Paare befinden (da Verzeichnisse in zwei Subnetzen ausgeführt werden):

- 10.0.1.0/24 und 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 und 192.168.2.0/24

Wir vermeiden Konflikte, indem wir das erste Oktett des `ETH1`-CIDR überprüfen. Wenn es mit einer 10 beginnt, dann wählen wir eine 192.168.0.0/16 VPC mit den Subnetzen 192.168.1.0/24 und 192.168.2.0/24. Wenn das erste Oktett etwas anderes als eine 10 ist, wählen wir eine 10.0.0.0/16 VPC mit den Subnetzen 10.0.1.0/24 und 10.0.2.0/24.

Der Auswahlalgorithmus berücksichtigt nicht die Routen auf Ihrer VPC. Es ist daher möglich, dass dieses Szenario zu einem IP-Routing-Konflikt führt.

Erstellen Sie Ihr Simple AD Active Directory

Gehen Sie wie folgt vorActive Directory, um ein neues Simple AD zu erstellen. Bevor Sie dieses Verfahren beginnen, stellen Sie sicher, dass Sie die in Simple-AD-Voraussetzungen angegebenen Voraussetzungen erfüllt haben.

So erstellen Sie ein Simple AD Active Directory

1. Wählen Sie im Navigationsbereich AWS Directory Service -Konsole den Eintrag Verzeichnisse und wählen Sie Verzeichnis einrichten aus.
2. Wählen Sie auf der Seite Verzeichnistyp auswählen die Option Simple AD aus und klicken Sie dann auf Weiter.
3. Geben Sie auf der Seite Enter directory information (Verzeichnisinformationen eingeben) die folgenden Informationen ein:

   Verzeichnisgröße

   Wählen Sie die Größenoption Small (Klein) oder Large (Groß). Weitere Informationen über Größen finden Sie unter Simple AD.

   Name der Organisation

   Ein eindeutiger Organisationsname für Ihr Verzeichnis, der für die Registrierung von Client-Geräten verwendet wird.

   Dieses Feld ist nur verfügbar, wenn Sie Ihr Verzeichnis im Rahmen des Starts erstellen WorkSpaces.

   DNS-Name des Verzeichnisses

   Den vollständig qualifizierten Namen für das Verzeichnis, z. B. `corp.example.com`.

   NetBIOS-Name des Verzeichnisses

   Die kurzen Namen für das Verzeichnis, z. B. `CORP`.

   Administrator password

   Das Passwort für den Verzeichnisadministrator. Mit der Verzeichniserstellung wird ein Administratorkonto mit dem Benutzernamen `Administrator` und diesem Passwort angelegt.

   Das Verzeichnisadministrator-Passwort unterscheidet zwischen Groß-/ Kleinschreibung und muss zwischen 8 und 64 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:

   - Kleinbuchstaben (a – z)
   - Großbuchstaben (A – Z)
   - Zahlen (0 – 9)

- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password (Passwort bestätigen)

Geben Sie das Administratorpasswort erneut ein.

Verzeichnisbeschreibung

Eine optionale Beschreibung des Verzeichnisses.

4. Geben Sie auf der Seite Choose VPC and subnets (VPC und Subnetze wählen) die folgenden Informationen an und wählen Sie dann Next (Weiter).

   VPC

   Die VPC für das Verzeichnis.

   Subnets

   Wählen Sie Subnetze für die Domain-Controller aus. Die beiden Subnetze müssen zu verschiedenen Availability-Zonen gehören.

5. Überprüfen Sie auf der Seite Review & create (Überprüfen und erstellen) die Verzeichnisinformationen und nehmen Sie gegebenenfalls Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen). Es dauert einige Minuten, bis das Verzeichnis erstellt wurde. Sobald sie erstellt wurden, ändert sich der Status in Active.

Was wird mit Ihrem Simple AD erstellt Active Directory

Wenn Sie eine Active Directory mit Simple AD erstellen, AWS Directory Service führt sie in Ihrem Namen die folgenden Aufgaben aus:

- Installiert ein Samba-basiertes Verzeichnis in der VPC.
- Erstellt ein Konto für den Verzeichnisadministrator mit dem Benutzernamen `Administrator` und dem angegebenen Passwort. Mit diesem Konto verwalten Sie das Verzeichnis.

> **Important**
>
> Achten Sie darauf, dieses Passwort zu speichern. AWS Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen werden. Sie können ein Passwort

jedoch über die AWS Directory Service Konsole oder mithilfe der ResetUserPasswordAPI zurücksetzen.

- Erstellt eine Sicherheitsgruppe für die Verzeichniscontroller.
- Erstellt ein Konto mit dem Namen `AWSAdminD-xxxxxxxx`, das Domain-Administrator-Berechtigungen hat. Dieses Konto wird von verwendet AWS Directory Service , um automatisierte Vorgänge zur Verzeichnisverwaltung durchzuführen, z. B. das Erstellen von Verzeichnis-Snapshots und FSMO-Rollenübertragungen. Die Anmeldeinformationen für dieses Konto werden von AWS Directory Service sicher gespeichert.
- Erstellt automatisch eine Elastic-Network-Schnittstelle (ENI) und ordnet sie jedem Ihrer Domain-Controller zu. Jede dieser ENIs ist für die Konnektivität zwischen Ihrer VPC und den AWS Directory Service Domänencontrollern unerlässlich und sollte niemals gelöscht werden. Sie können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, AWS Directory Service anhand der Beschreibung identifizieren: "Die Netzwerkschnittstelle wurde für die Verzeichnis-ID AWS erstellt“. Weitere Informationen finden Sie unter Elastic Network Interfaces im Amazon EC2 EC2-Benutzerhandbuch. Der Standard-DNS-Server von AWS Managed Microsoft AD Active Directory ist der VPC-DNS-Server bei Classless Inter-Domain Routing (CIDR) +2. Weitere Informationen finden Sie unter Amazon DNS-Server im Amazon VPC-Benutzerhandbuch.

> **Note**
>
> Domain-Controller werden standardmäßig in zwei Availability Zones in einer Region eingesetzt und mit Ihrer Amazon Virtual Private Cloud (VPC) verbunden. Backups werden automatisch einmal pro Tag erstellt, und die Volumes des Amazon Elastic Block Store (EBS) sind verschlüsselt, um sicherzustellen, dass die Daten im Ruhezustand sicher sind. Domain-Controller, die ausfallen, werden automatisch in derselben Availability Zone unter Verwendung derselben IP-Adresse ersetzt, und eine vollständige Notfallwiederherstellung kann unter Verwendung des letzten Backups durchgeführt werden.

DNS für Simple AD konfigurieren

Simple AD leitet DNS-Anfragen an die IP-Adresse des von Amazon bereitgestellten DNS-Servers für Ihre VPC weiter. Diese DNS-Server lösen Namen auf, die in Ihren Amazon Route 53 privat gehosteten Zonen konfiguriert sind. Indem Sie Ihre On-Premises-Computer auf Ihr Simple AD verweisen, können Sie nun DNS-Anfragen in der privaten gehosteten Zone auflösen. Weitere Informationen zu Route 53 finden Sie unter Was ist Route 53.

Beachten Sie, dass für die Bereitstellung Ihrer Simple AD, um externe DNS-Abfragen zu beantworten, die Netzwerk-Zugriffssteuerungsliste (ACL) für die VPC mit Ihrer Simple AD so konfiguriert sein muss, dass Datenverkehr von außerhalb der VPC zugelassen wird.

- Wenn Sie nicht Route 53 privat gehostete Zonen verwenden, werden Ihre DNS-Anfragen zu öffentlichen DNS-Servern weitergeleitet.
- Wenn Sie benutzerdefinierte DNS-Server verwenden, die außerhalb Ihrer VPC liegen, und private DNS verwenden möchten, müssen Sie neu konfigurieren, um benutzerdefinierte DNS-Server auf EC2-Instances innerhalb Ihrer VPC zu verwenden. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen.
- Wenn Sie möchten, dass Ihr Simple AD Namen mit DNS-Servern innerhalb Ihrer VPC und privaten DNS-Servern außerhalb Ihrer VPC auflöst, verwenden Sie hierzu einen DHCP-Optionssatz. Ein detailliertes Beispiel finden Sie in diesem Artikel.

> **Note**
>
> Dynamische DNS-Aktualisierungen werden von Simple-AD-Domains nicht unterstützt. Stattdessen können Sie die Änderungen direkt vornehmen, indem Sie Ihr Verzeichnis per DNS-Manager mit einer Instance verbinden, die Ihrer Domain zugeordnet ist.

So verwalten Sie Simple AD

In diesem Abschnitt werden alle Verfahren für die Ausführung und Verwaltung einer Simple-AD-Umgebung aufgeführt.

Themen

- Benutzer und Gruppen in Simple AD verwalten
- Ihr Simple-AD-Verzeichnis überwachen
- Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem Simple AD Active Directory
- Ihr Simple-AD-Verzeichnisses verwalten
- Aktivieren des Zugriffs auf AWS Anwendungen und Services
- Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren

Benutzer und Gruppen in Simple AD verwalten

„Benutzer“ sind Einzelpersonen oder Entitäten, die Zugriff auf Ihr Verzeichnis haben. Gruppen sind sehr nützlich, um Berechtigungen zu erteilen oder zu verweigern, anstatt diese Berechtigungen für jeden einzelnen Benutzer erstellen zu müssen. Wenn ein Benutzer zu einer anderen Organisation wechselt, verschieben Sie diesen Benutzer in eine andere Gruppe. Er erhält dann automatisch die Berechtigungen für die neue Organisation.

Um Benutzer und Gruppen in einem AWS Directory Service-Verzeichnis zu erstellen, müssen Sie eine beliebige Instance (entweder On-Premises oder EC2) verwenden, die mit Ihrem AWS Directory Service-Verzeichnis verbunden wurde, und als Benutzer angemeldet sein, der die Berechtigung hat, Benutzer und Gruppen zu erstellen. Sie müssen außerdem die Active-Directory-Tools auf Ihrer EC2-Instance installieren, sodass Sie Ihre Benutzer und Gruppen mit dem Active-Directory-Snap-in Benutzer und Computer hinzufügen können. Weitere Informationen zum Einrichten einer EC2-Instance und zum Installieren der notwendigen Tools finden Sie unter Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem Simple AD Active Directory.

> **Note**
>
> Für Ihre Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Dies ist die Standardeinstellung für neue Benutzerkonten und sie sollte nicht geändert werden. Weitere Informationen zu dieser Einstellung finden Sie unter Vorauthentifizierung auf Microsoft TechNet.

Im Folgenden erfahren Sie, wie Sie Benutzer und Gruppen erstellen und verwalten.

Themen

Installieren Sie die Active Directory-Verwaltungstools für Simple AD

Um Ihr Active Directory von einer Amazon EC2 Windows Server-Instance aus zu verwalten, müssen Sie die Active Directory Domain Services und Active Directory Lightweight Directory Services Tools auf der Instance installieren. Verwenden Sie das folgende Verfahren, um diese Tools auf einer EC2 Windows Server-Instance zu installieren.

Voraussetzungen

Bevor Sie mit diesem Verfahren beginnen können, gehen Sie wie folgt vor:

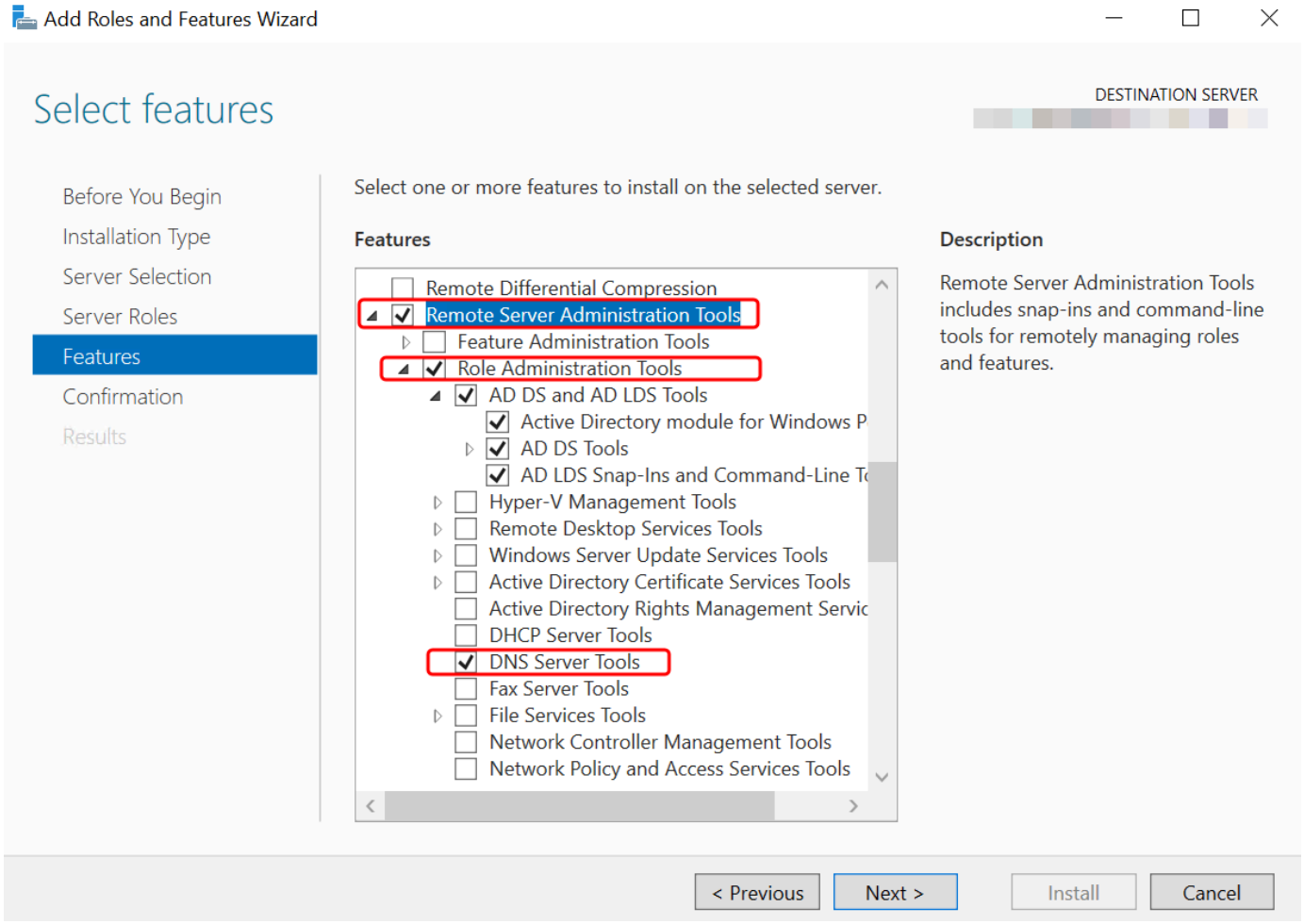
1. Erstellen Sie ein Simple AD Active Directory. Weitere Informationen finden Sie unter Erstellen Sie Ihr Simple AD Active Directory.
2. Starten Sie eine EC2 Windows Server-Instance und fügen Sie sie Ihrem Simple AD Active Directory hinzu. Die EC2-Instance benötigt die folgenden Richtlinien, um Benutzer und Gruppen zu erstellen: **`AWSSSMManagedInstanceCore`** und. **`AmazonSSMDirectoryServiceAccess`** Weitere Informationen finden Sie unter Fügen Sie eine Amazon EC2 Windows-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu.
3. Sie benötigen die Anmeldeinformationen für Ihren Active Directory-Domänenadministrator. Diese Anmeldeinformationen wurden bei der Erstellung des Simple AD erstellt. Wenn Sie das Verfahren unter befolgt habenErstellen Sie Ihr Simple AD Active Directory, enthält Ihr Administrator-Benutzername Ihren NetBIOS-Namen,**`corp\administrator`**.

Installieren Sie die Active Directory-Verwaltungstools auf der EC2 Windows Server-Instanz

Um die Active Directory-Verwaltungstools auf einer EC2 Windows Server-Instanz zu installieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Amazon-EC2-Konsole die Option Instances, wählen Sie die zuvor erstellte Windows-Server-Instance und wählen Sie dann Verbinden.
3. Wählen Sie auf der Seite Mit Instance verbinden die Option RDP-Client aus.
4. Wählen Sie auf der Registerkarte RDP-Client die Option Remotedesktop-Datei herunterladen und anschließend Passwort abrufen, um Ihr Passwort zu erhalten.
5. Wählen Sie unter Windows-Passwort abrufen die Option Datei mit privatem Schlüssel hochladen aus. Wählen Sie die .pem private Schlüsseldatei, die der Windows-Server-Instance zugeordnet ist. Nachdem Sie die private Schlüsseldatei hochgeladen haben, wählen Sie Passwort entschlüsseln.

6. Kopieren Sie im Dialogfeld Windows-Sicherheit Ihre lokalen Administratoranmeldeinformationen für den Windows Server-Computer, um sich anzumelden. Der Benutzername kann die folgenden Formate haben: ***NetBIOS-Name*****\administrator** oder***DNS-Name*****\administrator**. Dies **corp\administrator** wäre beispielsweise der Benutzername, wenn Sie das Verfahren in befolgen würdenErstellen Sie Ihr Simple AD Active Directory.
7. Nachdem Sie sich bei der Windows Server-Instanz angemeldet haben, öffnen Sie den Server-Manager im Startmenü, indem Sie Server-Manager wählen.
8. Wählen Sie im Server-Manager-Dashboard die Option Rollen und Features hinzufügen.
9. Wählen Sie im Assistent zum Hinzufügen von Rollen und Features die Option Installationstyp und Rollenbasierte oder featurebasierte Installation aus. Klicken Sie dann auf Weiter.
10. Stellen Sie sicher, dass unter Serverauswahl der lokale Server ausgewählt ist. Wählen Sie dann im linken Navigationsbereich Features aus.
11. Wählen und öffnen Sie im Baum Features Remote Server Administration Tools, Role Administration Tools und AD DS und AD LDS Tools. Wenn AD DS- und AD LDS-Tools ausgewählt sind, werden Active DirectoryModul für Windows PowerShell, AD DS-Tools und AD LDS-Snap-Ins und Befehlszeilentools ausgewählt. Scrollen Sie nach unten und wählen Sie DNS Server Tools und dann Weiter.



12. Prüfen Sie die Informationen und klicken Sie auf Installieren. Nach Abschluss der Featureinstallation sind die Tools für Active Directory Domain Services (AD DS) und Active Directory Lightweight Directory Services (AD LDS) vom Startmenü im Ordner Verwaltungstools verfügbar.

Alternative Methode zur Installation der Active Directory-Verwaltungstools auf einer EC2-Windows-Server-Instanz

- Hier ist eine weitere Methode zur Installation der Active Directory-Verwaltungstools:
  - Sie können optional wählen, ob Sie die Active Directory-Verwaltungstools mithilfe von installieren möchtenWindows PowerShell. Beispielsweise können Sie die Active Directory-Remoteverwaltungstools von einer PowerShell Eingabeaufforderung aus mit installieren`Install-WindowsFeature RSAT-ADDS`. Weitere Informationen finden Sie unter Install- WindowsFeature auf der Microsoft-Website.

Erstellen Sie einen Simple AD AD-Benutzer

Gehen Sie wie folgt vor, um einen Benutzer mit einer Amazon EC2 EC2-Instance zu erstellen, die mit Ihrem Simple AD AD-Verzeichnis verknüpft ist. Bevor Sie Benutzer erstellen können, müssen Sie die Verfahren unter Installation der Active-Directory-Verwaltungstools abschließen.

> **Note**
>
> Wenn Sie bei der Verwendung von Simple AD ein Benutzerkonto auf einer Linux-Instance mit der Option „Änderung des Passworts bei der nächsten Anmeldung erzwingen“ erstellen, kann dieser Benutzer sein Passwort nicht sofort mit kpasswd ändern. Zur erstmaligen Änderung des Passworts muss ein Domain-Administrator das Benutzerpasswort über die Active-Directory-Verwaltungstools aktualisieren.

Sie können eine der folgenden Methoden verwenden, um einen Benutzer zu erstellen:

- Active DirectoryVerwaltungstools
- Windows PowerShell

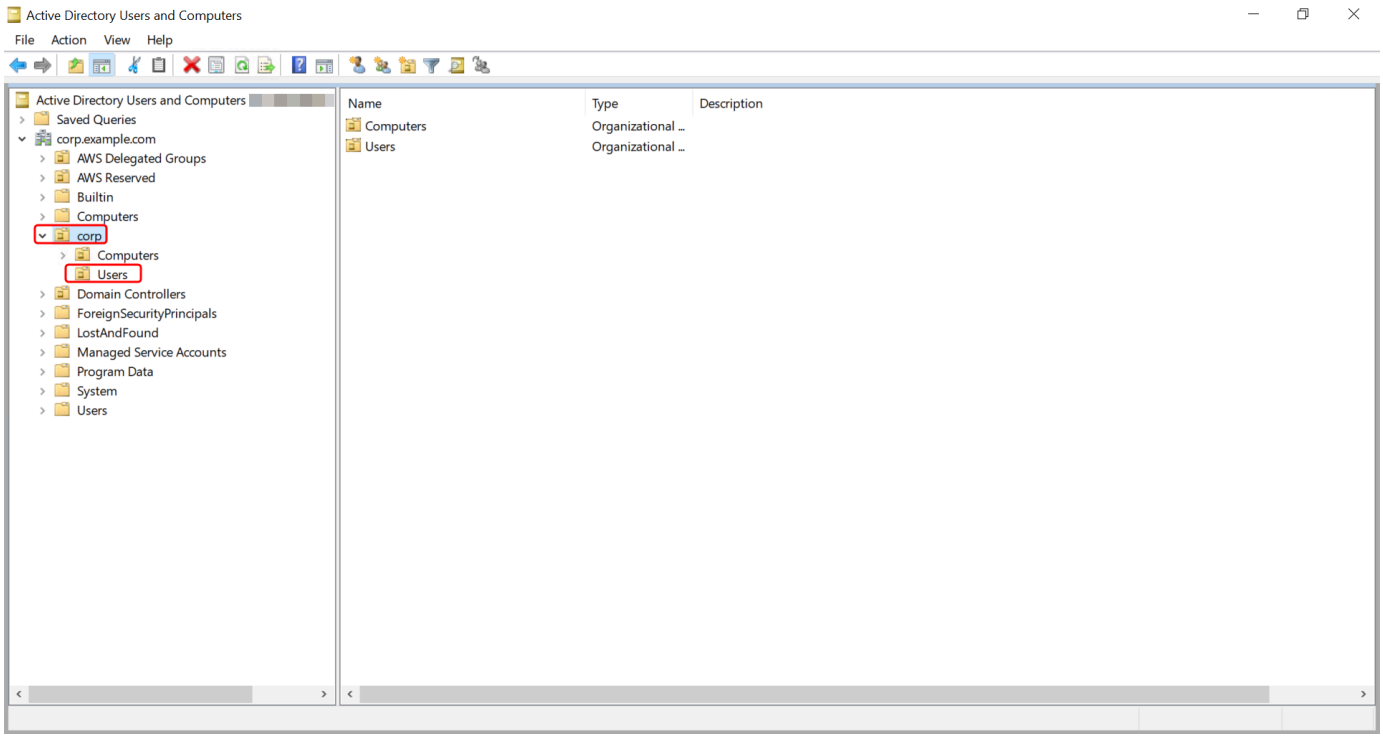
Erstellen Sie einen Benutzer mit den Active Directory Administrationstools

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool Active Directory-Benutzer und -Computer über das Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

   > **Tip**
   >
   > Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Wählen Sie in der Verzeichnisstruktur eine Organisationseinheit unter dem NetBIOS-Namen OU Ihres Verzeichnisses aus, in der Sie Ihren Benutzer speichern möchten (z. B.**`corp\Users`**).

Weitere Hinweise zur OU-Struktur, die von den Verzeichnissen in verwendet wird AWS, finden Sie unterWas wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.



4. Wählen Sie im Menü Aktionen die Option Neu und wählen Sie dann Benutzer, um den Assistenten für neue Benutzer zu öffnen.
5. Geben Sie auf der ersten Seite des Assistenten die Werte für die folgenden Felder ein und wählen Sie dann Weiter aus.
   - First name (Vorname)
   - Last name (Nachname)
   - Benutzeranmeldename
6. Geben Sie auf der zweiten Seite des Assistenten für neue Benutzer ein temporäres Passwort in Passwort und Passwort bestätigen ein. Stellen Sie sicher, dass die Option Benutzer muss Passwort bei nächster Anmeldung ändern ausgewählt ist. Keine der anderen Optionen sollte ausgewählt sein. Wählen Sie Weiter aus.
7. Überprüfen Sie auf der dritten Seite des Assistenten, ob die Informationen zum neuen Benutzer richtig sind, und klicken Sie auf Beenden. Der neue Benutzer wird im Ordner Users angezeigt.

Erstellen Sie einen Benutzer in Windows PowerShell

1. Stellen Sie als Active Directory Administrator Connect zu der Instanz her, die mit Ihrer Active Directory Domain verbunden ist.
2. Öffnen Sie Windows PowerShell.
3. Geben Sie den folgenden Befehl ein **`jane.doe`** und ersetzen Sie den Benutzernamen durch den Benutzernamen des Benutzers, den Sie erstellen möchten. Sie werden aufgefordertWindows PowerShell, ein Passwort für den neuen Benutzer einzugeben. Weitere Informationen zu den Anforderungen an die Komplexität von Active Directory Kennwörtern finden Sie in der MicrosoftDokumentation. Weitere Informationen zum Befehl New-ADUser finden Sie in der Dokumentation. Microsoft

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

Löschen Sie einen Simple AD AD-Benutzer

Gehen Sie wie folgt vor, um einen Benutzer mit einer Amazon EC2 EC2-Windows-Instance zu löschen, die mit Ihrem Simple AD AD-Verzeichnis verknüpft ist.

Sie können eine der folgenden Methoden verwenden, um einen Benutzer zu löschen:

- Active DirectoryVerwaltungstools
- Windows PowerShell

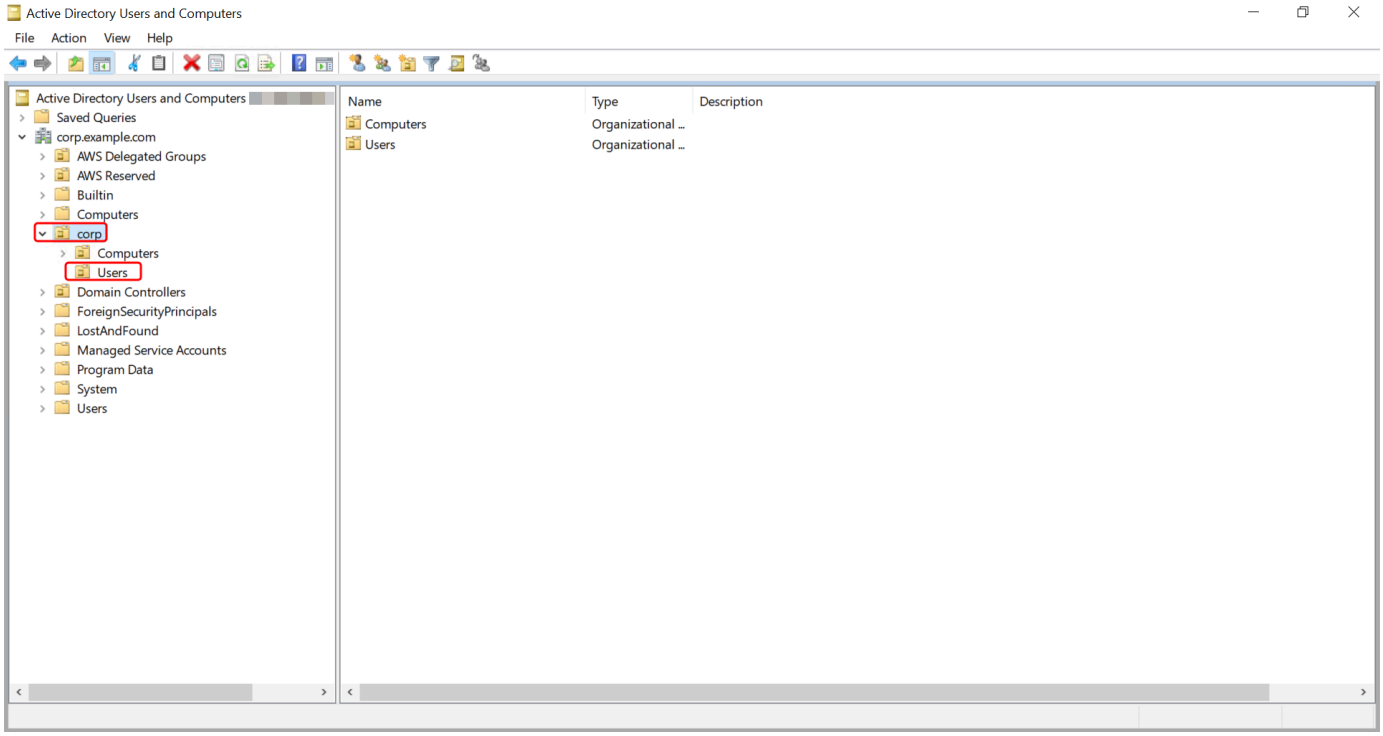
Löschen Sie einen Benutzer mit den Active Directory Administrationstools

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool „Active Directory-Benutzer und -Computer“ über das Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

> **Tip**
>
> Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.

```
%SystemRoot%\system32\dsa.msc
```

3. Wählen Sie in der Verzeichnisstruktur die Organisationseinheit aus, die den Benutzer enthält, den Sie löschen möchten (z. B.**`corp\Users`**).



4. Wählen Sie den Benutzer aus, den Sie löschen möchten. Wählen Sie im Menü Aktionen die Option Löschen.
5. Es erscheint ein Dialogfeld, in dem Sie bestätigen müssen, dass Sie den Benutzer löschen möchten. Wählen Sie Ja, um den Benutzer zu löschen. Dadurch wird der ausgewählte Benutzer dauerhaft gelöscht.

Löschen Sie einen Benutzer in Windows PowerShell

1. Stellen Sie als Active Directory Administrator Connect zu der Instanz her, die mit Ihrer Active Directory Domain verbunden ist.
2. Öffnen Sie Windows PowerShell.
3. Geben Sie den folgenden Befehl ein **`jane.doe`** und ersetzen Sie den Benutzernamen durch den Benutzernamen des Benutzers, den Sie löschen möchten. Weitere Informationen zum Befehl Remove-ADUser finden Sie in der Dokumentation. Microsoft

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

Setzen Sie ein Simple AD AD-Benutzerkennwort zurück

Benutzer müssen sich an die Passwortrichtlinien halten, wie sie in der definiert sindActive Directory. Manchmal kann dies dazu führen, dass Benutzer, einschließlich des Active Directory Administrators, ihr Passwort vergessen. In diesem Fall können Sie das Benutzerkennwort schnell zurücksetzen, indem Sie angeben, AWS Directory Service ob der Benutzer in Simple AD wohnt.

Sie müssen als Benutzer mit den erforderlichen Berechtigungen zum Zurücksetzen von Passwörtern angemeldet sein. Weitere Informationen zu Berechtigungen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Directory Service Ressourcen.

Sie können das Passwort für jeden Benutzer in Ihrem Konto zurücksetzen, Active Directory mit den folgenden Ausnahmen:

- Sie können das Passwort für jeden Benutzer innerhalb der Organisationseinheit (OU) zurücksetzen, das auf dem NetBIOS-Namen basiert, den Sie bei der Erstellung Ihres Active Directory verwendet haben. Wenn Sie beispielsweise das Verfahren unter befolgen würdenErstellen Sie Ihr Simple AD Active Directory, wäre Ihr NetBIOS-Name CORP und die Benutzerkennwörter, die Sie zurücksetzen könnten, wären Mitglieder der Organisationseinheit Corp/Users.
- Sie können das Kennwort eines Benutzers außerhalb der Organisationseinheit nicht zurücksetzen, das auf dem NetBIOS-Namen basiert, den Sie bei der Erstellung Ihres Active Directory verwendet haben. Weitere Informationen zur OU-Struktur für Simple AD finden Sie unterWas wird mit Ihrem Simple AD erstellt Active Directory.
- Sie können das Passwort für keinen Benutzer zurücksetzen, der Mitglied von zwei Domänen ist. Sie können auch nicht das Passwort eines Benutzers zurücksetzen, der Mitglied der Gruppe Domänen-Admins oder Unternehmensadministratoren ist, mit Ausnahme des Administratorbenutzers.
- Sie können das Passwort für keinen Benutzer zurücksetzen, der Mitglied der Gruppe Domänen-Admins oder Unternehmensadministratoren ist, mit Ausnahme des Administratorbenutzers.

Sie können eine der folgenden Methoden verwenden, um ein Benutzerkennwort zurückzusetzen:

- AWS Management Console

- AWS CLI
- Windows PowerShell

Setzen Sie ein Benutzerkennwort zurück in der AWS Management Console

1. Wählen Sie im Navigationsbereich der AWS Directory Service Konsole unter Active DirectoryVerzeichnisse aus, und wählen Sie dann Active Directory in der Liste das Objekt aus, für das Sie ein Benutzerkennwort zurücksetzen möchten.
2. Wählen Sie auf der Seite Verzeichnisdetails die Option Aktionen und anschließend die Option Benutzerpasswort zurücksetzen.
3. Geben Sie im Dialogfeld Benutzerkennwort zurücksetzen in das Feld Benutzername den Benutzernamen des Benutzers ein, dessen Passwort geändert werden muss.
4. Geben Sie ein Passwort unter Neues Passwort und Passwort bestätigen ein und wählen Sie dann Passwort zurücksetzen.

Setzen Sie ein Benutzerkennwort zurück in AWS CLI

1. Informationen zur AWS CLI Installation von finden Sie unter Installieren oder Aktualisieren der neuesten Version von AWS CLI.
2. Öffnen Sie das AWS CLI.
3. Geben Sie den folgenden Befehl ein und ersetzen Sie die Verzeichnis-ID, den Benutzernamen **`jane.doe`** und das Passwort **`P@ssw0rd`** durch Ihre Active Directory Verzeichnis-ID und die gewünschten Anmeldeinformationen. Weitere Informationen finden Sie reset-user-passwordin der AWS CLI Befehlsreferenz.

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

Setzen Sie ein Benutzerkennwort zurück in Windows PowerShell

1. Stellen Sie als Active Directory Administrator Connect zu der Instanz her, die mit Ihrer Active Directory Domain verbunden ist.
2. Öffnen Sie Windows PowerShell.
3. Geben Sie den folgenden Befehl ein und ersetzen Sie den Benutzernamen**`jane.doe`**, die Verzeichnis-ID und das Passwort **`P@ssw0rd`** durch Ihre Active Directory Verzeichnis-ID und die

gewünschten Anmeldeinformationen. Weitere Informationen finden Sie unter UserPassword Reset-DS-Cmdlet.

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

Erstellen Sie eine Simple AD AD-Gruppe

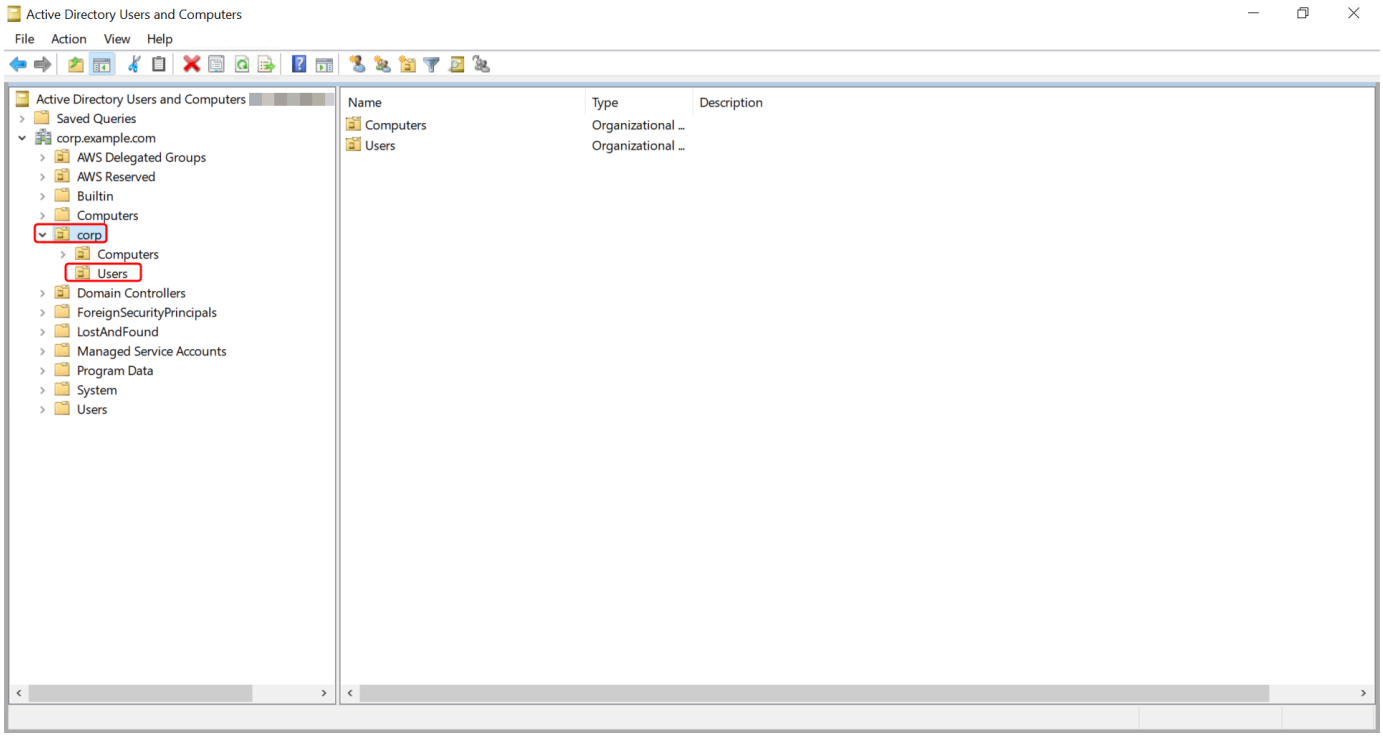
Gehen Sie wie folgt vor, um eine Sicherheitsgruppe mit einer Amazon EC2 EC2-Instance zu erstellen, die mit Ihrem Simple AD AD-Verzeichnis verknüpft ist. Bevor Sie Sicherheitsgruppen erstellen können, müssen Sie die Verfahren unter Installation der Active-Directory-Verwaltungstools abschließen.

So erstellen Sie eine Gruppe

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

   > **Tip**
   >
   > Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
   >
   > ```
   > %SystemRoot%\system32\dsa.msc
   > ```

3. Wählen Sie in der Verzeichnisstruktur eine OU unter dem OU-NetBIOS-Namen Ihres Verzeichnisses aus, in der Sie Ihre Gruppe speichern möchten (z. B. Corp\Users). Weitere Informationen zur OU-Struktur, die von Verzeichnissen in verwendet wird AWS, finden Sie unterWas wird mit Ihrem AWS Managed Microsoft AD Active Directory erstellt.



4. Klicken Sie im MenüAction auf New und dann auf Group, um den Assistenten für neue Gruppen aufzurufen.
5. Geben Sie unter Gruppenname einen Namen für die Gruppe ein, wählen Sie einen Gruppenumfang, der Ihren Anforderungen entspricht, und wählen Sie als Gruppentyp Sicherheit. Weitere Informationen über den Gruppenumfang von Active Directory und Sicherheitsgruppen finden Sie unter Active-Directory-Sicherheitsgruppen in der Microsoft-Windows-Server-Dokumentation.
6. Klicken Sie auf OK. Die neue Sicherheitsgruppe wird im Ordner Benutzer angezeigt.

Einen Simple AD AD-Benutzer zu einer Gruppe hinzufügen

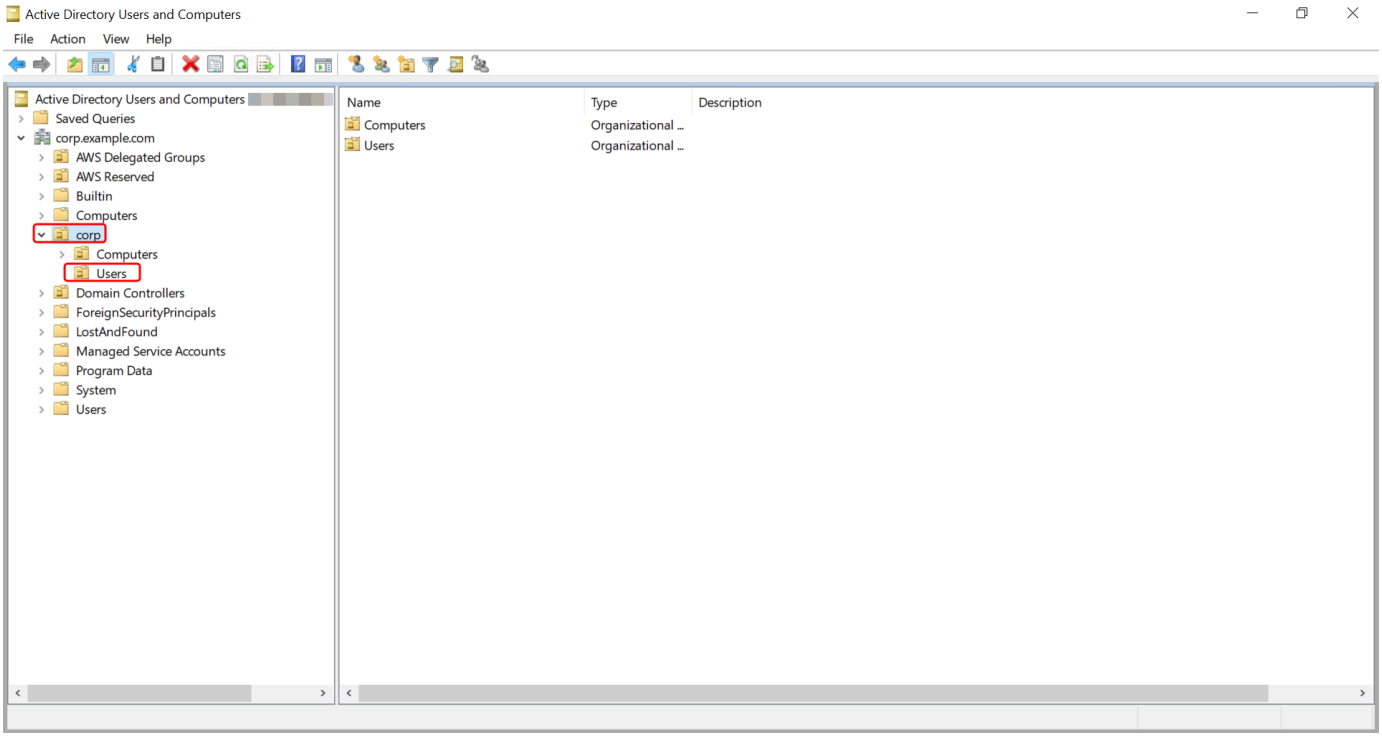
Gehen Sie wie folgt vor, um einen Benutzer zu einer Sicherheitsgruppe mit einer EC2-Instance hinzufügen, die mit Ihrem Simple-AD-Verzeichnis verbunden ist.

So fügen Sie einen neuen Benutzer zu einer Gruppe hinzu

1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

> **Tip**
>
> Sie können Folgendes von einer Eingabeaufforderung auf der Instance aus ausführen, um die Toolbox von Active Directory Users and Computers direkt zu öffnen.
>
> ```
> %SystemRoot%\system32\dsa.msc
> ```

3. Wählen Sie in der Verzeichnisstruktur die OU unter der OU mit dem NetBIOS-Namen Ihres Verzeichnisses aus, in der Sie Ihre Gruppe gespeichert haben, und wählen Sie die Gruppe, der Sie einen Benutzer als Mitglied hinzufügen möchten.



4. Klicken Sie im Menü Aktionen auf Eigenschaften, um das Dialogfeld Eigenschaften für die Gruppe zu öffnen.
5. Wählen Sie die Registerkarte Mitglieder und klicken Sie auf Hinzufügen.
6. Geben Sie unter Geben Sie die zu wählenden Objektnamen ein den Benutzernamen ein, den Sie hinzufügen möchten, und klicken Sie auf OK. Der Name wird in der Mitgliederliste angezeigt. Klicken Sie erneut auf OK, um die Gruppenmitgliedschaft zu aktualisieren.
7. Stellen Sie sicher, dass der Benutzer jetzt Mitglied der Gruppe ist, indem Sie den Benutzer im Ordner Benutzer auswählen und im Aktionsmenü auf Eigenschaften klicken, um das

Eigenschaftendialogfeld zu öffnen. Wählen sie die Registerkarte Mitglied von. Sie sollten den Namen der Gruppe in der Liste der Gruppen sehen, zu der der Benutzer gehört.

Ihr Simple-AD-Verzeichnis überwachen

Sie können Ihr Simple-AD-Verzeichnis mit folgenden Methoden überwachen:

Themen

- Erläuterungen zum Verzeichnisstatus
- Konfigurieren von Verzeichnisstatusbenachrichtigungen mit Amazon SNS

Erläuterungen zum Verzeichnisstatus

Im Folgenden sind die verschiedenen Zustandsangaben für ein Verzeichnis aufgeführt.

Aktiv

Das Verzeichnis funktioniert normal. AWS Directory Service hat keine Probleme für Ihr Verzeichnis erkannt.

Erstellen

Das Verzeichnis wird gerade erstellt. Die Verzeichniserstellung nimmt in der Regel 20 bis 45 Minuten in Anspruch, kann jedoch je nach Systemauslastung abweichen.

Deleted (Gelöscht)

Das Verzeichnis wurde gelöscht. Alle Ressourcen für das Verzeichnis wurden freigegeben. Ein Verzeichnis, das diesen Zustand erreicht hat, kann nicht wiederhergestellt werden.

Wird gelöscht

Das Verzeichnis wird gerade gelöscht. Das Verzeichnis bleibt in diesem Zustand, bis es vollständig gelöscht ist. Sobald ein Verzeichnis diesen Zustand erreicht, kann der Löschvorgang nicht mehr abgebrochen werden und das Verzeichnis ist nicht wiederherstellbar.

Fehlgeschlagen

Das Verzeichnis konnte nicht erstellt werden. Löschen Sie dieses Verzeichnis. Falls das Problem weiterhin besteht, kontaktieren Sie das AWS Support -Zentrum.

Beeinträchtigt

Das Verzeichnis wird nicht fehlerfrei ausgeführt. Mindestens ein Problem wurde erkannt und vermutlich wird nicht bei allen Verzeichnisvorgängen die volle Leistungskapazität erreicht. Es gibt viele mögliche Gründe dafür, dass sich das Verzeichnis in diesem Zustand befindet. Darunter fallen normale betriebliche Wartungsaktivitäten wie das Patchen oder die EC2-Instance-Rotation, das temporäre Hot-Spotting durch eine Anwendung auf einem Ihrer Domain-Controller oder Änderungen, die Sie an Ihrem Netzwerk vorgenommen haben und die versehentlich die Verzeichniskommunikation stören. Weitere Informationen finden Sie unter Problembehandlung bei AWS verwaltetem Microsoft AD, Fehlerbehebung in AD Connector, Beheben von Fehlern in Simple AD. AWS Behebt Probleme im Zusammenhang mit normalen Wartungsarbeiten innerhalb von 40 Minuten. Falls das Verzeichnis nach der Konsultation des Themas Fehlerbehebung länger als 40 Minuten den Status Beeinträchtigt aufweist, sollten Sie das AWS Support -Zentrum kontaktieren.

> **Important**
>
> Stellen Sie keinen Snapshot für ein Verzeichnis mit dem Status „Impaired“ (Beeinträchtigt) wieder her. Nur selten ist eine Snapshot-Wiederherstellung nötig, um Beeinträchtigungen zu beheben. Weitere Informationen finden Sie unter Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen.

Inoperable (Funktionsunfähig)

Das Verzeichnis ist nicht funktionsfähig. Alle Verzeichnisendpunkte haben Probleme gemeldet.

Angefragt

Eine Anforderung zum Erstellen Ihres Verzeichnisses steht zurzeit an.

RestoreFailed

Die Wiederherstellung des Verzeichnisses anhand eines Snapshots ist fehlgeschlagen. Versuchen Sie die Wiederherstellung erneut. Falls das Problem weiterhin besteht, versuchen Sie es mit einem anderen Snapshot oder wenden Sie sich an das AWS Support -Zentrum.

Restoring (Wiederherstellung läuft)

Das Verzeichnis wird zurzeit anhand eines automatischen oder manuellen Snapshots wiederhergestellt. Die Wiederherstellung anhand eines Snapshots dauert in der Regel einige Minuten, abhängig von der Größe der Verzeichnisdaten im Snapshot.

Weitere Informationen finden Sie unter Gründe für den Simple-AD-Verzeichnisstatus.

Konfigurieren von Verzeichnisstatusbenachrichtigungen mit Amazon SNS

Mit Amazon Simple Notification Service (Amazon SNS) können Sie E-Mail- oder Textnachrichten (SMS) erhalten, wenn sich der Status Ihres Verzeichnisses ändert. Sie werden benachrichtigt, wenn das Verzeichnis vom Status Aktiv zu Beeinträchtigt oder Funktionsunfähig wechselt. Außerdem erhalten Sie eine Benachrichtigung, wenn das Verzeichnis in einen aktiven Status zurückkehrt.

Funktionsweise

Amazon SNS verwendet „Themen“ zum Sammeln und Verteilen von Nachrichten. Jedes Thema hat einen oder mehrere Subscriber, die zu diesem Thema veröffentlichte Nachrichten empfangen. Mit den folgenden Schritten können Sie AWS Directory Service als Herausgeber zu einem Amazon SNS-Thema hinzufügen. Wenn eine Änderung des Status Ihres Verzeichnisses AWS Directory Service erkennt, veröffentlicht es eine Nachricht zu diesem Thema, die dann an die Abonnenten des Themas gesendet wird.

Sie können mehrere Verzeichnisse als Publisher zu einem einzelnen Thema zuordnen. Sie können auch Verzeichnis-Statusmeldungen zu Themen hinzufügen, die Sie zuvor in Amazon SNS erstellt haben. Sie haben umfassende Kontrolle, wer ein Thema veröffentlichen und abonnieren kann. Umfassende Informationen zu Amazon SNS finden Sie unter Was ist Amazon SNS?.

So aktivieren Sie SNS Messaging für Ihr Verzeichnis

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie die Registerkarte Wartung aus.
4. Wählen Sie im Abschnitt Verzeichnisüberwachung die Option Aktionen und dann Benachrichtigung erstellen aus.
5. Wählen Sie auf der Seite Benachrichtigung erstellen die Option Benachrichtigungstyp auswählen und dann Neue Benachrichtigung erstellen aus. Wenn Sie bereits über ein SNS-Thema verfügen, können Sie Vorhandenes SNS-Thema zuordnen wählen, um Status-Nachrichten aus diesem Verzeichnis zu diesem Thema zu senden.

> **Note**
>
> Wenn Sie Neue Benachrichtigung erstellen wählen, jedoch denselben Themen-Namen für ein SNS-Thema wählen, das bereits vorhanden ist, erstellt Amazon SNS kein neues Thema, sondern fügt die neue Abonnement-Information zum vorhandenen Thema hinzu. Wenn Sie Vorhandenes SNS-Thema zuordnen wählen, können Sie immer nur ein SNS-Thema wählen, das sich in derselben Region wie das Verzeichnis befindet.

6. Wählen Sie Empfängertyp und geben Sie die Kontaktinformationen für den Empfänger ein. Wenn Sie eine Telefonnummer für SMS eingeben, verwenden Sie nur Zahlen. Geben Sie keine Gedankenstriche, Leerzeichen oder Klammern ein.
7. (Optional) Geben Sie einen Namen für Ihr Thema und einen SNS-Anzeigenamen ein. Der Anzeigename ist ein kurzer Name von bis zu 10 Zeichen, der in alle SMS-Nachrichten zu diesem Thema aufgenommen wird. Bei der Verwendung der SMS-Option ist der Anzeigename erforderlich.

> **Note**
>
> Wenn Sie mit einem IAM-Benutzer oder einer IAM-Rolle angemeldet sind, die nur über die DirectoryServiceFullAccess verwaltete Richtlinie verfügt, muss Ihr Themenname mit „“ beginnenDirectoryMonitoring. Wenn Sie Ihren Themennamen anpassen möchten, benötigen Sie zusätzliche Berechtigungen für SNS.

8. Wählen Sie Erstellen.

Wenn Sie zusätzliche SNS-Abonnenten festlegen möchten, z. B. eine zusätzliche E-Mail-Adresse, Amazon SQS-Warteschlangen oder AWS Lambda, können Sie dies über die Amazon SNS-Konsole tun.

Verzeichnis-Status-Nachrichten aus einem Thema entfernen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Directory Service -Konsole.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie die Registerkarte Wartung aus.

4. Wählen Sie im Abschnitt Verzeichnisüberwachung einen SNS-Themennamen in der Liste aus, klicken Sie auf Aktionen und dann auf Entfernen.
5. Wählen Sie Remove (Entfernen) aus.

Dadurch wird Ihr Verzeichnis als Publisher für das ausgewählte SNS-Thema entfernt. Wenn Sie das gesamte Thema löschen möchten, können Sie dies über die Amazon SNS-Konsole tun.

> **Note**
>
> Stellen Sie vor dem Löschen eines Amazon-SNS-Themas mithilfe der SNS-Konsole sicher, dass kein Verzeichnis Status-Nachrichten zu diesem Thema sendet.
> Wenn Sie ein Amazon-SNS-Thema mithilfe der SNS-Konsole löschen, wird diese Änderung nicht sofort in der Directory-Services-Konsole sichtbar. Sie würden nur benachrichtigt werden, wenn das nächste Mal ein Verzeichnis eine Nachricht zu diesem gelöschten Thema veröffentlicht. In diesem Fall würden Sie einen aktualisierten Status auf der Registerkarte Monitoring sehen, der angibt, dass das Thema nicht gefunden wurde.
> Um zu vermeiden, dass wichtige Verzeichnisstatusmeldungen fehlen, ordnen Sie daher Ihr Verzeichnis vor dem Löschen eines Themas, das Nachrichten von empfängt AWS Directory Service, einem anderen Amazon SNS-Thema zu.

Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem Simple AD Active Directory

Sie können eine Amazon EC2 EC2-Instance nahtlos mit Ihrer Active Directory Domain verbinden, wenn die Instance gestartet wird. Weitere Informationen finden Sie unter Nahtloses Verbinden einer Amazon EC2 Windows-Instance mit Ihrem AWS Managed Microsoft AD Active Directory. Mit Automation können Sie auch direkt von der AWS Directory Service Konsole aus eine EC2-Instance starten und sie mit AWS Systems Manager einer Active Directory Domain verbinden.

Wenn Sie eine EC2-Instance manuell mit Ihrer Active Directory Domain verbinden müssen, müssen Sie die Instance in der richtigen Region und Sicherheitsgruppe oder dem richtigen Subnetz starten und dann die Instance mit der Domain verbinden.

Um eine Remote-Verbindung zu diesen Instances herstellen zu können, benötigen Sie eine IP-Verbindung zu den Instances von dem Netzwerk aus, von dem aus Sie sich verbinden. In den

meisten Fällen muss hierfür Ihrer VPC ein Internet-Gateway zugeordnet sein und die Instance muss eine öffentliche IP-Adresse haben.

Themen

Fügen Sie eine Amazon EC2 Windows-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu

Dieses Verfahren verbindet eine Amazon EC2 Windows-Instance nahtlos mit Ihrem Simple AD Active Directory.

Um einer EC2-Windows-Instance nahtlos beizutreten

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste dasselbe Verzeichnis AWS-Region wie das bestehende Verzeichnis aus.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.
4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Windows-EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.

6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) Windows im Schnellstartbereich aus. Sie können das Windows Amazon Machine Image (AMI) in der Dropdown-Liste Amazon Machine Image (AMI) ändern.
7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen.

   a. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen.

   b. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels.

   c. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk.

   d. Wählen Sie Schlüsselpaar erstellen aus.

   e. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

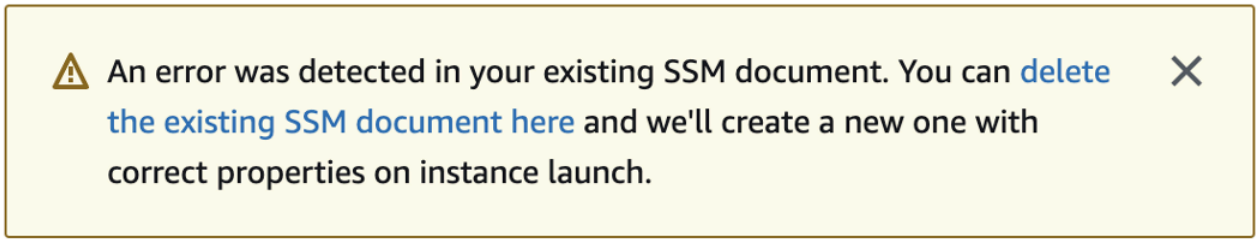
   > **Important**
   >
   > Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

    Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.

12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>
>
> Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:
>
> - Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
> - Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Für das IAM-Instance-Profil können Sie ein vorhandenes IAM-Instance-Profil auswählen oder ein neues erstellen. Wählen Sie aus der Dropdownliste für das IAM-Instanzprofil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM DirectoryServiceAccess angehängt sind. Um ein neues zu erstellen, wählen Sie den Link Neues IAM-Profil erstellen und gehen Sie dann wie folgt vor:

    1. Wählen Sie Rolle erstellen aus.
    2. Wählen Sie unter Vertrauenswürdige Entität auswählen die Option AWS -Service aus.

3. Wählen Sie unter Use case (Anwendungsfall) die Option EC2 aus.
4. Wählen Sie in der Liste der Richtlinien unter Berechtigungen hinzufügen die Richtlinien AmazonSSM ManagedInstanceCore und AmazonSSM aus. DirectoryServiceAccess Geben Sie im Suchfeld **SSM** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

   > **Note**
   >
   > AmazonSSM DirectoryServiceAccess stellt die Berechtigungen zum Hinzufügen von Instances zu einer Gruppe bereit, die von verwaltet wird. Active Directory AWS Directory ServiceAmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager -Benutzerhandbuch.

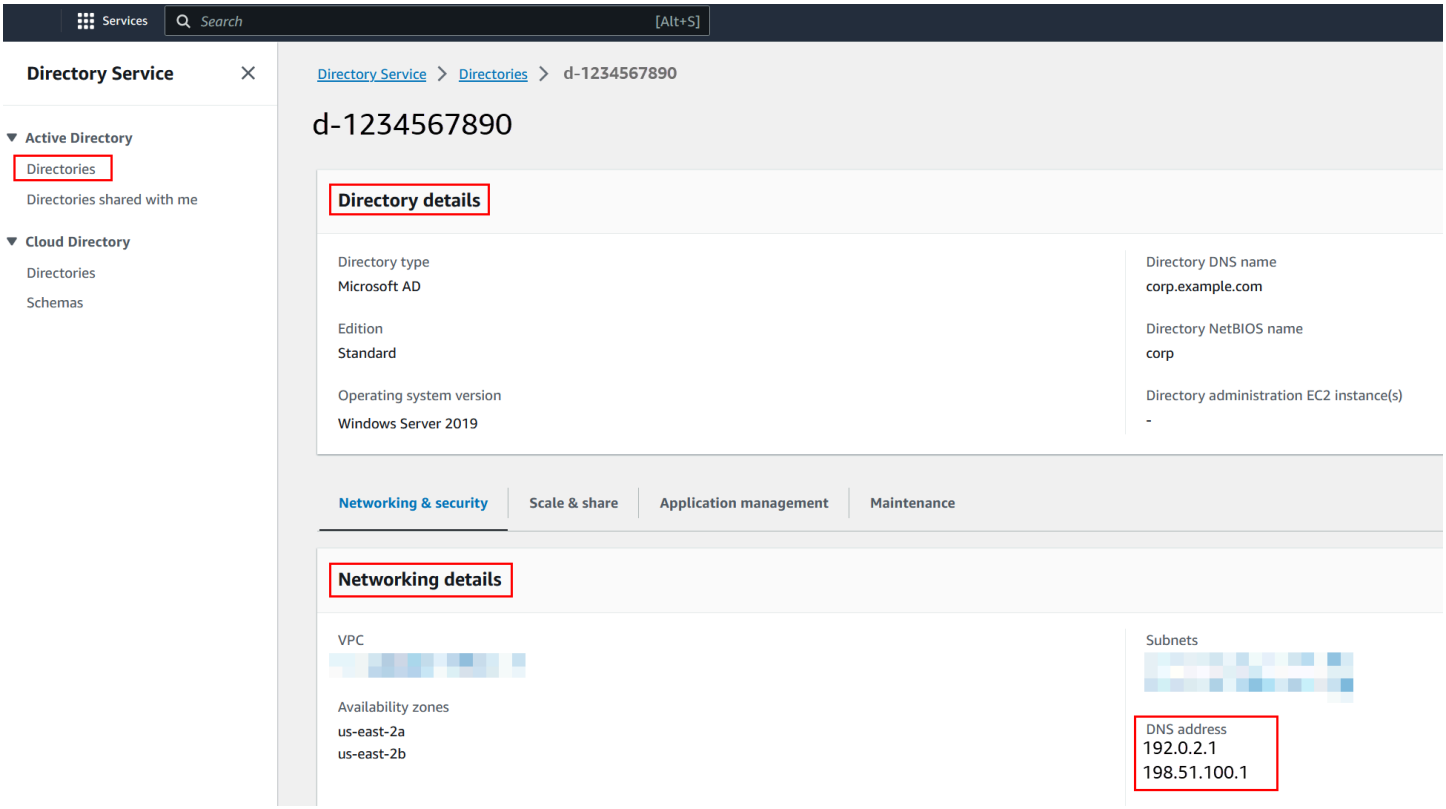
5. Geben Sie auf der Seite Benennen, überprüfen und erstellen einen Rollennamen ein. Sie benötigen diesen Rollennamen, um mit der EC2-Instance verbunden zu werden.
6. (Optional) Sie können im Feld Beschreibung eine Beschreibung des IAM-Instance-Profils angeben.
7. Wählen Sie Rolle erstellen aus.
8. Kehren Sie zur Seite Eine Instance starten zurück und wählen Sie das Aktualisierungssymbol neben dem IAM-Instance-Profil. Ihr neues IAM-Instance-Profil sollte in der Dropdown-Liste IAM-Instance-Profil sichtbar sein. Wählen Sie das neue Profil und belassen Sie die restlichen Einstellungen auf den Standardwerten.

16. Wählen Sie Launch Instance (Instance starten) aus.

Manuelles Hinzufügen einer Amazon EC2 EC2-Windows-Instance zu Ihrem Simple AD Active Directory

Um eine bestehende Amazon EC2 Windows-Instance manuell mit einem Simple AD Active Directory zu verbinden, muss die Instance mit den unter angegebenen Parametern gestartet werden. Fügen Sie eine Amazon EC2 Windows-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu

Sie benötigen die IP-Adressen der Simple AD DNS-Server. Diese Informationen finden Sie in den Abschnitten Verzeichnisservices > Verzeichnisse > dem Verzeichnis-ID-Link für Ihr Verzeichnis > Verzeichnisdetails und Netzwerk und Sicherheit.



So verbinden Sie eine Windows-Instanz mit einem Simple AD Active Directory

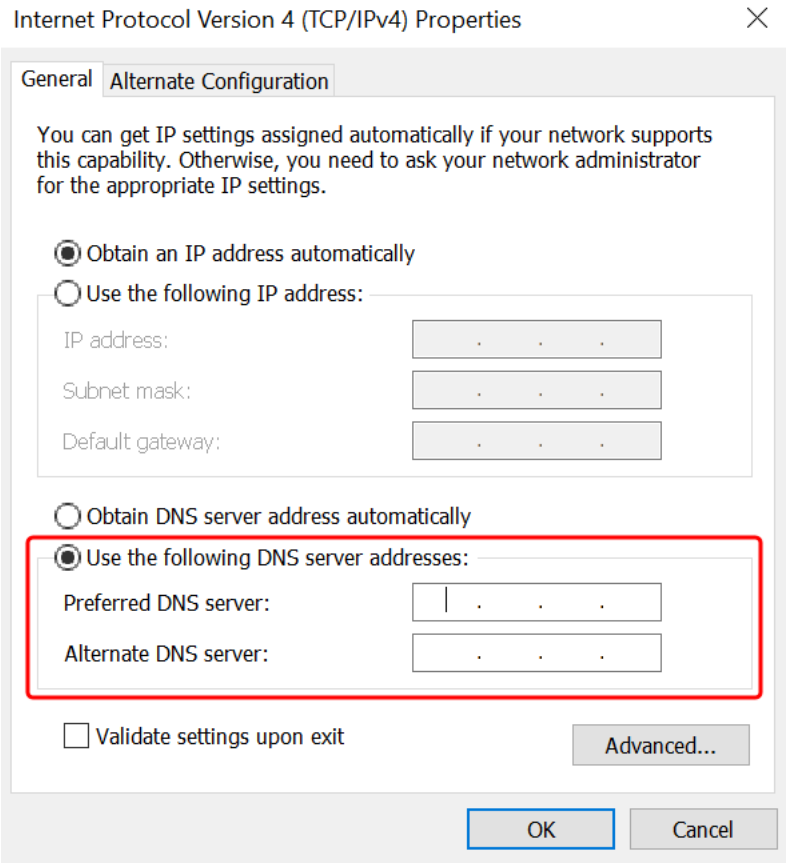
1. Verbinden Sie die Instance mithilfe eines beliebigen Remote Desktop Protocol-Clients.
2. Öffnen Sie in der Instance das Dialogfeld mit den Eigenschaften für TCP/IPv4.
   a. Öffnen Sie Network Connections.

> **Tip**
>
> Öffnen Sie Network Connections direkt, indem Sie folgenden Befehl über die Befehlszeile der Instance ausführen.
>
> ```
> %SystemRoot%\system32\control.exe ncpa.cpl
> ```

   b. Öffnen Sie für eine beliebige aktivierte Netzwerkverbindung per Rechtsklick das Kontextmenü und wählen Sie dann Properties aus.

c. Öffnen Sie im Dialogfeld für die Verbindungseigenschaften (per Doppelklick) Internet Protocol Version 4.

3. Wählen Sie Folgende DNS-Serveradressen verwenden aus, ändern Sie die bevorzugten DNS-Server - und alternativen DNS-Serveradressen in die IP-Adressen Ihrer von Simple AD bereitgestellten DNS-Server und wählen Sie OK.



4. Öffnen Sie das Dialogfeld System Properties für die Instance, wählen Sie die Registerkarte Computer Name und wählen Sie Change.

> **Tip**
>
> Öffnen Sie das Dialogfeld System Properties direkt, indem Sie folgenden Befehl über die Befehlszeile der Instance ausführen.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. Wählen Sie im Feld Mitglied von die Option Domain aus, geben Sie den vollqualifizierten Namen Ihres Simple AD Active Directory ein, und klicken Sie auf OK.

6. Wenn Sie zur Eingabe des Namens und des Kennworts für den Domänenadministrator aufgefordert werden, geben Sie den Benutzernamen und das Kennwort eines Kontos ein, das über Domänenbeitrittsrechte verfügt. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Berechtigungen zum Verbinden eines Verzeichnisses für Simple AD delegieren.

   > **Note**
   >
   > Sie können entweder den vollqualifizierten Namen Ihrer Domäne oder den NetBIOS-Namen, gefolgt von einem umgekehrten Schrägstrich (\) und dann den Benutzernamen eingeben. Der Benutzername wäre Administrator. Zum Beispiel **`corp.example.com\administrator`** oder **`corp\administrator`**.

7. Nachdem Sie in der Domain willkommen geheißen wurden, starten Sie die Instance neu, damit die Änderungen übernommen werden.

Nachdem Ihre Instanz der Simple AD Active Directory-Domäne hinzugefügt wurde, können Sie sich remote bei dieser Instanz anmelden und Dienstprogramme zur Verwaltung des Verzeichnisses installieren, z. B. zum Hinzufügen von Benutzern und Gruppen. Die Active Directory-Verwaltungstools können verwendet werden, um Benutzer und Gruppen zu erstellen. Weitere Informationen finden Sie unter Installieren Sie die Active Directory-Verwaltungstools für Simple AD.

Fügen Sie eine Amazon EC2 EC2-Linux-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu

Dieses Verfahren verbindet eine Amazon EC2 EC2-Linux-Instance nahtlos mit Ihrem Simple AD Active Directory.

Die folgenden Linux-Instance-Distributionen und -Versionen werden unterstützt:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-Bit x86)
- Red Hat Enterprise Linux 8 (HVM) (64-Bit x86)
- Ubuntu Server 18.04 LTS und Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Versionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 unterstützen das Feature der nahtlosen Domainverbindung nicht.

Voraussetzungen

Bevor Sie einen nahtlosen Domänenbeitritt zu einer Linux-Instance einrichten können, müssen Sie die Verfahren in diesem Abschnitt abschließen.

Ihr Servicekonto für die nahtlose Domainverbindung auswählen

Sie können Linux-Computer nahtlos mit Ihrer Simple-AD-Domain verbinden. Dazu müssen Sie ein Benutzerkonto mit der Berechtigung zum Erstellen eines Computerkontos erstellen, um die Computer mit der Domain zu verbinden. Mitglieder der Domain-Admins oder anderer Gruppen verfügen möglicherweise über ausreichende Rechte, um Computer mit der Domain zu verbinden, wir empfehlen dies jedoch nicht. Als bewährte Methode wird empfohlen, ein Servicekonto zu verwenden, das über die Mindestberechtigungen verfügt, die erforderlich sind, um die Computer mit der Domain zu verbinden.

Informationen zur Verarbeitung und Delegierung von Berechtigungen für Ihr Servicekonto zur Erstellung von Computerkonten finden Sie unter Zuweisen von Berechtigungen zu Ihrem Servicekonto.

Die Secrets zum Speichern des Domain-Servicekontos erstellen

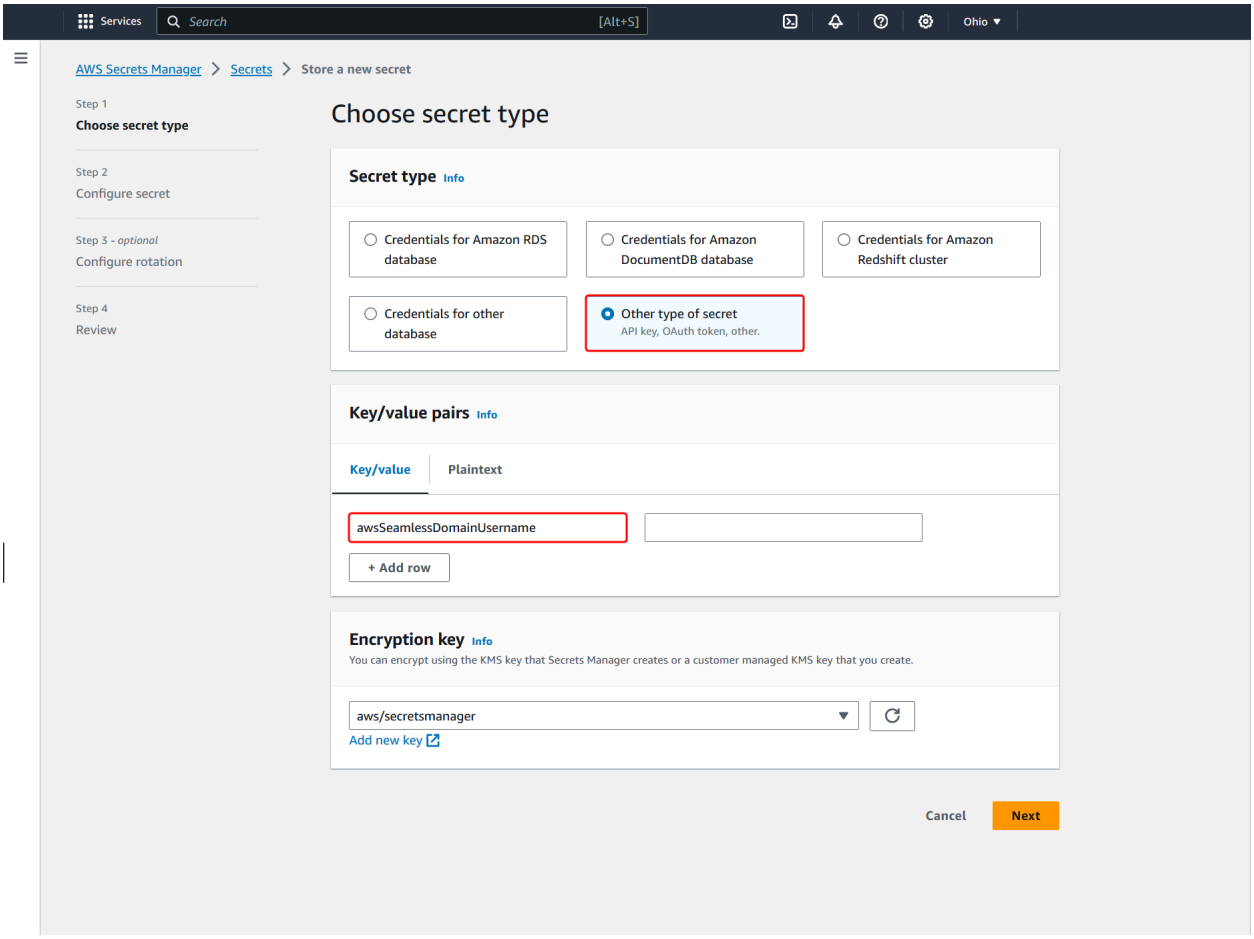
Sie können das Domänendienstkonto AWS Secrets Manager zum Speichern verwenden.

So erstellen Sie Secrets und speichern die Kontoinformationen des Domainservices

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die AWS Secrets Manager Konsole unter https://console.aws.amazon.com/secretsmanager/.
2. Wählen Sie Store a new secret (Ein neues Secret speichern).
3. Gehen Sie auf der Seite Neues Geheimnis speichern wie folgt vor:
   a. Wählen Sie unter Geheimtyp die Option Andere Art von Geheimnissen aus.
   b. Gehen Sie unter Schlüssel/Wert-Paare wie folgt vor:

i. Geben Sie im ersten Feld **`awsSeamlessDomainUsername`** ein. Geben Sie in derselben Zeile im nächsten Feld den Benutzernamen für Ihr Dienstkonto ein. Wenn Sie den PowerShell Befehl beispielsweise zuvor verwendet haben, wäre der Name des Dienstkontos**`awsSeamlessDomain`**.

> **Note**
>
> Sie müssen **`awsSeamlessDomainUsername`** genau so eingeben, wie er lautet. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.



ii. Wählen Sie Zeile hinzufügen.

iii. Geben Sie in der neuen Zeile im ersten Feld **`awsSeamlessDomainPassword`** ein. Geben Sie in derselben Zeile im nächsten Feld das Passwort für Ihr Servicekonto ein.

> **Note**
>
> Sie müssen **`awsSeamlessDomainPassword`** genau so eingeben, wie er lautet. Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.

iv. Behalten Sie unter Verschlüsselungsschlüssel den Standardwert bei`aws/secretsmanager`. AWS Secrets Manager verschlüsselt das Geheimnis immer, wenn Sie diese Option wählen. Sie können auch einen von Ihnen erstellten Schlüssel auswählen.

> **Note**
>
> Je nachdem AWS Secrets Manager, welches Geheimnis Sie verwenden, fallen Gebühren an. Die aktuelle vollständige Preisliste finden Sie unter AWS Secrets Manager – Preise.
> Sie können den AWS verwalteten Schlüssel`aws/secretsmanager`, den Secrets Manager erstellt, verwenden, um Ihre Geheimnisse kostenlos zu verschlüsseln. Wenn Sie Ihre eigenen KMS-Schlüssel zur Verschlüsselung Ihrer Geheimnisse erstellen, wird Ihnen der aktuelle AWS KMS Tarif AWS berechnet. Weitere Informationen finden Sie unter AWS Key Management Service -Preisgestaltung.

v. Wählen Sie Weiter aus.

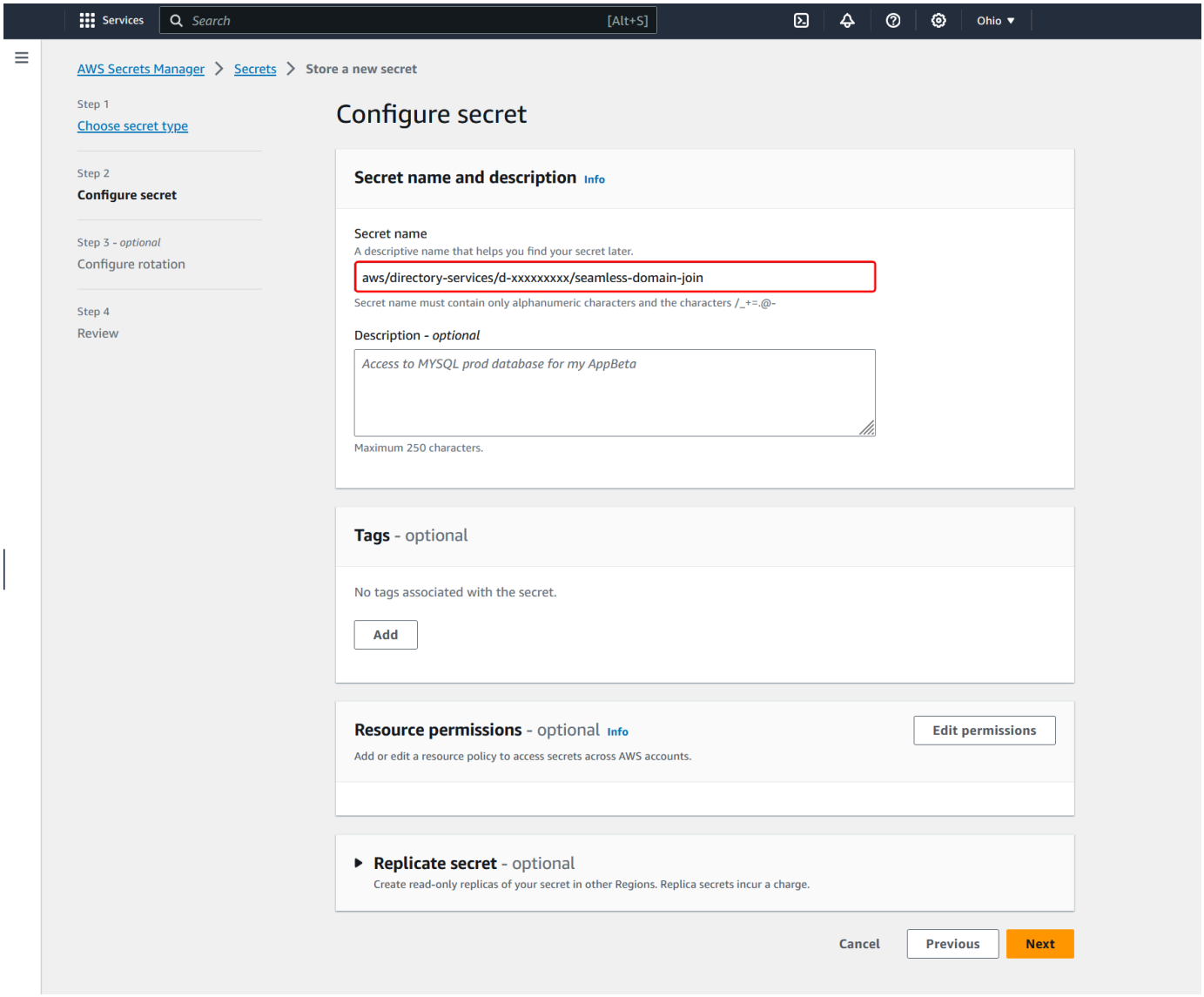
4. Geben Sie unter Geheimer Name einen geheimen Namen ein, der Ihre Verzeichnis-ID enthält. Verwenden Sie dabei das folgende Format und ersetzen Sie *`d-xxxxxxxxx`* durch Ihre Verzeichnis-ID:

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

Dies wird verwendet, um Secrets in der Anwendung abzurufen.

> **Note**
>
> Sie müssen **`aws/directory-services/d-xxxxxxxxx/seamless-domain-join`** genau so eingeben, wie es ist, aber *`d-xxxxxxxxx`* durch Ihre Verzeichnis-ID ersetzen.

Stellen Sie sicher, dass keine führenden oder abschließenden Leerzeichen vorhanden sind. Andernfalls schlägt die Domainverbindung fehl.



5. Belassen Sie alles andere auf den eingestellten Standardwerte und wählen Sie dann Weiter.
6. Wählen Sie unter Automatische Rotation konfigurieren die Option Automatische Rotation deaktivieren und wählen Sie dann Weiter.

   Sie können die Rotation für dieses Geheimnis aktivieren, nachdem Sie es gespeichert haben.
7. Überprüfen Sie die Einstellungen und wählen Sie dann Speichern, um Ihre Änderungen zu speichern. Die Secrets-Manager-Konsole zeigt Ihnen wieder die Liste der Secrets in Ihrem Konto an, in der Ihr neues Secret nun enthalten ist.

8. Wählen Sie Ihren neu erstellten Secret-Namen aus der Liste und notieren Sie sich den Wert des Secret-ARN. Sie brauchen diesen im nächsten Abschnitt.

Aktivieren Sie die Rotation für das geheime Domänendienstkonto

Wir empfehlen, dass Sie die geheimen Daten regelmäßig wechseln, um Ihre Sicherheitslage zu verbessern.

Um die Rotation für das geheime Domänendienstkonto zu aktivieren

- Folgen Sie den Anweisungen unter Automatische Rotation für AWS Secrets Manager geheime Daten einrichten im AWS Secrets Manager Benutzerhandbuch.

  Verwenden Sie für Schritt 5 die Rotationsvorlage Microsoft Active Directory-Anmeldeinformationen im AWS Secrets Manager Benutzerhandbuch.

  Hilfe finden Sie im AWS Secrets Manager Benutzerhandbuch unter Problembehandlung bei der AWS Secrets Manager Rotation.

Die erforderliche IAM-Richtlinie und -Rolle erstellen

Gehen Sie wie folgt vor, um eine benutzerdefinierte Richtlinie zu erstellen, die nur Lesezugriff auf Ihren Secrets Manager Seamless Domain Join Secret (den Sie zuvor erstellt haben) ermöglicht, und um eine neue DomainJoin LinuxEC2 IAM-Rolle zu erstellen.

Die IAM-Leserichtlinie zu Secrets Manager erstellen

Sie verwenden die IAM-Konsole, um eine Richtlinie zu erstellen, die schreibgeschützten Zugriff auf Ihr Secrets-Manager-Secret gewährt.

So erstellen Sie die IAM-Leserichtlinie zu Secrets Manager

1. Melden Sie sich AWS Management Console als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Dann öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Access Management die Option Richtlinien aus.
3. Wählen Sie Richtlinie erstellen aus.
4. Wählen Sie die Registerkarte JSON aus und kopieren Sie den Text aus dem folgenden JSON-Richtliniendokument. Fügen Sie ihn dann in das JSON-Textfeld ein.

> **Note**
>
> Stellen Sie sicher, dass Sie die Region und den Ressourcen-ARN durch die tatsächliche Region und den ARN des Secrets ersetzen, den Sie zuvor erstellt haben.

```
{
    "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. Wählen Sie danach Next aus. Die Richtlinienvalidierung meldet mögliche Syntaxfehler. Weitere Informationen finden Sie unter Validierung von IAM-Richtlinien.
6. Geben Sie auf der Seite Richtlinie überprüfen einen Namen für die Richtlinie ein, z. B. **`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. Überprüfen Sie den Abschnitt Zusammenfassung, um die Berechtigungen einzusehen, die Ihre Richtlinie gewährt. Wählen Sie dann Richtlinie erstellen aus, um Ihre Änderungen zu speichern. Die neue Richtlinie erscheint in der Liste der verwalteten Richtlinien und ist nun bereit, einer Identität zugeordnet zu werden.

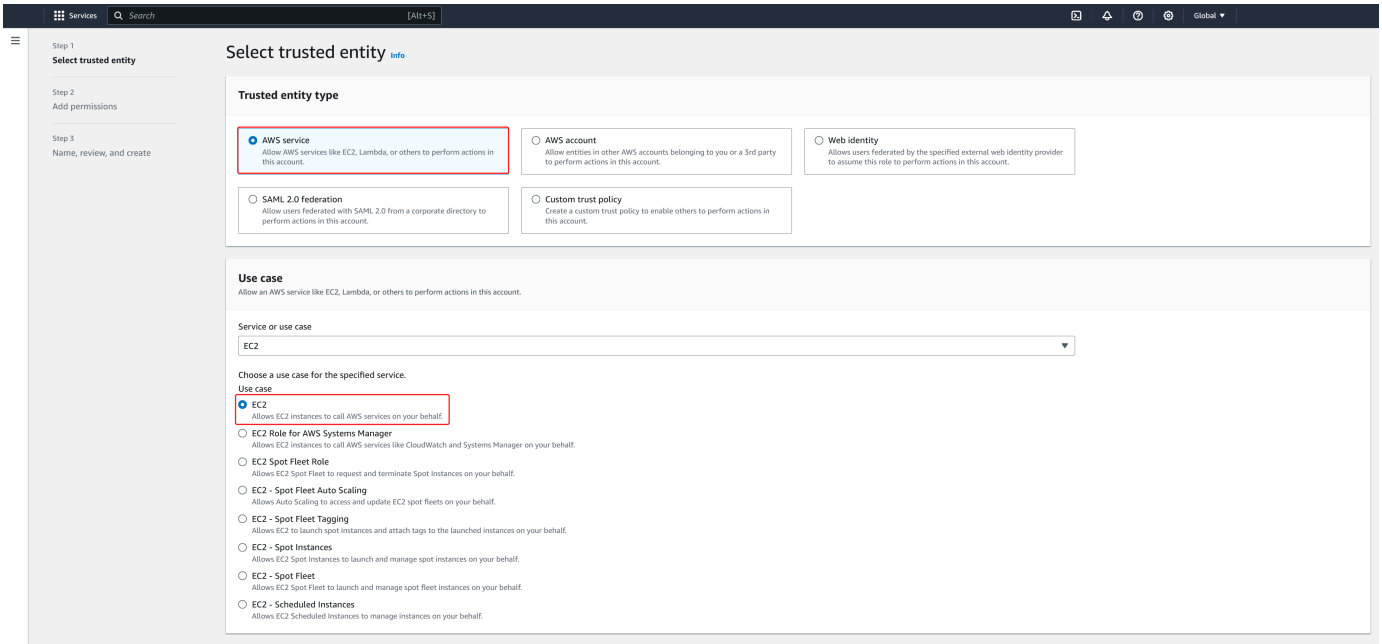
> **Note**
>
> Wir empfehlen Ihnen, eine Richtlinie pro Secret zu erstellen. Auf diese Weise wird sichergestellt, dass Instances nur auf das entsprechende Secret zugreifen können und die Auswirkungen einer Kompromittierung einer Instance minimiert werden.

Erstellen Sie die LinuxEC2-Rolle DomainJoin

Sie verwenden die IAM-Konsole, um die Rolle zu erstellen, die Sie für die Domainverbindung Ihrer Linux-EC2-Instance verwenden werden.

Um die LinuxEC2-Rolle zu erstellen DomainJoin

1. Melden Sie sich AWS Management Console als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Dann öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich unter Access Management die Option Rollen aus.
3. Wählen Sie im Inhaltsbereich die Option Rolle erstellen.
4. Wählen Sie unter Select type of trusted entity (Typ der vertrauenswürdigen Entität auswählen) die Option AWS -Service aus.
5. Wählen Sie unter Anwendungsfall die Option EC2 und dann Weiter aus.



6. Gehen Sie für Filterrichtlinien wie folgt vor:

   a. Geben Sie **`AmazonSSMManagedInstanceCore`** ein. Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

   b. Geben Sie **`AmazonSSMDirectoryServiceAccess`** ein. Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

   c. Geben Sie **`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`*`-Read`** ein (oder den Namen der Richtlinie, die Sie im vorherigen Verfahren erstellt haben). Aktivieren Sie dann das Kontrollkästchen für dieses Element in der Liste.

d. Nachdem Sie die drei oben aufgeführten Richtlinien hinzugefügt haben, wählen Sie Rolle erstellen aus.

> **Note**
>
> AmazonSSM DirectoryServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einer Datei, die von Active Directory verwaltet wird. AWS Directory Service AmazonSSM ManagedInstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des Service erforderlich sind. AWS Systems Manager Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter Ein IAM-Instance-Profil für Systems Manager erstellen im AWS Systems Manager - Benutzerhandbuch.

7. Geben Sie im Feld Rollenname einen Namen für Ihre neue Rolle ein, z. B. **`LinuxEC2DomainJoin`** oder einen anderen Namen, den Sie bevorzugen.
8. (Optional) Geben Sie im Feld Role description (Rollenbeschreibung) eine Beschreibung ein.
9. (Optional) Wählen Sie unter Schritt 3: Stichwörter hinzufügen die Option Neues Tag hinzufügen aus, um Stichwörter hinzuzufügen. Tag-Schlüssel-Wert-Paare werden verwendet, um den Zugriff für diese Rolle zu organisieren, nachzuverfolgen oder zu kontrollieren.
10. Wählen Sie Rolle erstellen aus.

Fügen Sie eine Linux-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu

Nachdem Sie nun alle erforderlichen Aufgaben konfiguriert haben, können Sie mit dem folgenden Verfahren eine nahtlose Verbindung zu Ihrer EC2-Linux-Instance herstellen.

Um Ihrer Linux-Instance nahtlos beizutreten

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Regionsauswahl in der Navigationsleiste dasselbe Verzeichnis aus AWS-Region wie das bestehende Verzeichnis.
3. Wählen Sie auf dem EC2-Dashboard im Abschnitt Instance starten die Option Instance starten aus.

4. Geben Sie auf der Seite Eine Instance starten im Abschnitt Name und Tags den Namen ein, den Sie für Ihre Linux EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüsselwertpaare hinzuzufügen, um den Zugriff auf diese EC2-Instance zu organisieren, zu verfolgen oder zu steuern.
6. Wählen Sie im Abschnitt Anwendungs- und Betriebssystem-Image (Amazon Machine Image) ein Linux-AMI aus, das Sie starten möchten.

> **Note**
>
> Das verwendete AMI muss AWS Systems Manager (SSM Agent) Version 2.3.1644.0 oder höher haben. Um die installierte SSM-Agent-Version in Ihrem AMI zu überprüfen, indem Sie eine Instance von diesem AMI aus starten, lesen Sie den Abschnitt Ermittlung der aktuell installierten SSM-Agent-Version. Wenn Sie den SSM Agent aktualisieren müssen, lesen Sie den Abschnitt Installieren und Konfigurieren von SSM Agent in EC2-Instances für Linux.
> SSM verwendet das `aws:domainJoin` Plugin, wenn eine Linux-Instance mit einer Domain verknüpft wird. Active Directory *`Das Plugin ändert den Hostnamen für die Linux-Instances in das Format EC2AMAZ- XXXXXXX.`* Weitere Informationen *`aws:domainJoin`* dazu finden Sie in der Plugin-Referenz zum AWS Systems Manager Befehlsdokument im Benutzerhandbuch.AWS Systems Manager

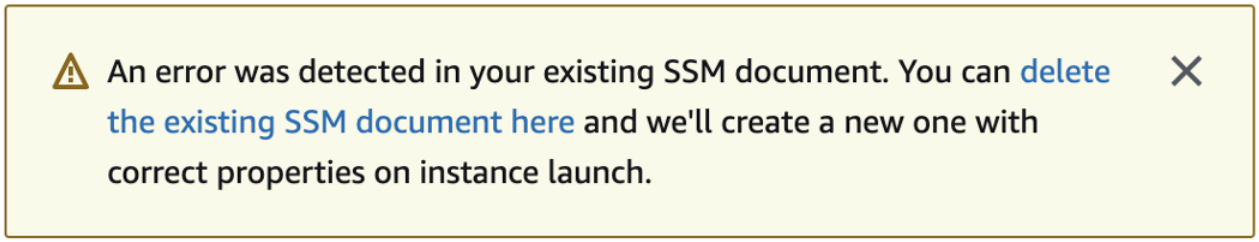
7. Wählen Sie im Abschnitt Instance-Typ den Instance-Typ, den Sie verwenden möchten, aus der Dropdown-Liste Instance-Typ aus.
8. Im Abschnitt Schlüsselpaar (Anmeldung) können Sie entweder ein neues Schlüsselpaar erstellen oder aus einem vorhandenen Schlüsselpaar auswählen. Um ein neues Schlüsselpaar zu erstellen, wählen Sie Neues Schlüsselpaar erstellen. Geben Sie einen Namen für das Schlüsselpaar ein und wählen Sie eine Option für den Schlüsselpaartyp und das Dateiformat des privaten Schlüssels. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie .pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie .ppk. Wählen Sie Schlüsselpaar erstellen aus. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

> **Important**
>
> Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

9. Wählen Sie auf der Seite Eine Instance starten im Abschnitt Netzwerkeinstellungen die Option Bearbeiten aus. Wählen Sie die VPC, in der Ihr Verzeichnis erstellt wurde, aus der Dropdown-Liste VPC – erforderlich aus.
10. Wählen Sie eines der öffentlichen Subnetze in Ihrer VPC aus der Dropdown-Liste Subnetz aus. Das von Ihnen gewählte Subnetz muss den gesamten externen Datenverkehr an ein Internet-Gateway weiterleiten. Ist dies nicht der Fall, können Sie keine Remote-Verbindung zur Instance einrichten.

    Weitere Informationen zur Verbindung mit einem Internet-Gateway finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
11. Wählen Sie unter Öffentliche IP automatisch zuweisen die Option Aktivieren.

    Weitere Informationen zur öffentlichen und privaten IP-Adressierung finden Sie unter Amazon EC2 EC2-Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.
12. Für die Einstellungen zu Firewall (Sicherheitsgruppen) können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
13. Für Speichereinstellungen konfigurieren können Sie die Standardeinstellungen verwenden oder an Ihre Bedürfnisse angepasste Änderungen vornehmen.
14. Wählen Sie den Abschnitt Erweiterte Details aus und wählen Sie Ihre Domain aus der Dropdown-Liste für das Domainverbindungs-Verzeichnis aus.

> **Note**
>
> Nachdem Sie das Domain-Join-Verzeichnis ausgewählt haben, sehen Sie möglicherweise:
>
> 
>

Dieser Fehler tritt auf, wenn der EC2-Startassistent ein vorhandenes SSM-Dokument mit unerwarteten Eigenschaften identifiziert. Sie können einen der folgenden Schritte ausführen:

- Wenn Sie das SSM-Dokument zuvor bearbeitet haben und die Eigenschaften erwartet werden, wählen Sie Schließen und fahren Sie fort, um die EC2-Instance ohne Änderungen zu starten.
- Wählen Sie den Link „Bestehendes SSM-Dokument hier löschen“, um das SSM-Dokument zu löschen. Dies ermöglicht die Erstellung eines SSM-Dokuments mit den richtigen Eigenschaften. Das SSM-Dokument wird automatisch erstellt, wenn Sie die EC2-Instance starten.

15. Wählen Sie für das IAM-Instanzprofil die IAM-Rolle aus, die Sie zuvor im Abschnitt Voraussetzungen erstellt haben. Schritt 2: LinuxEC2-Rolle erstellen. DomainJoin
16. Wählen Sie Launch Instance (Instance starten) aus.

> **Note**
>
> Wenn Sie eine nahtlose Domainverbindung mit SUSE Linux durchführen, ist ein Neustart erforderlich, bevor die Authentifizierungen funktionieren. Um SUSE vom Linux-Terminal aus neu zu starten, geben Sie sudo reboot ein.

Manuelles Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem Simple AD Active Directory

Neben Amazon EC2 EC2-Windows-Instances können Sie auch bestimmte Amazon EC2 EC2-Linux-Instances zu Ihrem Simple AD Active Directory hinzufügen. Die folgenden Linux-Instance-Distributionen und -Versionen werden unterstützt:

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64-Bit x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64-Bit x86)
- Ubuntu Server 18.04 LTS und Ubuntu Server 16.04 LTS
- CentOS 7 x86-64

- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Andere Linux-Distributionen und -Versionen können funktionieren, sind jedoch nicht getestet worden.

Voraussetzungen

Bevor Sie eine Amazon-Linux-, CentOS-, Red-Hat- oder Ubuntu-Instance mit Ihrem Verzeichnis verbinden können, muss die Instance zunächst wie unter Fügen Sie eine Amazon EC2 EC2-Linux-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu beschrieben gestartet werden.

> **Important**
>
> Einige der folgenden Verfahren können, wenn sie nicht richtig durchgeführt werden, Ihre Instance nicht erreichbar oder unbrauchbar machen. Aus diesem Grund empfehlen wir dringend, eine Sicherung anzufertigen oder einen Snapshot der Instance zu machen, bevor diese Verfahren ausgeführt werden.

So fügen Sie Ihrem Verzeichnis eine Linux-Instance hinzu

Folgen Sie den Schritten für Ihre spezifische Linux-Instance unter Verwendung einer der folgenden Registerkarten:

Amazon Linux

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instance so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre Amazon-Linux-64bit-Instance auf dem aktuellen Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen Amazon-Linux-Pakete auf Ihrer Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> Hilfe bei der Bestimmung der Amazon-Linux-Version, die Sie verwenden, finden Sie unter Identifizieren von Amazon-Linux-Images im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

Ein Konto in der *example.com* Domain, das eine Berechtigung zum Verbinden einer Domain hat. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

6. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

7. Nachdem die Instance neu gestartet wurde, stellen Sie eine Verbindung zu einem SSH-Client her und fügen Sie dann die Domain-Administratorengruppe der sudoers-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

   ```
   sudo visudo
   ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

CentOS

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Überprüfen Sie, ob Ihre CentOS 7-Instance auf dem aktuellen Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen CentOS 7-Pakete auf Ihre Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

Ein Konto in der *example.com* Domain, das eine Berechtigung zum Verbinden einer Domain hat. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

6. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

7. Nachdem die Instance neu gestartet wurde, stellen Sie eine Verbindung zu einem SSH-Client her und fügen Sie dann die Domain-Administratorengruppe der sudoers-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

   ```
   sudo visudo
   ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

Red hat

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Stellen Sie sicher, dass die Red Hat - 64bit-Instance auf dem neuesten Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen Red Hat-Pakete auf Ihrer Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

Das SaM AccountName für ein Konto in der Domäne *example.com*, das über Domänenbeitrittsrechte verfügt. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

6. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

7. Nachdem die Instance neu gestartet wurde, stellen Sie eine Verbindung zu einem SSH-Client her und fügen Sie dann die Domain-Administratorengruppe der sudoers-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

   ```
   sudo visudo
   ```

   b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

Ubuntu

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instance her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der AWS Directory Service bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instance einrichten. Für eine manuelle Einrichtung finden Sie im AWS -Wissenszentrum im Artikel zum Thema Wie weise ich einen statischen DNS-Server zu einer privaten Amazon-EC2-Instance zu? eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Stellen Sie sicher, dass Ihre Ubuntu - 64bit-Instance auf dem neuesten Stand ist.

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. Installieren Sie die erforderlichen Ubuntu-Pakete auf Ihrer Linux-Instance.

> **Note**
>
> Einige dieser Pakete sind möglicherweise bereits installiert.
> Wenn Sie die Pakete installieren, werden Ihnen mehrere Pop-up-Konfigurationsbildschirme gezeigt. Sie können in der Regel die Felder in diesen Bildschirmen leer lassen.

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. Deaktivieren Sie die Reverse DNS-Auflösung und legen Sie den Standardbereich auf den FQDN Ihrer Domain fest. Ubuntu-Instances müssen im DNS reverse-auflösbar sein, bevor der Bereich genutzt werden kann. Andernfalls müssen Sie Reverse DNS in der /etc/krb5.conf wie folgt deaktivieren:

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. Fügen Sie die Instance mit folgendem Befehl zur Instance hinzu.

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

Das SaM AccountName für ein Konto in der Domäne *example.com*, das über Domänenbeitrittsrechte verfügt. Geben Sie das Passwort für das Konto ein, wenn Sie dazu aufgefordert werden. Weitere Informationen zum Erteilen dieser Berechtigungen finden Sie unter Delegieren von Berechtigungen zum Verbinden eines Verzeichnisses für AWS Managed Microsoft AD.

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...
 * Successfully enrolled machine in realm
```

7. Konfigurieren Sie den SSH-Service so, dass die Passwortauthentifizierung zulässig ist.

   a. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Text-Editor.

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. Setzen Sie die Einstellung `PasswordAuthentication` auf `yes`.

   ```
   PasswordAuthentication yes
   ```

   c. Starten Sie den SSH-Service neu.

   ```
   sudo systemctl restart sshd.service
   ```

   Alternative Vorgehensweise:

   ```
   sudo service sshd restart
   ```

8. Nachdem die Instance neu gestartet wurde, stellen Sie eine Verbindung zu einem SSH-Client her und fügen Sie dann die Domain-Administratorengruppe der sudoers-Liste hinzu, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie die `sudoers` - Datei mit dem folgenden Befehl:

```
sudo visudo
```

b. Fügen Sie Folgendes am Ende der `sudoers`-Datei hinzu und speichern Sie die Datei.

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(Im obigen Beispiel wird „\<space>“ für das Linux-Leerzeichen verwendet.)

> **Note**
>
> Wenn Sie bei der Verwendung von Simple AD ein Benutzerkonto auf einer Linux-Instance mit der Option „Änderung des Passworts bei der nächsten Anmeldung erzwingen“ erstellen, kann dieser Benutzer sein Passwort nicht sofort mit kpasswd ändern. Zur erstmaligen Änderung des Passworts muss ein Domain-Administrator das Benutzerpasswort über die Active-Directory-Verwaltungstools aktualisieren.

Konten von eine Linux-Instance verwalten

Zum Verwalten von Konten in Simple AD über eine Linux-Instance müssen Sie spezifische Konfigurationsdateien folgendermaßen in Ihrer Linux-Instance aktualisieren:

1. Setzen Sie krb5_use_kdcinfo in der Datei /etc/sssd/sssd.conf auf False. Beispielsweise:

```
[domain/example.com]
    krb5_use_kdcinfo = False
```

2. Damit diese Konfiguration wirksam wird, müssen Sie den sssd-Service neu starten:

```
$ sudo systemctl restart sssd.service
```

Alternativ können Sie:

```
$ sudo service sssd start
```

3. Falls Sie Benutzer aus einer CentOS-Linux-Instance verwalten, müssen Sie auch die Datei /etc/smb.conf bearbeiten, um Folgendes einzubeziehen:

```
[global]
  workgroup = EXAMPLE.COM
  realm = EXAMPLE.COM
  netbios name = EXAMPLE
  security = ads
```

Einschränken des Kontoanmeldungszugriffs

Da alle Konten in Active Directory standardmäßig definiert sind, können sich alle Benutzer aus dem Verzeichnis bei der Instance anmelden. Mit ad_access_filter in sssd.conf können Sie festlegen, dass sich nur bestimmte Benutzer bei der Instance anmelden können. Beispielsweise:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

Gibt an, dass Benutzer nur Zugriff auf die Instance haben, wenn sie Mitglied einer bestimmten Gruppe sind.

cn

Der allgemeine Name der Gruppe, die Zugriff haben soll. In diesem Beispiel ist der Name der Gruppe *admins*.

ou

Dies ist die Organisationseinheit, in der sich die oben genannte Gruppe befindet. In diesem Beispiel ist die OU *Testou*.

dc

Dies ist die Domainkomponente Ihrer Domain. In diesem Beispiel *example*.

dc

Hierbei handelt es sich um eine zusätzliche Domainkomponente. In diesem Beispiel *com*.

Sie müssen ad_access_filter manuell zu /etc/sssd/sssd.conf hinzufügen.

Öffnen Sie die Datei /etc/sssd/sssd.conf in einem Text-Editor.

```
sudo vi /etc/sssd/sssd.conf
```

Danach sieht sssd.conf wie folgt aus:

```
[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)
```

Damit die Konfiguration wirksam wird, müssen Sie den sssd-Service neu starten:

```
sudo systemctl restart sssd.service
```

Alternativ können Sie:

```
sudo service sssd restart
```

ID-Zuordnung

Die ID-Zuordnung kann mit zwei Methoden durchgeführt werden, um eine einheitliche Benutzererfahrung zwischen UNIX/Linux User Identifier (UID) und Group Identifier (GID) sowie Windows- und Active Directory Security Identifier (SID) -Identitäten zu gewährleisten.

1. Zentralisiert

2. Verteilt

> **Note**
>
> Für die zentrale Zuordnung von Benutzeridentitäten Active Directory ist ein Portable Operating System Interface oder POSIX erforderlich.

Zentralisierte Zuordnung von Benutzeridentitäten

Active Directoryoder ein anderer LDAP-Dienst (Lightweight Directory Access Protocol) stellt den Linux-Benutzern UID und GID zur Verfügung. In Active Directory werden diese Identifikatoren in den Benutzerattributen gespeichert:

- UID — Der Linux-Benutzername (Zeichenfolge)
- UID-Nummer — Die Linux-Benutzer-ID-Nummer (Integer)
- GID-Nummer — Die Linux-Gruppen-ID-Nummer (Integer)

Um eine Linux-Instanz für die Verwendung der UID und GID zu konfigurierenActive Directory, legen Sie diese `ldap_id_mapping = False` in der Datei sssd.conf fest. Bevor Sie diesen Wert festlegen, stellen Sie sicher, dass Sie den Benutzern und Gruppen in eine UID, UID-Nummer und GID-Nummer hinzugefügt haben. Active Directory

Zuordnung verteilter Benutzeridentitäten

Wenn Sie Active Directory nicht über die POSIX-Erweiterung verfügen oder wenn Sie die Identitätszuweisung nicht zentral verwalten möchten, kann Linux die UID- und GID-Werte berechnen. Linux verwendet den eindeutigen Security Identifier (SID) des Benutzers, um die Konsistenz aufrechtzuerhalten.

Um die verteilte Benutzer-ID-Zuordnung zu konfigurieren, legen Sie dies `ldap_id_mapping = True` in der Datei sssd.conf fest.

Connect zur Linux-Instanz her

Wenn ein Benutzer die Verbindung zur Instance über einen SSH-Client herstellt, wird er zur Eingabe des Benutzernamens aufgefordert. Der Benutzer kann den Benutzernamen entweder im Format `username@example.com` oder `EXAMPLE\username` eingeben. Je nachdem, welche Linux-Distribution Sie verwenden, wird die Antwort etwa wie folgt aussehen:

Amazon Linux, Red Hat Enterprise Linux und 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%
```

Berechtigungen zum Verbinden eines Verzeichnisses für Simple AD delegieren

Wenn Sie einen Computer mit Ihrem Verzeichnis verbinden möchten, muss Ihr Konto über die entsprechenden Berechtigungen verfügen.

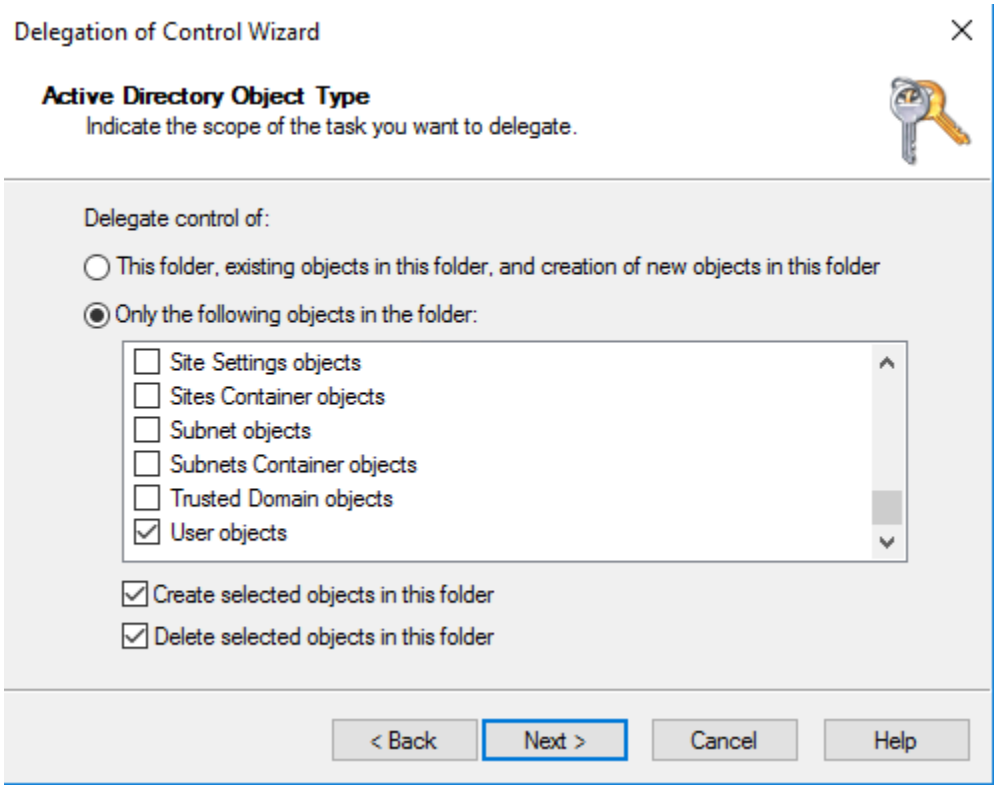
Bei Simple AD haben alle Mitglieder der Gruppe Domain-Admins alle erforderlichen Berechtigungen, um Computer mit einem Verzeichnis zu verbinden.

Als bewährte Methode empfehlen wir Ihnen, ein Konto zu verwenden, das nur die mindestens erforderlichen Berechtigungen hat. Die folgenden Schritte veranschaulichen, wie Sie eine neue Gruppe mit dem Namen `Joiners` erstellen und die Berechtigungen, die für die Verbindung von Computern mit dem Verzeichnis erforderlich sind, an diese Gruppe delegieren.

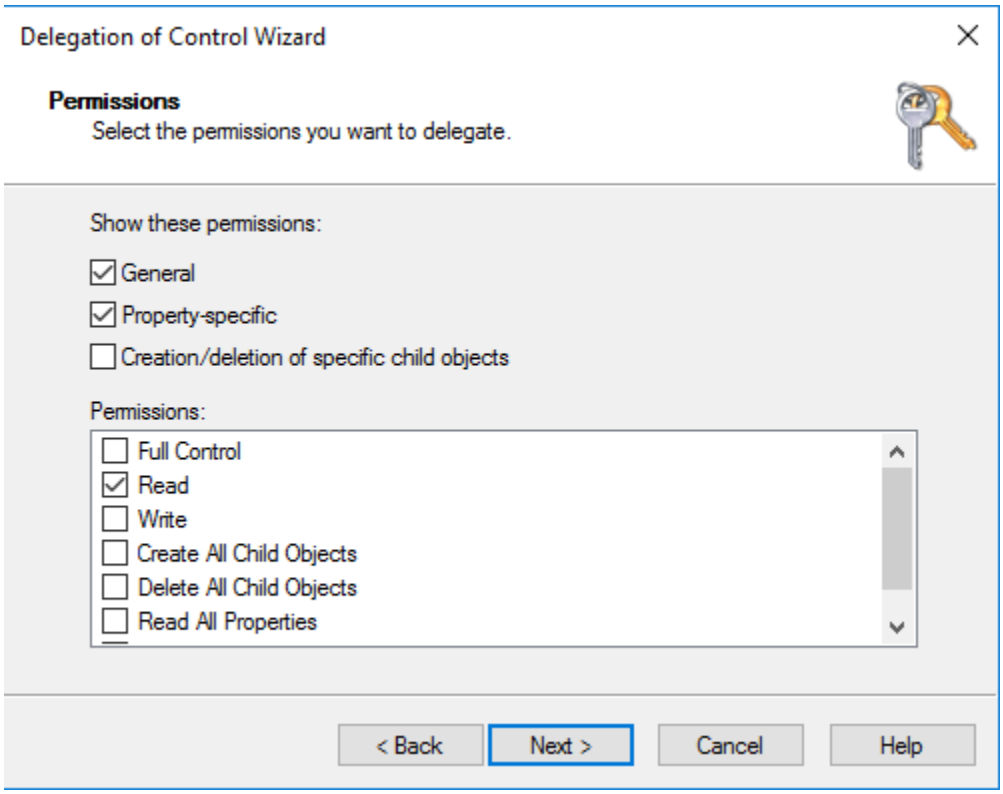
Sie müssen diesen Vorgang auf einem Computer durchführen, der mit Ihrem Verzeichnis verbunden ist und auf dem das MMC-Snap-In Active Directory Benutzer und Computer installiert ist. Außerdem müssen Sie als Domain-Administrator angemeldet sein.

So delegieren Sie Berechtigungen zum Verbinden eines Verzeichnisses für Simple AD

1. Öffnen Sie Active Directory User und Computer und wählen Sie in der Navigationsbaumstruktur Ihre Domain-Root aus.
2. Öffnen Sie links in der Navigationsstruktur mit einem Rechtsklick das Kontextmenü von Users und wählen Sie New und dann Group aus.
3. Geben Sie im Dialogfeld New Object - Group Folgendes ein und klicken Sie auf OK.
   - Geben Sie in Group Name (Gruppenname) **`Joiners`** ein.
   - Wählen Sie für Group scope die Option Global.
   - Wählen Sie für Group type die Option Security.
4. Wählen Sie in der Navigationsstruktur Ihre Domain Root aus. Wählen Sie im Menü Action die Option Delegate Control aus.
5. Wählen Sie auf der Seite Delegation of Control Wizard Next und dann Add.
6. Geben Sie in das Dialogfeld Select Users, Computers, or Groups `Joiners` ein und klicken Sie auf OK. Wenn mehr als ein Objekt gefunden wurde, wählen Sie die oben erstellte Gruppe `Joiners`. Wählen Sie Weiter aus.
7. Wählen Sie auf der Seite Tasks to Delegate Create a custom task to delegate und dann Next.
8. Wählen Sie Only the following objects in the folder und dann Computer objects.
9. Wählen Sie Create selected objects in this folder und Delete selected objects in this folder. Wählen Sie anschließend Weiter.



10. Wählen Sie Read und Write und dann Next.



11. Überprüfen Sie auf der Seite Den Assistenten für die Delegation der Kontrolle abschließen die Informationen und wählen Sie Fertigstellen.
12. Erstellen Sie einen Benutzer mit einem sicheren Passwort und fügen Sie diesen Benutzer zur Gruppe `Joiners` hinzu. Der Benutzer verfügt dann über ausreichende Rechte, um eine Verbindung mit dem AWS Directory Service Verzeichnis herzustellen.

Erstellen einer DHCP-Optionsliste

AWS empfiehlt, dass Sie einen DHCP-Optionssatz für Ihr AWS Directory Service Verzeichnis erstellen und den DHCP-Optionssatz der VPC zuweisen, in der sich Ihr Verzeichnis befindet. So können alle Instances in der entsprechenden VPC auf die angegebene Domain und die festgelegten DNS-Server verweisen, um ihre Domainnamen aufzulösen.

Weitere Informationen zur DHCP-Optionsliste finden Sie unter DHCP-Optionsliste im Amazon-VPC-Benutzerhandbuch.

So erstellen Sie eine DHCP-Optionsliste für Ihr Verzeichnis

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich DHCP Options Sets und anschließend Create DHCP Options Set aus.
3. Geben Sie auf der Seite DHCP-Optionsliste erstellen die folgenden Werte für Ihr Verzeichnis ein:

   Name

   Ein optionales Tag für die Optionsliste

   Domainname

   Den vollständig qualifizierten Namen Ihres Verzeichnisses, z. B. `corp.example.com`

   Domainnamenserver

   Die IP-Adressen der DNS-Server des von Ihnen AWS bereitgestellten Verzeichnisses.

   > **Note**
   >
   > Sie finden diese Adressen, indem Sie im Navigationsbereich der AWS Directory Service -Konsole die Option Verzeichnisse und anschließend die ID des gewünschten Verzeichnisses auswählen.

NTP-Server

Lassen Sie dieses Feld leer.

NetBIOS-Namenserver

Lassen Sie dieses Feld leer.

NetBIOS-Knotentyp

Lassen Sie dieses Feld leer.

4. Wählen Sie Create DHCP Options Set (DHCP-Optionsliste erstellen). Die neue DHCP-Optionsliste wird in der Liste der DHCP-Optionen angezeigt.
5. Notieren Sie sich die ID der neuen DHCP-Optionsliste (dopt-*xxxxxxxx*). Sie verwenden dies, um die neue Optionsliste mit Ihrer VPC zu verknüpfen.

So ändern Sie die DHCP-Optionsliste, die mit einer VPC verknüpft ist

Nach dem Erstellen einer DHCP-Optionsliste sind keine Änderungen an den Optionen mehr möglich. Falls Ihre VPC verschiedene DHCP-Optionslisten nutzen soll, müssen Sie eine neue Liste erstellen und diese dann mit der VPC verknüpfen. Sie können Ihre VPC auch so einrichten, dass keine DHCP-Optionen verwendet werden.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie die VPC und dann Aktionen, VPC-Einstellungen bearbeiten aus.
4. Wählen Sie unter DHCP-Optionssatz einen Optionssatz aus oder wählen Sie Kein DHCP-Optionssatz und dann Speichern.

Um den mit einer VPC verknüpften DHCP-Optionssatz über die Befehlszeile zu ändern, gehen Sie wie folgt vor:

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Ihr Simple-AD-Verzeichnisses verwalten

In diesem Abschnitt wird die Verwaltung allgemeiner Administrationsaufgaben für Ihre Simple AD-Umgebung beschrieben.

Themen

Ihr Simple AD löschen

Wenn ein Simple AD gelöscht wird, werden alle Verzeichnisdaten und Snapshots gelöscht und können nicht wiederhergestellt werden. Alle Instances, die dem Verzeichnis zugeordnet sind, bleiben erhalten, nachdem das Verzeichnis gelöscht wurde. Sie können sich jedoch nicht mit den Anmeldeinformationen Ihres Verzeichnisses bei diesen Instances anmelden. In dem Fall müssen Sie sich mit einem lokalen Benutzerkonto bei den jeweiligen Instances anmelden.

So löschen Sie ein Verzeichnis

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse. Stellen Sie sicher, dass Sie sich an dem AWS-Region Ort befinden, an dem Ihr Active Directory Gerät bereitgestellt wird. Weitere Informationen finden Sie unter Region auswählen.
2. Stellen Sie sicher, dass für das Verzeichnis, das Sie löschen möchten, keine AWS Anwendungen aktiviert sind. Aktivierte AWS Anwendungen verhindern, dass Sie Ihr AWS Managed Microsoft AD oder Simple AD löschen.

    a. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.

    b. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus. Im Bereich AWS Apps und Dienste sehen Sie, welche AWS Anwendungen für Ihr Verzeichnis aktiviert sind.

    - Deaktivieren Sie AWS Management Console den Zugriff. Weitere Informationen finden Sie unter AWS Management Console-Zugriff deaktivieren.
    - Um Amazon zu deaktivieren WorkSpaces, müssen Sie den Service aus dem Verzeichnis in der WorkSpaces Konsole abmelden. Weitere Informationen finden Sie unter Abmeldung von einem Verzeichnis im WorkSpaces Amazon-Administratorhandbuch.

- Um Amazon zu deaktivieren WorkDocs, müssen Sie die WorkDocs Amazon-Website in der WorkDocs Amazon-Konsole löschen. Weitere Informationen finden Sie unter Löschen einer Site im WorkDocs Amazon-Administratorhandbuch.
- Um Amazon zu deaktivieren WorkMail, müssen Sie die WorkMail Amazon-Organisation in der WorkMail Amazon-Konsole entfernen. Weitere Informationen finden Sie unter Organisation entfernen im WorkMail Amazon-Administratorhandbuch.
- Um Amazon FSx für Windows File Server zu deaktivieren, müssen Sie das Amazon-FSx-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter Arbeiten mit Active Directory in FSx for Windows File Server im Amazon FSx for Windows File Server Server-Benutzerhandbuch.
- Um Amazon Relational Database Service zu deaktivieren, müssen Sie die Amazon-RDS-Instance aus der Domain entfernen. Weitere Informationen finden Sie unter Verwalten einer DB-Instance in einer Domain im Amazon-RDS-Benutzerhandbuch.
- Um den AWS Client VPN Dienst zu deaktivieren, müssen Sie den Verzeichnisdienst vom Client-VPN-Endpunkt entfernen. Weitere Informationen finden Sie unter Active DirectoryAuthentifizierung im AWS Client VPN Administratorhandbuch.
- Zur Deaktivierung von Amazon Connect müssen Sie die Amazon Connect-Instance löschen. Weitere Informationen finden Sie unter Löschen einer Amazon-Connect-Instance im Administrationshandbuch für Amazon Connect.
- Um Amazon zu deaktivieren QuickSight, müssen Sie sich von Amazon abmelden QuickSight. Weitere Informationen finden Sie unter Schließen Ihres Amazon QuickSight Kontos im QuickSight Amazon-Benutzerhandbuch.

> **Note**
>
> Wenn Sie es verwenden AWS IAM Identity Center und es zuvor mit dem AWS verwalteten Microsoft AD-Verzeichnis verbunden haben, das Sie löschen möchten, müssen Sie zuerst die Identitätsquelle ändern, bevor Sie es löschen können. Weitere Informationen finden Sie unter Identitätsquelle ändern im Benutzerhandbuch zu IAM Identity Center.

3. Wählen Sie im Navigationsbereich Verzeichnisse aus.
4. Wählen Sie nur das Verzeichnis, das gelöscht werden soll, und klicken Sie auf Löschen. Es dauert einige Minuten, bis das Verzeichnis gelöscht wird. Wenn dieser Vorgang abgeschlossen ist, wird es aus Ihrer Verzeichnisliste entfernt.

Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen

AWS Directory Service bietet die Möglichkeit, manuelle Schnappschüsse von Daten für Ihr Simple AD AD-Verzeichnis zu erstellen. Diese Schnappschüsse können verwendet werden, um eine point-in-time Wiederherstellung Ihres Verzeichnisses durchzuführen. Sie können keine Snapshots von AD-Connector-Verzeichnissen erstellen.

Themen

Erstellen eines Snapshots Ihres Verzeichnisses

Mit einem Snapshot lässt sich Ihr Verzeichnis mit den Angaben wiederherstellen, die zum Zeitpunkt der Snapshot-Erstellung vorlagen. Gehen Sie zum Erstellen eines manuellen Snapshots Ihres Verzeichnisses folgendermaßen vor.

> **Note**
>
> Sie können maximal 5 manuelle Snapshots für jedes Verzeichnis erstellen. Falls Sie diesen Maximalwert bereits erreicht haben, müssen Sie einen vorhandenen manuellen Snapshot löschen, bevor Sie einen neuen erstellen.

So erstellen Sie einen manuellen Snapshot

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Directory details (Verzeichnisdetails) die Registerkarte Maintenance (Wartung) aus.
4. Wählen Sie im Abschnitt Snapshots die Option Aktionen und dann Snapshot erstellen aus.
5. Geben Sie im Dialogfeld Verzeichnis-Snapshot erstellen einen Namen für den Snapshot ein, falls gewünscht. Wenn Sie fertig sind, wählen Sie Erstellen.

Je nach Größe des Verzeichnisses kann es einige Minuten dauern, bis der Snapshot erstellt wurde. Wenn der Snapshot fertig ist, ändert sich der Wert von Status in `Completed`.

Wiederherstellen Ihres Verzeichnisses mithilfe eines Snapshots

Das Wiederherstellen eines Verzeichnisses mithilfe eines Snapshots entspricht dem Zurücksetzen eines Verzeichnisses auf einen bestimmten vergangenen Zeitpunkt. Verzeichnis-Snapshots gelten nur für das Verzeichnis, in dem sie erstellt wurden. Ein Snapshot kann nur in dem Verzeichnis wiederhergestellt werden, in dem er erstellt wurde. Darüber hinaus beträgt das maximal unterstützte Alter eines manuellen Snapshots 180 Tage. Weitere Informationen finden Sie unter Useful shelf life of a system-state backup of Active Directory auf der Microsoft-Website.

> **Warning**
>
> Wir empfehlen, dass Sie sich vor einer Snapshot-Wiederherstellung an das AWS Support - Zentrum wenden. Möglicherweise können wir Ihnen helfen, eine Snapshot-Wiederherstellung zu vermeiden. Wiederherstellungen aus Snapshots können zu Datenverlust führen, da sie zeitpunktbezogen sind. Es ist wichtig, dass Sie sich darüber im Klaren sind, dass alle dem Verzeichnis zugeordneten DCs und DNS-Server offline sind, bis die Wiederherstellung abgeschlossen ist.

Gehen Sie folgendermaßen vor, um Ihr Verzeichnis mithilfe eines Snapshots wiederherzustellen.

So stellen Sie ein Verzeichnis mithilfe eines Snapshots wieder her

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Directory details (Verzeichnisdetails) die Registerkarte Maintenance (Wartung) aus.
4. Wählen Sie im Abschnitt Snapshots einen Snapshot in der Liste aus, klicken Sie auf Aktionen und anschließend auf Snapshot wiederherstellen.
5. Überprüfen Sie im Dialogfeld Verzeichnis-Snapshot wiederherstellen die Informationen und wählen Sie dann Wiederherstellen aus.

Bei einem Simple-AD-Verzeichnis dauert es vermutlich einige Minuten, bis das Verzeichnis wiederhergestellt ist. Nach einer erfolgreichen Wiederherstellung ändert sich der Wert Status für das

Verzeichnis zu `Active`. Alle Änderungen, die nach dem Datum vorgenommen wurden, an dem der Snapshot erstellt wurde, werden überschrieben.

Löschen eines Snapshots

So löschen Sie einen Snapshot

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Registerkarte Directory details (Verzeichnisdetails) die Registerkarte Maintenance (Wartung) aus.
4. Wählen Sie im Bereich Snapshots die Option Aktionen und anschließend die Option Snapshot löschen.
5. Überprüfen Sie, ob der Snapshot wirklich gelöscht werden soll, und wählen Sie dann Löschen aus.

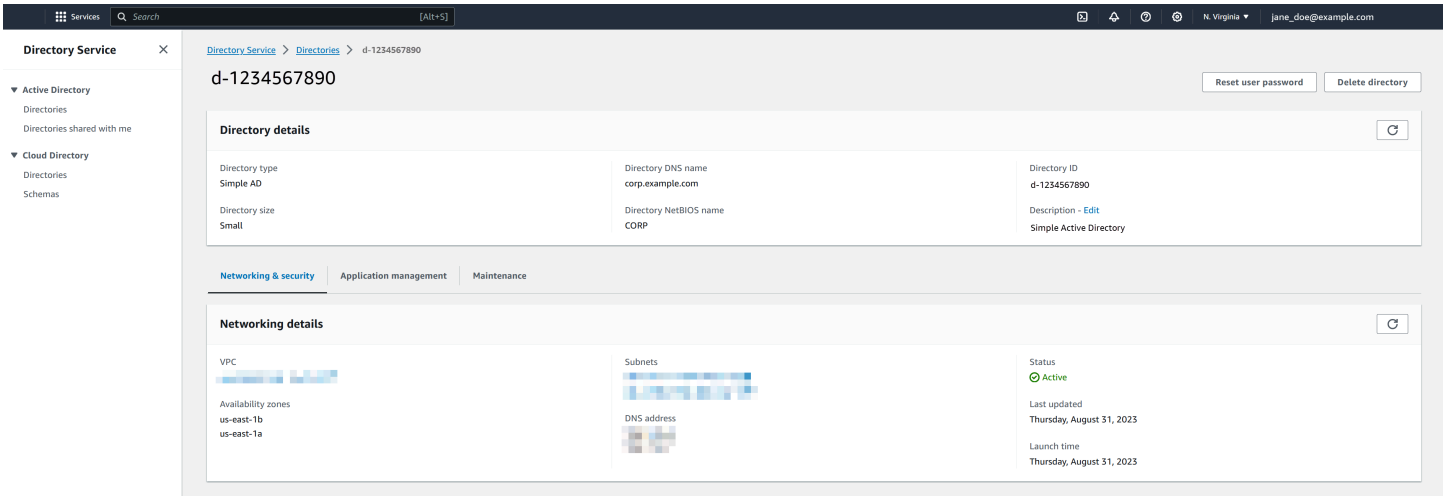
Verzeichnisinformationen anzeigen

Sie können detaillierte Informationen zu einem Verzeichnis einsehen.

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

1. Wählen Sie im Navigationsbereich der AWS Directory Service Konsole unter Active Directory Verzeichnisse aus.
2. Klicken Sie auf den Link der Verzeichnis-ID. Informationen über das Verzeichnis werden auf der Seite Verzeichnisdetails angezeigt.

Weitere Informationen zum Feld Status finden Sie unter Erläuterungen zum Verzeichnisstatus.



Aktivieren des Zugriffs auf AWS Anwendungen und Services

Benutzer können Simple AD autorisieren, AWS Anwendungen und Services wie Amazon WorkSpacesZugriff auf Ihr zu gewährenActive Directory. Die folgenden AWS Anwendungen und Services können für die Arbeit mit Simple AD aktiviert oder deaktiviert werden.

AWS Anwendung/Service	Weitere Informationen …
Amazon Chime	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Chime.
Amazon WorkDocs	Weitere Informationen finden Sie im Amazon-WorkDocs Administratorhandbuch.
Amazon WorkMail	Weitere Informationen finden Sie im Amazon-WorkMail Administratorhandbuch.
Amazon WorkSpaces	Sie können Simple AD, AWS Managed Microsoft AD oder AD Connector direkt aus erstellen WorkSpaces. Starten Sie einfach Advanced Setup bei der Erstellung Ihres Workspace. Weitere Informationen finden Sie im Amazon-WorkSpaces Administratorhandbuch.

AWS Anwendung/Service	Weitere Informationen …
AWS Management Console	Weitere Informationen finden Sie unter Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren.

Nach der Aktivierung verwalten Sie den Zugriff auf Ihre Verzeichnisse in der Konsole der Anwendung oder dem Service, denen Sie Zugriff auf Ihr Verzeichnis gewähren wollen. Führen Sie die folgenden Schritte aus, um die oben beschriebenen AWS Anwendungs- und Servicelinks in der AWS Directory Service Konsole zu finden.

Zum Anzeigen der Anwendungen und Services für ein Verzeichnis

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Sehen Sie sich die Liste im Abschnitt AWS -Anwendungen und -Services an.

Weitere Informationen zum Autorisieren oder Aufheben der Autorisierung von AWS Anwendungen und Services mit finden Sie AWS Directory Serviceunter Autorisierung für AWS Anwendungen und Dienste mit AWS Directory Service.

Themen

- Erstellen einer Zugriffs-URL
- Single Sign-On

Erstellen einer Zugriffs-URL

Eine Zugriffs-URL wird bei AWS-Anwendungen und -Services wie Amazon WorkDocs verwendet, um eine Anmeldeseite zu erreichen, die mit Ihrem Verzeichnis verknüpft ist. Die URL muss global eindeutig sein. Folgen Sie der Anleitung unten, um eine Zugriffs-URL für Ihr Verzeichnis zu erstellen.

> **Warning**
>
> Nachdem die URL für den Anwendungszugriff für dieses Verzeichnis erstellt wurde, kann sie nicht mehr geändert werden. Nachdem eine Zugriffs-URL erstellt wurde, kann sie nicht mehr von anderen verwendet werden. Beim Löschen Ihres Verzeichnisses wird auch die Zugriffs-URL gelöscht. Dann kann sie in einem anderen Konto genutzt werden.

So erstellen Sie eine Zugriffs-URL

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Wenn dem Verzeichnis keine Zugriffs-URL zugewiesen ist, wird im Bereich Application access URL (URL für den Anwendungszugriff) die Schaltfläche Create (Erstellen) angezeigt. Geben Sie einen Verzeichnisalias ein und wählen Sie Create (Erstellen) aus. Falls der Fehler Entity bereits vorhanden zurückgegeben wird, wurde das angegebene Alias bereits einem anderen Verzeichnis zugewiesen. Wählen Sie ein anderes Alias aus und wiederholen Sie die Schritte.

   Ihre Zugriffs-URL wird im Format `<alias>`.awsapps.com angegeben.

Single Sign-On

AWS Directory Service bietet die Möglichkeit, Ihren Benutzern den Zugriff auf Amazon WorkDocs von einem Computer aus zu ermöglichen, der mit dem Verzeichnis verbunden ist, ohne ihre Anmeldeinformationen separat eingeben zu müssen.

Bevor Sie Single Sign-On aktivieren, müssen Sie zusätzliche Schritte durchführen, um die Webbrowser Ihrer Benutzer zur Unterstützung von Single Sign-On vorzubereiten. Benutzer müssen eventuell ihre Web-Browser-Einstellungen ändern, um Single Sign-On zu ermöglichen.

> **Note**
>
> Single Sign-On funktioniert nur mit einem Computer, der dem AWS Directory Service - Verzeichnis beigetreten ist. Es kann nicht auf Computern verwendet werden, die nicht an das Verzeichnis angebunden sind.

Wenn es sich bei Ihrem Verzeichnis um ein AD Connector-Verzeichnis handelt und das AD Connector-Servicekonto nicht über die Berechtigung zum Hinzufügen oder Entfernen des Service-Prinzipalnamensattributs verfügt, stehen Ihnen für die folgenden Schritte 5 und 6 zwei Optionen zur Verfügung:

1. Sie können fortfahren und werden zur Eingabe des Benutzernamens und des Passworts für einen Verzeichnisbenutzer aufgefordert, der über diese Berechtigung zum Hinzufügen oder Entfernen des Service-Prinzipalnamensattributs für das AD Connector-Servicekonto verfügt. Diese Anmeldeinformationen werden nur verwendet, um Single Sign-On zu aktivieren, und werden nicht vom Service gespeichert. Die Berechtigungen des AD Connector-Servicekontos werden nicht geändert.
2. Sie können Berechtigungen delegieren, um es dem AD Connector Connector-Dienstkonto zu ermöglichen, das Dienstprinzipalnamenattribut für sich selbst hinzuzufügen oder zu entfernen. Sie können die folgenden PowerShell Befehle von einem Computer aus ausführen, der mit einer Domäne verbunden ist, und verwenden dabei ein Konto, das über die Berechtigungen für das AD Connector Connector-Dienstkonto verfügt. Der folgende Befehl gibt dem AD Connector-Servicekonto die Möglichkeit, ein Service-Prinzipalnamenattribut nur für sich selbst hinzuzufügen und zu entfernen.

```
$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"
```

Um Single Sign-On bei Amazon zu aktivieren oder zu deaktivieren WorkDocs

1. Wählen Sie im Navigationsbereich der AWS Directory Service -Konsole Verzeichnisse.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Wählen Sie im Abschnitt URL für den Anwendungszugriff die Option Aktivieren aus, um Single Sign-On für Amazon WorkDocs zu aktivieren.

   Wenn die Schaltfläche Aktivieren nicht angezeigt wird, müssen Sie zuerst eine Access-URL erstellen, bevor diese Option angezeigt wird. Weitere Informationen zum Erstellen einer Zugriffs-URL finden Sie unter Erstellen einer Zugriffs-URL.
5. Wählen Sie im Dialogfeld Single Sign-On für dieses Verzeichnis aktivieren die Option Aktivieren. Single Sign-On ist für das Verzeichnis aktiviert.
6. Wenn Sie Single Sign-On mit Amazon später deaktivieren möchten WorkDocs, wählen Sie Deaktivieren und wählen Sie dann im Dialogfeld Single Sign-On für dieses Verzeichnis deaktivieren erneut Deaktivieren aus.

Themen

- Single Sign-On für IE und Chrome
- Single Sign-On für Firefox

Single Sign-On für IE und Chrome

Damit die Browser Microsoft Internet Explorer (IE) und Google Chrome Single Sign-On unterstützen, müssen auf dem Client-Computer die folgenden Aufgaben durchgeführt werden:

- Fügen Sie Ihre Zugriffs-URL (z. B. https://*<alias>*.awsapps.com) zur Liste der zulässigen Websites für Single Sign-On hinzu.
- Aktivieren Sie Active Scripting (). JavaScript
- Erlauben Sie die automatische Anmeldung.
- Aktivieren Sie die integrierte Authentifizierung.

Sie oder Ihre Benutzer können diese Aufgaben manuell ausführen, oder Sie können diese Einstellungen mithilfe von Gruppenrichtlinieneinstellungen ändern.

Themen

Manuelles Update für Single Sign-On in Windows

Um Single Sign-On in einem Windows-Computer manuell zu aktivieren, führen Sie die folgenden Schritte auf dem Client-Computer aus. Einige dieser Einstellungen können bereits korrekt eingestellt sein.

Single Sign-On für Internet Explorer und Chrome unter Windows manuell aktivieren

1. Um das Dialogfeld Internet Properties zu öffnen, wählen Sie das Start-Menü, geben `Internet Options` in das Suchfeld ein, und wählen Internet Options.
2. Fügen Sie Ihre Zugriffs-URL zur Liste der zulässigen Websites für Single Sign-On hinzu, indem Sie die folgenden Schritte ausführen:
   a. Wählen Sie im Dialogfeld Internet Properties die Registerkarte Security.
   b. Wählen Sie Local intranet und Sites.
   c. Wählen Sie im Dialogfeld Local intranet die Option Advanced.
   d. Fügen Sie Ihre Zugriffs-URL zur Liste der Websites hinzu und klicken Sie auf Close.
   e. Wählen Sie im Dialogfeld Local intranet OK.
3. Zum Aktivieren der aktiven Skripts, führen Sie die folgenden Schritte aus:
   a. Wählen Sie auf der Registerkarte Security im Dialogfeld Internet Properties die Option Custom level.
   b. Scrollen Sie im Dialogfeld Security Settings - Local Intranet Zone nach unten bis Scripting und wählen Sie Enable unter Active scripting.
   c. Wählen Sie im Dialogfeld Security Settings - Local Intranet Zone OK.
4. Zum Aktivieren der automatischen Anmeldung, führen Sie die folgenden Schritte aus:

a. Wählen Sie auf der Registerkarte Security im Dialogfeld Internet Properties die Option Custom level.

b. Scrollen Sie im Dialogfeld Security Settings - Local Intranet Zone nach unten bis User Authentication und wählen Sie Automatic logon only in Intranet zone unter Logon.

c. Wählen Sie im Dialogfeld Security Settings - Local Intranet Zone OK.

d. Wählen Sie im Dialogfeld Security Settings - Local Intranet Zone OK.

5. Zum Aktivieren der integrierten Authentifizierung, führen Sie die folgenden Schritte aus:

a. Wählen Sie im Dialogfeld Internet Properties die Registerkarte Advanced.

b. Scrollen Sie nach unten bis Security, und wählen Sie Enable Integrated Windows Authentication.

c. Wählen Sie im Dialogfeld Internet Properties OK.

6. Schließen Sie den Browser und öffnen Sie ihn erneut, damit diese Änderungen wirksam werden.

Manuelles Update für Single Sign-On in OS X

Um manuell Single Sign-On für Chrome in OS X zu aktivieren, führen Sie die folgenden Schritte aus. Sie benötigen Administratorrechte auf Ihrem Computer, um diese Schritte ausführen zu können.

Single Sign-On für Chrome auf OS X manuell aktivieren

1. Fügen Sie der AuthServerAllowlistRichtlinie Ihre Zugriffs-URL hinzu, indem Sie den folgenden Befehl ausführen:

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. Öffnen Sie System Preferences, wechseln Sie in den Bereich Profiles und löschen Sie das Profil `Chrome Kerberos Configuration`.
3. Starten Sie Chrome neu und öffnen Sie chrome://policy in Chrome, um zu bestätigen, dass die neuen Einstellungen vorhanden sind.

Gruppenrichtlinieneinstellungen für Single Sign-On

Der Domain-Administrator kann Gruppenrichtlinieneinstellungen implementieren, um die Single-Sign-On-Änderungen auf Client-Computern durchzuführen, die mit der Domain verbunden sind.

> **Note**
>
> Wenn Sie die Chrome-Webbrowser auf den Computern in Ihrer Domain mit Chrome-Richtlinien verwalten, müssen Sie Ihre Zugriffs-URL zur AuthServerAllowlistRichtlinie hinzufügen. Weitere Informationen zum Einrichten von Chrome-Richtlinien finden Sie unter Policy-Einstellungen in Chrome.

Single Sign-On für Internet Explorer und Chrome mit Gruppenrichtlinieneinstellungen aktivieren

1. Erstellen Sie ein neues Gruppenrichtlinienobjekt, indem Sie die folgenden Schritte ausführen:
   a. Öffnen Sie das Tool für die Gruppenrichtlinienverwaltung, navigieren Sie zu Ihrer Domain und wählen Sie Group Policy Objects.
   b. Wählen Sie im Hauptmenü Action und dann New.
   c. Geben Sie in das Dialogfeld Neues GPO einen aussagekräftigen Namen für das Gruppenrichtlinienobjekt ein, wie beispielsweise `IAM Identity Center Policy`, und behalten Sie für Source Starter GPO den Eintrag (kein) bei. Klicken Sie auf OK.
2. Fügen Sie die Zugriffs-URL zur Liste der zulässigen Websites für Single Sign-On hinzu, indem Sie die folgenden Schritte ausführen:
   a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Gruppenrichtlinienobjekte, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre IAM-Identity-Center-Richtlinie und wählen Sie Bearbeiten.
   b. Navigieren Sie in der Richtlinien-Baumstruktur zu User Configuration > Preferences > Windows Settings.
   c. Öffnen Sie in der Liste Windows Settings das Kontextmenü (Rechtsklick) für Registry und wählen Sie New registry item.
   d. Geben Sie im Dialogfeld New Registry Properties die folgenden Einstellungen ein, und wählen Sie OK:

      Action (Aktion)

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

Pfad

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

Der Wert für den *<alias>* wird von Ihrer Zugriffs-URL abgeleitet. Wenn Ihre Zugriffs-URL `https://examplecorp.awsapps.com` ist, wird `examplecorp` der Alias und der Registrierungsschlüssel wird `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`.

Wertname

```
https
```

Werttyp

```
REG_DWORD
```

Wertdaten

```
1
```

3. Zum Aktivieren der aktiven Skripts, führen Sie die folgenden Schritte aus:

   a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Gruppenrichtlinienobjekte, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre IAM-Identity-Center-Richtlinie und wählen Sie Bearbeiten.

   b. Navigieren Sie in der Richtlinien-Baumstrukturzu Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

   c. Öffnen Sie in der Liste Intranet Zone das Kontextmenü (Rechtsklick) für Allow active scripting und wählen Sie Edit.

   d. Geben Sie im Dialogfeld Allow active scripting die folgenden Einstellungen ein, und wählen Sie OK:

      - Wählen Sie das Optionsfeld Enabled.
      - Setzen Sie unter Options die Option Allow active scripting auf Enable.

4. Zum Aktivieren der automatischen Anmeldung, führen Sie die folgenden Schritte aus:

a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Group Policy Objects, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre SSO-Richtlinie und wählen Sie Bearbeiten.

b. Navigieren Sie in der Richtlinien-Baumstrukturzu Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone.

c. Öffnen Sie in der Liste Intranet Zone das Kontextmenü (Rechtsklick) für Logon options und wählen Sie Edit.

d. Geben Sie im Dialogfeld Logon options die folgenden Einstellungen ein, und wählen Sie OK:

   - Wählen Sie das Optionsfeld Enabled.
   - Setzen Sie unter Options die Logon options auf Automatic logon only in Intranet zone.

5. Zum Aktivieren der integrierten Authentifizierung, führen Sie die folgenden Schritte aus:

a. Im Tool für die Gruppenrichtlinienverwaltung navigieren Sie zu Ihrer Domain, wählen Sie Gruppenrichtlinienobjekte, öffnen Sie das Kontextmenü (Rechtsklick) für Ihre IAM-Identity-Center-Richtlinie und wählen Sie Bearbeiten.

b. Navigieren Sie in der Richtlinien-Baumstruktur zu User Configuration > Preferences > Windows Settings.

c. Öffnen Sie in der Liste Windows Settings das Kontextmenü (Rechtsklick) für Registry und wählen Sie New registry item.

d. Geben Sie im Dialogfeld New Registry Properties die folgenden Einstellungen ein, und wählen Sie OK:

   Action (Aktion)

   ```
   Update
   ```

   Hive

   ```
   HKEY_CURRENT_USER
   ```

   Pfad

   ```
   Software\Microsoft\Windows\CurrentVersion\Internet Settings
   ```

   Wertname

   ```
   EnableNegotiate
   ```

Werttyp

`REG_DWORD`

Wertdaten

1

6. Schließen Sie das Fenster Group Policy Management Editor, falls es noch geöffnet ist.
7. Weisen Sie die neue Richtlinie Ihrer Domain zu, indem Sie die folgenden Schritte ausführen:
   a. Öffnen Sie im Gruppenrichtlinien-Baum das Kontextmenü (Rechtsklick) für Ihre Domain, und wählen Sie Link an Existing GPO.
   b. Wählen Sie in der Liste Gruppenrichtlinienobjekte Ihre IAM-Identity-Center-Richtlinie, und wählen Sie OK.

Diese Änderungen werden nach dem nächsten Gruppenrichtlinien-Update auf dem Client wirksam, oder wenn sich der Benutzer das nächste Mal anmeldet.

Single Sign-On für Firefox

Damit der Mozilla Firefox-Browser Single Sign-On unterstützt, fügen Sie Ihre Zugriffs-URL (z. B. https://*<alias>*.awsapps.com) der Liste der genehmigten Websites für Single Sign-On hinzu. Dies kann manuell oder automatisiert durch ein Skript erfolgen.

Themen

- Manuelles Update für Single Sign-On
- Automatisches Update für Single Sign-On

Manuelles Update für Single Sign-On

Um manuell Ihre Zugriffs-URL zur Liste der zulässigen Websites in Firefox hinzuzufügen, führen Sie die folgenden Schritte auf dem Client-Computer aus.

So fügen Sie manuell Ihre Zugriffs-URL zur Liste der zulässigen Websites in Firefox hinzu

1. Öffnen Sie Firefox und öffnen Sie die Seite `about:config`.
2. Öffnen Sie die Einstellung `network.negotiate-auth.trusted-uris` und fügen Sie Ihre Zugriffs-URL der Liste der Websites hinzu. Verwenden Sie ein Komma (,), um mehrere Einträge zu trennen.

Automatisches Update für Single Sign-On

Als Domainadministrator können Sie ein Skript hinzufügen, um Ihre Zugriffs-URL auf allen Computern in Ihrem Netzwerk der Firefox-Benutzereinstellung `network.negotiate-auth.trusted-uris` hinzuzufügen. Weitere Informationen finden Sie unter https://support.mozilla.org/en-US/questions/939037.

Den Zugriff auf die AWS Management Console mit AD-Anmeldeinformationen aktivieren

AWS Directory Service ermöglicht es Ihnen, Mitgliedern Ihres Verzeichnisses Zugriff auf AWS Management Console zu gewähren. Standardmäßig haben die Mitglieder Ihres Verzeichnisses keinen Zugriff auf AWS-Ressourcen. Sie weisen Ihren Verzeichnismitgliedern IAM-Rollen zu, um ihnen Zugriff auf die verschiedenen AWS-Services und Ressourcen zu geben. Die IAM-Rolle definiert die Services, Ressourcen und Zugriffsebenen, die für das Mitglied Ihres Verzeichnisses verfügbar sind.

Bevor Sie den Mitgliedern Ihres Verzeichnisses Konsolenzugriff gewähren können, muss das Verzeichnis über eine Zugriffs-URL verfügen. Weitere Informationen zum Abrufen von Verzeichnisdetails und der Zugriffs-URL finden Sie unter Verzeichnisinformationen anzeigen. Weitere Informationen zum Erstellen einer Zugriffs-URL finden Sie unter Erstellen einer Zugriffs-URL.

Weitere Informationen zum Erstellen von IAM-Rollen und zum Zuweisen dieser Rollen zu den Mitgliedern Ihres Verzeichnisses finden Sie unter Benutzern und Gruppen den Zugriff auf AWS - Ressourcen gewähren.

Themen

- AWS Management Console-Zugriff aktivieren
- AWS Management Console-Zugriff deaktivieren
- Die Dauer der Anmeldesitzung festlegen

Zugehöriger Blog-Artikel zur AWS-Sicherheit

- Wie Sie mit AWS Managed Microsoft AD und Ihren On-Premises-Anmeldeinformationen auf die AWS Management Console zugreifen

AWS Management Console-Zugriff aktivieren

Standardmäßig ist der Konsolenzugriff für kein Verzeichnis aktiviert. Gehen Sie zum Aktivieren des Konsolenzugriffs für Benutzer und Gruppen in Ihrem Verzeichnis folgendermaßen vor:

So aktivieren Sie den Konsolenzugriff

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Wählen Sie unter dem Abschnitt AWS Management Console die Option Aktivieren aus. Der Konsolenzugriff ist jetzt für Ihr Verzeichnis aktiviert.

   Bevor sich die Benutzer mit Ihrer Zugangs-URL bei der Konsole anmelden können, müssen Sie Ihre Benutzer zunächst der Rolle hinzufügen. Weitere Informationen zum Zuweisen von Benutzern zu IAM-Rollen finden Sie unter Zuweisen von Benutzern oder Gruppen zu einer vorhandenen Rolle. Nachdem die IAM-Rollen zugewiesen wurden, können die entsprechenden Benutzer über die Zugriffs-URL auf die Konsole zugreifen. Lautet die Zugriffs-URL Ihres Verzeichnisses zum Beispiel „example-corp.awsapps.com“, lautet die URL für den Zugriff auf die Konsole „https://example-corp.awsapps.com/console/“.

AWS Management Console-Zugriff deaktivieren

Gehen Sie zum Deaktivieren des Konsolenzugriffs für Benutzer und Gruppen in Ihrem Verzeichnis folgendermaßen vor:

So deaktivieren Sie den Konsolenzugriff

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Wählen Sie im Abschnitt AWS Management Console die Option Deaktivieren aus. Der Konsolenzugriff ist jetzt für Ihr Verzeichnis deaktiviert.
5. Nach dem Zuweisen von IAM-Rollen zu Benutzern oder Gruppen im Verzeichnis ist die Schaltfläche Deaktivieren möglicherweise nicht mehr verfügbar. In diesem Fall müssen Sie alle

IAM-Rollenzuweisungen für das Verzeichnis entfernen, bevor Sie fortfahren, einschließlich der Zuweisungen für Benutzer oder Gruppen in Ihrem Verzeichnis, die gelöscht wurden, was als Gelöschter Benutzer oder Gelöschte Gruppe angezeigt wird.

Nachdem alle IAM-Rollenzuweisungen entfernt wurden, wiederholen Sie die oben genannten Schritte.

Die Dauer der Anmeldesitzung festlegen

Standardmäßig haben die Benutzer 1 Stunde Zeit, um nach dem Anmelden in der Konsole eine Sitzung zu nutzen, bevor sie abgemeldet werden. Nach dieser Zeit müssen sich die Benutzer erneut anmelden, um eine weitere 1-stündige Sitzung zu starten, bevor sie erneut abgemeldet werden. Gehen Sie folgendermaßen vor, um die Dauer auf bis zu 12 Stunden pro Sitzung zu ändern.

So legen Sie die Dauer der Anmeldesitzung fest

1. Wählen Sie im Navigationsbereich der AWS Directory Service-Konsole Directories aus.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Application Management (Anwendungsverwaltung) aus.
4. Wählen Sie unter dem Abschnitt AWS-Anwendungen und -Services die Option AWS-Managementkonsole.
5. Wählen Sie im Dialogfeld Zugriff auf AWS-Ressourcen verwalten die Option Fortfahren.
6. Bearbeiten Sie auf der Seite Assign users and groups to IAM roles unter Set login session length den Zahlenwert, und wählen Sie dann Save.

Tutorial: Erstellen Sie ein Simple AD Active Directory

Das folgende Tutorial führt Sie durch alle Schritte, die zum Einrichten eines Simple AD Active Directory erforderlich sind. Es soll Ihnen einen Active Directory schnellen und einfachen Einstieg in Simple AD ermöglichen, ist jedoch nicht für den Einsatz in einer umfangreichen Produktionsumgebung vorgesehen.

Tutorial-Voraussetzungen

In diesem Tutorial wird von Folgendem ausgegangen:

- Sie haben eine aktive AWS-Konto.
- Ihr Konto hat das Limit an Amazon VPCs für die Region, in der Sie Simple AD verwenden möchten, nicht erreicht. Weitere Informationen zu VPC finden Sie unter Was ist Amazon VPC? und Subnetze in Ihrer VPC im Amazon VPC-Benutzerhandbuch.
- Sie haben in der Region keine bestehende VPC mit einem CIDR von. `10.0.0.0/16`

Weitere Informationen finden Sie unter Simple-AD-Voraussetzungen.

Schritt 1: Erstellen und konfigurieren Sie Ihre Amazon VPC für Simple AD Active Directory

Erstellen und konfigurieren Sie eine Amazon VPC für die Verwendung mit Simple AD. Bevor Sie dieses Verfahren beginnen, stellen Sie sicher, dass Sie die Tutorial-Voraussetzungen erfüllt haben.

Erstellen Sie eine VPC für Ihr Simple AD Active Directory

Erstellen Sie eine VPC mit zwei öffentlichen Subnetzen. AWS Directory Service erfordert zwei Subnetze in Ihrer VPC, und jedes Subnetz muss sich in einer anderen Availability Zone befinden.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard VPC erstellen aus.
3. Wählen Sie unter VPC-Einstellungen die Option VPC und mehr aus.
4. Füllen Sie die Felder wie folgt aus:
    - Lassen Sie die Option Automatisch generiert unter Automatische Generierung von Namens-Tags ausgewählt. Ändern Sie Projekt zu `ADS VPC`.
    - Der IPv4-CIDR-Block sollte `10.0.0.0/16` sein.
    - Lassen Sie die Option Kein IPv6-CIDR-Block ausgewählt.
    - Die Tenancy sollte Standard bleiben.
    - Wählen Sie für Anzahl der Availability Zones (AZs) den Wert 2.
    - Wählen Sie für Anzahl der öffentlichen Subnetze den Wert 2 aus. Die Anzahl der privaten Subnetze kann auf 0 geändert werden.
    - Wählen Sie Subnetz-CIDR-Blöcke anpassen, um den IP-Adressbereich des öffentlichen Subnetzes zu konfigurieren. Die CIDR-Blöcke des öffentlichen Subnetzes sollten `10.0.0.0/20` und `10.0.16.0/20` sein.
5. Wählen Sie VPC erstellen aus. Es dauert einige Minuten, bis die VPC erstellt wird.

Schritt 2: Erstellen Sie Ihr Simple AD Active Directory

Gehen Sie wie folgt vor, um ein neues Simple AD Active Directory zu erstellen. Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie die unter Schritt 1: Erstellen Tutorial-Voraussetzungen und Konfigurieren Ihrer Amazon VPC für Simple AD Active Directory genannten Voraussetzungen erfüllt haben.

So erstellen Sie ein Simple AD Active Directory

1. Wählen Sie im Navigationsbereich AWS Directory Service -Konsole den Eintrag Verzeichnisse und wählen Sie Verzeichnis einrichten aus.
2. Wählen Sie auf der Seite Verzeichnistyp auswählen die Option Simple AD aus und klicken Sie dann auf Weiter.
3. Geben Sie auf der Seite Enter directory information (Verzeichnisinformationen eingeben) die folgenden Informationen ein:

   Verzeichnisgröße

   Wählen Sie die Größenoption Small (Klein) oder Large (Groß). Weitere Informationen über Größen finden Sie unter Simple AD.

   Name der Organisation

   Ein eindeutiger Organisationsname für Ihr Verzeichnis, der für die Registrierung von Client-Geräten verwendet wird.

   Dieses Feld ist nur verfügbar, wenn Sie Ihr Verzeichnis im Rahmen des Starts erstellen WorkSpaces.

   DNS-Name des Verzeichnisses

   Den vollständig qualifizierten Namen für das Verzeichnis, z. B. `corp.example.com`.

   NetBIOS-Name des Verzeichnisses

   Die kurzen Namen für das Verzeichnis, z. B. `CORP`.

   Administrator password

   Das Passwort für den Verzeichnisadministrator. Beim Erstellen des Verzeichnisses wird ein Administratorkonto mit dem Benutzernamen `Administrator` und diesem Passwort erstellt.

Das Verzeichnisadministrator-Passwort unterscheidet zwischen Groß-/ Kleinschreibung und muss zwischen 8 und 64 Zeichen lang sein. Zudem muss es mindestens ein Zeichen aus dreien der vier folgenden Kategorien enthalten:

- Kleinbuchstaben (a – z)
- Großbuchstaben (A – Z)
- Zahlen (0 – 9)
- Nicht-alphanumerische Zeichen (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

Confirm password (Passwort bestätigen)

Geben Sie das Administratorpasswort erneut ein.

Verzeichnisbeschreibung

Eine optionale Beschreibung des Verzeichnisses.

4. Geben Sie auf der Seite Choose VPC and subnets (VPC und Subnetze wählen) die folgenden Informationen an und wählen Sie dann Next (Weiter).

   VPC

   Die VPC für das Verzeichnis.

   Subnets

   Wählen Sie Subnetze für die Domain-Controller aus. Die beiden Subnetze müssen zu verschiedenen Availability-Zonen gehören.

5. Überprüfen Sie auf der Seite Review & create (Überprüfen und erstellen) die Verzeichnisinformationen und nehmen Sie gegebenenfalls Änderungen vor. Wenn die Informationen richtig sind, wählen Sie Create directory (Verzeichnis erstellen). Es dauert einige Minuten, bis das Verzeichnis erstellt wurde. Sobald sie erstellt wurden, ändert sich der Status in Active.

Bewährte Methoden für Simple AD

Hier sind einige Vorschläge und Richtlinien, die Sie berücksichtigen sollten, um Probleme zu vermeiden und Simple AD optimal zu nutzen.

Einrichten: Voraussetzungen

Beachten Sie die folgenden Richtlinien, bevor Sie Ihr Verzeichnis erstellen.

Sicherstellen, dass Sie den richtigen Verzeichnistyp verwenden

AWS Directory Service bietet mehrere Möglichkeiten zur Verwendung Microsoft Active Directory mit anderen AWS Diensten. Sie können den Verzeichnisdienst mit den Funktionen wählen, die Sie benötigen, ohne Ihr Budget zu überlasten:

- AWS Der Directory Service für Microsoft Active Directory ist ein funktionsreicher, verwalteter Dienst, der in der Microsoft Active Directory AWS Cloud gehostet wird. AWS Managed Microsoft AD ist die beste Wahl, wenn Sie mehr als 5.000 Benutzer haben und eine Vertrauensbeziehung zwischen einem AWS gehosteten Verzeichnis und Ihren lokalen Verzeichnissen einrichten möchten.
- AD Connector verbindet einfach Ihr vorhandenes lokales System Active Directory mit AWS. AD Connector ist die beste Wahl, wenn Sie Ihr vorhandenes On-Premises-Verzeichnis mit AWS - Services verwenden möchten.
- Simple AD ist ein niedriges, kostengünstiges Verzeichnis mit grundlegender Active Directory Kompatibilität. Es unterstützt 5 000 oder weniger Benutzer, Samba-4-kompatible Anwendungen und LDAP-Kompatibilität für LDAP-fähige Anwendungen.

Einen detaillierteren Vergleich der AWS Directory Service Optionen finden Sie unterWelche sollte man auswählen.

Sicherstellen, dass Ihre VPCs und Instances korrekt konfiguriert sind

Um eine Verbindung zu Ihren Verzeichnissen herzustellen, sie zu verwalten und zu nutzen, müssen Sie die VPCs, denen die Verzeichnisse zugeordnet sind, ordnungsgemäß konfigurieren. Weitere Informationen über die Anforderungen zur VPC-Sicherheit und Netzwerken finden Sie unter AWS Voraussetzungen für verwaltetes Microsoft AD, AD-Connector-Voraussetzungen oder Simple-AD-Voraussetzungen.

Wenn Sie Ihrer Domain eine Instance hinzufügen, stellen Sie sicher, dass Sie eine Verbindung und Remote-Zugriff auf Ihre Instance haben, wie in Verbinden Sie eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD Active Directory beschrieben.

Sich der eigenen Grenzen bewusst sein

Erfahren Sie mehr über die verschiedenen Beschränkungen für Ihren spezifischen Verzeichnistyp. Der verfügbare Speicherplatz und die Gesamtgröße Ihrer Objekte sind die einzigen Einschränkungen in Bezug auf die Anzahl der Objekte, die Sie in Ihrem Verzeichnis speichern können. Einzelheiten zu dem von Ihnen ausgewählten Verzeichnis finden Sie unter AWS Verwaltete Microsoft AD-Kontingente, Kontingente für AD Connector oder Kontingente für Simple AD.

Machen Sie sich mit der Konfiguration und Verwendung der AWS Sicherheitsgruppen in Ihrem Verzeichnis vertraut

AWS erstellt eine Sicherheitsgruppe und fügt sie den elastischen Netzwerkschnittstellen des Domänencontrollers Ihres Verzeichnisses hinzu. AWS konfiguriert die Sicherheitsgruppe so, dass unnötiger Datenverkehr zum Verzeichnis blockiert wird, und lässt notwendigen Datenverkehr zu.

Ändern der Verzeichnissicherheitsgruppe

Wenn Sie die Sicherheit der Sicherheitsgruppen Ihrer Verzeichnisse ändern möchten, können Sie dies tun. Nehmen Sie diese Änderungen nur vor, wenn Sie verstehen, wie Sicherheitsgruppenfilter funktionieren. Weitere Informationen finden Sie unter Amazon-EC2-Sicherheitsgruppen für Linux-Instances im Amazon-EC2-Benutzerhandbuch. Unsachgemäße Änderungen können zum Verlust der Kommunikation mit den vorgesehenen Computern und Instanzen führen. AWS empfiehlt, nicht zu versuchen, zusätzliche Ports für Ihr Verzeichnis zu öffnen, da dies die Sicherheit Ihres Verzeichnisses beeinträchtigt. Sehen Sie sich das AWS -Modell übergreifender Verantwortlichkeit genau an.

> **Warning**
>
> Es ist technisch möglich, dass Sie die Sicherheitsgruppe des Verzeichnisses anderen von Ihnen erstellten EC2-Instances zuordnen. AWS Empfiehlt jedoch von dieser Vorgehensweise ab. AWS kann Gründe haben, die Sicherheitsgruppe ohne vorherige Ankündigung zu ändern, um den Funktions- oder Sicherheitsanforderungen des verwalteten Verzeichnisses gerecht zu werden. Solche Änderungen wirken sich auf alle Instances aus, denen Sie die Verzeichnis-Sicherheitsgruppe zuordnen, und können den Betrieb der dazugehörigen Instances stören. Außerdem entsteht durch die Zuordnung der Verzeichnis-Sicherheitsgruppe zu Ihren EC2-Instances möglicherweise ein potenzielles Sicherheitsrisiko für Ihre EC2-Instances.

Verwenden Sie AWS Managed Microsoft AD, wenn Vertrauensstellungen erforderlich sind

Simple AD unterstützt keine Vertrauensstellungen. Wenn Sie eine Vertrauensstellung zwischen Ihrem AWS Directory Service Verzeichnis und einem anderen Verzeichnis einrichten müssen, sollten Sie den AWS Directory Service für Microsoft Active Directory verwenden.

Einrichten: Erstellen Ihres Verzeichnisses

Hier finden Sie einige Vorschläge, wie Sie Ihr Verzeichnis erstellen.

Ihre Administratoren-ID und das Passwort nicht vergessen

Wenn Sie Ihr Verzeichnis einrichten, geben Sie ein Passwort für das Administratorkonto ein. Die Konto-ID für Simple AD lautet Administrator. Merken Sie sich das Passwort, das Sie für dieses Konto erstellen. Andernfalls können Sie keine Objekte in Ihrem Verzeichnis hinzufügen.

Machen Sie sich mit Benutzernamenbeschränkungen für AWS Anwendungen vertraut

AWS Directory Service unterstützt die meisten Zeichenformate, die bei der Erstellung von Benutzernamen verwendet werden können. Es gibt jedoch Zeichenbeschränkungen, die für Benutzernamen gelten, die für die Anmeldung bei AWS Anwendungen wie WorkSpaces Amazon, Amazon oder Amazon WorkDocs verwendet werden. WorkMail QuickSight Diese Einschränkungen verlangen, dass die folgenden Zeichen nicht verwendet werden:

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

> **Note**
>
> Das Symbol @ ist zulässig, wenn es einem UPN-Suffix vorausgeht.

Programmieren Ihrer Anwendungen

Stellen Sie folgende Überlegungen an, ehe Sie Ihre Anwendungen programmieren:

Den Windows-DC-Suchservice verwenden

Verwenden Sie bei der Entwicklung von Anwendungen den Windows DC Locator Service oder den Dynamic DNS (DDNS) -Dienst Ihres AWS verwalteten Microsoft AD, um nach Domänencontrollern (DCs) zu suchen. Nehmen Sie keine Hartkodierung an Anwendungen mit der Adresse eines Domain-Controllers vor. Der DC-Suchdienst sorgt für eine Verteilung der Verzeichnislast und ermöglicht Ihnen die Nutzung einer horizontalen Skalierung durch das Hinzufügen von Domain-Controllern zu Ihrer Bereitstellung. Wenn Sie Ihre Anwendung an einen bestimmten DC binden und ein Patchen oder eine Wiederherstellung des DCs durchgeführt wird, verliert Ihre Anwendung den Zugriff auf den DC und kann die restlichen DCs nicht nutzen. Darüber hinaus kann eine feste DC-Kodierung dazu führen, dass ein einzelner DC zu einem Hotspot wird. In extremen Fällen kann dies dazu führen, dass Ihr DC nicht mehr reagiert. Solche Fälle können auch dazu führen, dass die AWS Verzeichnisautomatisierung das Verzeichnis als beeinträchtigt kennzeichnet und Wiederherstellungsprozesse auslöst, die den nicht reagierenden DC ersetzen.

Auslastungstests vor der Inbetriebnahme

Führen Sie Labortests mit Objekten und Anforderungen durch, die Ihren Produktions-Workload darstellen, um sicherzustellen, dass das Verzeichnis entsprechend der Arbeitslast Ihrer Anwendung skaliert wird. Wenn Sie zusätzliche Kapazität benötigen, sollten Sie Microsoft Active Directory verwenden AWS Directory Service , mit dem Sie Domänencontroller hinzufügen können, um eine hohe Leistung zu erzielen. Weitere Informationen finden Sie unter Bereitstellen zusätzlicher Domain-Controller.

Effiziente LDAP-Abfragen verwenden

Umfassende LDAP-Abfragen für einen Domain-Controller über Tausende von Objekten können umfangreiche CPU-Zyklen auf einem einzelnen DC verursachen und ein Hot Spotting nach sich ziehen. Dies kann Auswirkungen auf Anwendungen haben, die während der Abfrage denselben DC verwenden.

Kontingente für Simple AD

Im Allgemeinen sollten Sie nicht mehr als 500 Benutzer zu einem kleinen Simple-AD-Verzeichnis und nicht mehr als 5 000 Benutzer zu einem großen Simple-AD-Verzeichnis hinzufügen. Für flexiblere Skalierungsoptionen und zusätzliche Active-Directory-Features sollten Sie stattdessen AWS Directory Service for Microsoft Active Directory (Standard Edition oder Enterprise Edition) verwenden.

Im Folgenden sind die Standardgrenzwerte für Simple AD aufgeführt. Jedes Kontingent gilt pro Region, sofern nicht anders angegeben.

Kontingente für Simple AD

Ressource	Standardkontingent
Verzeichnisse in Simple AD	10
Manuelle Snapshots*	5 pro Simple AD

* Das Kontingent für manuelle Snapshots kann nicht geändert werden.

> **Note**
>
> Sie können Ihrer Elastic Network-Schnittstelle (ENI) von AWS öffentliche IP-Adresse zuweisen.

Richtlinie zur Anwendungskompatibilität für Simple AD

Simple AD ist eine Samba-Implementierung, die viele der grundlegenden Features von Active Directory bereitstellt. Aufgrund der Masse an benutzerdefinierten und kommerziellen Standardanwendungen, die Active Directory nutzen, führt AWS keine formale oder umfangreiche Verifizierung der Kompatibilität von Drittanbieteranwendungen mit Simple AD durch. Obwohl AWS mit Kunden an der Überwindung möglicher Schwierigkeiten bei der Anwendungsinstallation arbeitet, können wir nicht garantieren, dass alle Anwendungen mit Simple AD kompatibel sind oder kompatibel bleiben.

Die folgenden Anwendungen von Drittanbietern sind mit Simple AD kompatibel:

- Microsoft Internet Information Services (IIS) auf den folgenden Plattformen:
  - 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 (Express, Web und Standard Editionen)
  - SQL Server 2008 R2 (Express, Web und Standard Editionen)
  - SQL Server 2012 (Express, Web und Standard Editionen)
  - SQL Server 2014 (Express, Web und Standard Editionen)
- Microsoft SharePoint:
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

Kunden können sich für die Verwendung von AWS Directory Service für Microsoft Active Directory (AWS Verwaltetes Microsoft AD) für einen höheren Grad an Kompatibilität basierend auf dem tatsächlichen Active Directory entscheiden.

Beheben von Fehlern in Simple AD

Die folgenden Informationen können Ihnen beim Beheben von ein paar gängigen Problemen behilflich sein, die beim Erstellen oder Benutzen Ihres Verzeichnisses auftreten können.

Themen

Wiederherstellen des Passworts

Wenn ein Benutzer ein Passwort vergisst oder Probleme hat, sich in Ihrem Simple AD- oder AWS Managed Microsoft AD-Verzeichnis anzumelden, können Sie sein Passwort entweder mit dem AWS Management Console, Windows PowerShell oder dem AWS CLI zurücksetzen.

Weitere Informationen finden Sie unter Setzen Sie ein Simple AD AD-Benutzerkennwort zurück.

Beim Hinzufügen eines Benutzers zu Simple AD wird der Fehler „KDC kann die angeforderte Option nicht erfüllen“ angezeigt

Dies kann passieren, wenn der Samba CLI-Client die net-Befehle nicht ordnungsgemäß an alle Domain-Controller sendet. Falls Sie diese Fehlermeldung bei der Verwendung des Befehls „net ads“ zum Hinzufügen eines Benutzers zu Ihrem Simple AD-Verzeichnis verwenden, verwenden Sie das -S Argument und geben Sie die IP-Adresse von einem Ihrer Domain-Controller an. Falls immer noch ein Fehler angezeigt wird, testen Sie den anderen Domain-Controller. Sie können auch die Active Directory-Verwaltungstools verwenden, um Ihrem Verzeichnis Benutzer hinzuzufügen. Weitere Informationen finden Sie unter Installieren Sie die Active Directory-Verwaltungstools für Simple AD.

Ich kann den DNS-Namen oder die IP-Adresse einer meiner Domain zugeordneten Instance nicht aktualisieren (dynamische DNS-Aktualisierung).

Dynamische DNS-Aktualisierungen werden von Simple-AD-Domains nicht unterstützt. Stattdessen können Sie die Änderungen direkt vornehmen, indem Sie Ihr Verzeichnis per DNS-Manager mit einer Instance verbinden, die Ihrer Domain zugeordnet ist.

Ich kann mich mit einem SQL-Serverkonto nicht dort anmelden.

Möglicherweise wird ein Fehler angezeigt, wenn Sie versuchen, SQL Server Management Studio (SSMS) zusammen mit einem SQL-Server-Konto für die Anmeldung bei einem SQL Server zu verwenden, der in einer R2-EC2-Instance von Windows 2012 ausgeführt wird. Das Problem tritt auf, wenn SSMS als Domain-Benutzer ausgeführt wird, und kann auch bei gültigen Anmeldeinformationen dazu führen, dass der Fehler „Fehlgeschlagene Benutzeranmeldung” angezeigt wird. Dies ist ein bekanntes Problem und wir AWS arbeiten aktiv daran, es zu lösen.

Um das Problem zu umgehen, können Sie sich anstelle einer SQL- mit einer Windows-Authentifizierung beim SQL-Server anmelden. Oder Sie starten SSMS als lokalen anstatt als Simple AD-Domain-Benutzer.

Mein Verzeichnis bleibt dauerhaft im Status „Angefragt”

Wenn sich Ihr Verzeichnis länger als fünf Minuten im „Angefragt”-Status befindet, löschen Sie das Verzeichnis und erstellen es neu. Wenn dieses Problem weiterhin besteht, wenden Sie sich an das AWS Support -Zentrum.

Der Fehler „Beschränktes AZ” wird angezeigt, wenn ich ein Verzeichnis erstellen will

Einige AWS Konten, die vor 2012 erstellt wurden, haben möglicherweise Zugriff auf Availability Zones in den Regionen USA Ost (Nord-Virginia), USA West (Nordkalifornien) oder Asien-Pazifik (Tokio), die keine AWS Directory Service Verzeichnisse unterstützen. Wenn während der Erstellung eines Verzeichnisses ein Fehler wie dieser angezeigt wird, wählen Sie ein Subnetz aus einer anderen Availability Zone und erstellen Sie das Verzeichnis erneut.

Einige meiner Benutzer können sich in meinem Verzeichnis nicht authentifizieren.

Für Ihre Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Das ist die Standardeinstellung für neue Benutzerkonten und sollte nicht geändert werden. Weitere Informationen zu dieser Einstellung finden Sie unter Vorauthentifizierung auf Microsoft TechNet.

Weitere Ressourcen

Die folgenden Ressourcen können Ihnen bei der Problembehandlung bei der Arbeit mit AWS helfen.

- AWS Knowledge Center — Hier finden Sie häufig gestellte Fragen und Links zu anderen Ressourcen, die Ihnen bei der Behebung von Problemen helfen.
- AWS Support Center — Holen Sie sich technischen Support.
- AWS Premium Support Center — Holen Sie sich erstklassigen technischen Support.

Themen

Gründe für den Simple-AD-Verzeichnisstatus

Wenn ein Verzeichnis beeinträchtigt oder nicht funktionsfähig ist, enthält die Verzeichnis-Statusmeldung weitere Informationen. Die Statusmeldung wird in der AWS Directory Service-Konsole angezeigt oder in dem `DirectoryDescription.StageReason`-Mitglied von der `DescribeDirectories`-API zurückgegeben. Weitere Informationen über den Verzeichnisstatus finden Sie unter Erläuterungen zum Verzeichnisstatus.

Die folgenden Meldungen sind Statusmeldungen für ein Simple-AD-Verzeichnis:

Themen

Die Elastic-Network-Schnittstelle des Verzeichnisdienstes ist nicht verbunden

Beschreibung

Die entscheidende Elastic-Network-Schnittstelle (ENI), die in Ihrem Namen bei der Verzeichniserstellung erstellt wurde, um die Netzwerkkonnektivität mit Ihrer VPC herzustellen, ist nicht mit der Directory-Instance verbunden. AWS-Anwendungen, die von diesem Verzeichnis unterstützt werden, werden nicht funktionieren. Ihr Verzeichnis kann keine Verbindung zu Ihrem On-Premises-Netzwerk herstellen.

Fehlerbehebung

Wenn die ENI getrennt ist, aber immer noch existiert, wenden Sie sich an AWS Support. Wenn die ENI gelöscht wird, gibt es keine Möglichkeit, das Problem zu lösen, und Ihr Verzeichnis ist dauerhaft unbrauchbar. Sie müssen Ihr Verzeichnis löschen und ein neues erstellen.

Probleme wurden von der Instance erkannt

Beschreibung

Ein interner Fehler wurde von der Instance festgestellt. Dies bedeutet in der Regel, dass der Überwachungsdienst aktiv versucht, die beeinträchtigten Instances wiederherzustellen.

Fehlerbehebung

In den meisten Fällen handelt es sich um ein vorübergehendes Problem, und das Verzeichnis kehrt schließlich in den Status Aktiv zurück. Falls das Problem weiterhin besteht, kontaktieren Sie AWS Support, um weitere Unterstützung zu erhalten.

Der für den kritischen AWS Directory Service reservierte Benutzer fehlt im Verzeichnis

Beschreibung

Wenn ein Simple AD erstellt wird, erstellt AWS Directory Service ein Servicekonto im Verzeichnis mit dem Namen `AWSAdmin`*`D-xxxxxxxxx`*. Dieser Fehler wird empfangen, wenn dieses Service-Konto nicht gefunden wird. Ohne dieses Konto kann AWS Directory Service keine Verwaltungsfunktionen auf dem Verzeichnis ausführen, weshalb das Verzeichnis nicht verwendungsfähig ist.

Fehlerbehebung

Um dieses Problem zu beheben, stellen Sie das Verzeichnis mit einem früheren Snapshot wieder her, der erstellt wurde, bevor das Service-Konto gelöscht wurde. Automatische Snapshots werden von Ihrem Simple-AD-Verzeichnis einmal pro Tag erstellt. Wenn mehr als fünf Tage nach dem Löschen des Kontos vergangen sind, können Sie das Verzeichnis nicht auf einen Zustand wiederherstellen, in dem dieses Konto vorhanden ist. Wenn Sie das Verzeichnis nicht anhand eines Snapshots wiederherstellen können, in dem dieses Konto vorhanden ist, könnte Ihr Verzeichnis dauerhaft unbenutzbar werden. Wenn dies der Fall ist, müssen Sie Ihr Verzeichnis löschen und ein neues erstellen.

Der für den kritischen AWS Directory Service reservierte Benutzer muss zu der Domain-Admins-Gruppe gehören

Beschreibung

Wenn ein Simple AD erstellt wird, erstellt AWS Directory Service ein Servicekonto im Verzeichnis mit dem Namen `AWSAdminD-xxxxxxxxxx`. Dieser Fehler wird empfangen, wenn dieses Service-Konto kein Mitglied der `Domain Admins`-Gruppe ist. Die Mitgliedschaft in dieser Gruppe ist erforderlich, damit AWS Directory Service die benötigten Berechtigungen zu Wartungs- und Recovery-Operationen hat, wie zum Beispiel die Übertragung von FSMO-Rollen, Einbindung der Domain in neue Verzeichnis-Controller und die Wiederherstellung von Snapshots.

Fehlerbehebung

Verwenden Sie das Tool Active Directory-Benutzer und -Computer, um das Service-Konto der `Domain Admins`-Gruppe wieder hinzuzufügen.

Der kritische AWS Directory Service reservierte Benutzer ist deaktiviert

Beschreibung

Wenn ein Simple AD erstellt wird, erstellt AWS Directory Service ein Servicekonto im Verzeichnis mit dem Namen `AWSAdminD-xxxxxxxxxx`. Dieser Fehler wird empfangen, wenn dieses Service-Konto deaktiviert ist. Dieses Konto muss aktiviert werden, damit AWS Directory Service Wartungs- und Recovery-Operationen im Verzeichnis ausführen kann.

Fehlerbehebung

Verwenden Sie das Tool Active Directory-Benutzer und -Computer, um das Service-Konto wieder zu aktivieren.

Der Haupt-Domain-Controller hat nicht alle FSMO-Rollen

Beschreibung

Nicht alle FSMO-Rollen sind im Besitz des Simple-AD-Verzeichnis-Controllers. AWS Directory Service kann bestimmte Verhalten und Funktionalitäten nicht garantieren, wenn die FSMO-Rollen nicht zum richtigen Simple-AD-Verzeichnis-Controller gehören.

Fehlerbehebung

Verwenden Sie Active Directory-Tools zum Verschieben der FSMO-Rollen zurück zum ursprünglichen Arbeitsverzeichnis-Controller. Weitere Informationen zu der Verschiebung der FSMO-Rollen finden Sie unter https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. Wenn das Problem damit nicht behoben wird, wenden Sie sich bitte an den AWS Support, um weitere Unterstützung zu erhalten.

Domain-Controller Replikationsfehler

Beschreibung

Die Simple-AD-Verzeichnis-Controller können nicht miteinander replizieren. Dies kann durch eines oder mehrere der folgenden Probleme verursacht werden:

- Die Sicherheitsgruppen für die Verzeichnis-Controller haben nicht die richtigen Ports geöffnet.
- Die Netzwerk-ACLs sind zu restriktiv.
- Die VPC-Routing-Tabelle routet den Netzwerkverkehr zwischen den Verzeichnis-Controllern nicht korrekt.
- Eine andere Instance wurde zu einem Domain-Controller im Verzeichnis.

Fehlerbehebung

Weitere Informationen über Ihre VPC-Netzwerk-Anforderungen finden Sie unter AWS Managed Microsoft AD AWS Voraussetzungen für verwaltetes Microsoft AD, AD Connector AD-Connector-Voraussetzungen oder Simple AD Simple-AD-Voraussetzungen. Wenn ein unbekannter Domain-Controller in Ihrem Verzeichnis ist, müssen Sie diesen herabstufen. Wenn Ihr VPC-Netzwerk korrekt eingerichtet ist, aber der Fehler weiterhin besteht, wenden Sie sich bitte an den AWS Support, um weitere Unterstützung zu erhalten.

Sicherheit in AWS Directory Service

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der geteilten Verantwortung beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der AWS -Compliance-Programme regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für gelten AWS Directory Service, finden Sie unter AWS Services in Umfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Nutzung anwenden können AWS Directory Service. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen AWS Directory Service , um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer AWS Directory Service Ressourcen unterstützen.

Sicherheitsthemen

Die folgenden Sicherheitsthemen finden Sie in diesem Abschnitt:

- Identitäts- und Zugriffsmanagement für AWS Directory Service
- Einloggen und Überwachen AWS Directory Service
- Konformitätsprüfung für AWS Directory Service
- Resilienz in AWS Directory Service
- Sicherheit der Infrastruktur in AWS Directory Service

Zusätzliche Sicherheitsthemen

Die folgenden zusätzlichen Sicherheitsthemen finden Sie in diesem Handbuch:

Konten, Trusts und AWS Ressourcenzugriff

- Berechtigungen für das Administratorkonto
- Gruppenverwaltete Service-Konten
- Erstellen einer Vertrauensstellung
- Eingeschränkte Kerberos-Delegierung
- Benutzern und Gruppen den Zugriff auf AWS -Ressourcen gewähren
- Autorisierung für AWS Anwendungen und Dienste mit AWS Directory Service

Ihr Verzeichnis sichern

- Ihr Verzeichnis in AWS Managed Microsoft AD sichern
- Ihr AD-Connector-Verzeichnis sichern

Protokollierung und Überwachung

- Ihr AWS Managed Microsoft AD überwachen
- Ihr AD-Connector-Verzeichnis überwachen

Ausfallsicherheit

- Patchen und Wartung für AWS Managed Microsoft AD

Identitäts- und Zugriffsmanagement für AWS Directory Service

Für den Zugriff auf AWS Directory Service sind Anmeldeinformationen erforderlich, mit denen Sie Ihre Anfragen authentifizieren AWS können. Diese Anmeldeinformationen müssen über Berechtigungen für den Zugriff auf AWS Ressourcen verfügen, z. B. auf ein AWS Directory Service Verzeichnis. In den folgenden Abschnitten erfahren Sie, wie Sie AWS Identity and Access Management (IAM) verwenden und AWS Directory Service wie Sie Ihre Ressourcen schützen können, indem Sie kontrollieren, wer darauf zugreifen kann:

- Authentifizierung

- Zugriffskontrolle

Authentifizierung

Erfahren Sie, wie Sie AWS mithilfe von IAM-Identitäten darauf zugreifen können.

Zugriffskontrolle

Sie können über gültige Anmeldeinformationen verfügen, um Ihre Anfragen zu authentifizieren, aber ohne die entsprechenden Berechtigungen können Sie keine Ressourcen erstellen oder darauf zugreifen. AWS Directory Service Sie müssen beispielsweise über Berechtigungen zum Erstellen eines AWS Directory Service Verzeichnisses oder zum Erstellen eines Verzeichnissnapshots verfügen.

In den folgenden Abschnitten wird beschrieben, wie Sie Berechtigungen für verwalten AWS Directory Service. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Directory Service Ressourcen
- Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Directory Service
- AWS Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Directory Service Ressourcen

Jede AWS Ressource gehört einem AWS Konto, und die Berechtigungen zum Erstellen oder Zugreifen auf die Ressourcen werden durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator kann IAM-Identitäten (d. h. Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuordnen, und einige Dienste (z. B. AWS Lambda) unterstützen auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

> **Note**
>
> Ein Kontoadministrator (oder Administratorbenutzer) ist ein Benutzer mit Administratorrechten. Weitere Informationen finden Sie unter Bewährte Methoden für IAM im IAM-Benutzerhandbuch.

Themen

- AWS Directory Service Ressourcen und Operationen
- Grundlegendes zum Eigentum an Ressourcen
- Verwalten des Zugriffs auf Ressourcen
- Angeben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale
- Angeben von Bedingungen in einer Richtlinie

AWS Directory Service Ressourcen und Operationen

AWS Directory Service In ist die primäre Ressource ein Verzeichnis. AWS Directory Service unterstützt auch Verzeichnis-Snapshot-Ressourcen. Sie können jedoch nur Snapshots im Kontext mit einem bestehenden Verzeichnis erstellen. Aus diesem Grund wird ein Snapshot eine Subressource genannt.

Diesen Ressourcen sind eindeutige Amazon-Ressourcennamen (ARN) zugeordnet, siehe nachfolgende Tabelle.

Ressourcentyp	ARN-Format
Verzeichnis	`arn:aws:ds:` *`region`*`:`*`account-id`* `:directory/` *`external-directory-id`*
Snapshot	`arn:aws:ds:` *`region`*`:`*`account-id`* `:snapshot/` *`external-snapshot-id`*

AWS Directory Service bietet eine Reihe von Operationen für die Arbeit mit den entsprechenden Ressourcen. Eine Liste der verfügbaren Operationen finden Sie unter Verzeichnisservice-Aktionen.

Grundlegendes zum Eigentum an Ressourcen

Ein Ressourcenbesitzer ist das AWS Konto, das eine Ressource erstellt hat. Das heißt, der Ressourcenbesitzer ist das AWS Konto der Prinzipalentität (das Root-Konto, ein IAM-Benutzer oder eine IAM-Rolle), das die Anforderung authentifiziert, mit der die Ressource erstellt wird. Die Funktionsweise wird anhand der folgenden Beispiele deutlich:

- Wenn Sie die Root-Kontoanmeldeinformationen Ihres AWS Kontos verwenden, um eine AWS Directory Service Ressource, z. B. ein Verzeichnis, zu erstellen, ist Ihr AWS Konto der Eigentümer dieser Ressource.
- Wenn Sie in Ihrem AWS Konto einen IAM-Benutzer erstellen und diesem Benutzer Berechtigungen zum Erstellen von AWS Directory Service Ressourcen gewähren, kann der Benutzer auch AWS Directory Service Ressourcen erstellen. Ihr AWS Konto, zu dem der Benutzer gehört, besitzt jedoch die Ressourcen.
- Wenn Sie in Ihrem AWS Konto eine IAM-Rolle mit Berechtigungen zum Erstellen von AWS Directory Service Ressourcen erstellen, kann jeder, der die Rolle übernehmen kann, AWS Directory Service Ressourcen erstellen. Ihr AWS Konto, zu dem die Rolle gehört, besitzt die AWS Directory Service Ressourcen.

Verwalten des Zugriffs auf Ressourcen

Eine Berechtigungsrichtlinie beschreibt, wer Zugriff auf welche Objekte hat. Im folgenden Abschnitt werden die verfügbaren Optionen zum Erstellen von Berechtigungsrichtlinien erläutert.

> **Note**
>
> In diesem Abschnitt wird die Verwendung von IAM im Kontext von AWS Directory Service beschrieben. Er enthält keine detaillierten Informationen über den IAM-Service. Eine umfassende IAM-Dokumentation finden Sie unter Was ist IAM? im IAM-Benutzerhandbuch. Informationen zur IAM-Richtliniensyntax und -Beschreibungen finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Richtlinien, die mit einer IAM-Identität verknüpft sind, werden als identitätsbasierte Richtlinien (IAM-Richtlinien) bezeichnet, und Richtlinien, die einer Ressource zugeordnet sind, werden als ressourcenbasierte Richtlinien bezeichnet. AWS Directory Service unterstützt nur identitätsbasierte Richtlinien (IAM-Richtlinien).

Themen

- Identitätsbasierte Richtlinien (IAM-Richtlinien)
- Ressourcenbasierte Richtlinien

Identitätsbasierte Richtlinien (IAM-Richtlinien)

Richtlinien können IAM-Identitäten angefügt werden. Sie können z. B. Folgendes tun:

- Ordnen Sie einem Benutzer oder einer Gruppe in Ihrem Konto eine Berechtigungsrichtlinie zu — Ein Kontoadministrator kann mithilfe einer Berechtigungsrichtlinie, die einem bestimmten Benutzer zugeordnet ist, diesem Benutzer Berechtigungen zum Erstellen einer AWS Directory Service Ressource, z. B. eines neuen Verzeichnisses, gewähren.
- Einer Rolle eine Berechtigungsrichtlinie zuweisen (kontoübergreifende Berechtigungen gewähren) – Sie können einer IAM-Rolle eine identitätsbasierte Berechtigungsrichtlinie zuweisen, um kontoübergreifende Berechtigungen zu erteilen.

  Weitere Informationen zum Delegieren von Berechtigungen mithilfe von IAM finden Sie unter Zugriffsverwaltung im IAM-Benutzerhandbuch.

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen für einen Benutzer, alle Aktionen auszuführen, die mit beginne `Describe`. Diese Aktionen zeigen Informationen über eine AWS Directory Service Ressource an, z. B. ein Verzeichnis oder einen Snapshot. Beachten Sie, dass das Platzhalterzeichen (*) im `Resource` Element angibt, dass die Aktionen für alle AWS Directory Service Ressourcen zulässig sind, die dem Konto gehören.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit AWS Directory Service finden Sie unter. Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Directory

Service Weitere Informationen zu Benutzern, Gruppen, Rollen und Berechtigungen finden Sie unter Identitäten (Benutzer, Gruppen und Rollen) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Andere Services, z. B. Amazon-S3, unterstützen auch ressourcenbasierte Berechtigungsrichtlinien. Sie können beispielsweise eine Richtlinie an einen S3-Bucket anhängen, um die Zugriffsberechtigungen für diesen Bucket zu verwalten. AWS Directory Service unterstützt keine ressourcenbasierten Richtlinien.

Angeben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale

Für jede AWS Directory Service Ressource definiert der Dienst eine Reihe von API-Vorgängen. Weitere Informationen finden Sie unter AWS Directory Service Ressourcen und Operationen. Eine Liste der verfügbaren API-Operationen finden Sie unter Verzeichnisservice-Aktionen.

AWS Directory Service Definiert eine Reihe von Aktionen, die Sie in einer Richtlinie angeben können, um Berechtigungen für diese API-Operationen zu gewähren. Zur Durchführung einer API-Operation können Berechtigungen für mehrere Aktionen erforderlich sein.

Grundlegende Richtlinienelemente:

- Ressource – In einer Richtlinie wird der Amazon-Ressourcenname (ARN) zur Identifizierung der Ressource verwendet, für die die Richtlinie gilt. Für AWS Directory Service Ressourcen verwenden Sie in IAM-Richtlinien immer das Platzhalterzeichen (*). Weitere Informationen finden Sie unter AWS Directory Service Ressourcen und Operationen.
- Aktion – Mit Aktionsschlüsselwörtern geben Sie die Ressourcenoperationen an, die Sie zulassen oder verweigern möchten. Die `ds:DescribeDirectories`-Berechtigung erteilt dem Benutzer zum Beispiel Berechtigungen zum Ausführen der AWS Directory Service `DescribeDirectories`-Operation.
- Effekt: Die von Ihnen festgelegte Auswirkung, wenn ein Benutzer die jeweilige Aktion anfordert. Das kann entweder "allow" (Zugriffserlaubnis) oder "deny" (Zugriffsverweigerung) sein. Wenn Sie den Zugriff auf eine Ressource nicht ausdrücklich gestatten („Allow“), wird er automatisch verweigert. Sie können den Zugriff auf eine Ressource auch explizit verweigern. So können Sie sicherstellen, dass Benutzer nicht darauf zugreifen können, auch wenn der Zugriff durch eine andere Richtlinie gestattet wird.
- Prinzipal – In identitätsbasierten Richtlinien (IAM-Richtlinien) ist der Benutzer, dem die Richtlinie zugewiesen ist, automatisch der Prinzipal. Bei ressourcenbasierten Richtlinien geben Sie den Benutzer, das Konto, den Dienst oder die andere Entität an, für die Sie Berechtigungen erhalten

möchten (gilt nur für ressourcenbasierte Richtlinien). AWS Directory Service unterstützt keine ressourcenbasierten Richtlinien.

Weitere Informationen zur Syntax sowie Beschreibungen von IAM-Richtlinien finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch.

Eine Tabelle mit allen AWS Directory Service API-Aktionen und den Ressourcen, für die sie gelten, finden Sie unter. AWS Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen

Angeben von Bedingungen in einer Richtlinie

Beim Erteilen von Berechtigungen können Sie mithilfe der Sprache der Zugriffsrichtlinie die Bedingungen angeben, wann die Richtlinie wirksam werden soll. Beispielsweise kann festgelegt werden, dass eine Richtlinie erst ab einem bestimmten Datum gilt. Weitere Informationen zum Angeben von Bedingungen in einer Richtliniensyntax finden Sie im Thema Bedingung im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für AWS Directory Service gibt es keine speziellen Bedingungsschlüssel. Es gibt jedoch AWS Bedingungsschlüssel, die Sie je nach Bedarf verwenden können. Eine vollständige Liste der AWS Schlüssel finden Sie unter Verfügbare globale Bedingungsschlüssel im IAM-Benutzerhandbuch.

Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für AWS Directory Service

In diesem Thema finden Sie Beispiele für identitätsbasierte Richtlinien, in denen ein Kontoadministrator den IAM-Identitäten (Benutzer, Gruppen und Rollen) Berechtigungsrichtlinien anfügen kann.

> **Important**
>
> Wir empfehlen Ihnen, zunächst die einführenden Themen zu lesen, in denen die grundlegenden Konzepte und Optionen erläutert werden, mit denen Sie den Zugriff auf Ihre Ressourcen verwalten können. AWS Directory Service Weitere Informationen finden Sie unter Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre AWS Directory Service Ressourcen.

Dieses Thema besteht aus folgenden Abschnitten:

- Für die Verwendung der AWS Directory Service Konsole sind Berechtigungen erforderlich
- AWS verwaltete (vordefinierte) Richtlinien für AWS Directory Service
- Beispiele für vom Kunden verwaltete Richtlinien
- Verwenden von Tags mit IAM-Richtlinien

Dies ist ein Beispiel für eine Berechtigungsrichtlinie.

```
{
   "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"
                }
            }
        }
    ]
}
```

Die Richtlinie umfasst Folgendes:

- Die erste Anweisung erteilt die Erlaubnis, ein AWS Directory Service Verzeichnis zu erstellen. AWS Directory Service unterstützt keine Berechtigungen für diese spezielle Aktion auf Ressourcenebene. Daher, gibt die Richtlinie ein Platzhalterzeichen (*) für den `Resource`-Wert an.
- Die zweite Anweisung erteilt Berechtigungen für bestimmte IAM-Aktionen. Der Zugriff auf IAM-Aktionen ist erforderlich, damit Sie in Ihrem Namen IAM-Rollen lesen und erstellen AWS Directory Service können. Das Platzhalterzeichen (*) am Ende des `Resource`-Werts bedeutet, dass die Anweisung Berechtigungen für die IAM-Aktionen für die IAM-Rolle zulässt. Um diese Berechtigungen auf eine bestimmte Rolle zu beschränken, ersetzen Sie das Platzhalterzeichen (*) im ARN der Ressource durch den spezifischen Rollennamen. Weitere Informationen finden Sie unter IAM-Aktionen.
- Die dritte Anweisung gewährt Berechtigungen für einen bestimmten Satz von Amazon EC2 EC2-Ressourcen, die erforderlich sind, um die zugehörigen Verzeichnisse erstellen, konfigurieren und löschen AWS Directory Service zu können. Das Platzhalterzeichen (*) am Ende des `Resource` Werts bedeutet, dass die Anweisung Berechtigung für die EC2-Aktionen oder beliebige EC2-Ressource- oder Subressource-Aktionen zulässt. Um diese Berechtigung auf eine bestimmte Rolle zu beschränken, ersetzen Sie das Platzhalterzeichen (*) im ARN der Ressource durch die spezifische Ressource oder Subressource. Weitere Informationen finden Sie unter Amazon-EC2-Aktionen.

Das Element `Principal` ist in der Richtlinie nicht angegeben, da in identitätsbasierten Richtlinien die Angabe des Prinzipals als Empfänger der Berechtigung nicht erforderlich ist. Wenn Sie einem Benutzer eine Richtlinie zuweisen, ist der Benutzer automatisch der Prinzipal. Wird die

Berechtigungsrichtlinie einer IAM-Rolle zugewiesen, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen.

Eine Tabelle mit allen AWS Directory Service API-Aktionen und den Ressourcen, für die sie gelten, finden Sie unterAWS Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen.

Für die Verwendung der AWS Directory Service Konsole sind Berechtigungen erforderlich

Damit ein Benutzer mit der AWS Directory Service Konsole arbeiten kann, muss er über die in der vorherigen Richtlinie aufgeführten Berechtigungen oder über die Berechtigungen verfügen, die durch die Verzeichnisdienst-Vollzugriffsrolle oder die Directorydienst-Rolle (Read Only) gewährt wurden, wie unter beschriebenAWS verwaltete (vordefinierte) Richtlinien für AWS Directory Service.

Wenn Sie eine IAM-Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Benutzer mit dieser IAM-Richtlinie.

AWS verwaltete (vordefinierte) Richtlinien für AWS Directory Service

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung eigenständiger IAM-Richtlinien, die von erstellt und verwaltet AWS werden. Die verwalteten Richtlinien erteilen die erforderlichen Berechtigungen für viele häufige Anwendungsfälle, sodass Sie nicht mühsam ermitteln müssen, welche Berechtigungen erforderlich sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

Die folgenden AWS verwalteten Richtlinien, die Sie Benutzern in Ihrem Konto zuordnen können, sind spezifisch für AWS Directory Service:

- AWSDirectoryServiceReadOnlyAccess— Gewährt einem Benutzer oder einer Gruppe schreibgeschützten Zugriff auf alle AWS Directory Service Ressourcen, EC2-Subnetze, EC2-Netzwerkschnittstellen und Amazon Simple Notification Service (Amazon SNS) -Themen und Abonnements für das Root-Konto. AWS Weitere Informationen finden Sie unter Verwendung von AWS verwalteten Richtlinien mit AWS Directory Service.
- AWSDirectoryServiceFullAccess – Gewährt einem Benutzer oder einer Gruppe Folgendes:
  - Voller Zugriff auf AWS Directory Service
  - Für die Nutzung ist Zugriff auf wichtige Amazon EC2-Services erforderlich AWS Directory Service
  - Möglichkeit, Amazon-SNS-Themen aufzulisten

- Möglichkeit, Amazon SNS SNS-Themen zu erstellen, zu verwalten und zu löschen, deren Name mit „“ DirectoryMonitoring beginnt

Weitere Informationen finden Sie unter Verwendung von AWS verwalteten Richtlinien mit AWS Directory Service.

Darüber hinaus gibt es weitere AWS verwaltete Richtlinien, die für die Verwendung mit anderen IAM-Rollen geeignet sind. Diese Richtlinien werden den Rollen zugewiesen, die Benutzern in Ihrem AWS Directory Service Verzeichnis zugeordnet sind. Diese Richtlinien sind erforderlich, damit diese Benutzer Zugriff auf andere AWS Ressourcen wie Amazon EC2 haben. Weitere Informationen finden Sie unter Benutzern und Gruppen den Zugriff auf AWS -Ressourcen gewähren.

Sie können auch benutzerdefinierte IAM-Richtlinien erstellen, mit denen Benutzer Zugriff auf die erforderlichen -API-Aktionen und Ressourcen erhalten. Die benutzerdefinierten Richtlinien können Sie dann den IAM-Benutzern oder -Gruppen zuweisen, die diese Berechtigungen benötigen.

Beispiele für vom Kunden verwaltete Richtlinien

In diesem Abschnitt finden Sie Beispiele für Benutzerrichtlinien, die Berechtigungen für verschiedene AWS Directory Service Aktionen gewähren.

> **Note**
>
> In allen Beispielen werden die Region USA West (Oregon) (`us-west-2`) und fiktive Konto-IDs verwendet.

Beispiele

- Beispiel 1: Erlauben Sie einem Benutzer, eine Beschreibe-Aktion für eine beliebige AWS Directory Service Ressource auszuführen
- Beispiel 2: Einem Benutzer das Erstellen eines Verzeichnisses erlauben

Beispiel 1: Erlauben Sie einem Benutzer, eine Beschreibe-Aktion für eine beliebige AWS Directory Service Ressource auszuführen

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen für einen Benutzer, alle Aktionen auszuführen, die mit beginne `Describe`. Diese Aktionen zeigen Informationen über eine AWS

Directory Service Ressource, z. B. ein Verzeichnis oder einen Snapshot. Beachten Sie, dass das Platzhalterzeichen (*) im `Resource` Element angibt, dass die Aktionen für alle AWS Directory Service Ressourcen zulässig sind, die dem Konto gehören.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

Beispiel 2: Einem Benutzer das Erstellen eines Verzeichnisses erlauben

Die folgende Berechtigungsrichtlinie gewährt Berechtigungen, um zu ermöglichen, dass ein Benutzer ein Verzeichnis und alle anderen verwandten Ressourcen, z. B. Snapshots und Vertrauensstellungen erstellen kann. Dafür sind auch Berechtigungen für bestimmte Amazon EC2-Services erforderlich.

```
{
   "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":"*"
         ]
```

```
      }
   ]
}
```

Verwenden von Tags mit IAM-Richtlinien

In den IAM-Richtlinien, die Sie für die meisten API-Aktionen verwenden, können Sie tagbasierte Berechtigungen auf Ressourcenebene anwenden. AWS Directory Service Dies ermöglicht Ihnen eine bessere Kontrolle darüber, welche Ressourcen ein Benutzer erstellen, ändern oder verwenden kann. Sie können das `Condition`-Element (auch als `Condition`-Block bezeichnet) mit den folgenden Bedingungskontextschlüsseln und Werten in einer IAM-Richtlinie zum Steuern des Benutzerzugriffs (Berechtigungen) basierend auf den Tags einer Ressource verwenden:

- Verwenden Sie `aws:ResourceTag/`**`tag-key`**: **`tag-value`**, um Benutzern Aktionen auf Ressourcen mit bestimmten Tags zu gestatten oder zu verweigern.
- Verwenden Sie `aws:ResourceTag/`**`tag-key`**: **`tag-value`**, um zu verlangen, dass ein bestimmter Tag verwendet wird (oder nicht), wenn eine API-Anforderung zum Erstellen einer Ressource durchgeführt wird, die Tags zulässt.
- Verwenden Sie `aws:TagKeys`: [**`tag-key`**, ...], um zu verlangen, dass ein bestimmter Satz von Tag-Schlüsseln verwendet wird (oder nicht), wenn eine API-Anforderung zum Erstellen einer Ressource durchgeführt wird, die Tags zulässt.

> **Note**
>
> Die Bedingungskontextschlüssel und -werte in einer IAM-Richtlinie gelten nur für die AWS Directory Service -Aktionen, bei denen eine Kennung für eine Ressource, die Tags zulässt, ein erforderlicher Parameter ist.

Zugriffssteuerung mit Tags im IAM-Benutzerhandbuch enthält zusätzliche Informationen über die Verwendung von Tags. Der Abschnitt IAM-JSON-Richtlinienreferenz dieses Handbuchs enthält die detaillierte Syntax sowie Beschreibungen und Beispiele für Elemente, Variablen und die Auswertungslogik von JSON-Richtlinien in IAM.

Mit der folgenden Beispielrichtlinie gestatten Sie alle `ds`-Aufrufe, solange diese das Tag-Schlüssel-Paar "`fooKey`":"`fooValue`" enthält.

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

Mit der folgenden Beispielrichtlinie gestatten Sie alle ds-Aufrufe, solange die Ressource die Verzeichnis-ID "d-1234567890" enthält.

```
{
   "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":"*"
        }
    ]
}
```

Weitere Informationen zu ARNs finden Sie unter Amazon Resource Names (ARNs) und AWS Service Namespaces.

Die folgende Liste von AWS Directory Service API-Vorgängen unterstützt tagbasierte Berechtigungen auf Ressourcenebene:

- 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 API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen

Wenn Sie Zugriffskontrolle einrichten und Berechtigungsrichtlinien schreiben, die Sie an eine IAM-Identität anhängen können (identitätsbasierte Richtlinien), können Sie die AWS Directory Service

API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen-Tabelle als Referenz verwenden. Jeder API-Eintrag in der enthält Folgendes:

- Name des AWS Directory Service API-Vorgangs
- Die entsprechenden Aktionen, für die Sie Berechtigungen zum Ausführen der Aktion erteilen können
- Die AWS Ressource, für die Sie die Berechtigungen erteilen können

Die Aktionen geben Sie im Feld `Action` und den Wert für die Ressource im Feld `Resource` der Richtlinie an. Um eine Aktion anzugeben, verwenden Sie das Präfix `ds:` gefolgt vom Namen der API-Operation (z. B. `ds:CreateDirectory`). Einige AWS Anwendungen erfordern in ihren Richtlinien möglicherweise die Verwendung von nichtöffentlichen AWS Directory Service API-Vorgängen wie `ds:AuthorizeApplication` `ds:CheckAlias` `ds:CreateIdentityPoolDirectoryds:GetAuthorizedApplicationDetails`,`ds:UpdateAuthori` und`ds:UnauthorizeApplication`.

Einige AWS Directory Service APIs können nur über die AWS Management Console aufgerufen werden. Sie sind keine öffentlichen APIs in dem Sinne, dass sie nicht programmgesteuert aufgerufen werden können, und sie werden von keinem SDK bereitgestellt. Sie akzeptieren Benutzeranmeldedaten. Zu diesen API-Operationen gehören `ds:DisableRoleAccessds:EnableRoleAccess`, und`ds:UpdateDirectory`.

Sie können in Ihren AWS Directory Service Richtlinien AWS globale Bedingungsschlüssel verwenden, um Bedingungen auszudrücken. Eine vollständige Liste der AWS Schlüssel finden Sie unter Verfügbare globale Bedingungsschlüssel im IAM-Benutzerhandbuch.

Verwandte Themen

- Zugriffskontrolle

Autorisierung für AWS Anwendungen und Dienste mit AWS Directory Service

Autorisieren einer AWS Anwendung in einem Active Directory

AWS Directory Service gewährt den ausgewählten Anwendungen spezifische Berechtigungen, sodass sie sich nahtlos in Ihr Active Directory integrieren lassen, wenn Sie eine AWS Anwendung

autorisieren. AWS Anwendungen erhalten nur den Zugriff, der für ihren Anwendungsfall erforderlich ist. Nachfolgend sind die internen Berechtigungen aufgeführt, die Anwendungen und Anwendungsadministratoren nach der Autorisierung gewährt werden:

> **Note**
>
> Die `ds:AuthorizationApplication` Genehmigung ist erforderlich, um eine neue AWS Anwendung in Active Directory zu autorisieren. Berechtigungen für diese Aktion sollten nur Administratoren gewährt werden, die Integrationen mit Directory Service konfigurieren.

- Lesezugriff auf Active Directory-Benutzer-, Gruppen-, Organisationseinheiten-, Computer- oder Zertifizierungsstellendaten in allen Organisationseinheiten (OU) von AWS verwalteten Microsoft AD-, Simple AD- und AD Connector-Verzeichnissen sowie vertrauenswürdigen Domänen für AWS Managed Microsoft AD, sofern eine Vertrauensbeziehung dies zulässt.
- Schreibzugriff auf Benutzer, Gruppen, Gruppenmitgliedschaften, Computer oder Zertifizierungsstellendaten in Ihrer Organisationseinheit von AWS Managed Microsoft AD. Schreibzugriff auf alle OUs von Simple AD.
- Authentifizierung und Sitzungsverwaltung von Active-Directory-Benutzern für alle Verzeichnistypen.

Bestimmte AWS verwaltete Microsoft AD-Anwendungen wie Amazon RDS und Amazon FSx lassen sich über eine direkte Netzwerkverbindung in Ihr Active Directory integrieren. In diesem Fall verwenden die Verzeichnisinteraktionen native Active-Directory-Protokolle wie LDAP und Kerberos. Die Berechtigungen dieser AWS Anwendungen werden durch ein Verzeichnisbenutzerkonto gesteuert, das während der Anwendungsautorisierung in der AWS Reserved Organizational Unit (OU) erstellt wurde. Dazu gehören DNS-Verwaltung und Vollzugriff auf eine benutzerdefinierte OU, die für die Anwendung erstellt wurde. Um dieses Konto verwenden zu können, benötigt die Anwendung Berechtigungen für `ds:GetAuthorizedApplicationDetails`-Aktionen über die Anmeldeinformationen des Anrufers oder eine IAM-Rolle.

Weitere Informationen zu AWS Directory Service API-Berechtigungen finden Sie unterAWS Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen.

Weitere Informationen zum Aktivieren von AWS Anwendungen und Diensten für AWS Managed Microsoft AD finden Sie unterErmöglichen Sie den Zugriff auf AWS Anwendungen und Dienste. Weitere Informationen zum Aktivieren von AWS Anwendungen und Diensten für AD Connector finden Sie unterAktivieren des Zugriffs auf AWS Anwendungen und Services. Weitere Informationen

zum Aktivieren von AWS Anwendungen und Diensten für Simple AD finden Sie unterAktivieren des Zugriffs auf AWS Anwendungen und Services.

Deautorisierung einer AWS Anwendung in einem Active Directory

Um einer AWS Anwendung die Zugriffsberechtigungen für das Active Directory zu entziehen, ist die `ds:UnauthorizedApplication` entsprechende Berechtigung erforderlich. Folgen Sie den von der Anwendung bereitgestellten Schritten, um sie zu deaktivieren.

Einloggen und Überwachen AWS Directory Service

Als bewährte Methode überwachen Sie Ihre Organisation, um sicherzustellen, dass Änderungen protokolliert werden. Auf diese Weise können Sie sicherstellen, dass alle unerwarteten Änderungen untersucht und unerwünschte Änderungen rückgängig gemacht werden können. AWS Directory Service unterstützt derzeit die folgenden beiden AWS Dienste, sodass Sie Ihr Unternehmen und die darin stattfindenden Aktivitäten überwachen können.

- Amazon CloudWatch — Sie können CloudWatch Ereignisse mit dem Verzeichnistyp AWS Managed Microsoft AD verwenden. Weitere Informationen finden Sie unter Protokollweiterleitung aktivieren. Darüber hinaus können Sie CloudWatch Metrics verwenden, um die Leistung von Domain-Controllern zu überwachen. Weitere Informationen finden Sie unter Ermitteln Sie, wann Domänencontroller mit CloudWatch Metriken hinzugefügt werden sollen.
- AWS CloudTrail - Sie können es CloudTrail mit allen AWS Directory Service Verzeichnistypen verwenden. Weitere Informationen finden Sie unter Protokollieren von AWS Directory Service API-Aufrufen mit CloudTrail.

Konformitätsprüfung für AWS Directory Service

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen

und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Bereitstellung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

> **Note**
>
> AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.

- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Resilienz in AWS Directory Service

Die AWS globale Infrastruktur basiert auf AWS Regionen und Availability Zones. AWS Regionen bieten mehrere physisch getrennte und isolierte Availability Zones, die über Netzwerke mit niedriger Latenz, hohem Durchsatz und hoher Redundanz miteinander verbunden sind. Mithilfe von Availability Zones können Sie Anwendungen und Datenbanken erstellen und ausführen, die automatisch Failover zwischen Availability Zones ausführen, ohne dass es zu Unterbrechungen kommt. Availability Zones sind besser hoch verfügbar, fehlertoleranter und skalierbarer als herkömmliche Infrastrukturen mit einem oder mehreren Rechenzentren.

Weitere Informationen zu AWS Regionen und Availability Zones finden Sie unter AWS Globale Infrastruktur.

Zusätzlich zur AWS globalen Infrastruktur AWS Directory Service bietet es die Möglichkeit, zu jedem Zeitpunkt manuelle Snapshots von Daten zu erstellen, um Ihre Anforderungen an Datenstabilität und Datensicherung zu erfüllen. Weitere Informationen finden Sie unter Ein Snapshot Ihres Verzeichnisses herstellen oder es wiederherstellen.

Sicherheit der Infrastruktur in AWS Directory Service

Als verwalteter Service AWS Directory Service ist er durch die AWS globalen Netzwerksicherheitsverfahren geschützt, die im Whitepaper Amazon Web Services: Sicherheitsprozesse im Überblick beschrieben sind.

Sie verwenden AWS veröffentlichte API-Aufrufe, um AWS Directory Service über das Netzwerk darauf zuzugreifen. Clients müssen Transport Layer Security (TLS) unterstützen. Wir empfehlen TLS 1.2 oder höher. Clients müssen außerdem Verschlüsselungssammlungen mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi.

Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere

Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Außerdem müssen Anforderungen mit einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Alternativ können Sie mit AWS Security Token Service (AWS STS) temporäre Sicherheitsanmeldeinformationen erstellen, um die Anforderungen zu signieren.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine juristische Stelle, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine privilegiertere juristische Stelle zwingen kann, die Aktion auszuführen. In AWS kann ein dienstübergreifendes Identitätswechsels zu dem Problem mit dem verwirrten Stellvertreter führen. Ein dienstübergreifender Identitätswechsel kann auftreten, wenn ein Dienst (der Anruf-Dienst) einen anderen Dienst anruft (den aufgerufenen Dienst). Der aufrufende Service kann manipuliert werden, um seine Berechtigungen zu verwenden, um Aktionen auf die Ressourcen eines anderen Kunden auszuführen, für die er sonst keine Zugriffsberechtigung haben sollte. Um dies zu verhindern, bietet AWS Tools, mit denen Sie Ihre Daten für alle Services mit Serviceprinzipalen schützen können, die Zugriff auf Ressourcen in Ihrem Konto erhalten haben.

Es wird empfohlen, die Kontextschlüssel `aws:SourceArn`und die `aws:SourceAccount`globalen Bedingungsschlüssel in Ressourcenrichtlinien zu verwenden, um die Berechtigungen einzuschränken, die der AWS Directory Service für Microsoft Active Directory einem anderen Dienst für die Ressource gewährt. Wenn der `aws:SourceArn`-Wert die Konto-ID nicht enthält, z. B. einen Amazon-S3-Bucket-ARN, müssen Sie beide globale Bedingungskontextschlüssel verwenden, um Berechtigungen einzuschränken. Wenn Sie beide globale Bedingungskontextschlüssel verwenden und der `aws:SourceArn`-Wert die Konto-ID enthält, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird. Verwenden Sie `aws:SourceArn`, wenn Sie nur eine Ressource mit dem betriebsübergreifenden Zugriff verknüpfen möchten. Verwenden Sie `aws:SourceAccount`, wenn Sie zulassen möchten, dass Ressourcen in diesem Konto mit der betriebsübergreifenden Verwendung verknüpft werden.

Für das folgende Beispiel `aws:SourceArn` muss der Wert von eine CloudWatch Protokollgruppe sein.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. z. B. `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in AWS Managed Microsoft AD verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

```
{
  "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"
      }
    }
  }
}
```

Für das folgende Beispiel muss der Wert von `aws:SourceArn` ein SNS-Thema in Ihrem Konto sein. Sie können beispielsweise etwas verwenden, `arn:aws:sns:ap-`

`southeast-1:123456789012:DirectoryMonitoring_d-966739499f` wobei „ap-southeast-1“ Ihre Region, „123456789012" Ihre Kundennummer und" DirectoryMonitoring _d-966739499f“ der von Ihnen erstellte Amazon SNS SNS-Themenname ist.

Der effektivste Weg, um sich vor dem Confused-Deputy-Problem zu schützen, ist die Verwendung des globalen Bedingungskontext-Schlüssels `aws:SourceArn` mit dem vollständigen ARN der Ressource. Wenn Sie den vollständigen ARN der Ressource nicht kennen oder wenn Sie mehrere Ressourcen angeben, verwenden Sie den globalen Bedingungskontext-Schlüssel `aws:SourceArn` mit Platzhaltern (*) für die unbekannten Teile des ARN. z. B. `arn:aws:`*`servicename`*`:*:`*`123456789012`*`:*`.

Das folgende Beispiel zeigt, wie Sie die Kontextschlüssel `aws:SourceArn` und die `aws:SourceAccount` globalen Bedingungsschlüssel in AWS Managed Microsoft AD verwenden können, um das Problem des verwirrten Stellvertreters zu verhindern.

```
{
  "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"
      }
```

```
    }
  }
}
```

Das folgende Beispiel zeigt eine IAM-Vertrauensrichtlinie für eine Rolle, der der Konsolenzugriff delegiert wurde. Der Wert von `aws:SourceArn` muss eine Verzeichnisressource in Ihrem Konto sein. Weitere Informationen finden Sie unter Ressourcentypen, definiert von AWS Directory Service. Sie können beispielsweise `arn:aws:ds:us-east-1:123456789012:directory/d-1234567890` angeben, wo `123456789012` Ihre Kunden-ID und `d-1234567890` Ihre Verzeichnis-ID ist.

```
{
  "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 und Schnittstelle Amazon VPC-Endpunkte mit AWS PrivateLink

Sie können eine private Verbindung zwischen Ihrer Amazon VPC und Ihren AWS Directory Service API-Endpunkten herstellen, indem Sie einen VPC-Schnittstellen-Endpunkt erstellen. Schnittstellenendpunkte werden von unterstütz AWS PrivateLink.

AWS PrivateLink ermöglicht Ihnen den privaten Zugriff auf AWS Directory Service API-Operationen ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oder Verbindung. AWS Direct Connect Datenverkehr zwischen Ihrer VPC und verlässt das AWS Netzwerk AWS Directory Service nicht.

Jeder Schnittstellenendpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Weitere Informationen zur elastic network interface finden Sie unter Elastic Network Interface im Amazon EC2 EC2-Benutzerhandbuch.

Weitere Informationen zu VPC-Endpunkten finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Schnittstellen-Endpunkts im Amazon VPC-Benutzerhandbuch. Weitere Informationen zu AWS Directory Service API-Vorgängen finden Sie unter API-Referenz.AWS Directory Service

Überlegungen zu VPC-Endpunkten

Bevor Sie einen VPC-Schnittstellen-Endpunkt für AWS Directory Service API-Endpunkte einrichten, stellen Sie sicher, dass Sie den Abschnitt Zugriff und AWS-Service Verwendung eines Schnittstellen-VPC-Endpunkts im Handbuch lesen.AWS PrivateLink

Alle AWS Directory Service API-Operationen, die für die Verwaltung von AWS Directory Service Ressourcen relevant sind, sind in Ihrer VPC verfügbar unter AWS PrivateLink.

VPC-Endpunktrichtlinien werden für Directory Service API-Endpunkte unterstützt. Standardmäßig ist der vollständige Zugriff auf Verzeichnisdienst-API-Operationen über den Endpunkt zulässig. Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon VPC-Benutzerhandbuch.

Verfügbarkeit

AWS Directory Service unterstützt VPC-Endpunkte in den folgenden Bereichen: AWS-Regionen

AWS-Region Verfügbarkeit

- USA Ost (Nord-Virginia)
- USA Ost (Ohio)
- USA West (Nordkalifornien)
- USA West (Oregon)
- Africa (Cape Town)

- Asien-Pazifik (Hongkong)
- Asien-Pazifik (Hyderabad)
- Asien-Pazifik (Jakarta)
- Asien-Pazifik (Melbourne)
- Asien-Pazifik (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Tokio)
- Canada (Central)
- Kanada West (Calgary)
- China (Peking und Ningxia)
- Asien-Pazifik (Hongkong)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europa (Milan)
- Europa (Paris)
- Europa (Spain)
- Europa (Stockholm)
- Europa (Zürich)
- Israel (Tel Aviv)
- Naher Osten (Bahrain)
- Naher Osten (VAE)
- Südamerika (São Paulo)
- AWS GovCloud (US-Ost)
- AWS GovCloud (US-West)

Einen Schnittstellen-Endpunkt für die AWS Directory Service API erstellen

Sie können einen VPC-Schnittstellenendpunkt für die AWS Directory Service API entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellen eines VPC-Endpunkts im AWS PrivateLink -Leitfaden.

Erstellen Sie einen Schnittstellenendpunkt für die AWS Directory Service API mit dem folgenden Servicenamen: `com.amazonaws.region.ds`

AWS Directory Service Mit Ausnahme AWS-Regionen von China können Sie, wenn Sie privates DNS für den Endpunkt aktivieren, API-Anfragen an den VPC-Endpunkt stellen AWS-Region, indem Sie beispielsweise `ds.us-east-1.amazonaws.com` dessen Standard-DNS-Namen für den verwenden. Für China (Peking und Ningxia) AWS-Regionen können Sie API-Anfragen mit dem VPC-Endpunkt jeweils mit `ds-api.cn-north-1.amazonaws.com.cn` und `ds-api.cn-northwest-1.amazonaws.com.cn` stellen.

Weitere Informationen finden Sie unter Zugreifen und AWS-Service Verwenden eines VPC-Endpunkts mit einer Schnittstelle im Amazon VPC-Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie für die AWS Directory Service -API

Sie können eine Endpunktrichtlinie an Ihren VPC-Endpunkt anhängen, der den Zugriff auf die AWS Directory Service -API steuert. Die Richtlinie gibt die folgenden Informationen an:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuern des Zugriffs auf VPC-Endpunkte mithilfe von Endpunktrichtlinien im Amazon VPC-Benutzerhandbuch.

Beispiel: VPC-Endpunktrichtlinie für AWS Directory Service API-Aktionen

Im Folgenden finden Sie ein Beispiel für eine Endpunktrichtlinie für AWS Directory Service API. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten AWS Directory Service API-Aktionen.

```
{
   "Statement": [
```

```
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeCertificate",
         ],
         "Resource":"*"
      }
   ]
}
```

Beispiel: VPC-Endpunktrichtlinie, die jeglichen Zugriff von einem bestimmten AWS-Konto

Die folgende VPC-Endpunktrichtlinie verweigert AWS-Konto *123456789012* jeglichen Zugriff auf Ressourcen, die den Endpunkt verwenden. Die Richtlinie erlaubt alle Aktionen von anderen Konten.

```
{
   "Statement": [
      {
         "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal:" "*"
      },
      {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "*",
        "Principal": {
            "AWS": [
               "123456789012"
            ]
         }
      ]
}
```

Service Level Agreement für AWS Directory Service

AWS Directory Service ist ein hochverfügbarer Dienst, der auf einer von AWS verwalteten Infrastruktur basiert. Er wird durch ein Service Level Agreement ergänzt, das unsere Richtlinie zur Serviceverfügbarkeit definiert.

Weitere Informationen finden Sie unter Service Level Agreement für AWS Directory Service.

Verfügbarkeit in der Region für AWS Directory Service

Die folgende Tabelle enthält eine Liste mit regionsspezifischen Endpunkten, die von dem Verzeichnistyp unterstützt werden.

Name der Region	Region	Endpunkt	Protokoll	AWS Verwaltetes Microsoft AD	AD Connector	Simple AD
USA Ost (Nord-Virginia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	Ja	Ja	Ja
USA Ost (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	Ja	Ja	Nein
USA West (Nordkalifornien)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	Ja	Ja	Nein
USA West (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	Ja	Ja	Ja
Afrika (Kapstadt)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	Ja	Ja	Nein
Asien-Pazifik	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	Ja	Ja	Nein

Name der Region	Region	Endpunkt	Protokoll	AWS Verwaltetes Microsoft AD	AD Connector	Simple AD
(Hongkong)						
Asien-Pazifik (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Asien-Pazifik (Jakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Asien-Pazifik (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Asien-Pazifik (Mumbai)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Asien-Pazifik (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Asien-Pazifik (Seoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Asien-Pazifik (Singapur)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja

Name der Region	Region	Endpunkt	Protokoll	AWS Verwaltetes Microsoft AD	AD Connector	Simple AD
Asien-Pazifik (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja
Asien-Pazifik (Tokio)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja
Kanada (Zentral)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Kanada West (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
China (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 Ja	 Ja	 Nein
China (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	 Ja	 Ja	 Nein
Europa (Frankfurt)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Europa (Irland)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja

Name der Region	Region	Endpunkt	Protokoll	AWS Verwaltetes Microsoft AD	AD Connector	Simple AD
Europa (London)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Europa (Mailand)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Europa (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Europa (Spanien)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Europa (Stockholm)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Europa (Zürich)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Israel (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Naher Osten (Bahrain)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein

Name der Region	Region	Endpunkt	Protokoll	AWS Verwaltetes Microsoft AD	AD Connector	Simple AD
Naher Osten (VAE)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
Südamerika (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
AWS GovCloud (USA, Westen)	us-gov-west-1	ds. us-gov-west-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein
AWS GovCloud (US-Ost)	us-gov-east-1	ds. us-gov-east-1.amazonaws.com	HTTPS	 Ja	 Ja	 Nein

Informationen zur Nutzung AWS Directory Service in den Regionen AWS GovCloud (USA West) und AWS GovCloud (USA Ost) finden Sie unter Service-Endpunkte.

Informationen zur Verwendung AWS Directory Service in den Regionen Peking und Ningxia finden Sie unter Endpunkte und ARNs für Amazon Web Services in China.

Browserkompatibilität

AWS Anwendungen und Dienste wie Amazon WorkSpaces, Amazon Connect WorkMail, Amazon Chime WorkDocs, Amazon und AWS IAM Identity Center alle benötigen gültige Anmeldedaten von einem kompatiblen Browser, bevor Sie darauf zugreifen können. Die folgende Tabelle beschreibt nur die Browser und Browser-Versionen, die für Anmeldungen kompatibel sind.

Browser	Version	Kompatibilität
Microsoft Edge	Die letzten 3 Versionen	Kompatibel
Mozilla Firefox	Letzte 3 Versionen	Kompatibel
Google Chrome	Letzte 3 Versionen	Kompatibel
Apple Safari	Letzte 3 Versionen	Kompatibel

Nachdem Sie überprüft haben, dass Sie eine unterstützte Version Ihres Browsers verwenden, empfehlen wir, außerdem anhand des Abschnitts unten sicherzustellen, dass Ihr Browser für die Verwendung der Transport Layer Security(TLS)-Einstellung konfiguriert wurde, die für AWS benötigt wird.

Was ist TLS?

TLS ist ein Protokoll, das von Webbrowsern und anderen Anwendungen für den sicheren Datenaustausch über ein Netzwerk genutzt wird. TLS stellt durch Verschlüsselung und Überprüfung der Endpunktidentität sicher, dass eine Verbindung mit dem beabsichtigten Endpunkt hergestellt wird. Die aktuellen Versionen von TLS sind TLS 1.0, 1.1, 1.2 und 1.3.

Welche TLS-Versionen werden von IAM Identity Center unterstützt?

AWS Anwendungen und Dienste unterstützen TLS 1.1, 1.2 und 1.3 für sichere Anmeldungen. Ab dem 30. Oktober 2019 wird TLS 1.0 nicht mehr unterstützt. Daher ist es wichtig, dass alle Browser so konfiguriert sind, dass sie TLS 1.1 oder höher unterstützen. Das bedeutet, dass Sie sich nicht mehr

bei AWS -Anwendungen und -Services anmelden können, wenn Sie auf sie zugreifen, während TLS 1.0 aktiviert ist. Wenden Sie sich für Unterstützung bei der Vornahme dieser Änderungen an Ihren Administrator.

Wie aktiviere ich die unterstützten TLS-Versionen in meinem Browser?

Dies ist von Ihrem Browser abhängig. In der Regel finden Sie diese Einstellung unter dem Bereich der erweiterten Einstellungen in den Browser-Einstellungen. Beispiel: In Internet Explorer finden Sie verschiedene TLS-Optionen unter Internet-Eigenschaften auf der Registerkarte Erweitert im Bereich Sicherheit. Überprüfen Sie die Hilfe-Website Ihres Browser-Herstellers auf spezifische Anweisungen.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen seit der letzten Veröffentlichung des Administratorhandbuchs für AWS Directory Service beschrieben.

Änderung	Beschreibung	Datum
Zertifikatsbasierte Authentifizierungseinstellungen	Inhalt zu zwei neuen Sicherheitseinstellungen für AWS Managed Microsoft AD hinzugefügt.	11. April 2023
AWS PrivateLink	Inhalt über AWS PrivateLink hinzugefügt.	31. März 2023
Simple-AD-VPC-Endpunkte	Inhalt hinzugefügt, welche VPC-Endpunkte nicht konfiguriert werden sollten.	25. August 2021
AD-Connector-VPC-Endpunkte	Inhalt hinzugefügt, welche VPC-Endpunkte nicht konfiguriert werden sollten.	25. August 2021
Smartcard-Unterstützung	Inhalt zur Unterstützung von Smartcards und Amazon WorkSpaces Application Manager in der Region AWS GovCloud (USA West) hinzugefügt	1. Dezember 2020
Zurücksetzen des Passworts	Es wurden Inhalte zum Zurücksetzen von Benutzerkennwörtern mithilfe von AWS Management Console, Windows PowerShell und AWS CLI hinzugefügt.	2. Januar 2019

Verzeichnisfreigabe	Es wurden Inhalte zur Verwendung der Verzeichnisfreigabe mit AWS Managed Microsoft AD hinzugefügt.	25. September 2018
Inhalt in das neue Entwicklerhandbuch von Amazon Cloud Directory migriert	Der Inhalt von Amazon Cloud Directory wurde aus diesem Handbuch in das neue Entwicklerhandbuch für Amazon Cloud Directory verschoben.	21. Juni 2018
Vollständige Überarbeitung des Inhaltsverzeichnisses des Admin-Leitfadens	Der Inhalt wurde neu strukturiert, um die Bedürfnisse der Kunden besser zu erfüllen. Außerdem wurden neue Inhalte nach Bedarf hinzugefügt.	5. April 2018
AWS delegierte Gruppen	Es wurde eine Liste AWS delegierter Gruppen hinzugefügt, die lokalen Benutzern zugewiesen werden können.	8. März 2018
Differenzierte Passwortrichtlinien	Inhalt über neue Richtlinien für Passwörter hinzugefügt.	5. Juli 2017
Zusätzliche Domain-Controller	Es wurden Inhalte zum Hinzufügen weiterer Domänencontroller zu Ihrem Verzeichnis in AWS Managed Microsoft AD hinzugefügt.	30. Juni 2017
Tutorials	Es wurden neue Tutorials zum Testen einer AWS verwalteten Microsoft AD-Laborumgebung hinzugefügt.	21. Juni 2017

MFA mit AWS verwaltetem Microsoft AD	Es wurden Inhalte zur Verwendung von MFA mit AWS Managed Microsoft AD hinzugefügt.	13. Februar 2017
Amazon Cloud Directory	Inhalt zu einem neuen Verzeichnistyp hinzugefügt.	26. Januar 2017
Schemaerweiterungen	Inhalt zu Schemaerweiterungen mit AWS Directory Service für Microsoft Active Directory hinzugefügt.	14. November 2016
Umfassende Reorganisation des AWS Directory Service Administratorhandbuchs	Der Inhalt wurde neu strukturiert, um die Bedürfnisse der Kunden besser zu erfüllen.	14. November 2016
SNS-Benachrichtigungen	Inhalt zu SNS-Benachrichtigungen hinzugefügt.	25. Februar 2016
Autorisierung und Authentifizierung	Es wurden Inhalte zur Verwendung von IAM mit hinzugefügt. AWS Directory Service	25. Februar 2016
AWS Verwaltetes Microsoft AD	Es wurden Inhalte zu AWS Managed Microsoft AD und kombinierte Anleitungen in einem einzigen Leitfaden hinzugefügt.	17. November 2015
Linux-Instances die Verbindung mit einem Simple-AD-Verzeichnis erlauben	Es wurden Inhalte zum Hinzufügen einer Linux-Instance zu einem Simple-AD-Verzeichnis hinzugefügt.	23. Juli 2015

Aufteilung des Handbuchs	Teilen Sie das AWS Directory Service -Administrationshandbuch in separate Anleitungen auf.	14. Juli 2015
Unterstützung von Single Sign-on	Es wurden Inhalte zur Unterstützung von Single Sign-On hinzugefügt.	31. März 2015
Neues Handbuch	Dies ist die erste Version des AWS Directory Service - Administrationshandbuch.	21. Oktober 2014

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.