



Administratorhandbuch

AWS Directory Service



Version 1.0

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

AWS Directory Service: Administratorhandbuch

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

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist AWS Directory Service?	1
AWS Directory Service Optionen	1
Welche sollte man auswählen	5
Arbeiten mit Amazon EC2	6
AWS Verwaltetes Microsoft AD	7
Welche sollte man auswählen	8
Topics	9
AWS Verwaltetes Microsoft AD (Hybrid Edition)	9
Voraussetzungen für Hybridverzeichnisse	10
Ein Hybridverzeichnis erstellen	18
Ein Hybridverzeichnis anzeigen und bearbeiten	19
Löschen eines Hybridverzeichnisses	22
Verzeichnisbewertungen	23
Fehlerbehebung	26
Erste Schritte	66
AWS Voraussetzungen für verwaltetes Microsoft AD	67
AWS IAM Identity Center Voraussetzungen	68
Voraussetzungen für Multifaktor-Authentifizierung	68
Ihr AWS verwaltetes Microsoft AD erstellen	69
Was wird mit Ihrem AWS Managed Microsoft AD erstellt	72
Administratorkonto und Gruppenberechtigungen	85
Schlüsselkonzepte und bewährte Verfahren	88
Die wichtigsten Konzepte	89
Best Practices	93
Anwendungsfälle	104
Anwendungsfall 1: Melden Sie sich mit Active Directory-Anmeldeinformationen bei AWS Anwendungen und Diensten an	105
Anwendungsfall 2: Verwalten von Amazon EC2-Instances	110
Anwendungsfall 3: Stellen Sie Verzeichnisdienste für Ihre Active Directory-fähigen Workloads bereit	110
Anwendungsfall 4: für Office 365 und andere AWS IAM Identity Center Cloud- Anwendungen	110
Anwendungsfall 5: Erweitern Sie Ihr lokales Active Directory auf AWS Cloud	111

Anwendungsfall 6: Teilen Sie Ihr Verzeichnis, um Amazon EC2 EC2-Instances kontenübergreifend AWS nahtlos mit einer Domain zu verbinden	112
Ihr Verzeichnis verwalten	112
Verzeichnisinformationen anzeigen	113
Ihr Verzeichnis mit Schnappschüssen wiederherstellen	115
Bereitstellen zusätzlicher Domänencontroller	121
Ihr AWS verwaltetes Microsoft AD aktualisieren	125
Netzwerktyp des Verzeichnisses aktualisieren	128
Alternative UPN-Suffixe hinzufügen	130
Umbenennen des Site-Namens Ihres Verzeichnisses	130
Löschen Ihres AWS verwalteten Microsoft AD	131
Ihr Verzeichnis sichern	133
Kennwortrichtlinien verstehen	134
Aktivieren der Multifaktor-Authentifizierung	140
Aktivieren Sie Secure LDAP oder LDAPS	145
Compliance für Ihr Verzeichnis verwalten	158
Verbesserung der Netzwerksicherheit	161
Sicherheitseinstellungen für Verzeichnisse bearbeiten	177
Aktivieren Sie die Kryptografie mit öffentlichen Schlüsseln für die Erstauthentifizierung (PKINIT)	192
AWS Private CA Connector für AD einrichten	195
Ihr Verzeichnis überwachen	201
Erläuterungen zum Verzeichnisstatus	202
Aktivieren von Verzeichnisstatusbenachrichtigungen mit Amazon SNS	204
Grundlegendes zu Ihren Verzeichnisprotokollen	207
CloudWatch Amazon-Protokollweiterleitung aktivieren	209
Wird CloudWatch zur Überwachung Ihres Verzeichnisses verwendet	213
CloudWatch Amazon-Protokollweiterleitung deaktivieren	217
Überwachen des DNS-Servers mit Microsoft Event Viewer	218
Zugriff auf AWS Anwendungen und Dienste	219
Anwendungskompatibilität	219
Aktivieren des Zugriffs auf AWS Anwendungen und Dienste	223
Aktivieren des Zugriffs auf die AWS-Managementkonsole	225
Erstellen einer Zugriffs-URL	229
Aktivieren des einmaligen Anmeldens	230
Zugriff auf Ressourcen gewähren AWS	239

Erstellen einer neuen Rolle	239
Bearbeiten der Vertrauensstellung für eine vorhandene Rolle	241
Zuweisen von Benutzern oder Gruppen zu einer vorhandenen Rolle	242
Anzeigen von Benutzern und Gruppen, die einer Rolle zugewiesen sind	243
Entfernen eines Benutzers oder einer Gruppe aus einer Rolle	245
AWS Verwaltete Richtlinien verwenden	245
Konfigurieren Sie die Replikation mit mehreren Regionen	247
Funktionsweise	248
Vorteile	250
Globale und regionale Features	251
Primäre Regionen im Vergleich zu zusätzlichen Regionen	252
Eine replizierte Region hinzufügen	253
Löschen einer replizierten Region	256
Freigeben Ihres Verzeichnisses	256
Die wichtigsten Konzepte	257
Überlegungen	259
Tutorial: Teilen Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnis	259
Die Freigabe Ihres Verzeichnisses aufheben	272
Migration von Active Directory-Benutzern zu AWS Managed Microsoft AD	273
Connect Ihre bestehende Active Directory-Infrastruktur	273
Erstellen einer Vertrauensstellung	274
Hinzufügen von IP-Routen	281
Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer selbstverwalteten Active Directory-Domäne	282
Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen AWS verwalteten Microsoft AD-Domänen	294
Erweitern Sie Ihr Verzeichnisschema	301
Wann Sie Ihr AWS Managed Microsoft AD-Schema erweitern sollten	301
Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas	302
Möglichkeiten, eine Instance Ihrem Verzeichnis hinzuzufügen	309
Starten einer Verzeichnisverwaltungsinstanz	310
Einer Windows-Instance beitreten	314
Einer Linux-Instance beitreten	322
Einer Mac-Instanz beitreten	378
Delegieren von Rechten für den Verzeichnisbeitritt	381
Einen DHCP-Optionssatz erstellen oder ändern	383

Benutzer- und Gruppenverwaltung	385
AWS-Managementkonsole	386
AWS CLI	387
AWS -Tools für PowerShell	388
Lokale oder Amazon EC2 EC2-Instance	388
Verwalten Sie Benutzer und Gruppen mit der Konsole, CLI oder PowerShell	389
Benutzer und Gruppen mit einer EC2 Amazon-Instance verwalten	437
Verzeichnisdienstdaten	449
Replikation und Konsistenz	450
AWS Verzeichnisdienst-Datenattribute	451
Gruppentyp und Gruppenumfang	457
Herstellen einer Verbindung mit Microsoft Entra Connect Sync	458
Voraussetzungen	459
Erstellen Sie einen Active Directory-Domänenbenutzer	459
Herunterladen von Entra Connect Sync	459
PowerShellSkript ausführen	460
Installieren Entra Connect Sync	462
AWS Tutorials für verwaltete Microsoft AD-Testlabore	465
Tutorial: Richten Sie Ihr AWS Managed Microsoft AD-Basis-Testlabor ein	466
Tutorial: Eine Vertrauensstellung von AWS Managed Microsoft AD zu einer selbstverwalteten AD-Installation auf EC2 erstellen	485
Kontingente	497
Fehlerbehebung	499
Probleme mit Ihrem AWS Managed Microsoft AD	499
Probleme mit Netlogon und sicherer Kanalkommunikation	499
Sie erhalten die Fehlermeldung „Antwortstatus: 400 Bad Request“, wenn Sie versuchen, das Passwort eines Benutzers zurückzusetzen	500
Wiederherstellen des Passworts	500
Weitere Ressourcen	500
Fehler beim Domänenbeitritt der Amazon EC2 EC2-Linux-Instance	501
Geringer verfügbarer Speicherplatz	504
Fehler in Zusammenhang mit Schemaerweiterungen	508
Gründe für den Status der Vertrauensstellung	510
AD Connector	516
Erste Schritte	517
AD-Connector-Voraussetzungen	517

Einen AD Connector erstellen	534
Was wird mit Ihrem AD Connector erstellt	536
Best Practices	537
Einrichten: Voraussetzungen	537
Programmieren Ihrer Anwendungen	540
Verwenden Ihres Verzeichnisses	540
Ihr Verzeichnis verwalten	541
Verzeichnisinformationen anzeigen	541
Netzwerktyp des Verzeichnisses aktualisieren	542
Aktualisierung der DNS-Adresse für Ihren AD Connector	543
Ihren AD Connector löschen	544
Ihr Verzeichnis sichern	546
Aktivieren der Multifaktor-Authentifizierung	546
Clientseitiges LDAPS aktivieren	549
mTLS-Authentifizierung aktivieren	555
Die Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos aktualisieren	565
AWS Private CA Connector für AD einrichten	566
Ihr Verzeichnis überwachen	568
Erläuterungen zum Verzeichnisstatus	569
Aktivieren von Verzeichnisstatusbenachrichtigungen mit Amazon SNS	570
Zugriff auf AWS Anwendungen und Dienste	572
Anwendungskompatibilität	573
Zugriff auf AWS Anwendungen und Dienste über AD Connector ermöglichen	574
Möglichkeiten, eine EC2 Amazon-Instance mit Ihrem Active Directory zu verbinden	576
Kontingente	577
Fehlerbehebung	577
Probleme bei der Erstellung	578
Probleme mit der Verbindung	580
Probleme bei der Authentifizierung	582
Probleme mit der Wartung	591
Ich kann meinen AD Connector nicht löschen	592
Allgemeine Tools zur Untersuchung von AD Connector Connector-Emittenten	592
Simple AD	594
Erste Schritte	595
Simple-AD-Voraussetzungen	596
Erstellen Sie Ihr Simple AD	598

Was wird mit Ihrem Simple AD erstellt	601
Best Practices	602
Einrichten: Voraussetzungen	602
Einrichten: Erstellen Ihres Verzeichnisses	605
Programmieren Ihrer Anwendungen	605
Ihr Verzeichnis verwalten	606
Verzeichnisinformationen anzeigen	607
Netzwerktyp des Verzeichnisses aktualisieren	607
Konfiguration von DNS-Servern	609
Wiederherstellung Ihres Verzeichnisses mit Snapshot	610
Löschen Sie Ihr Simple AD	613
Ihr Verzeichnis sichern	615
Setzen Sie das Passwort für das krbtgt-Konto zurück	615
Ihr Verzeichnis überwachen	620
Erläuterungen zum Verzeichnisstatus	621
Aktivieren von Verzeichnisstatusbenachrichtigungen mit Amazon Simple Notification Service	623
Zugriff auf AWS Anwendungen und Dienste	625
Anwendungskompatibilität	626
Aktivierung des Zugriffs auf AWS Anwendungen und Dienste	627
Aktivierung des Zugriffs auf AWS-Managementkonsole	628
Erstellen einer Zugriffs-URL	631
Aktivieren des einmaligen Anmeldens	631
Möglichkeiten, eine Instance Ihrem Verzeichnis hinzuzufügen	640
Einer Windows-Instance beitreten	641
Treten Sie einer Linux-Instanz	649
Delegieren von Rechten für den Verzeichnisbeitritt	675
Erstellen einer DHCP-Optionsliste	678
Verwaltung von Benutzern und Gruppen	680
Installation der AD-Verwaltungstools	681
Erstellen eines Benutzers	683
Löschen eines Benutzers	685
Ein Benutzerkennwort zurücksetzen	687
Eine Gruppe erstellen	688
Einen Benutzer zu einer Gruppe hinzufügen	690
Kontingente	691

Fehlerbehebung	692
Wiederherstellen des Passworts	693
Ich erhalte die Fehlermeldung „KDC kann die angeforderte Option nicht erfüllen“, wenn ich einen Benutzer zu Simple AD hinzufüge	693
Ich kann den DNS-Namen oder die IP-Adresse einer meiner Domain zugeordneten Instance nicht aktualisieren (dynamische DNS-Aktualisierung).	693
Ich kann mich nicht mit einem SQL Server-Konto bei SQL Server anmelden	693
Mein Simple AD steckt im Status „Angefordert“ fest	694
Ich erhalte die Fehlermeldung „AZ constrained“, wenn ich ein Simple AD erstelle	694
Einige meiner Benutzer können sich nicht mit meinem Simple AD authentifizieren	694
Weitere Ressourcen	500
Problembehandlung bei Verzeichnisstatusmeldungen	695
Sicherheit	699
Identity and Access Management	700
Authentifizierung	701
Zugriffskontrolle	701
Übersicht über die Verwaltung von Zugriffsberechtigungen	701
AWS verwaltete Richtlinien	706
Verwenden von identitätsbasierten Richtlinien (IAM-Richtlinien)	711
Directory Service Referenz zu API-Berechtigungen	721
Bedingungsschlüssel Directory Service Verzeichnisdienstdaten	723
Autorisierung für AWS Anwendungen und Dienste, die Directory Service	730
Autorisieren einer AWS Anwendung in einem Active Directory	730
AWS Anwendungsautorisierung mit Directory Service Data	731
Verwenden von servicegebundenen Rollen	733
Mit dem Dienst verknüpfte Rollenberechtigungen für Directory Service	733
Erstellung einer dienstbezogenen Rolle für Directory Service	734
Bearbeiten einer serviceverknüpften Rolle für Directory Service	735
Löschen einer dienstbezogenen Rolle für Directory Service	735
Unterstützte Regionen für serviceverknüpfte Rollen Directory Service	736
Protokollierung und Überwachung	737
AWS Directory Service protokolliert	738
AWS Verzeichnisdienst-Datenprotokolle	741
Compliance-Validierung	751
Ausfallsicherheit	751
Sicherheit der Infrastruktur	752

Serviceübergreifende Confused-Deputy-Prävention	752
AWS PrivateLink	756
Überlegungen	756
Verfügbarkeit	757
Erstellen Sie einen Amazon VPC-Endpunkt mit Schnittstelle	757
Erstellen einer Endpunktrichtlinie	757
Service Level Agreement	760
Verfügbarkeit in Regionen	761
Unterstützt AWS-Regionen für Verzeichnisdienstdaten	768
Browserkompatibilität	772
Was ist TLS?	772
Welche TLS-Versionen werden von IAM Identity Center unterstützt?	772
Wie aktiviere ich die unterstützten TLS-Versionen in meinem Browser?	773
Dokumentverlauf	774
.....	dcclxxix

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 Verzeichnisooptionen. Es bietet auch Entwicklern, die ein Verzeichnis zur Verwaltung von Benutzern, Gruppen, Geräten und Zugriffen benötigen, dieselben Optionen.

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, basiert auf einem echten Microsoft Windows Server Active Directory (AD), 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 Quick](#), [Amazon Chime](#), [Amazon Connect](#) und [Amazon Relational Database Service für Microsoft SQL Server \(Amazon RDS für SQL Server, Amazon RDS für und Amazon RDS for Oracle PostgreSQL\)](#).

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 arbeiten mit Benutzer-Anmeldeinformationen, die Sie in AWS Managed Microsoft AD speichern. Alternativ können Sie eine [Verbindung mit Ihrer vorhandenen AD-Infrastruktur](#) mit Vertrauensstatus einrichten und Anmeldeinformationen aus einem Active Directory verwenden, das On-Premises oder auf EC2 Windows ausgeführt wird. 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 Verbundanwendungsfälle mit Active Directory-Anmeldeinformationen. Allein mit AWS Managed Microsoft AD können Sie sich bei der anmelden [AWS-Managementkonsole](#). Mit [AWS IAM Identity Center](#) können 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 als Azure 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 ein LDAP-Verzeichnis ist, 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 verwalteten 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 ein eigenständiges Active Directory in der AWS Cloud benötigen, das 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 Quick und [Amazon EC2](#) für Windows Server Instances mit Ihrem vorhandenen lokalen Microsoft Active Directory zu verbinden. Mit AD Connector können Sie einfach [ein Servicekonto](#) zu Ihrem Active Directory hinzufügen. 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 Quick hinzufügen, liest AD Connector Ihr vorhandenes 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, darunter [Amazon WorkSpaces](#), [Amazon WorkDocs](#), [Amazon Quick](#), [Amazon Chime](#), [Amazon Connect](#) und [Amazon WorkMail](#). Sie können [Ihre Windows EC2-Instances auch über AD Connector mit Ihrer lokalen Active Directory-Domäne verbinden](#), indem Sie [Seamless Domain Join](#) verwenden. Mit AD Connector können Ihre Benutzer auch auf die AWS Ressourcen zugreifen AWS-Managementkonsole 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 Ihr Active Directory weiterhin wie derzeit üblich. Beispielsweise können Sie unter Verwendung der Active Directory-Standardverwaltungstools aus Ihrem On-Premises-Active-Directory neue Benutzer und Gruppen hinzufügen und Passwörter aktualisieren. Auf diese Weise können Sie Ihre Sicherheitsrichtlinien wie Ablauf von Kennwörtern, Kennwortverlauf und Kontosperrungen konsistent durchsetzen, unabhängig davon, ob Benutzer lokal oder in der Cloud auf Ressourcen zugreifen. AWS

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 Dienstes.

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 Active-Directory-fähige Anwendungen und Tools verwenden, die grundlegende Active-Directory-Features erfordern. Simple AD ist mit den folgenden AWS Anwendungen kompatibel: [Amazon WorkSpaces](#), [Amazon WorkDocs](#), [Amazon Quick](#) und [Amazon WorkMail](#). Sie können sich auch AWS-Managementkonsole 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 echten Microsoft Active Directory benötigen oder beabsichtigen, 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](#).

Eine Liste der unterstützten Verzeichnistypen pro Region finden Sie unter [Verfügbarkeit in der Region für Directory Service](#).

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 ein aktuelles Microsoft Active Directory in der AWS Cloud benötigen, das Active Directory-fähige Workloads oder AWS Anwendungen und Dienste wie Amazon WorkSpaces und Amazon Quick unterstützt, oder wenn Sie LDAP-Unterstützung für Linux-Anwendungen benötigen.
	Verwenden Sie den AWS Directory Service für Microsoft Active Directory (Hybrid Edition), um Ihr vorhandenes selbstverwaltetes AD um AWS Cloud AWS Directory Service
	Verwenden Sie AD Connector, wenn Sie Ihren lokalen Benutzern nur erlauben müssen, sich mit ihren Active Directory-Anmeldeinformationen bei AWS Anwendung en und Diensten anzumelden. Sie können auch AD Connector verwenden, um Amazon-EC2-Instances mit Ihrer bestehenden Domain von Active Directory zu verbinden.

Was müssen Sie als Nächstes tun?	Empfohlene AWS Directory Service Optionen
	Verwenden Sie Simple AD, wenn Sie ein kleines, kostengünstiges Verzeichnis mit grundlegender Active-Directory-Kompatibilität benötigen, das mit Samba 4 kompatible Anwendungen unterstützt, oder wenn Sie LDAP-Kompatibilität für LDAP-fähige Anwendungen benötigen.
Ich entwickle SaaS-Anwendungen.	Verwenden Sie Amazon Cognito, wenn Sie umfangreiche 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 Verzeichnisooptionen finden Sie unter [So wählen Sie Active Directory-Lösungen auf AWS](#).

Arbeiten mit Amazon EC2

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

- [Was ist Amazon EC2?](#) im Amazon EC2 EC2-Benutzerhandbuch.
- [Starten Sie eine Amazon EC2 EC2-Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
- [Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances im Amazon EC2](#) EC2-Benutzerhandbuch.
- [Was ist Amazon VPC?](#) im Amazon-VPC-Benutzerhandbuch.
- [Connect Sie Ihre VPC mithilfe AWS Virtual Private Network des Amazon VPC-Benutzerhandbuchs mit Remote-Netzwerken](#).

AWS Verwaltetes Microsoft AD

AWS Der Directory Service für Microsoft Active Directory, auch als AWS Managed Microsoft AD bezeichnet, wird Microsoft Active Directory als verwalteter Dienst ausgeführt, der von Windows Server 2019 unterstützt wird. Es erstellt ein hochverfügbares Paar von Domain-Controllern in Ihrer Amazon VPC über verschiedene Availability Zones hinweg, wobei Host-Überwachung, Wiederherstellung, Datenreplikation, Snapshots und Softwareupdates AWS automatisch verwaltet werden. Mit diesem Service können Sie verzeichnisabhängige Workloads ausführen, Benutzer und Gruppen verwalten, Single Sign-On bereitstellen, Gruppenrichtlinien erstellen und anwenden und eine sichere Verbindung zu Amazon EC2 EC2-Instances herstellen.

Directory Service bietet zwei Microsoft Active Directory Lösungen: AWS Directory Service for Microsoft Active Directory bietet einen vollständig verwalteten Active Directory-Dienst in der AWS Cloud, während AWS Managed Microsoft AD (Hybrid Edition) Ihr bestehendes selbstverwaltetes AD um AWS erweitert.

AWS Managed Microsoft AD (Standard Edition und Enterprise Edition) erstellt neue verwaltete AD-Domänen zur Verwaltung von Benutzern, Geräten und Computern AWS. Diese Verzeichnisse richten Ressourcengesamtstrukturen ein, die Vertrauensbeziehungen zu Ihren vorhandenen AD-Domänen vor Ort AWS, in oder in Multi-Cloud-Umgebungen herstellen. Benutzer können mit ihren vorhandenen Anmeldeinformationen von Ihren aktuellen AD-Domänen aus auf AWS Ressourcen zugreifen. Benutzeridentitäten verbleiben in Ihren vorhandenen AD-Domänen, während die Ressourcengesamtstruktur Ihre AWS Ressourcen verwaltet. Dadurch wird die betriebliche Isolierung zwischen den Umgebungen gewährleistet und gleichzeitig ein nahtloses Single Sign-On gewährleistet.

AWS Managed Microsoft AD (Hybrid Edition) verbindet Ihr selbstverwaltetes Active Directory mit dem AWS Directory Service für Microsoft Active Directory und schafft so eine integrierte Identitätsumgebung, die sowohl Ihre Infrastruktur als auch die. AWS Cloud Diese Lösung erweitert Ihre Verzeichnisdienste AWS ohne Synchronisation von Benutzeridentitäten, stellt Vertrauensbeziehungen zwischen Umgebungen her und ermöglicht einen nahtlosen Zugriff mit vorhandenen Anmeldeinformationen.

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 Vertrauensstellungen zwischen AWS Managed Microsoft AD und Ihrem vorhandenen selbstverwalteten Microsoft Active Directory konfigurieren, sodass Benutzer und Gruppen mithilfe AWS IAM Identity Center von.

Welche sollte man auswählen

Sie können zwischen zwei AWS Directory Service Diensten mit den Funktionen und der Skalierbarkeit wählen, die Ihren Anforderungen am besten entsprechen. Anhand der folgenden Tabelle können Sie ermitteln, welche Directory Service Option für Ihr Unternehmen am besten geeignet ist.

Anwendungsfall	Empfohlene Lösung
Führen Sie verzeichnissensitive Workloads, AWS Anwendungen oder Linux-Anwendungen aus, die LDAP-Unterstützung benötigen	AWS Managed Microsoft AD (Standard Edition und Enterprise Edition) erstellt neue verwaltete AD-Domänen zur Verwaltung von Benutzern, Geräten und Computern AWS. Diese Verzeichnisse richten Ressourcengesamtstrukturen ein, die Vertrauensbeziehungen zu Ihren vorhandenen AD-Domänen vor Ort AWS, in oder in Multi-Cloud-Umgebungen herstellen. Benutzer können mit ihren vorhandenen Anmeldeinformationen von Ihren aktuellen AD-Domänen aus auf AWS Ressourcen zugreifen. Benutzeridentitäten verbleiben in Ihren vorhandenen AD-Domänen, während die Ressourcengesamtstruktur Ihre AWS Ressourcen verwaltet. Dadurch wird die betriebliche Isolierung zwischen den Umgebungen gewährleistet und gleichzeitig ein nahtloses Single Sign-On gewährleistet.
Erweitern Sie das bestehende Active Directory auf AWS	AWS Managed Microsoft AD (Hybrid Edition) verbindet Ihr selbstverwaltetes Active Directory mit dem AWS Directory Service für Microsoft Active Directory und schafft so eine integrierte Identitätsumgebung, die sowohl Ihre Infrastruktur als auch die AWS Cloud. Diese Lösung erweitert Ihre Verzeichnisdienste AWS ohne Synchronisation von Benutzeridentitäten, stellt Vertrauensbeziehungen zwischen Umgebungen her und ermöglicht einen nahtlosen Zugriff mit vorhandenen Anmeldeinformationen.

Topics

- [Erste Schritte mit AWS Managed Microsoft AD](#)
- [Grundlegendes zu AWS Managed Microsoft AD \(Hybrid Edition\)](#)

Grundlegendes zu AWS Managed Microsoft AD (Hybrid Edition)

AWS Managed Microsoft AD (Hybrid Edition) ermöglicht es Ihnen, Ihr bestehendes Active Directory AWS Cloud mit AWS Managed Microsoft AD zu erweitern. Diese Funktion erleichtert die Migration Ihrer AD-abhängigen Workloads AWS, die Einführung von AWS Diensten und die Erhöhung Ihrer Active Directory-Redundanz. AWS führt in regelmäßigen Abständen Verzeichnisbewertungen für Ihr Hybridverzeichnis durch, die Sie in der Konsole einsehen können. Directory Service

Ein Hybridverzeichnis Directory Service verbindet Ihr vorhandenes AWS Verzeichnis Microsoft Active Directory mit dem Directory Service für Microsoft Active Directory (AWS Managed Microsoft AD). Dadurch entsteht eine integrierte Identitätsumgebung, AWS die sich über lokale Infrastrukturen und Multi-Cloud-Infrastrukturen erstreckt, sodass Sie eine einzige Identitätsquelle verwalten und gleichzeitig Ihre Verzeichnisdienste auf erweitern können. AWS

Eine hybride Verzeichniskonfiguration bietet mehrere wichtige Funktionen:

- Erweiterung von selbstverwaltetem AD auf die, AWS Cloud ohne dass eine Vertrauensbeziehung aufgebaut werden muss
- Nahtlose Authentifizierung und Autorisierung in allen Umgebungen mithilfe vorhandener Active Directory-Anmeldeinformationen
- Konsistente Benutzeranmeldedaten und Gruppenmitgliedschaften in Ihren beiden AD-Umgebungen
- Zentralisierte Verwaltung der AD-Zugriffsrichtlinien und -berechtigungen

Themen

- [Voraussetzungen für Hybridverzeichnisse](#)
- [Ein Hybridverzeichnis erstellen](#)
- [Ein Hybridverzeichnis anzeigen und bearbeiten](#)
- [Löschen eines Hybridverzeichnisses](#)
- [Verzeichnisbewertungen für hybride Verzeichnisse](#)

- [Fehlerbehebung bei der Bewertung von Hybridverzeichnissen und Verzeichnissen](#)

Voraussetzungen für Hybridverzeichnisse

Das Hybridverzeichnis erweitert Ihr selbstverwaltetes Active Directory um das AWS Cloud. Bevor Sie ein Hybridverzeichnis erstellen, stellen Sie sicher, dass Ihre Umgebung die folgenden Anforderungen erfüllt:

Microsoft Active Directory Domain-Anforderungen

Stellen Sie vor dem Erstellen eines Hybridverzeichnisses sicher, dass Ihre selbstverwaltete AD-Umgebung und Infrastruktur die folgenden Anforderungen erfüllen, und stellen Sie die erforderlichen Informationen zusammen.

Anforderungen an die Domäne

Ihre selbstverwaltete AD-Umgebung muss die folgenden Anforderungen erfüllen:

- Verwendet eine Windows Server 2012 R2 oder 2016 funktionale Ebene.
- Verwendet Standard-Domänencontroller, die für die Erstellung von Hybridverzeichnissen bewertet werden. Read-Only Domain Controller (RODC) können nicht für die Erstellung von Hybridverzeichnissen verwendet werden.
- Hat zwei Domänencontroller, auf denen alle Active Directory-Dienste ausgeführt werden.
- Der primäre Domänencontroller (PDC) muss jederzeit routingfähig sein.

Insbesondere müssen der PDC-Emulator und der RID-Master IPs Ihres selbstverwalteten AD zu einer der folgenden Kategorien gehören:

- Teil der RFC1918 privaten IP-Adressbereiche (10.0.0.0/8, 172.16.0.0/12 oder 192.168.0.0/16)
- Innerhalb Ihres VPC CIDR-Bereichs
- Ordnen Sie dem Verzeichnis den DNS IPs Ihrer selbstverwalteten Instances zu

Sie können zusätzliche IP-Routen für das Verzeichnis hinzufügen, nachdem das Hybridverzeichnis erstellt wurde.

Erforderliche Informationen

Sammeln Sie die folgenden Informationen über Ihr selbstverwaltetes AD:

- DNS-Name des Verzeichnisses
- Verzeichnis-DNS IPs
- Anmeldeinformationen für das Dienstkonto mit Administratorberechtigungen für Ihr selbstverwaltetes AD
- AWS Geheimer ARN zum Speichern der Anmeldeinformationen Ihres Dienstkontos (siehe [AWS Geheimer ARN für Hybridverzeichnis](#))

AWS Geheimer ARN für Hybridverzeichnis

Um ein Hybridverzeichnis mit Ihrem selbstverwalteten AD zu konfigurieren, müssen Sie einen KMS-Schlüssel erstellen, um Ihr AWS Geheimnis zu verschlüsseln, und dann das Geheimnis selbst erstellen. Beide Ressourcen müssen in derselben Ressource erstellt werden, die das AWS-Konto das Hybridverzeichnis enthält.

Erstellen Sie einen KMS-Schlüssel

Der KMS-Schlüssel wird verwendet, um Ihr AWS Geheimnis zu verschlüsseln.

Important

Verwenden Sie für Verschlüsselungsschlüssel nicht den standardmäßigen AWS-KMS-Schlüssel. Stellen Sie sicher, dass Sie den AWS KMS-Schlüssel in demselben Ordner erstellen, der das Hybridverzeichnis enthält AWS-Konto, das Sie für die Verbindung mit Ihrem selbstverwalteten AD erstellen möchten.

Um einen AWS KMS-Schlüssel zu erstellen

1. Wählen Sie in der AWS KMS Konsole **Create Key** aus.
2. Wählen Sie für Schlüsseltyp **Symmetrisch** aus.
3. Wählen Sie für Schlüsselnutzung die Option **Verschlüsseln und Entschlüsseln** aus.
4. Für **Advanced options** (Erweiterte Optionen):
 - a. Wählen Sie unter **Schlüsselmaterialursprung** **KMS** aus.
 - b. Wählen Sie für **Regionality** die Option **Single Region Key** und dann **Next** aus.
5. Geben Sie für **Alias** einen Namen für den KMS-Schlüssel an.
6. (Optional) Geben Sie unter **Beschreibung** eine Beschreibung des KMS-Schlüssels an.

7. (Optional) Fügen Sie für Tags Tags für den KMS-Schlüssel hinzu und wählen Sie Weiter.
8. Wählen Sie für Schlüsseladministratoren einen IAM-Benutzer aus.
9. Behalten Sie für das Löschen von Schlüsseln die Standardauswahl für Schlüsseladministratoren das Löschen dieses Schlüssels zulassen bei und wählen Sie Weiter.
10. Wählen Sie für Key-Benutzer denselben IAM-Benutzer aus dem vorherigen Schritt aus und klicken Sie auf Weiter.
11. Prüfen Sie die Konfiguration.
12. Fügen Sie unter Schlüsselrichtlinie die folgende Erklärung zur Richtlinie hinzu:
13. Wählen Sie Finish (Abschließen).

Erstellen Sie ein AWS Geheimnis

Erstellen Sie in Secrets Manager ein Geheimnis, um die Anmeldeinformationen für Ihr selbstverwaltetes AD-Benutzerkonto zu speichern.

Important

Erstellen Sie das Geheimnis in demselben Verzeichnis AWS-Konto, das das Hybridverzeichnis enthält, das Sie mit Ihrem selbstverwalteten AD verbinden möchten.

So erstellen Sie ein Secret

- Wählen Sie im Secrets Manager die Option Neues Geheimnis speichern
 - Wählen Sie für Geheimtyp die Option Anderer Geheimtyp
 - Fügen Sie für Schlüssel/Wert-Paare Ihre beiden Schlüssel hinzu:
1. Fügen Sie den Benutzernamenschlüssel hinzu
 - a. Geben Sie als ersten Schlüssel `customerAdAdminDomainUsername` ein.
 - b. Geben Sie als Wert für den ersten Schlüssel nur den Benutzernamen (ohne das Domain-Präfix) des AD-Benutzers ein. Geben Sie den Domain-Namen nicht an, da dies dazu führt, dass die Instance-Erstellung fehlschlägt.
 2. Fügen Sie den Passwortschlüssel hinzu
 - a. Geben Sie als zweiten Schlüssel `customerAdAdminDomainPassword` ein.

- b. Geben Sie als Wert des zweiten Schlüssels das Passwort ein, das Sie für den AD-Benutzer in Ihrer Domain erstellt haben.

Vervollständigen Sie die geheime Konfiguration

1. Wählen Sie unter Verschlüsselungsschlüssel den KMS-Schlüssel aus, den Sie in erstellt haben, [Erstellen Sie einen KMS-Schlüssel](#) und klicken Sie auf Weiter.
2. Geben Sie unter Geheimer Name eine Beschreibung für das Geheimnis ein.
3. (Optional) Geben Sie unter Beschreibung eine Beschreibung für das Geheimnis ein.
4. Wählen Sie Weiter aus.
5. Behalten Sie für Rotationseinstellungen konfigurieren die Standardwerte bei und wählen Sie Weiter aus.
6. Überprüfen Sie die Einstellungen für das Geheimnis und wählen Sie Speichern aus.
7. Wählen Sie das von Ihnen erstellte Secret aus und kopieren Sie den Wert für den Secret-ARN. Sie werden diesen ARN im nächsten Schritt verwenden, um Ihr selbstveraltetes Active Directory einzurichten.

Anforderungen an die Infrastruktur

Bereiten Sie die folgenden Infrastrukturkomponenten vor:

- Zwei AWS Systems Manager Knoten mit Administratorrechten für SSM-Agenten
 - Wenn Ihr Active Directory außerhalb von selbst verwaltet wird AWS Cloud, benötigen Sie zwei Systems Manager Manager-Knoten für eine Hybrid- und Multi-Cloud-Umgebung. Weitere Informationen zur Bereitstellung dieser Knoten finden Sie unter [Systems Manager für Hybrid- und Multicloud-Umgebungen einrichten](#).
 - Wenn Ihr Active Directory innerhalb von selbst verwaltet wird AWS Cloud, benötigen Sie zwei von Systems Manager verwaltete EC2-Instances. Weitere Informationen zur Bereitstellung dieser Instances finden Sie unter [EC2-Instances mit Systems Manager verwalten](#).

Erforderliche Active Directory-Dienste

Stellen Sie sicher, dass die folgenden Dienste auf Ihrem selbstverwalteten AD ausgeführt werden:

- Active Directory Domain Services

- Active Directory-Webdienst (ADWS)
- COM+-Ereignissystem
- DFS-Replikation (Distributed File System Replication, DFSR)
- Domain Name System (DNS)
- DNS-Server
- Gruppenrichtlinien-Client
- Standortübergreifendes Messaging
- Remote Procedure Call (RPC)
- Manager für Sicherheitskonten
- Windows-Zeitserver

Note

Für das Hybridverzeichnis muss sowohl der UDP-Port 123 geöffnet als auch der Windows Time Server aktiviert und funktionsfähig sein. Wir synchronisieren die Uhrzeit mit Ihrem Domänencontroller, um sicherzustellen, dass die hybride Verzeichnisreplikation ordnungsgemäß funktioniert.

Anforderungen an die Kerberos-Authentifizierung

Für Ihre Benutzerkonten muss die Kerberos-Vorauthentifizierung aktiviert sein. Ausführliche Anweisungen zur Aktivierung dieser Einstellung finden Sie unter [Stellen Sie sicher, dass die Kerberos-Vorauthentifizierung](#) aktiviert ist. [Allgemeine Informationen zu dieser Einstellung finden Sie unter Vorauthentifizierung ein.](#) Microsoft TechNet

Unterstützte Verschlüsselungstypen

Hybrid Directory unterstützt die folgenden Verschlüsselungstypen bei der Authentifizierung über Kerberos bei Ihren Active Directory-Domänencontrollern:

- AES-256-HMAC

Anforderungen an Netzwerkports

AWS Um Ihre selbstverwalteten Active Directory-Domänencontroller zu erweitern, muss die Firewall für Ihr vorhandenes Netzwerk die folgenden Ports CIDRs für beide Subnetze in Ihrer Amazon VPC geöffnet haben:

- TCP/UDP 53 – DNS
- TCP/UDP 88 – Kerberos-Authentifizierung
- UDP 123 — Zeitserver
- TCP 135 — Remoteprozeduraufruf
- TCP/UDP 389 – LDAP
- TCP 445 – SMB
- TCP 636 — Wird nur für Umgebungen mit Lightweight Directory Access Protocol Secure (LDAPS) benötigt
- TCP 49152-65535 — RPC hat nach dem Zufallsprinzip hohe TCP-Ports zugewiesen
- TCP 3268 und 3269 — Globaler Katalog
- TCP 9389 Active Directory-Webdienste (ADWS)

Dies sind die Mindestports, die zum Erstellen eines Hybridverzeichnisses erforderlich sind. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports.

Note

Das DNS, das für Ihre Domain-Controller und FSMO-Rolleninhaber IPs bereitgestellt wird, muss die oben genannten Ports CIDRs für beide Subnetze in der Amazon VPC offen haben.

Note

Für das Hybridverzeichnis muss sowohl der UDP-Port 123 geöffnet als auch der Windows Time Server aktiviert und funktionsfähig sein. Wir synchronisieren die Uhrzeit mit Ihrem Domänencontroller, um sicherzustellen, dass die hybride Verzeichnisreplikation ordnungsgemäß funktioniert.

AWS-Konto Berechtigungen

Sie benötigen Berechtigungen für die folgenden Aktionen in Ihrem AWS-Konto:

- ec2: AuthorizeSecurityGroupEgress
- ec2: AuthorizeSecurityGroupIngress
- ec2: CreateNetworkInterface
- ec2: CreateSecurityGroup
- ec2: DescribeNetworkInterfaces
- ec2: DescribeSubnets
- ec2: DescribeVpcs
- ec2: CreateTags
- ec2: CreateNetworkInterfacePermission
- ssm: ListCommands
- ssm: GetCommandInvocation
- ssm: GetConnectionStatus
- ssm: SendCommand
- Verwalter von Geheimnissen: DescribeSecret
- Geheimnismanager: GetSecretValue
- ich bin: GetRole
- ich bin: CreateServiceLinkedRole

Amazon VPC-Netzwerkanforderungen

Eine VPC mit den folgenden Eigenschaften:

- Mindestens zwei Subnetze. Jedes der Subnetze muss sich in einer anderen Availability Zone befinden
- Die VPC muss über eine Standardmietdauer verfügen

Sie können kein Hybridverzeichnis in einer VPC mit Adressen im 198.18.0.0/15-Adressraum erstellen.

Directory Service verwendet eine Struktur mit zwei VPCs. Die EC2-Instances, aus denen Ihr Verzeichnis besteht AWS-Konto, werden außerhalb Ihres Verzeichnisses ausgeführt und von diesem 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 für Ihr Verzeichnis lautet 198.18.0.0/15.

Weitere Informationen finden Sie unter den folgenden Themen im Amazon VPC Benutzerhandbuch:

- [Was ist Amazon VPC?](#)
- [Was ist Amazon VPC?](#)
- [VPCs und Subnetze](#)
- [Was ist AWS Site-to-Site VPN?](#)

Weitere Informationen zu AWS Direct Connect finden Sie unter [Was ist AWS Direct Connect?](#)

AWS Konfiguration der Sicherheitsgruppe

AWS Fügt standardmäßig eine Sicherheitsgruppe hinzu, um den Netzwerkzugriff auf die AWS Systems Manager verwalteten Knoten in Ihrer VPC zu ermöglichen. Sie können optional Ihre eigene Sicherheitsgruppe angeben, die Netzwerkverkehr zu und von Ihren selbstverwalteten Domänencontrollern außerhalb Ihrer VPC ermöglicht.

Sie können optional Ihre eigene Sicherheitsgruppe angeben, die Netzwerkverkehr zu und von Ihren selbstverwalteten Domänencontrollern außerhalb Ihrer VPC ermöglicht. Wenn Sie Ihre eigene Sicherheitsgruppe angeben, müssen Sie:

- Ihre VPC CIDR Bereiche und selbst verwalteten Bereiche auf die Zulassungsliste setzen.
- Stellen Sie sicher, dass sich diese Bereiche nicht mit [AWS reservierten](#) IP-Bereichen überschneiden

Überlegungen zur Verzeichnisbewertung

Bei der Erstellung von Verzeichnisbewertungen und der Anzahl der Bewertungen, die Sie in Ihrem Verzeichnis haben können, sollten Sie Folgendes beachten AWS-Konto:

- Eine Verzeichnisbewertung wird automatisch erstellt, wenn Sie ein Hybridverzeichnis erstellen. Es gibt zwei Arten von Bewertungen: CUSTOMER und SYSTEM. Ihre AWS-Konto hat ein Limit von 100 CUSTOMER Verzeichnisbewertungen.
- Wenn Sie versuchen, ein Hybridverzeichnis zu erstellen, und Sie bereits über 100 CUSTOMER Verzeichnisbewertungen verfügen, tritt ein Fehler auf. Löschen Sie die Bewertungen, um Kapazität freizugeben, bevor Sie es erneut versuchen.
- Sie können eine Erhöhung Ihres Kontingents für die CUSTOMER Verzeichnisbewertung beantragen, indem Sie sich an CUSTOMER wenden Support oder bestehende Kundenverzeichnisbewertungen löschen, um Speicherplatz freizugeben.

Ein Hybridverzeichnis erstellen

Bevor Sie ein Hybridverzeichnis erstellen, müssen Sie eine Verzeichnisbewertung erstellen und diese erfolgreich bestehen, um die Konnektivität und Interoperabilität mit Ihrem selbstverwalteten Active Directory zu überprüfen

Erstellen Sie ein Hybridverzeichnis mit Ihrem selbstverwalteten AD

Gehen Sie wie folgt vor, um ein Hybridverzeichnis mit Ihrem selbstverwalteten AD zu erstellen:

Um ein Hybridverzeichnis zu erstellen

1. Öffnen Sie die Directory Service Konsole für die gewünschte Region.
2. Wählen Sie auf der Seite Verzeichnistyp auswählen die Option AWS Managed Microsoft AD aus.
3. Wählen Sie unter Erste Schritte mit AWS verwaltetem Microsoft AD die Option Erweitern Sie Ihre AD-Domäne um ein Hybridverzeichnis — neu aus und klicken Sie dann auf Weiter. Dadurch werden Sie zur Bewertungsseite „Verzeichnis erstellen“ weitergeleitet.
4. Bevor Sie ein Hybridverzeichnis erstellen können, müssen Sie zunächst eine Verzeichnisbewertung erstellen und diese erfolgreich bestehen. Gehen Sie wie unter beschrieben vor, um eine Verzeichnisbewertung zu erstellen [Verzeichnisbewertungen werden erstellt](#). Sobald Sie eine Verzeichnisbewertung erfolgreich bestanden haben, können Sie mit diesem Verfahren fortfahren.
5. Sobald Sie eine Verzeichnisbewertung erfolgreich bestanden haben, navigieren Sie zur Seite Verzeichnisse.

6. Wählen Sie auf der Seite Verzeichnisse unter Trial Hybrid Directory Assessments eine Bewertungs-ID mit dem Status Trial ausSUCCESS. Wählen Sie dann Hybridverzeichnis erstellen aus, wodurch Sie zur Seite mit den Bewertungsdetails weitergeleitet werden
7. Bestätigen Sie diese Aktion auf der Seite mit den Bewertungsdetails, indem Sie Hybridverzeichnis erstellen auswählen. Daraufhin wird die Seite Hybridverzeichnis mit Assessment-ID erstellen geöffnet.
8. Überprüfen Sie auf der Seite Hybridverzeichnis mithilfe der Assessment-ID erstellen die Informationen zum selbstverwalteten Active Directory. Nachdem Sie die Informationen bestätigt haben, wählen Sie Hybridverzeichnis erstellen aus.

Nachdem Sie Hybridverzeichnis erstellen ausgewählt haben, AWS führt Sie auf der Grundlage dieser Informationen eine weitere Verzeichnisbewertung durch, um zu bestätigen, dass Ihre selbstverwaltete AD-Konfiguration noch gültig ist. Wenn die Verzeichnisbewertung erfolgreich abgeschlossen wurde, erstellen wir das Hybridverzeichnis.

9. Wenn Sie „Hybridverzeichnis erstellen“ wählen, kehren Sie zur Seite „Verzeichnisse“ zurück.
 - a. Sobald das Hybridverzeichnis erfolgreich erstellt wurde, erscheint ein grünes Banner.
 - b. Ein rotes Banner erscheint, wenn die Erstellung des Hybridverzeichnisses fehlschlägt. Bereinigen Sie Fehler bei der Erstellung von Hybridverzeichnissen, indem Sie wie folgt vorgehen:
 1. Löschen Sie das fehlgeschlagene Hybridverzeichnis in der Konsole.
 2. Löschen Sie alle verbleibenden AWS Reserved OUs in Ihrem selbstverwalteten AD.

Weitere Informationen

- [Löschen eines Hybridverzeichnisses](#)
- [Fehlerbehebung](#)

Ein Hybridverzeichnis anzeigen und bearbeiten

Gehen Sie wie folgt vor, um Ihr Hybridverzeichnis anzuzeigen oder zu bearbeiten.

Ein Hybridverzeichnis anzeigen

Sie können ein Hybridverzeichnis in der Directory Service Konsole anzeigen.

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

1. Wählen Sie im Navigationsbereich der [Directory Service -Konsole](#) Directories aus.
2. Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis. Informationen über das Verzeichnis werden auf der Seite mit den Verzeichnisdetails angezeigt.

Informationen zum selbstverwalteten Active Directory

Dieser Abschnitt enthält Informationen zu Ihrem selbstverwalteten Active Directory, das mit AWS der Infrastruktur verknüpft ist.

- Typ des Verzeichnisses
- Verzeichnis-ID
- Status des Verzeichnisses
- Netzwerkdetails für Ihr selbstverwaltetes AD, z. B.:
 - VPC
 - Subnets
 - DNS-Adressen
- Von Systems Manager verwaltete Knoten

Registerkarten für hybride Verzeichnisse

Sie können die folgenden Informationen zu Ihrem AWS Managed Microsoft AD finden:

- Auf der Registerkarte Teilen und Teilen können Sie Ihr AWS verwaltetes Microsoft AD für andere AWS Konten freigeben und die Netzwerkdetails für Ihre Domänencontroller anzeigen.
- Auf der Registerkarte Anwendungsverwaltung können Sie eine Anwendungszugriffs-URL für Ihr AWS verwaltetes Microsoft AD und AWS Anwendungen und Dienste für Ihr AWS verwaltetes Microsoft AD aktivieren.
- Auf der Registerkarte Wartung können Sie SNS aktivieren, um Benachrichtigungen über Ihren AWS verwalteten Microsoft AD-Status zu erhalten und Snapshots von Ihrem AWS verwalteten Microsoft AD zu überprüfen.
- Weitere Informationen zum Feld Status finden Sie unter [Den Status Ihres AWS verwalteten Microsoft AD-Verzeichnisses verstehen](#).

Ein Hybridverzeichnis aktualisieren

Sie können ein Hybridverzeichnis in der Directory Service Konsole aktualisieren, um die DNS-Einstellungen zu ändern oder den Zugriff auf das Administratorkonto wiederherzustellen.

Um Informationen zum Hybridverzeichnis zu aktualisieren

1. Wählen Sie im Navigationsbereich der [Directory Service -Konsole](#) Directories aus.
2. Wählen Sie den Verzeichnis-ID-Link für Ihr Verzeichnis, um die Seite mit den Verzeichnisdetails zu öffnen.
3. Wählen Sie Aktionen und anschließend Hybridverzeichnisinformationen aktualisieren aus.
4. Auf der Informationsseite zum Hybridverzeichnis aktualisieren können Sie Ihre DNS-Einstellungen aktualisieren oder Ihr Administratorkonto wiederherstellen.

Aktualisieren Sie die DNS-Einstellungen (optional)

Unter Informationen zum selbstverwalteten Active Directory können Sie Folgendes ändern:

- a. DNS-Name des Verzeichnisses
- b. DNS-IP-Adressen

Sie können beide Einstellungen zusammen oder einzeln aktualisieren. Für den Aktualisierungsvorgang ist mindestens eine Änderung erforderlich.

5. Stellen Sie das Administratorkonto für das Hybridverzeichnis wieder her

Um Ihr Hybrid-Verzeichnis-Administratorkonto wiederherzustellen, benötigen wir temporären Zugriff auf einen Benutzer. Dieser Zugriff erfolgt über ein Secret von Secrets Manager. Wir verwenden diese Anmeldeinformationen nur einmal während der Wiederherstellung und speichern sie nicht. Wenn Ihr Hybrid-Directory-Administratorkonto bereits vorhanden ist, müssen Sie dieses Geheimnis nicht aktualisieren, auch wenn Sie Ihren selbstverwalteten Active Directory-Administratorbenutzer aktualisiert haben.

- Geheime Administratoranmeldedaten — Wir erstellen ein Hybrid-Verzeichnis-Administratorkonto, wenn wir ein Hybridverzeichnis erstellen. Wenn Sie dieses Geheimnis gelöscht haben, geben Sie Ihr Secrets Manager Manager-Geheimnis für Ihren selbstverwalteten AD-Administratorbenutzer ein.

Löschen eines Hybridverzeichnisses

Wenn Sie ein Hybridverzeichnis löschen, werden alle Verzeichnisdaten und Snapshots gelöscht und können nicht wiederhergestellt werden. Nach dem Löschen des Verzeichnisses bleiben alle Instanzen, die dem Verzeichnis hinzugefügt wurden, intakt. Sie können die Verzeichnisanmeldedaten jedoch nicht verwenden, um sich bei diesen Instanzen anzumelden. Sie müssen sich mit einem lokalen Benutzerkonto bei diesen Instanzen anmelden.

So löschen Sie ein Verzeichnis

1. Wählen Sie im Navigationsbereich der [Directory Service -Konsole](#) Verzeichnisse. Stellen Sie sicher, dass Sie sich AWS-Region an dem Ort befinden, an dem Ihr Hybridverzeichnis 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 Hybridverzeichnis löschen.
3. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
4. 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.
 - a. Deaktivieren Sie AWS-Managementkonsole den Zugriff. Weitere Informationen finden Sie unter [Deaktivieren des Zugriffs auf die AWS Managementkonsole](#).
 - b. Um Amazon FSx for Windows File Server zu deaktivieren, müssen Sie das FSx Amazon-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter [Arbeiten mit Active Directory in FSx für Windows File Server](#) im Amazon FSx for Windows File Server-Benutzerhandbuch.
 - c. 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.
5. Wählen Sie im Navigationsbereich Verzeichnisse aus.
6. Wählen Sie nur das Verzeichnis aus, das gelöscht werden soll, und wählen Sie Löschen. Es dauert einige Minuten, bis das Verzeichnis gelöscht wird. Wenn dieser Vorgang abgeschlossen ist, wird es aus Ihrer Verzeichnisliste entfernt.

7. Löschen Sie manuell alle verbleibenden Domänencontroller-Objekte, einschließlich aller AWS reservierten Objekte OUs. Sie können das gesamte AWS reservierte Verzeichnis löschen, um die Bereinigung Ihrer Umgebung abzuschließen.

Verzeichnisbewertungen für hybride Verzeichnisse

Bei einer Verzeichnisbewertung wird Ihre selbstverwaltete Active Directory-Umgebung untersucht, um sicherzustellen, dass sie die Anforderungen für die Erstellung eines Hybridverzeichnisses erfüllt. Bei dieser Bewertung werden die Netzwerkkonnektivität, die Konfiguration des Domänencontrollers und die erforderlichen Dienste überprüft, um potenzielle Probleme zu identifizieren und zu lösen, bevor eine Verbindung zwischen Ihrem selbstverwalteten AD und hergestellt wird. Directory Service

Es gibt zwei Arten von Verzeichnisbewertungen:

- *CUSTOMER*Bewertungen — Von Ihnen in der Konsole initiiert, wenn Sie mit der Einrichtung eines Hybridverzeichnisses beginnen. Sie können Bewertungen aus dem Kundenverzeichnis löschen, auch wenn sie noch in Bearbeitung sind. Sie können bis zu 100 Kundenbeurteilungen haben.
- *SYSTEM*Bewertungen — werden automatisch erstellt AWS und nach erfolgreicher Erstellung regelmäßig ausgeführt. Sie können SYSTEM Assessments nicht löschen.

Verzeichnisbewertungen liefern wertvolle Informationen über die Eignung Ihrer Umgebung, darunter:

- Konnektivität zwischen Ihrem selbstverwalteten AD und AWS
- Verfügbarkeit der erforderlichen Dienste auf Ihren Domänencontrollern
- Konfigurationskompatibilität mit den Anforderungen des AWS Directory Service
- Mögliche Probleme, die eine erfolgreiche Erstellung eines Hybridverzeichnisses verhindern könnten

Bevor Sie ein Hybridverzeichnis erstellen können, ist eine erfolgreiche (bestandene) Verzeichnisbewertung erforderlich. Schlägt eine Bewertung fehl, können Sie sich den detaillierten Bericht ansehen, um die Probleme zu identifizieren und zu beheben, bevor Sie es erneut versuchen. AWS löscht SYSTEM Bewertungen nach 30 Tagen.

Themen

- [Verzeichnisbewertungen werden erstellt](#)
- [Verzeichnisbewertungen anzeigen](#)

- [Verzeichnisbewertungen werden gelöscht](#)

Verzeichnisbewertungen werden erstellt

Sie können eine Verzeichnisbewertung als Teil der Erstellung eines Hybridverzeichnisses oder manuell erstellen. Um eine Bewertung manuell zu erstellen, öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>. Wählen Sie auf der Seite Verzeichnisse im Abschnitt Verzeichnisbewertungen die Option Bewertung erstellen aus.

Um eine Verzeichnisbewertung zu erstellen

1. Geben Sie auf der Seite „Verzeichnisbewertung erstellen“ unter Verzeichnis-DNS-Name Ihren selbstverwalteten Active Directory-DNS-Namen ein.
2. Geben Sie für DNS-IP-Adressen zwei DNS-IP-Adressen für Ihr selbstverwaltetes AD ein.
3. Für das Hybrid-Verzeichnis ist eine Amazon-VPC mit mindestens zwei Subnetzen erforderlich. Wenn Sie diese noch nicht haben, können Sie sie erstellen. Geben Sie im Abschnitt Netzwerk Folgendes an:
 - a. Wählen Sie für VPC Ihre VPC-ID aus.
 - b. Wählen Sie für Subnetze den Bezeichner für jedes der beiden Subnetze aus. Jedes Subnetz muss sich in unterschiedlichen Availability Zones befinden. Weitere Informationen finden Sie unter [Amazon VPC-Netzwerkanforderungen](#).
 - c. Wählen Sie für Sicherheitsgruppe die Sicherheitsgruppen-ID aus. AWS Fügt standardmäßig eine Sicherheitsgruppe hinzu, um den Netzwerkzugriff auf die AWS Secrets Manager verwalteten Knoten in Ihrer Amazon VPC zu ermöglichen. Sie können optional Ihre eigene Sicherheitsgruppe angeben, die Netzwerkverkehr zu und von Ihren selbstverwalteten Domain-Controllern außerhalb Ihrer Amazon VPC ermöglicht.
4. Wählen Sie im Abschnitt AWS Systems Manager Knoten zwei Systems Manager Manager-Knoten oder -Instanzen aus, die den folgenden Anforderungen entsprechen:
 - Wenn Ihr Active Directory außerhalb von selbst verwaltet wird AWS Cloud, benötigen Sie zwei Systems Manager Manager-Knoten für eine Hybrid- und Multi-Cloud-Umgebung. Weitere Informationen zur Bereitstellung dieser Knoten finden Sie unter [Systems Manager für Hybrid- und Multicloud-Umgebungen einrichten](#).
 - Wenn Ihr Active Directory innerhalb von selbst verwaltet wird AWS Cloud, benötigen Sie zwei von Systems Manager verwaltete EC2 Instanzen. Weitere Informationen zur Bereitstellung dieser Instanzen finden Sie unter [EC2 Instanzen mit Systems Manager verwalten](#).

5. Wählen Sie Weiter, um die Seite mit der Verzeichnisbewertung überprüfen und erstellen zu öffnen.
6. Überprüfen Sie auf der Seite Verzeichnisbewertung überprüfen und erstellen die Informationen zur Verzeichnisbewertung und nehmen Sie die erforderlichen Änderungen vor. Wenn die Informationen korrekt sind, wählen Sie Bewertung erstellen aus. Das Erstellen der Verzeichnisbewertung dauert etwa 30 Minuten. Sie kehren zur Seite mit den Verzeichnisdetails zurück. Ein grünes Banner wird angezeigt, wenn die Verzeichnisbewertung erfolgreich ist.

 Warning

Um ein Hybridverzeichnis zu erstellen, muss die Verzeichnisbewertung den Status SUCCESS annehmen. Sie können kein Hybridverzeichnis erstellen, ohne zuvor eine Verzeichnisbewertung erfolgreich bestanden zu haben.

Verzeichnisbewertungen anzeigen

Sie können die Bewertungsverzeichnisse im einsehen AWS-Managementkonsole , um die Bewertungsergebnisse zu überprüfen und Ihre Bewertungsberichte zu verwalten.

Um eine Bewertung im Verzeichnis einzusehen

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie auf der Seite Verzeichnisse im Abschnitt Testversionen von Hybrid-Verzeichnisbewertungen die Bewertung aus, die Sie sich ansehen möchten. Dadurch wird die Seite mit den Bewertungsdetails geöffnet.
3. Auf der Seite mit den Bewertungsdetails können Sie Folgendes wählen:
 - Laden Sie den Bewertungsbericht für das Verzeichnis herunter, um ihn als CSV-Datei herunterzuladen.
 - Löschen, um den Bewertungsbericht für das Verzeichnis zu löschen.
 - Bewertung erstellen, um eine neue Verzeichnisbewertung zu erstellen.
4. Auf der Seite mit den Bewertungsdetails können Sie die folgenden Informationen einsehen:
 - a. Bewertungsinformationen, wie z. B. die Bewertungs-ID, der Status, ob sie vom Kunden oder vom System erstellt wurde und wann sie zuletzt aktualisiert wurde.

- b. Selbstverwaltete AD-Details wie DNS-Name, VPC und Subnetze.
- c. AWS Systems Manager verwaltete Knoteninformationen wie IP-Adresse, Bewertungsstatus und Anzahl der bestandenen und fehlgeschlagenen Bewertungstests.
- d. Bewertungsstatus für Domänencontroller. Sie können auch die Einzelheiten des Bewertungstests überprüfen, indem Sie die Domänencontroller auswählen. Fehlercodes für fehlgeschlagene Bewertungstests werden in der Spalte Status angezeigt.

Verzeichnisbewertungen werden gelöscht

Sie können von Kunden erstellte Verzeichnisbewertungen in der AWS-Managementkonsole löschen. Sie können vom System initiierte Bewertungen, die automatisch erstellt werden, AWS nicht löschen.

Um eine Bewertung aus dem Kundenverzeichnis zu löschen

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie auf der Seite Verzeichnisse im Abschnitt Verzeichnisbewertungen die Kundenbewertung aus, die Sie löschen möchten. Alternativ können Sie das Kontrollkästchen neben den Verzeichnisbewertungen, die Sie löschen möchten, aktivieren und dann im Menü Aktionen die Option Löschen auswählen.
3. Sie werden zur Seite mit den Bewertungsdetails weitergeleitet. Wählen Sie „Aktionen“ und anschließend „Bewertung löschen“. Das Dialogfeld „Verzeichnisbewertung löschen“ wird angezeigt. Wählen Sie Löschen aus.

Fehlerbehebung bei der Bewertung von Hybridverzeichnissen und Verzeichnissen

Um ein Hybridverzeichnis zu erstellen, ist eine Verzeichnisbewertung erforderlich. Bewertungstests werden auf jedem Domänencontroller ausgeführt. Die Bewertungstests untersuchen verschiedene Bereiche und führen zu dem Status „Bestanden“ oder „Fehlgeschlagen“. Wenn Ihre Verzeichnisbewertung fehlschlägt, können Sie sich die Bewertungstests Ihrer Domänencontroller ansehen, um festzustellen, welche Probleme den Fehler verursacht haben.

 Important

Ein Hybridverzeichnis kann erstellt werden, wenn der Status der Verzeichnisbewertung „Mit Warnung bestanden“ lautet. Wir empfehlen Ihnen, das Problem, das die Warnung verursacht hat, zu beheben, bevor Sie ein Hybridverzeichnis erstellen

Themen

- [Fehlerbehebung bei fehlgeschlagener Bewertung des Hybridverzeichnisses](#)
- [Fehler im Verzeichnisstatus](#)
- [Fehlermeldungen bei der Verzeichnisbewertung](#)
- [Fehlermeldungen beim Assessment Test](#)
- [Warnmeldungen für den Bewertungstest](#)

Fehlerbehebung bei fehlgeschlagener Bewertung des Hybridverzeichnisses

Sie können eine fehlgeschlagene Verzeichnisbewertung auf der Seite Verzeichnisse im beheben AWS-Managementkonsole.

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Abschnitt Verzeichnisbewertungen die fehlgeschlagene Hybrid-Verzeichnisbewertung aus.
3. Überprüfen Sie auf der Seite mit den Bewertungsdetails die Verzeichnisbewertung und ermitteln Sie, welche Tests fehlgeschlagen sind.
 - Die Bewertungstests des Domänencontrollers enthalten weitere Informationen darüber, welche Tests erfolgreich waren oder nicht. In der Spalte Status finden Sie weitere Informationen zur Ursache des fehlgeschlagenen Tests. Informationen zu den Bewertungstests Ihres Domänencontrollers finden Sie unter [Verzeichnisbewertungen anzeigen](#).
4. Beheben Sie die Probleme, die die Fehler in Ihrem selbstverwalteten Active Directory oder AWS Managed Microsoft AD verursacht haben. Weitere Informationen finden Sie unter [Fehlermeldungen bei der Verzeichnisbewertung](#) und [Fehlermeldungen beim Assessment Test](#).

5. Kehren Sie in der Directory Service Konsole zur fehlgeschlagenen Bewertung zurück. Wählen Sie in der roten Warnmeldung Bewertung erstellen aus. Weitere Informationen [Erstellen Sie ein Hybridverzeichnis mit Ihrem selbstverwalteten AD](#) zum Erstellen einer Verzeichnisbewertung finden Sie unter.

Fehler im Verzeichnisstatus

Directory Service Verzeichnisse können verschiedene Zustände aufweisen, die auf unterschiedliche Arten von Problemen hinweisen. Wenn Sie diese Zustände verstehen, können Sie die geeigneten Schritte zur Problembehandlung ermitteln.

Typen des Verzeichnisstatus

Status	Description	Maßnahme erforderlich
Aktiv	Die Verzeichniserstellung wurde erfolgreich abgeschlossen und funktioniert normal.	Es ist keine Aktion erforderlich.
Beeinträchtigt	Das Verzeichnis wurde erfolgreich erstellt, aber auf dem Domänencontroller traten danach Probleme auf. Das System versucht eine automatische Wiederherstellung.	Überwachen Sie den Verzeichnisstatus. Wenn das Problem weiterhin besteht, wenden Sie sich an den AWS Support.
Fehlgeschlagen	Die Verzeichniserstellung ist fehlgeschlagen und kann nicht wiederhergestellt werden.	Löschen Sie das fehlgeschlagene Verzeichnis und erstellen Sie ein neues.
Nicht funktionsfähig (nur Hybrid-AD)	AWS hat ein Sicherheitsproblem erkannt und das Verzeichnis zum Schutz automatisch isoliert. Das Verzeichnis wird vollständig unbrauchbar, bis es wiederhergestellt ist.	Wenden Sie sich sofort an AWS Support das Center . Dieser Status erfordert ein Support Eingreifen, um das Verzeichnis zu untersuchen und wiederherzustellen.

Fehlermeldungen bei der Verzeichnisbewertung

Um ein Hybridverzeichnis zu erstellen, müssen Sie die Verzeichnisbewertung bestanden haben. Verzeichnisbewertungen können aus verschiedenen Gründen fehlschlagen.

Die folgende Tabelle enthält Fehlermeldungen bei der Verzeichnisbewertung und zeigt, wie sie behoben werden können.

Fehlermeldungen und Lösungen bei der Verzeichnisbewertung

Fehlermeldung bei der Verzeichnisbewertung	Auflösung
Bei dieser Bewertung wurden mehrere Tests auf beiden verwalteten Instanzen nicht bestanden. Untersuchen Sie die fehlgeschlagenen Tests, indem Sie jede verwaltete Instanz auswählen und sie in Ihrem lokalen Verzeichnis lösen. Erstellen Sie anschließend eine neue Bewertung.	Einer oder mehrere Tests zur Verzeichnisbewertung sind für Ihr selbstverwaltetes AD fehlgeschlagen. Fehlermeldungen beim Assessment Test Weitere Informationen zu bestimmten Testfehlern und deren Behebung finden Sie unter.
Diese Bewertung ist aufgrund einer internen Serviceausnahme fehlgeschlagen. Bitte versuchen Sie es erneut, indem Sie eine neue Bewertung erstellen, oder wenden Sie sich zur Problembehandlung an den Service.	Versuchen Sie, eine neue Verzeichnisbewertung zu erstellen. Wenn dieser Fehler weiterhin auftritt, wenden Sie sich an Support.
Diese Bewertung schlug fehl, weil die Erlaubnis zum Ausführen einer Aktion wie <code>ec2:CreateSecurityGroup</code> <code>ec2:DeleteSecurityGroup</code> „<code>ec2:CreateNetworkInterface</code>“, <code>ec2:DeleteNetworkInterface</code> <code>ec2:DescribeSubnets</code> , und fehlte <code>ec2:DescribeNetworkInterface</code> .	Um eine Verzeichnisbewertung zu erstellen, AWS-Konto benötigen Sie die erforderlichen Informationen AWS-Konto Berechtigungen.
Diese Bewertung schlug fehl, weil die Erlaubnis zum Ausführen einer Aktion <code>iam:GetConnectionStatus</code> „	Um eine Verzeichnisbewertung zu erstellen , benötigen Sie zwei Systems Manager Manager-Knoten mit den erforderlichen Informationen AWS-Konto Berechtigungen.

Fehlermeldung bei der Verzeichnisbewertung	Auflösung
<code>ssm:GetCommandInvocation</code> <code>ssm:ListCommands</code> , fehlt <code>ssm:SendCommand</code> . Diese Bewertung ist fehlgeschlagen, da Sie das Limit für die Anzahl der Netzwerkschnittstellen, die Sie erstellen können, erreicht haben. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.	Um eine Verzeichnisbewertung zu erstellen , müssen Sie eine Netzwerkschnittstelle und Sicherheitsgruppen erstellen. Die Anzahl der VPC-Ressourcen, die Sie erstellen können, ist begrenzt, Sie können jedoch einige dieser Grenzwerte anpassen. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.
Diese Bewertung ist fehlgeschlagen, da Sie das Limit für die Anzahl der Sicherheitsgruppen, die Sie erstellen oder einer Instance zuweisen können, erreicht haben. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.	Um eine Verzeichnisbewertung zu erstellen , müssen Sie eine Netzwerkschnittstelle und Sicherheitsgruppen erstellen. Die Anzahl der VPC-Ressourcen, die Sie erstellen können, ist begrenzt, Sie können jedoch einige dieser Grenzwerte anpassen. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.
Diese Bewertung ist fehlgeschlagen. Es konnte keine Verbindung zu Kundeninstanzen von hergestellt AWS Systems Manager werden.	Um eine Verzeichnisbewertung zu erstellen , benötigen Sie zwei AWS Systems Manager Knoten, die den Status „Verbunden“ haben. Weitere Informationen finden Sie unter Problembehandlung beim SSM-Agenten.
Bei dieser Bewertung wurden mehrere kritische Tests nicht bestanden. Untersuchen Sie die fehlgeschlagenen Tests, indem Sie jede verwaltete Instanz auswählen und sie in Ihrem lokalen Verzeichnis beheben. Erstellen Sie anschließend eine neue Bewertung.	Einer oder mehrere Tests zur Verzeichnisbewertung sind für Ihr selbstverwaltetes AD fehlgeschlagen. Weitere Informationen Fehlermeldungen beim Assessment Test finden Sie in.

Fehlermeldungen beim Assessment Test

In der folgenden Tabelle werden Fehlermeldungen beschrieben, die bei Bewertungstests auftreten können. Diese Fehler weisen auf Blockierungsprobleme hin, die behoben werden müssen, bevor mit der Einrichtung des Hybridverzeichnisses fortgefahren werden kann.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Active Directory ServicesTests	testActiveDirectoryServices	AD_CRITICAL_SERVICES_NOT_RUNNING	Critical AD Services: [service_list] not running on hostname.	Tritt auf, wenn die erforderlichen AD Dienste in Ihrem selbstverwalteten AD nicht ausgeführt werden.	Bestimmte erforderliche AD Dienste müssen in Ihrem selbstverwalteten AD ausgeführt werden. Weitere Informationen finden Sie unter Erforderliche Active Directory-Dienste .
Active Directory ServicesTests	testActiveDirectoryServices	DOMAIN_CONTROLLER_NOT_FOUND	No domain controllers found for testActiveDirectoryServices.	Occurs if your self-managed AD domain controllers could not be both detected and queried during AD service validation.	Stellen Sie sicher, dass Ihre selbstverwalteten AD-Domänencontroller betriebsbereit und erreichbar sind. Überprüfen Sie die Netzwerkonnektivität und DNS Auflösung für Ihre selbstverwalteten AD-

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
					Domänencontroller.
ADTest der Kennwortrichtlinie	testPasswordPolicies	PASSWORD_POLICY_VIOLATIONS	<i>ErrorMessage</i>	Tritt auf, wenn Ihre selbstverwaltete AD-Passwortrichtlinie die Anforderungen von AWS Managed Microsoft AD nicht erfüllt.	Ihre selbstverwaltete AD-Passwortrichtlinie muss die Anforderungen für AWS verwaltete Microsoft AD-Passwörter erfüllen. Weitere Informationen finden Sie unter Grundlegendes zu AWS verwalteten Microsoft AD-Passwortrichtlinien .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Test „Admin-Benutzer vorhanden“	testAwsAdminUserExists	ADMINISTRATOR_ACCOUNT_MISSING	AWS Admin user not found or invalid.	Tritt auf, wenn der Hybrid-Verzeichnis-Administratorbenutzer in OU Ihrem selbstverwalteten AD nicht in AWS Reserved vorhanden ist.	Stellen Sie sicher, dass der Administratorbenutzer für das Hybridverzeichnis in Ihrem selbstverwalteten AWS AD OU unter Reserved vorhanden ist. Wenn der Benutzer fehlt, überprüfen Sie, ob das Konto bei der Einrichtung des Hybridverzeichnisses korrekt erstellt wurde. Ein Hybridverzeichnis aktualisieren . Wenn Ihr Hybrid-Verzeichnisstatus nicht funktionsfähig ist, wenden Sie sich an Support .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Admin-Benutzertest SPN	testNoSpnOnAwsAdminAccount	SPN_FOUND_ON_AWS_ADMIN	Found <i>spnCount</i> Service Principal Names (SPNs) set on AWS admin user <i>Username</i> . Please remove all SPNs from this account.	Tritt auf, wenn der Hybrid-Verzeichnis-Administratorbenutzer einen auf Ihrem selbstverwalteten AD SPNs konfiguriert hat.	Entfernen Sie alle Dienstprinzipalnamen (SPNs) aus dem Administratorkonto für das AWS Hybridverzeichnis. Für den Administratorbenutzer des Hybridverzeichnisses dürfen keine SPNs konfiguriert sein, da sie die Hybrid-Verzeichnisauthentifizierung beeinträchtigen können.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Test „Domänencontroller nicht FSMO Besitzer“	testAwsDomainControllerNotFSMOWriter	AWS_DC_HOLDS_FSMO_ROLE	AWS Domain Controller owns FSMO roles: <i>rolesList</i> . Please remove these roles.	Tritt auf, wenn Sie FSMO Rollen (PDC EmulatorRID Master, oderInfrastructure Master) von Ihrem selbstverwalteten AD auf den Hybridzeichnis-Domänencontroller übertragen haben.	Übertragen Sie alle FSMO Rollen (PDC Emulator, RID Master, Infrastructure Master) zurück auf Ihre selbstverwalteten AD-Domänencontroller, bevor Sie fortfahren. Weitere Informationen finden Sie in der Microsoft Dokumentation zur Übertragung von FSMO Rollen .
AWS Test der Mitgliedschaft in einer reservierten Gruppe	testValidateAwsReservedGroupMembership	AWS_RESERVED_OU_NOT_FOUND	AWS Reserved OU not found.	Tritt auf, wenn AWS Reserved OU auf Ihrem selbstverwalteten AD nicht vorhanden ist.	AWS Reserved OU muss in Ihrem selbstverwalteten AD vorhanden sein, um die Gruppenmitgliedschaft zu validieren. Wenden Sie sich an Support .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Test der reservierten Gruppenmitgliedschaft	testValidateAwsReservedGroupMembership	GROUP_MEMBERSHIP_MISMATCH	AWS Reserved OU Group [GroupNameA]: Missing User(s) [Object1], [Object2] and Extra user(s) [Object3].	Tritt auf, wenn Gruppen in der Gruppe AWS Reserved OU auf Ihrem selbstverwalteten AD nicht autorisierte Benutzer enthalten.	Entfernen Sie alle nicht autorisierten Benutzer aus den AWS reservierten OU Gruppen in Ihrem selbstverwalteten AD.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Reservierter Test OU ACLs	testReservedOuAclsPermissions	RESERVED_OU_NON_COMPLIANT_ACL	AWS Reserved OU ACLs permissions are invalid.	Tritt auf, wenn AWS Reserved OU ACLs auf Ihrem selbstverwalteten AD keine Leseberechtigungen für nicht verwaltete Entitäten erzwingen AWS und unbefugten Zugriff AWS auf Ressourcen nicht verhindern.	Überprüfen und korrigieren Sie die Berechtigungen für AWS Reserved OU ACLs auf Ihrem selbstverwalteten AD. Stellen Sie sicher, dass AWS Nicht-Entitäten nur über Leseberechtigungen (ListChildren, ReadProperty, ListObjectReadControl, Synchronize) verfügen GenericRead, und entfernen Sie alle übermäßigen Berechtigungen.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Test für reservierte OU GPO Verknüpfungen	testReservedOuGPOs	AWS_RESERVED_OU_NO_NN_RESERVED_OU_FOUNDED	Found non-AWS GPOs attached to the AWS Reserved OU: AWS Reserved OU (<i>count</i> unauthorized). Allowed GPOs: [<i>allowedAwsGpos</i>]. Domain Controllers OU (<i>count</i> unauthorized). Allowed GPOs: [<i>allowedDcGpos</i>]. Please, remove extra GPOs from the AWS Reserved OU.	Tritt auf, wenn die AWS reservierten Controller OU und die Domänencontroller OU auf Ihrem selbstverwalteten AD mit nicht autorisierten GPOs Verbindungen verknüpft sind.	(Nur AWS verwaltete Gruppenrichtlinienobjekte (GPOs) können mit diesen OUs verknüpft werden. Entfernen Sie alle nicht autorisierten GPOs Verbindungen zu den AWS reservierten Controllern OU und den Domänencontrollern OU auf Ihrem selbstverwalteten AD.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Test reservierter OU Ressourcen	testAwsReservedOUResources	AWS_RESERVED_OU_NOT_FOUND	The AWS Reserved OU does not exist. Please contact AWS Support.	Tritt auf, wenn AWS Reserved OU nicht in Ihrem selbstverwalteten AD vorhanden ist, was für die AWS verwaltete Microsoft AD-Verzeichnisfunktionalität erforderlich ist.	Das AWS Reserved OU muss bei der Einrichtung des Hybridverzeichnisses automatisch erstellt werden und sollte nicht gelöscht werden. Wenn dieser Fehler weiterhin besteht, wenden Sie sich an Support .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Test reservierter OU Ressourcen	testAwsReservedOUs	AWS_RESERVED_OUSOURCES_MISMATCH	The following required resources are missing from AWS Reserved OU - Objects: <i>missing objects</i> , GPOs: <i>missing GPOs</i> . The following resources should not exist but were found in AWS Reserved OU: Objects: <i>unexpected objects</i> , GPOs: <i>unexpected GPOs</i>	Tritt auf, wenn das AWS Reserved, das auf Ihrem selbstverwalteten AD OU erstellt wurde, nicht die erforderlichen Objekte enthält und GPOs das Hybridverzeichnis ordnungsgemäß funktioniert.	Stellen Sie sicher, dass niemand das AWS Reserved bearbeitet. OU Es muss die erforderlichen AWS verwalteten Ressourcen enthalten. Entfernen Sie alle nicht autorisierten Objekte oder kontaktieren Sie unsGPOs, Support falls benötigte Ressourcen fehlen.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
AWS Reservierter OU Test	testClean AwsReservedOU	AWS_RESERVED_RESOURCES_STILL_EXISTS	AWS Reserved OU or AWS Reserved GPO still exists, please delete.	Tritt auf, wenn AWS reservierte Ressourcen, die in Ihrem selbstverwalteten AD aus einem früheren Hybridverzeichnis-Setup gefunden wurden, noch vorhanden sind.	Löschen Sie das bestehende ausgefallene Hybridverzeichnis aus der Konsole. Löschen Sie anschließend alle AWS reservierten OU und verwandten Verzeichnisse GPOs aus Ihrem selbstverwalteten AD, bevor Sie fortfahren.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
BridgeheadTest zum Benennungskontext	testBridgeheadNamingContext	NAMING_CONTEXT_INCONSISTENT	<i>failureDetails</i>	Tritt auf, wenn die selbstverwaltete AD-Replikation zwischen Standorten unter Verwendung Bridgehead nicht wie erwartet funktioniert. Es kann auch auftreten, wenn die Namenskontexte nicht zwischen den Standorten synchronisiert sind.	Ihre selbstverwaltete bridgehead AD-Site muss erfolgreich sein. Sie können weitere Diagnosen stellen mit: <code>repadmin /bridgehead /verbose</code> . Gehen Sie auf die Probleme aus dieser Bewertung ein, bevor Sie fortfahren.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Domain-Test für Kinder	testChildDomain	CHILD_DOMAIN_NOT_SUPPORTED	Child Domains are not supported for Hybrid Directory.	Tritt auf, wenn Ihre selbstverwaltete AD-Gesamtstruktur untergeordnete Domänen enthält, die von AWS verwalteten Microsoft AD-Verzeichnissen nicht unterstützt werden.	AWS Verwalte Microsoft AD-Verzeichnisse unterstützen keine untergeordneten Domänen. Sie müssen eine Gesamtstruktur mit einer einzelnen Domäne für Ihr selbstverwaltetes AD verwenden. Weitere Informationen finden Sie unter Microsoft Active Directory Domain-Anforderungen .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
DcDiagTests	testDcDiag	DCDIAG_TEST_FAILED	DCDiag test failed due to issue from [formattedFailedTests].	Tritt auf, wenn Microsoft DCDiag Tests auf Ihrem selbstverwalteten AD fehlschlagen.	AWS verwendet DCDiag, um Ihr selbstverwaltetes AD zu testen. Wenn es Fehler gibt, können Sie kein Hybridverzeichnis erstellen. Weitere Informationen finden Sie in der Microsoft-Dokumentation .
DNSIP-Überprüfungstest	testDnsIpMatch	DNS_IP_MISMATCH	DNS IP address does not match expected IP addresses.	Tritt auf, wenn die angegebenen DNS IP-Adressen Ihres selbstverwalteten AD nicht mit den DNS IP-Adressen auf Ihren selbstverwalteten AD-Domänencontrollern übereinstimmen, die für aktiviert sind. AWS Systems Manager	Geben Sie die richtigen DNS IP-Adressen ein.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
DNSTest zur Namensübereinstimmung	testDnsNameMatch	DOMAIN_DNS_NAME_MISMATCH	DNS name does not match expected domain name.	Tritt auf, wenn der für Ihr selbstverwaltetes AD angegebene DNS Name nicht mit dem DNS Namen auf Ihren selbstverwalteten AD-Domänencontrollern übereinstimmt, die für aktiviert sind. AWS Systems Manager	Geben Sie den richtigen DNS Namen ein.
DNSAnzeigen, Test	testDnsRecords	DNS_RECORD_MISSING	Unable to resolve the following DNS queries: [<i>missingRecordsString</i>].	Tritt auf, wenn keine Windows DNS Datensätze für den TypA,NS, und festgelegt sindSOA, SRV und kann abgefragt werden.	Die DNS Datensätze für Address (A), Namespace (NS), State of Authority (SOA) und Service Record (SRV) müssen festgelegt sein und können abgefragt werden. Weitere Informationen finden Sie in der Microsoft-Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Test auf Funktions-ebene der Domänen- und Gesamtstruktur	testDomainForestFunctionalLevel	UNSUPPORTED_FUNCTIONAL_LEVEL	Detected unsupported domain functional level: <i>DomainFunctionalLevel</i> , we require minimum of <i>MinimumDomainMode</i> . Detected unsupported forest functional level: <i>ForestFunctionalLevel</i> , we require minimum of <i>MinimumForestMode</i> .	Tritt auf, wenn die Funktions-ebenen Ihrer selbstverwalteten AD-Domänen und -Gesamtstruktur die Mindestanforderungen nicht erfüllen.	Ihr selbstverwaltetes AD muss unsere Windows 2012 R2 2016 Funktionsebene verwenden. Weitere Informationen finden Sie in der Microsoft-Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Domain-Ge-sundheits-tests	testOnPremDcNumber	DC_NUMBER_BELOW_LIMIT	On-Prem DC count is lower than required number. DC count is <i>NumberOfDc</i> , AWS required number is <i>DcMinimum</i> .	Tritt auf, wenn Ihr selbstverwaltetes AD nicht über die erforderliche Mindestanzahl an Domänencontrollern verfügt.	Stellen Sie sicher, dass in Ihrem selbstverwalteten AD mindestens zwei Domänencontroller aktiviert sind. AWS Systems Manager Weitere Informationen finden Sie unter Microsoft Active Directory Domain-Anforderungen .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Bestehender Domänentest	testDomainAlreadyJoined	DOMAIN_ALREADY_JOINED	Instance is already joined to a domain.	Tritt auf, wenn Ihre selbstverwaltete AD-Domäne bereits mit einem vorhandenen Hybridverzeichnis verknüpft ist.	Ihre selbstverwaltete AD-Domäne ist bereits mit einem vorhandenen Hybridverzeichnis verknüpft. Jede selbstverwaltete AD-Domäne, die mit einem Hybridverzeichnis verknüpft ist, muss eindeutig sein. Erstellen Sie eine neue selbstverwaltete AD-Domäne oder entfernen Sie sie aus der Hybridverzeichniskonfiguration, mit der sie verknüpft sind.

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
FSMOKonnktivitätstest	testFsmoConnectivity	FSMO_ROLE_HOLDER_NOT_ROUTABLE	(PDCEmulator Ip: 1.1.1.1, RIDMaster Ip: 1.1.1.1) is not in routable ranges: [2.2.0.0/16, 3.3.0.0/16, 4.4.0.0/16, 5.5.0.0/16, 6.6.0.0/16].	Tritt auf, wenn FSMO RollenPDC Emulator,, and/or RID Master IPs auf Ihrem selbstverwalteten AD nicht routbar sind.	Der primäre Domänencontroller (PDC) muss jederzeit routingfähig sein. Insbesondere das Ende PDC Emulator RID Master IPs Ihres selbstverwalteten AD. Weitere Informationen finden Sie unter Microsoft Active Directory Domain-Anforderungen .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
FSMOKonnktivitätstest	testFsmConnectivity	FSMO_ROLE_MISSING	FSMO role(s): <i>[missingRolesString]</i> missing or DNS Record not found.	Tritt auf, wenn Ihre selbstverwalteten AD-Domänencontroller nicht auf Ihre FSMO Rollen zugreifen können.	Ihre Flexible Single Master Operation (FSMO) -Rolle in Ihrem selbstverwalteten AD muss mit Ihren selbstverwalteten AD-Domänencontrollern verbunden sein. Weitere Informationen finden Sie in der Microsoft-Dokumentation .
IP-Konflikttest	testIpConflict	IP_RANGE_CONFLICT	Conflicting IP address detected: <i>ipOverlaps</i>	Tritt auf, wenn sich Ihre selbstverwalteten AD-IP-Bereiche mit AWS reservierten Bereichen überschneiden.	Ihr selbstverwaltetes AD kann keinen IP-Adressbereich verwenden, der sich mit reservierten AWS IP-Bereichen überschneidet. Weitere Informationen finden Sie unter Microsoft Active Directory Domain-Anforderungen .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
KerberosTesten	testKerberos	KERBEROS_AUTHENTICATION_FAILED	Unable to get kerberos TGT.	Tritt auf, wenn Kerberos es nicht richtig konfiguriert ist und verwendet wird.	Kerberos muss auf Ihrem selbstverwalteten AD aktiviert sein. Weitere Informationen finden Sie in der Microsoft Dokumentation .
LDAPKonnektivitätstest	testLdapConnectivity	LDAP_TEST_FAILED	Unable to query LDAP with rootDSE call.	Tritt auf, wenn LDAP es nicht funktioniert.	Das Lightweight Directory Access Protocol (LDAP) muss aktiviert sein und auf Ihrem selbstverwalteten AD funktionieren. Weitere Informationen finden Sie in der Microsoft Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Nicht schreibgeschützter Domänencontroller für Tests FSMO	testNotReadOnlyForFsmo	FSMO_FOUNDED_ON_RODC	FSMO Role Found on RODC	Tritt auf, wenn Ihre selbstverwaltete FSMO AD-Domänencontroller-Rolle RODC	Der Domänencontroller für Ihr selbstverwaltetes AD darf nicht die Rolle eines schreibgeschützten Domänencontrollers (RODC) und des flexiblen Einzelmaschinbetriebes () verwenden. FSMO Weitere Informationen finden Sie in der Microsoft-Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Test zur Kennwortreplikation des Domänencontrollers mit Schreibschutz	testRdcPasswordReplication	RODC_REPLICATION_PASSWORD_DENIED	ReadOnly Domain Controller password replication is not explicitly denied for following groups: <i>[missingGroupsString]</i> .	Tritt auf, wenn der berechtigte RODC ist, Administratorkennwörter zu replizieren.	Dem RODC für Ihr selbstverwaltetes AD muss ausdrücklich die Berechtigung zum Replizieren von Admin-Passwörtern verweigert werden. Weitere Informationen finden Sie in der Microsoft-Dokumentation .
Domänencontroller-Test mit Schreibschutz	testIsDCROdc	DC_READONLY_MODE	Provided Domain Controller is set to Read-Only mode.	Tritt auf, wenn sich Ihre selbstverwalteten AD-Domänencontroller im ReadOnlyDC Modus befinden.	Bei Ihrem selbstverwalteten AD muss es sich um Domänencontroller mit Lese-/Schreibzugriff handeln. Weitere Informationen zu Domänencontrollertypen finden Sie in der Dokumentation . Microsoft

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Test der Remote-Port-Konnektivität	testPortConnectivity	PORT_TEST_FAILED	Connection to <i>TargetDestination</i> failed for TCP ports [<i>failed TCP ports</i>]. UDP ports [<i>failed UDP ports</i>].	Tritt auf, wenn die erforderlichen Ports in Ihrem AWS Subnetz und Ihr selbstverwalteter AD-Domänencontroller nicht geöffnet sind.	Stellen Sie sicher, dass alle erforderlichen Ports zwischen Ihrem AWS Subnetz und Ihrem selbstverwalteten AD geöffnet sind. Weitere Informationen finden Sie unter Anforderungen an Netzwerke .
Replikationstest	testReplication	REPLICATION_FAILED	Replication failed for [<i>failedDSASString</i>].	Tritt auf, wenn die Replikation Ihrer selbstverwalteten AD-Domänencontroller fehlgeschlagen ist.	Der Replikationsstatus Ihrer selbstverwalteten AD-Domänencontroller muss erfolgreich sein. Weitere Informationen finden Sie in der Microsoft-Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
SMBV1Testen	testSMBV1	INSECURE_SETTING_MB	SMBv1 is enabled on the system.	Tritt auf, wenn das selbstverwaltete AD derzeit SMBv1 für die Authentifizierung verwendet.	SMBv1 ist bekanntermaßen unsicher und muss auf Ihrem selbstverwalteten AD deaktiviert werden. Weitere Informationen finden Sie in der Microsoft-Dokumentation .
SSMTest der Benutzerberechtigungen	testSSMUserPermissions	INSUFFICIENT_PERMISSIONS	Systems Manager user does not have required elevated privileges.	Tritt auf, wenn der Windows Benutzer, der von verwendet wird, nicht SSM über ausreichende Rechte verfügt.	Sie benötigen Windows Administratorrechte für die AWS System Manager (SSM)-Agenten auf Ihrem selbstverwalteten AD. Weitere Informationen finden Sie unter AWS-Konto Berechtigungen .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
SysvolReplikationstest	testSysvolReplication	DFSR_FAILURE_DETECTED	Failed DFSR event logs: <i>failedLog sString</i> .	Tritt auf, wenn Ihr selbstverwaltetes AD nicht über die richtige sysvol Replikationsmethode (DFSR) verfügt und wenn eine Replikationsmethode während eines DFSR Replikationsereignisses DCs fehlgeschlagen ist.	Ihre selbstverwaltete sysvol AD-Replikationsmethode (DFSR) muss erfolgreich sein. Weitere Informationen finden Sie in der Microsoft-Dokumentation .
Test auf höchstem Niveau GPO	testTopLevelEnforcedGPO	TOP_LEVEL_ENFORCED_GPO_FOUND	GroupPolicy cannot be set to Enforced at the Domain Root, Found GPOs: [<i>GposEnforced</i>] set as Enforced.	Tritt auf, wenn für Ihr selbstverwaltetes AD die Option Top Level auf GPOs Durchgesetzt gesetzt ist.	Stellen Sie sicher, dass das Gruppenrichtlinienobjekt auf oberster Ebene für Ihre selbstverwaltete AD-Domäne (GPO) nicht auf Durchgesetzt gesetzt ist. Weitere Informationen finden Sie in der Microsoft-Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Vertrauenstypen testen	testTrustTypes	INVALID_TRUST_TYPE	Invalid trust types detected: [<i>InvalidTrustString</i>], only Uplevel (Microsoft AD) is currently supported.	Tritt auf, wenn Ihr selbstverwaltetes AD Vertrauensstypen nicht unterstützt.	Uplevel ist der einzige Vertrauensstyp, der vom Hybridverzeichnis unterstützt wird. Ihr selbstverwaltetes AD kann die folgenden Vertrauensstypen nicht haben: DCE, MIT, Downlevel. Weitere Informationen zu Vertrauensstypen finden Sie in der Microsoft Dokumentation .

Name des Tests	Kurzname	Fehlercode	Fehlermeldung	Description	Auflösung
Gültiger Domänencontrollertest	testValidDC	COMPUTER_NOT_DC	Provided instance is not a domain controller.	Tritt auf, wenn es sich bei den bereitgestellten selbstverwalteten AD-Instanzen nicht um Domänencontroller handelt oder wenn sie bereits Teil eines anderen Hybridverzeichnisses sind.	Stellen Sie selbstverwaltete AD-Domänencontroller bereit, die nur für dieses Hybridverzeichnis gelten. Versuchen Sie es erneut mit einem neuen Verzeichnis. Stellen Sie sicher, dass Sie das ausgefallene Hybridverzeichnis und alle Verzeichnisse AWS OU in Ihrem selbstverwalteten AD gelöscht haben.

Warnmeldungen für den Bewertungstest

In der folgenden Tabelle werden Warnmeldungen beschrieben, die bei Bewertungstests auftreten können. Diese Warnungen stellen Empfehlungen für eine optimale Konfiguration dar, verhindern jedoch nicht die Einrichtung eines Hybridverzeichnisses.

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
Domain-Ge-sundheits-tests	testDisabledStaleUserNumber	STALE_USERS_FOUND	<i>StaleUser Count</i> users were found to be stale, they have not logged in for <i>StaleThresholdInDays</i> days.	Tritt auf, wenn es in Ihrem selbstverwalteten AD Benutzerkonten gibt, die sich über einen längeren Zeitraum nicht angemeldet haben und als veraltet oder inaktiv angesehen werden können.	Bereinigen Sie veraltete Benutzerkonten.
Zeitquellentest für den Domänencontroller	testDCTimeSource	DC_BAD_TIME_SOURCE	Time sources not properly configured for PDC, should use an authoritative source. Time sources not properly configured for <i>dcHostName</i> , should use PDC as source	Tritt auf, wenn das selbstverwaltete AD über die richtige Zeitquellenkonfiguration verfügt und im Vergleich zu einer AWS Zeitquelle kein großes Zeitgefälle besteht.	Der Zeitserver Ihres primären Domänencontrollers (PDC) wird weitergeleitet. 169.254.169.123 Ihre nicht-primären Domänencontroller sollten auf den PDC als Quelle verweisen. Weitere Informationen finden Sie unter Keeping time

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
					with Amazon Time Sync Service.
Testen Sie den freien Speicherplatz	testFreeSpace	DISK_SPACE_EXCEEDED	Supported service max capacity of 7 GB exceeded; SysVol + NTDS is currently using: 24 GB)	Tritt auf, wenn Ihr selbst verwaltetes AD kombiniert NTDS und die Sysvol Nutzung das unterstützte Kontingent übersteigt.	Ihr selbstverwaltetes AD sollte über 24 GB Festplatte Speicher für Hybridverzeichnisse verfügen.

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
FSMO RolesTesten	testFSMORoles	FSMO_ROLE_TEST_FAILED	PDC Emulator (<i>dc1.example.com</i>) is not among the provided domain controllers. RID Master (<i>dc1.example.com</i>) is not among the provided domain controllers.	Tritt auf, wenn FSMO-Rollen (PDC-Emulator und RID-Master) nicht zu den beiden Domänencontrollern gehören, die beim Erstellen eines Hybridverzeichnisses bereitgestellt werden.	Ihr Hybridverzeichnis sollte unter den beiden Domänencontrollern, die Sie beim Erstellen eines Hybridverzeichnisses angeben, über beide FSMO-Rollen (PDC-Emulator und RID-Master) verfügen. Weitere Informationen finden Sie unter So zeigen Sie Rollen an und übertragen sie . FSMO
SSPS-Kanal-Test	testSchannelSSP	TLS_1_2_NOT_ENABLED	Disabled protocol <i>DisabledProtocol</i> is still enabled.	Tritt auf, wenn ein selbstverwaltetes AD keine AES256 Verschlüsselung verwendet TLS1.2.	Ihr selbstverwaltetes AD muss TLS 1.2 und AES256 für Hybridverzeichnisse verwenden.
Test auf Festplattenbeschädigung	testDiskCorruption	DISK_CORRUPTION	Disk corruption detected on <i>Drive</i> .	Tritt auf, wenn in Ihrem selbstverwalteten AD ein Festplattenfehler vorliegt.	Ihre selbstverwalteten AD-Festplatten sollten nicht beschädigt sein.

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
Test der Spezifikationen für den Domänencontroller	testDcSpecs	INSUFFICIENT_RESOURCES	<i>numAvailableCores</i> detected when <i>requiredCores</i> cores recommended. <i>gbAvailableRam</i> GB ram detected when <i>requiredRam</i> GB recommended.	Tritt auf, wenn Ihre selbstverwalteten AD-Domänencontroller die erforderlichen Spezifikationen nicht erfüllen.	Ihre selbstverwalteten AD-Domänencontroller sollten über mindestens 7 GB RAM und 2 CPU-Kerne für das Hybridverzeichnis verfügen.
DllPlugin-Test auf Serverebene	testServerLevelPluginDll	SERVER_LEVEL_PLUGIN_DLL_IS_NOT_SET	ServerLevelPluginDll registry configuration is not permitted.	Tritt auf, wenn ServerLevelPluginDll es auf Ihren selbstverwalteten AD-Domänencontrollern eingerichtet ist.	Ihre selbstverwalteten AD-Domänencontroller sollten nicht konfiguriert worden ServerLevelPluginDll sein.

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
NT4Crypto-Test zulassen	testAllowNT4Crypto	NT4_CRYPT0_NOT_ALLOWED	Registry key AllowNt4Crypto is not allowed.	Tritt auf, wenn selbstverwaltetes AD NT4 Kryptografie zulässt.	Ihr selbstverwaltetes AD sollte Kryptografie nicht verwenden. Weitere Informationen finden Sie in der Microsoft-Dokumentation.
Test für verwaiste Admin-Benutzer	testOrphanedAdminUsers	ORPHANED_ADMIN_USER_FOUND	<i>OrphanedUsersCount</i> Orphaned Admin Users Found: [<i>OrphanedUserNames</i>].	Tritt auf, wenn es in Ihrem selbstverwalteten AD verwaiste Admin-Benutzer gibt.	Entfernen Sie verwaiste Benutzer in Ihrem selbstverwalteten AD, bevor Sie fortfahren.
Test der Anzahl privilegierter Benutzer	testPrivilegedUserCount	DOMAIN_ADMIN_COUNT_EXCEEDED	Number of Domain Admins (<i>daCount</i>) exceeded allowance of (<i>allowedDomainAdminCount</i>).	Wird durchgeführt, wenn die Gesamtzahl Ihrer integrierten Administratoren, Domänenadministratoren und Unternehmensadministratoren in Ihrem selbstverwalteten AD mehr als 5 beträgt.	Ihre selbstverwaltete AD-Umgebung sollte nicht über mehrere privilegierte Konten verfügen. Bevor Sie fortfahren, sollten Sie zu viele Administratorkonten entfernen.

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
Test der Anzahl privilegierter Benutzer	testPrivilegedUserCount	ENTERPRISE_ADMIN_COUNT_EXCEEDED	Number of Enterprise Admins (<i>eaCount</i>) exceeded allowance of (<i>allowedEnterpriseAdminCount</i>).	Wird durchgeführt, wenn die Gesamtzahl Ihrer integrierten Administratoren, Domänenadministratoren und Unternehmensadministratoren in Ihrem selbstverwalteten AD a mehr als 5 beträgt.	Ihre selbstverwaltete AD-Umgebung sollte nicht über mehrere privilegierte Konten verfügen. Bevor Sie fortfahren, sollten Sie zu viele Administratorkonten entfernen.
Test der Anzahl privilegierter Benutzer	testPrivilegedUserCount	BUILTIN_ADMIN_COUNT_EXCEEDED	Number of Built-in Admins (<i>baCount</i>) exceeded allowance of (<i>allowedAdminCount</i>).	Wird durchgeführt, wenn die Gesamtzahl Ihrer integrierten Administratoren, Domänenadministratoren und Unternehmensadministratoren in Ihrem selbstverwalteten AD a mehr als 5 beträgt.	Ihre selbstverwaltete AD-Umgebung sollte nicht über mehrere privilegierte Konten verfügen. Bevor Sie fortfahren, sollten Sie zu viele Administratorkonten entfernen.

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
NTLMTesten	testNTLM	INSECURE_SETTING_NTLM	NTLMv1 is enabled.	Tritt auf, wenn die Authentifizierung auf Ihrem selbstverwalteten AD aktiviert NTLMv1 ist.	NT LAN Manager Version 1 (NTLMv1) weist bekannte Sicherheitslücken auf und sollte nicht verwendet werden. Deaktivieren Sie es NTLMv1 auf Ihrem selbstverwalteten AD. Weitere Informationen finden Sie in der Microsoft-Dokumentation .

Name des Tests	Kurzname	Warnungscode	Warnmeldung	Description	Auflösung
Tombstone Lifetime-Test	testTombstoneLifetime	TOMBSTONE_LIFETIME_ABOVE_LIMIT	Tombstone Lifetime is too long. DC Tombstone Lifetime is <i>Tombstone LifeTime</i> , AWS suggested number is <i>Tombstone Maximum</i> days.	Tritt auf, wenn die Tombstone-Lebensdauer auf Ihrem selbstverwalteten AD mehr als 180 Tage beträgt.	Die Tombstone-Lebensdauer ist die Anzahl der Tage, bevor ein gelöschttes Objekt entfernt wird. AD Der Tombstone-Lebenszeitwert für Ihr selbstverwaltetes AD sollte 180 Tage oder weniger betragen. Weitere Informationen finden Sie in der Microsoft-Dokumentation .

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, 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 [Bereitstellung zusätzlicher Domänencontroller für Ihr AWS verwaltetes Microsoft AD](#).

Eine Demo und einen Überblick über AWS Managed Microsoft AD finden Sie im folgenden YouTube Video.

AWS Managed Microsoft AD Demo und Überblick

Themen

- [Voraussetzungen für die Erstellung eines AWS verwalteten Microsoft AD](#)
- [AWS IAM Identity Center Voraussetzungen](#)
- [Voraussetzungen für Multifaktor-Authentifizierung](#)
- [Ihr AWS verwaltetes Microsoft AD erstellen](#)
- [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#)
- [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#)

Voraussetzungen für die Erstellung eines AWS verwalteten Microsoft AD

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

- Mindestens zwei Subnetze. Jedes der Subnetze muss sich in einer anderen Availability Zone befinden und denselben Netzwerktyp haben.

Sie können es IPv6 für Ihre VPC verwenden. Weitere Informationen finden Sie unter [IPv6 Support für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

- 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.

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 Verwaltungs-IP-Bereich des ETH0 Netzwerks Ihres Verzeichnisses ist 198.18.0.0/15.

Ein Tutorial zum Erstellen der AWS Umgebung und von AWS Managed Microsoft AD finden Sie unter [AWS Tutorials für verwaltete Microsoft AD-Testlabore](#).

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 Managed 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 repräsentieren AWS. 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 dar DCs , die von verwendet werden AWS.

Note

Wenn Ihr RADIUS-Server DNS-Adressen unterstützt, müssen Sie nur eine RADIUS-Client-Konfiguration erstellen. Andernfalls müssen Sie für jedes AWS verwaltete Microsoft AD DC eine RADIUS-Clientkonfiguration 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 dem AWS Managed Microsoft AD DCs und dem RADIUS-Server konfigurieren. Die unterstützten Protokolle sind PAP, CHAP MS- und MS CHAPv1 -. CHAPv2 MS- CHAPv2 wird empfohlen, da es die stärkste 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 (AWS verwaltete Microsoft DCs AD-DNS-Adressen, 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 unter [Aktivierung der Multi-Faktor-Authentifizierung für AWS Managed Microsoft AD](#).

Ihr AWS verwaltetes Microsoft AD erstellen

Gehen Sie wie folgt vor, um ein neues AWS verwaltetes Microsoft AD Active Directory zu erstellen. Bevor Sie dieses Verfahren beginnen, stellen Sie sicher, dass Sie die in [Voraussetzungen für die Erstellung eines AWS verwalteten Microsoft AD](#) angegebenen Voraussetzungen erfüllt haben.

So erstellen Sie ein AWS verwaltetes Microsoft AD

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. Diese Beschreibung kann nach der Erstellung Ihres AWS Managed Microsoft AD geändert werden.

Administratorpasswort

Das Passwort für den Verzeichnisadministrator. Mit der Verzeichniserstellung wird ein Administratorkonto mit dem Benutzernamen Admin und diesem Passwort angelegt. Sie können das Admin-Passwort ändern, nachdem Sie Ihr AWS Managed Microsoft AD erstellt haben.

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.

(Optional) Benutzer- und Gruppenverwaltung

Um die AWS verwaltete Microsoft AD-Benutzer- und Gruppenverwaltung von zu aktivieren AWS-Managementkonsole, wählen Sie Benutzer- und Gruppenverwaltung verwalten in der AWS-Managementkonsole. Weitere Informationen zur Verwendung der Benutzer- und Gruppenverwaltung finden Sie unter [the section called “Verwalten Sie Benutzer und Gruppen mit der Konsole, CLI oder PowerShell”](#).

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

Wählen Sie die VPC für das Verzeichnis aus.

Netzwerktyp

Das Internet Protocol (IP) -Adressierungssystem, das mit Ihrer VPC und Ihren Subnetzen verknüpft ist.

Wählen Sie den CIDR-Block aus, der Ihrer vorhandenen VPC zugeordnet ist. Ressourcen in Ihrem Subnetz können so konfiguriert werden, dass sie IPv4 nur, IPv6 nur oder beides verwenden IPv6 (IPv4 Dual-Stack). Weitere Informationen finden Sie unter [Compare IPv4 und IPv6](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Subnets

Wählen Sie die 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.

Weitere Informationen darüber, was mit Ihrem AWS Managed Microsoft AD erstellt wird, finden Sie im Folgenden:

- [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#)
- [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#)

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 Directory Service](#)
- [So erhöhen Sie die Redundanz und Leistung Ihres 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-Managementkonsole 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](#)

Was wird mit Ihrem AWS Managed Microsoft AD erstellt

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

- Erstellt automatisch eine Elastic-Netzwerk-Schnittstelle (ENI) und ordnet sie jedem Ihrer Domain-Controller zu. Jedes dieser Elemente ist für ENIs die Konnektivität zwischen Ihrer VPC und den Directory Service Domänencontrollern unerlässlich und sollte niemals gelöscht werden. Sie können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, 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 des AWS verwalteten 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 [Bereitstellung zusätzlicher Domänencontroller für Ihr AWS verwaltetes Microsoft AD](#).

 Note

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

- Erstellt eine [AWS Sicherheitsgruppe](#) `sg-1234567890abcdef0`, die Netzwerkregeln für den Verkehr zu und von Ihren Domänencontrollern festlegt. Die Standardregel für ausgehenden Datenverkehr lässt den gesamten Datenverkehr zu allen IPv4 Adressen zu. Die Standardregeln für eingehenden Datenverkehr lassen nur Datenverkehr über Ports zu, die für Active Directory aus dem primären IPv4 CIDR-Block erforderlich sind, der dem VPC-Hosting für Ihr AWS verwaltetes Microsoft AD zugeordnet ist. Um zusätzliche Sicherheit zu gewährleisten, sind ENIs die erstellten Dateien nicht mit Elastic IPs verknüpft und Sie sind nicht berechtigt, ihnen eine Elastic IP zuzuweisen. ENIs Daher ist der einzige eingehende Datenverkehr, der mit Ihrem AWS verwaltetes Microsoft AD kommunizieren kann, standardmäßig die lokale VPC. Sie können die Sicherheitsgruppenregeln ändern, um zusätzliche Datenverkehrsquellen zuzulassen, z. B. von anderen Datenverkehrsquellen, die über VPN CIDRs erreichbar sind VPCs oder über VPN erreichbar sind. Seien Sie äußerst vorsichtig, wenn Sie versuchen, diese Regeln zu ändern, da Sie die Fähigkeit zur Kommunikation mit Ihren Domain-Controllern beeinträchtigen können.

Weitere Informationen erhalten Sie unter [AWS Bewährte Methoden für verwaltetes Microsoft AD](#) und [Verbesserung Ihrer AWS Managed Microsoft AD-Netzwerksicherheitskonfiguration](#).

Sie können [Präfixlisten](#) verwenden, um Ihre CIDR-Blöcke innerhalb der Sicherheitsgruppenregeln zu verwalten. Präfixlisten erleichtern die Verwaltung und Konfiguration von Sicherheitsgruppen und Routing-Tabellen. Sie können mehrere CIDR-Blöcke mit demselben Port und denselben Protokollen konsolidieren, um Ihren Netzwerkverkehr zu skalieren.

- In einer Windows Umgebung kommunizieren Clients häufig über [Server Message Block \(SMB\)](#) oder Port 445. Dieses Protokoll ermöglicht verschiedene Aktionen wie die gemeinsame Nutzung von Dateien und Druckern und die allgemeine Netzwerkkommunikation. Sie sehen den Client-Verkehr auf Port 445 zu den Verwaltungsschnittstellen Ihrer AWS verwalteten Microsoft AD-Domänencontroller.

Dieser Datenverkehr tritt auf, da SMB-Clients auf die DNS- (Port 53) und NetBIOS-Namensauflösung (Port 138) angewiesen sind, um Ihre AWS verwalteten Microsoft AD-Domänenressourcen zu finden. Diese Clients werden bei der Suche nach Domänenressourcen an jede verfügbare Schnittstelle auf den Domänencontrollern weitergeleitet. Dieses Verhalten wird erwartet und tritt häufig in Umgebungen mit mehreren Netzwerkadaptern auf, in denen [SMB Multichannel](#) es Clients ermöglicht, Verbindungen über verschiedene Schnittstellen herzustellen, um die Leistung und Redundanz zu verbessern.

Die folgenden AWS Sicherheitsgruppenregeln werden standardmäßig erstellt:

Regeln für eingehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp	Verwendung von Active Directory
ICMP	–	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	Ping	LDAP Keep Alive, DFS

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP und UDP	53	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauensstellungen
TCP und UDP	88	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauensstellungen auf Gesamtstrukturebene
TCP und UDP	389	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
TCP und UDP	445	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	SMB/CIFS	Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP und UDP	464	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	Kerberos Passwort ändern/ei nrichten	Replikation, Benutzer- und Computera uthentifizierung, Vertrauen sstellungen
TCP	135	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	Replikation	RPC, EPM
TCP	636	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	1024 - 65535	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	RPC	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	3268 - 3269	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauensstellungen
UDP	123	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	Windows-Uhrzeit	Windows-Uhrzeit, Vertrauensstellungen
UDP	138	AWS Verwaltetes Microsoft AD VPC CIDR IPv4	DFSN und NetLogon	DFS, Gruppenrichtlinie
Alle	Alle	AWS hat eine Sicherheitsgruppe für Domänencontroller erstellt (<i>sg-1234567890abcdef0</i>)	Gesamter Datenverkehr	

Regeln für ausgehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Ziel	Datenverkehrstyp	Verwendung von Active Directory
Alle	Alle	0.0.0.0/0	Gesamter Datenverkehr	

- Weitere Informationen zu den von Active Directory verwendeten Ports und Protokollen finden Sie in der Microsoft Dokumentation unter [Dienstübersicht und Netzwerkportanforderungen für Windows](#).
- Erstellt ein Verzeichnisadministratorkonto mit dem Benutzernamen Admin und dem angegebenen Passwort. Dieses Konto befindet sich unter Users OU (z. B. Unternehmen > Benutzer). Sie verwenden dieses Konto, um Ihr Verzeichnis in der zu verwalten AWS Cloud. Weitere Informationen finden Sie unter [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#).

 Important

Achten Sie darauf, dieses Passwort zu speichern. Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen werden. Sie können ein Passwort jedoch über die Directory Service Konsole oder mithilfe der [ResetUserPassword](#) API zurücksetzen.

- Erstellt die folgenden drei Organisationseinheiten (OUs) unter dem Domänenstamm:

Name der Organisationseinheit	Description
AWS Delegated Groups	Speichert alle Gruppen, die Sie verwenden können, um AWS bestimmte Berechtigungen an Ihre Benutzer zu delegieren.
AWS Reserved	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-

Name der Organisationseinheit	Description
	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. In dieser Organisationseinheit OUs gibt es standardmäßig zwei untergeordnete Elemente: Computer und Benutzer. Beispiel: • Corp • Computers (Computer) • Benutzer

- Erstellt die folgenden Gruppen in AWS Delegated Groups OU:

Gruppenname	Description
AWS Delegated Account Operators	Mitglieder dieser Sicherheitsgruppe verfügen über begrenzte Funktionen zur Kontoverwaltung, wie beispielsweise das Zurücksetzen von Passwörtern
AWS Delegated Active Directory Based Activation Administrators	Mitglieder dieser Sicherheitsgruppe können Active-Directory-Volumenlizenzaktivierungsobjekte erstellen, die es Unternehmen ermöglichen, Computer über eine Verbindung zu ihrer Domain zu aktivieren.
AWS Delegated Add Workstations To Domain Users	Mitglieder dieser Sicherheitsgruppe können einer Domain 10 Computer hinzufügen.
AWS Delegated Administrators	Mitglieder dieser Sicherheitsgruppe können AWS Managed Microsoft AD verwalten, haben volle Kontrolle über alle Objekte in Ihrer Organisationseinheit und können Gruppen

Gruppenname	Description
	verwalten, die in der enthalten sindAWS D elegated Groups OU.
AWS Delegated Allowed to Authenticate Objects	Mitglieder dieser Sicherheitsgruppe haben die Möglichkeit, sich bei Computerressourcen in der zu authentifizieren AWS Reserved OU (wird nur für lokale Objekte mit aktivierter selektiver Authentifizierung benötigt).
AWS Delegated Allowed to Authenticate to Domain Controllers	Mitgliedern dieser Sicherheitsgruppe wird die Möglichkeit gegeben, sich bei Computerr essourcen in der zu authentifizieren Domain Controllers OU (wird nur für lokale Objekte mit aktivierter selektiver Authentifizierung benötigt).
AWS Delegated Deleted Object Lifetime Administrators	Mitglieder dieser Sicherheitsgruppe können das msDS-DeletedObjectLifetime Objekt ändern, wodurch festgelegt wird, wie lange ein gelöshtes Objekt für die Wiederherstellung aus dem AD-Papierkorb verfügbar ist.
AWS Delegated Distributed File System Administrators	Mitglieder dieser Sicherheitsgruppe können FRS-, DFS-R- und DFS-Namensräume hinzufügen.
AWS Delegated Domain Name System Administrators	Mitglieder dieser Sicherheitsgruppe können das in Active-Directory-integrierte DNS verwalten.
AWS Delegated Dynamic Host Configuration Protocol Administrators	Mitglieder dieser Sicherheitsgruppe können Windows DHCP-Servern im Unternehmen autorisieren.
AWS Delegated Enterprise Certificate Authority Administrators	Mitglieder dieser Sicherheitsgruppe können die Microsoft Enterprise Certificate Authority- Infrastruktur bereitstellen und verwalten.

Gruppenname	Description
AWS Delegated Fine Grained Password Policy Administrators	Mitglieder dieser Sicherheitsgruppe können vorab festgelegte differenzierte Passwortrichtlinien abändern.
AWS Delegated FSx Administrators	Mitglieder dieser Sicherheitsgruppe erhalten die Möglichkeit, FSx Amazon-Ressourcen zu verwalten.
AWS Delegated Group Policy Administrators	Mitglieder dieser Sicherheitsgruppe können Verwaltungsaufgaben für Gruppenrichtlinien durchführen (erstellen, bearbeiten, löschen, verlinken).
AWS Delegated Kerberos Delegation Administrators	Mitglieder dieser Sicherheitsgruppe können eine Delegation auf Computer- und Benutzerkontenobjekten aktivieren.
AWS Delegated Managed Service Account Administrators	Mitglieder dieser Sicherheitsgruppe können Managed Service-Konten erstellen und löschen.
AWS Delegated MS-NPRC Non-Compliant Devices	Mitglieder dieser Sicherheitsgruppe werden von der Anforderung einer Secure Channel Kommunikation mit Domain-Controllern ausgenommen. Diese Gruppe ist für Computerkonten vorgesehen.
AWS Delegated Remote Access Service Administrators	Mitglieder dieser Sicherheitsgruppe können RAS-Server aus der Gruppe der RAS- und IAS-Server hinzufügen und entfernen.
AWS Delegated Replicate Directory Changes Administrators	Mitglieder dieser Sicherheitsgruppe können Profilinformationen in Active Directory mit dem SharePoint Server synchronisieren.

Gruppenname	Description
AWS Delegated Server Administrators	Mitglieder dieser Sicherheitsgruppe sind in der lokalen Administratorgruppe auf allen mit der Domain verknüpften Computern enthalten.
AWS Delegated Sites and Services Administrators	Mitglieder dieser Sicherheitsgruppe können das Default-First-Site-Name Objekt in Active Directory-Standorten und -Diensten umbenennen.
AWS Delegated System Management Administrators	Mitglieder dieser Sicherheitsgruppe können Objekte im Systemverwaltungscontainer erstellen und verwalten.
AWS Delegated Terminal Server Licensing Administrators	Mitglieder dieser Sicherheitsgruppe können der Terminal Server License Servers-Gruppe Terminal Server License Server hinzufügen und sie daraus entfernen.
AWS Delegated User Principal Name Suffix Administrators	Mitglieder dieser Sicherheitsgruppe können Suffixe für den Benutzer-Prinzipalnamen hinzufügen und entfernen.

 Note

Sie können diese hinzufügenAWS Delegated Groups.

- 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 AWS Verwendung vorbehalten sind. Sie können sie bei Bedarf mit OUs denen verknüpfen, die Sie kontrollieren.

Gruppenrichtliniennamen	Gilt für	Description
Default Domain Policy	Domain	Beinhaltet Domainpasswort und Kerberos-Richtlinien.
ServerAdmins	Alle Computerkonten, die keine Domain-Controller sind	Fügt den 'AWS Delegated Server Administrators' als Mitglied der hinzuBUILTIN Administrators Group.
AWS Reserved Policy:User	AWS Reserved user accounts	Legt die empfohlenen Sicherheitseinstellungen für alle Benutzerkonten in der festAWS Reserved OU.
AWS Managed Active Directory Policy	Alle Domain-Controller	Legt die empfohlenen Sicherheitseinstellungen auf allen Domain-Controllern fest.
TimePolicyNT5DS	Alle PDCe Nicht-Domänencontroller	Legt die Zeitrichtlinie für alle PDCe Nicht-Domänencontroller fest, dass sie Windows Time (NT5DS) verwenden.
TimePolicyPDC	Der PDCe Domänencontroller	Legt die Zeitrichtlinie des PDCe Domänencontrollers auf die Verwendung des Network Time Protocol (NTP) fest.
Default Domain Controllers Policy	Nicht verwendet	Die AWS verwaltete Active Directory-Richtlinie, die während der Domänenereinstellung bereitgestellt wird, wird stattdessen verwendet.

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

- Erstellt Folgendes default local accounts für das AWS verwaltete Microsoft AD-Management:

 Important

Achten Sie darauf, das Admin-Passwort zu speichern. Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen werden. Sie [können ein Passwort jedoch über die Directory Service Konsole](#) oder mithilfe der [ResetUserPasswordAPI](#) zurücksetzen.

Admin

Das Admin wird directory administrator account erstellt, wenn das AWS verwaltete Microsoft AD zum ersten Mal erstellt wird. Sie geben ein Passwort für dieses Konto an, wenn Sie ein AWS verwaltetes Microsoft AD erstellen. Dieses Konto befindet sich unter Users OU (z. B. Unternehmen > Benutzer). Sie verwenden dieses Konto, um Ihr Active Directory im zu verwalten AWS. Weitere Informationen finden Sie unter [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#).

AWS_**111111111111**

Jeder Kontoname, der mit einem AWS gefolgt von einem Unterstrich beginnt und sich in befindet, AWS Reserved OU ist ein vom Dienst verwaltetes Konto. Dieses vom Dienst verwaltete Konto wird von für AWS die Interaktion mit dem Active Directory verwendet. Diese Konten werden erstellt, wenn AWS Directory Service Data aktiviert ist und wenn jede neue AWS Anwendung in Active Directory autorisiert wird. Auf diese Konten können nur AWS Dienste zugreifen.

krbtgt account

Das krbtgt account spielt eine wichtige Rolle bei den Kerberos-Ticketbörsen, die von Ihrem AWS Managed Microsoft AD verwendet werden. Das krbtgt account ist ein spezielles Konto, das für die Kerberos-Ticket-Granting-Ticket-Verschlüsselung (TGT) verwendet wird und eine entscheidende Rolle für die Sicherheit des Kerberos-Authentifizierungsprotokolls spielt. Weitere Informationen finden Sie in der [Microsoft-Dokumentation](#).

AWS wechselt das krbtgt account Passwort für Ihr AWS verwaltetes Microsoft AD automatisch zweimal alle 90 Tage. Zwischen den beiden aufeinanderfolgenden Rotationen liegt alle 90 Tage eine Wartezeit von 24 Stunden.

Weitere Informationen zum Administratorkonto und anderen von Active Directory erstellten Konten finden Sie in der [MicrosoftDokumentation](#).

AWS Veraltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen

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 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 Gruppenverwaltung in AWS Managed Microsoft AD](#).
- Hinzufügen von Ressourcen zu Ihrer Domain, etwa Datei- oder Druckserver, und anschließendes Gewähren der zugehörigen Ressourcenberechtigungen für Benutzer und Gruppen in der OU.
- Erstellen Sie zusätzliche OUs Container.
- Delegieren Sie die Autorität für zusätzliche Container OUs und Container. Weitere Informationen finden Sie unter [Delegieren von Verzeichnisbeitrittsberechtigungen für AWS Managed Microsoft AD](#).
- Erstellen und Verknüpfen von Gruppenrichtlinien.
- Wiederherstellen von gelöschten Objekten aus dem Active Directory-Papierkorb.
- Führen Sie Active Directory- und 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 Sicherheitereignisprotokollen

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.

Überlegungen

- 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](#).
- 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.

Note

AWS hat die ausschließliche Kontrolle über die privilegierten Benutzer und Gruppen des Domänenadministrators und des Unternehmensadministrators. Dies ermöglicht AWS die operative Verwaltung Ihres Verzeichnisses.

Privilegierte Enterprise- und Domainadministrator-Konten

AWS wechselt das integrierte Administratorkennwort automatisch alle 90 Tage zu einem zufälligen Passwort. Jedes Mal, wenn das integrierte Administratorkennwort für den menschlichen Gebrauch angefordert wird, wird ein AWS Ticket erstellt und beim Directory Service Team protokolliert. Die Kontoanmeldeinformationen werden verschlüsselt und über sichere Kanäle verwaltet. Außerdem können die Anmeldeinformationen für das Administratorkonto nur vom 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 request/notification System zur Gewährung des Zugriffs. 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 [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#).

Die IDs Sicherheitsereignisse 4624, 4672 und 4648 werden alle protokolliert, wenn sich jemand interaktiv an einem DC anmeldet. Sie können das Windows-Sicherheitsereignisprotokoll jedes DCs mit der Event Viewer Microsoft Management Console (MMC) von einem Windows-Computer aus anzeigen, der einer Domäne angehört. Sie können auch [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#) alle Sicherheitsereignisprotokolle an die CloudWatch Protokolle 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 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 DCs zur Fehlerbehebung interaktiver Zugriff auf die erforderlich ist, wird außerdem ein temporäres Benutzerkonto erstellt, das ein Directory Service Techniker verwenden kann. 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 Directory Service Managementteam benachrichtigt wird.

Wichtige Konzepte und bewährte Methoden für AWS Managed Microsoft AD

Sie können mehr aus Ihrem AWS Managed Microsoft AD herausholen, indem Sie sich mit den wichtigsten Konzepten und bewährten Methoden vertraut machen. Die wichtigsten Konzepte helfen Ihnen zu verstehen, wie AWS Managed Microsoft AD funktioniert. Zu den wichtigsten Konzepten gehören weitere Informationen zum Active Directory-Schema, zum Patching-Zeitplan und zu Group Managed Service Accounts. Das Active Directory-Schema umfasst Elemente wie Attribute, Klassen und Objekte, aus denen AWS Managed Microsoft AD besteht. AWS patcht Ihre AWS verwalteten Microsoft AD-Domänencontroller in Ihrem Namen mit Microsoft Updates. Sie können auch mehr über verwaltete Gruppendienstkonten (gMSAs) erfahren und diese mit Ihrem AWS verwalteten Microsoft AD verwenden.

Sie können Probleme mit Ihrem AWS verwalteten Microsoft AD vermeiden, indem Sie bewährte Methoden berücksichtigen. Zu diesen bewährten Methoden gehören:

- Denken Sie bei der Einrichtung Ihres AWS verwalteten Microsoft AD und der Konfiguration der Sicherheitsgruppen nach Ihren Bedürfnissen an Ihre Administratorkonto-ID und Ihr Kennwort und aktivieren Sie die bedingte Weiterleitungseinstellung.
- Wenn Sie Ihr AWS verwaltetes Microsoft AD verwenden, ändern Sie nicht die Organisationseinheit, die bei der AWS Erstellung des Verzeichnisses erstellt wurde, überwachen Sie die Leistung mit Tools wie Amazon CloudWatch und Amazon SNS und verwenden Sie SMB 2.x-Clients.
- Wenn Sie Anwendungen so programmieren, dass sie mit AWS Managed Microsoft AD funktionieren, verwenden Sie den Windows DC Locator Service, laden Sie Änderungen, bevor Sie sie in Produktionsumgebungen bereitstellen, und verwenden Sie effiziente LDAP-Abfragen, um erhebliche CPU-Zyklen in einem Domänencontroller zu vermeiden.

Themen

- [AWS Schlüsselkonzepte für verwaltetes Microsoft AD](#)
- [AWS Bewährte Methoden für verwaltetes Microsoft AD](#)

AWS Schlüsselkonzepte für verwaltetes Microsoft AD

Sie werden mehr aus AWS Managed Microsoft AD herausholen, wenn Sie sich mit den folgenden Schlüsselkonzepten vertraut machen.

Themen

- [Active-Directory-Schema](#)
- [Patching und Wartung für AWS Managed Microsoft AD](#)
- [Gruppenverwaltete Service-Konten](#)
- [Eingeschränkte Kerberos-Delegierung](#)

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. Einige Beispiele für Benutzerklassenattribute können der Vorname, der Nachname, die Telefonnummer usw. des Benutzers sein.

Schemaelemente

Attribute, Klassen und Objekte sind die grundlegenden Elemente zum Erstellen von Objektdefinitionen im Schema. Im Folgenden finden Sie Einzelheiten zu Schemaelementen, die Sie unbedingt kennen sollten, bevor Sie mit der Erweiterung Ihres AWS verwalteten 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 [Merkmale 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 [Merkmale 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 wie Sie sie erhalten, finden Sie unter [Object Identifiers](#) auf der MSDN-Website.

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 [verknüpfen Attributen](#).

Verwandte Themen

- [Wann Sie Ihr AWS Managed Microsoft AD-Schema erweitern sollten](#)
- [Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas](#)

Patching und Wartung für AWS Managed Microsoft AD

AWS Der Directory Service für Microsoft Active Directory, auch bekannt als AWS DS für AWS Managed Microsoft AD, ist eigentlich Microsoft Active Directory Domain Services (AD DS), der als verwalteter Dienst bereitgestellt wird. Das System verwendet Microsoft Windows Server 2019 für die Domänencontroller (DCs) und AWS fügt Software DCs für Dienstverwaltungszwecke hinzu. AWS Updates (Patches) DCs , um neue Funktionen hinzuzufügen und die Microsoft Windows Server-Software auf dem neuesten Stand zu halten. Während des Patchings kann Ihr Verzeichnis weiterhin genutzt werden.

Sicherstellen der Verfügbarkeit

Standardmäßig besteht jedes Verzeichnis aus zwei Verzeichnissen DCs, die jeweils in einer anderen Availability Zone installiert sind. Nach Ihrer Wahl können Sie weitere hinzufügen, DCs um die Verfügbarkeit weiter zu erhöhen. Für kritische Umgebungen, in denen hohe Verfügbarkeit und Fehlertoleranz erforderlich sind, empfehlen wir die Bereitstellung zusätzlicher Komponenten. DCs AWS patcht Sie DCs sequentiell. Während dieser Zeit AWS ist der DC, der aktiv patcht, nicht verfügbar. Für den Fall, dass einer oder mehrere Ihrer Server vorübergehend DCs außer Betrieb sind, verschiebt das AWS Patchen, bis mindestens zwei Verzeichnisse betriebsbereit sind. DCs Auf diese Weise können Sie den anderen Betrieb DCs während des Patch-Vorgangs verwenden, der in der Regel 30 bis 45 Minuten pro DC dauert, obwohl diese Zeit variieren kann. Um sicherzustellen, dass Ihre Anwendungen ein operierendes DC erreichen können, falls eines oder mehrere DCs aus irgendeinem Grund nicht verfügbar sind, einschließlich Patches, sollten Ihre Anwendungen den Windows DC Locator Service und keine statischen DC-Adressen verwenden.

Verstehen des Patch-Zeitplans

Um die Microsoft Windows Server-Software auf Ihrem aktuellen Stand zu halten DCs, AWS verwendet Microsoft-Updates. Da Microsoft monatliche Rollup-Patches für Windows Server zur Verfügung AWS stellt, bemüht man sich nach besten Kräften, den Rollup DCs innerhalb von drei Kalenderwochen für alle Kunden zu testen und anzuwenden. Überprüft außerdem Updates, AWS die Microsoft außerhalb des monatlichen Rollups veröffentlicht, auf der Grundlage ihrer Anwendbarkeit und Dringlichkeit. DCs Bei Sicherheitspatches, die Microsoft als kritisch oder wichtig einstuft und für die sie relevant sind DCs, AWS bemüht man sich, den Patch innerhalb von fünf Tagen zu testen und bereitzustellen.

Gruppenverwaltete Service-Konten

Mit Windows Server 2012 hat Microsoft eine neue Methode eingeführt, mit der Administratoren Dienstkonten verwalten können, die als Gruppe Managed Service Accounts (gMSAs) bezeichnet wird. Mit g MSAs mussten Dienstadministratoren die Kennwortsynchronisierung zwischen Dienstinstanzen 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 Berechtigungen zu gewähren, damit sie eine gMSA erstellen können, müssen Sie ihre Konten als Mitglied der Sicherheitsgruppe AWS Delegated Managed Service Account Administrators hinzufügen. Standardmäßig ist das Admin-Konto ein Mitglied dieser Gruppe. Weitere Informationen zu g MSAs finden Sie auf der TechNet Microsoft-Website unter [Group Managed Service Accounts Overview](#).

Verwandter Blogbeitrag zum Thema AWS Sicherheit

- [Wie AWS Managed Microsoft AD dazu beiträgt, die Bereitstellung zu vereinfachen und die Sicherheit von Active Directory-integrierten .NET-Anwendungen zu verbessern](#)

Eingeschränkte Kerberos-Delegierung

Die eingeschränkte Kerberos-Delegierung ist ein Feature in Windows Server. Diese Funktion gibt Dienstadministratoren die Möglichkeit, Vertrauensgrenzen für Anwendungen festzulegen und durchzusetzen, indem sie den Bereich einschränken, in dem Anwendungsdienste im Namen eines Benutzers 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.

Nehmen wir zum Beispiel an, der 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, für die die entsprechenden Berechtigungen gelten hr-app-service, und nicht mit den konfigurierten Berechtigungen von jsmith. Sie müssen der Personalabrechnungsanwendung den Zugriff auf die SQL Server-Datenbank mit den Anmeldeinformationen 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 Benutzern in AWS Managed Microsoft AD Berechtigungen zu gewähren, die es Benutzern ermöglichen, die eingeschränkte Kerberos-Delegierung zu konfigurieren, müssen Sie ihre Konten als Mitglied der Sicherheitsgruppe AWS Delegated Kerberos Delegation Administrators 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.

AWS Bewährte Methoden für verwaltetes 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.

Themen

- [Bewährte Methoden für die Einrichtung eines AWS verwalteten Microsoft AD](#)
- [Bewährte Methoden bei der Verwendung eines AWS verwalteten Microsoft AD-Verzeichnisses](#)
- [Bewährte Methoden bei der Programmierung Ihrer Anwendungen für ein AWS verwaltetes Microsoft AD](#)

Bewährte Methoden für die Einrichtung eines AWS verwalteten Microsoft AD

Im Folgenden finden Sie einige Vorschläge und Richtlinien für die Einrichtung Ihres AWS verwalteten Microsoft AD:

Themen

- [Voraussetzungen](#)
- [Ihr AWS verwaltetes Microsoft AD erstellen](#)

Voraussetzungen

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

Sicherstellen, dass Sie den richtigen Verzeichnistyp verwenden

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 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 einfaches 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 Directory Service Optionen finden Sie unter [Welche sollte man auswählen](#).

Stellen Sie sicher, dass Ihre VPCs und Instances korrekt konfiguriert sind

Um eine Verbindung zu Ihren Verzeichnissen herzustellen, sie zu verwalten und zu verwenden, müssen Sie die Verzeichnisse, VPCs denen die Verzeichnisse zugeordnet sind, ordnungsgemäß konfigurieren. Weitere Informationen über die Anforderungen zur VPC-Sicherheit und Netzwerken finden Sie unter [Voraussetzungen für die Erstellung eines AWS verwalteten 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 [Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD zu verbinden](#) 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 Ihres Verzeichnisses vertraut

AWS erstellt eine [Sicherheitsgruppe](#) und fügt sie den [elastischen Netzwerkschnittstellen](#) des Domänencontrollers Ihres Verzeichnisses hinzu. Diese Sicherheitsgruppe blockiert unnötigen Datenverkehr zum Domänencontroller und lässt den für die Active Directory-Kommunikation erforderlichen Datenverkehr zu. 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 der AWS verwalteten Microsoft AD VPC IPv4 CIDR-Adresse. AWS fügt die Sicherheitsgruppe Ihren Domänencontroller-Schnittstellen hinzu, auf die von Ihrem Peering aus zugegriffen werden kann oder deren Größe geändert wurde. [VPCs](#) 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 Ihrer Verzeichnissicherheitsgruppen erhöhen möchten, können Sie sie so ändern, dass sie Datenverkehr von einer restriktiveren Liste von IP-Adressen akzeptieren. Sie könnten beispielsweise die akzeptierten Adressen aus Ihrem IPv4 VPC-CIDR-Bereich in einen CIDR-Bereich ändern, der für ein einzelnes Subnetz oder einen einzelnen Computer spezifisch 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 Verzeichnissicherheitsgruppe akzeptiert Datenverkehr auf den erforderlichen Active Directory-Ports von der AWS verwalteten Microsoft AD VPC IPv4 CIDR-Adresse. 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.

Ihr AWS verwaltetes Microsoft AD erstellen

Im Folgenden finden Sie einige Vorschläge, die Sie bei der Erstellung Ihres AWS Managed Microsoft AD berücksichtigen sollten.

Themen

- [Ihre Administratoren-ID und das Passwort nicht vergessen](#)
- [Erstellen einer DHCP-Optionsliste](#)
- [Aktivieren Sie die Einstellung für die bedingte Weiterleitung](#)
- [Bereitstellen zusätzlicher Domain-Controller](#)
- [Machen Sie sich mit Benutzernamenbeschränkungen für AWS Anwendungen vertraut](#)

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 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 [Einen DHCP-Optionssatz für AWS Managed Microsoft AD erstellen oder ändern](#).

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 sichergestellt, dass die Einstellung für die bedingte Weiterleitung dauerhaft ist, wenn ein Knoten aufgrund eines Infrastruktur- oder Überlastungsausfalls ersetzt wird.

Bedingte Weiterleitungen sollten auf einem Domänencontroller erstellt werden, wobei die vorherige Einstellung aktiviert ist. Dies ermöglicht die Replikation auf andere Domänencontroller.

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 [Verwenden Sie den Windows DC Locator-Dienst](#).

Machen Sie sich mit Benutzernamenbeschränkungen für AWS Anwendungen vertraut

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 WorkDocs WorkMail, Amazon oder Quick verwendet werden. Diese Einschränkungen verlangen, dass die folgenden Zeichen nicht verwendet werden:

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

 Note

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

Bewährte Methoden bei der Verwendung eines AWS verwalteten Microsoft AD-Verzeichnisses

Im Folgenden finden Sie einige Vorschläge, die Sie bei der Verwendung von AWS Managed Microsoft AD beachten sollten.

Themen

- [Keine vordefinierten Benutzer, Gruppen und Organisationseinheiten ändern](#)
- [Automatisch mit Domains verbinden](#)
- [Vertrauensstellungen korrekt einrichten](#)
- [Die Leistung Ihres Domain-Controllers verfolgen](#)
- [Schemaerweiterungen sorgfältig planen](#)
- [Über Load Balancer](#)
- [Ein Backup Ihrer Instance erstellen](#)
- [SNS-Messaging einrichten](#)
- [Verzeichnisdienst-Einstellungen anwenden](#)
- [Amazon Enterprise-Anwendungen vor dem Löschen eines Verzeichnisses entfernen](#)
- [Beim Zugriff auf die SYSVOL- und NETLOGON-Freigaben SMB 2.x-Clients verwenden](#)

Keine vordefinierten Benutzer, Gruppen und Organisationseinheiten ändern

Wenn Sie 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 erstellt](#).

Automatisch mit Domains verbinden

Beim Starten einer Windows-Instanz, die Teil einer 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 [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten 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 Vertrauentyp 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 Domännennamen (FQDNs) als auch NetBIOS-Namen müssen zwischen Gesamtstrukturen/Domänen eindeutig sein

Weitere Details und Anweisungen zum Einrichten einer Vertrauensstellung finden Sie unter [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#).

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 [Wird verwendet CloudWatch , um die Leistung Ihrer AWS verwalteten Microsoft AD-Domänencontroller zu 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 [Erweitern Sie Ihr AWS verwaltetes Microsoft AD-Schema](#).

Über Load Balancer

Verwenden Sie keinen Load Balancer vor den AWS verwalteten Microsoft AD-Endpunkten. Microsoft Active Directory (AD) für die Verwendung mit einem Erkennungsalgorithmus für Domänencontroller (DC) konzipiert, der ohne externen Lastenausgleich den am schnellsten funktionierenden Domänencontroller findet. Externe Netzwerklastenausgleichsdienste erkennen fälschlicherweise aktiv DCs und können dazu führen, dass Ihre Anwendung an einen Domänencontroller gesendet wird, der demnächst eingerichtet, aber noch nicht einsatzbereit 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 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 [Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots](#).

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 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 [Statusbenachrichtigungen für AWS verwaltete Microsoft AD-Verzeichnisse mit Amazon Simple Notification Service aktivieren](#).

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 [UpdateSettingsAPI](#) folgen.

Weitere Informationen finden Sie unter [Sicherheitseinstellungen für AWS verwaltete Microsoft AD-Verzeichnisse bearbeiten](#).

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 WorkDocs, Amazon oder Amazon WorkMail Relational Database Service (Amazon RDS) verknüpft ist, müssen Sie zunächst jede Anwendung entfernen. WorkSpaces AWS-Managementkonsole Weitere Informationen zum Entfernen dieser Anwendungen finden Sie unter [Löschen Ihres AWS verwalteten 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 der SMBv2 neueren Versionen bieten eine Reihe von Funktionen, die die Leistung der Clients verbessern und die Sicherheit Ihrer Domänencontroller und Clients erhöhen. Diese Änderung

folgt den Empfehlungen des [Computer Emergency Readiness Teams der Vereinigte Staaten](#) und von [Microsoft](#) zur Deaktivierung SMBv1.

Important

Wenn Sie derzeit SMBv1 Clients für den Zugriff auf die SYSVOL- und NETLOGON-Shares Ihres Domänencontrollers verwenden, müssen Sie diese Clients aktualisieren, damit sie sie verwenden oder eine neuere Version verwenden können. SMBv2 Ihr Verzeichnis wird ordnungsgemäß funktionieren, aber Ihre SMBv1 Clients können keine Verbindung zu den SYSVOL- und AWS NETLOGON-Shares Ihrer verwalteten Microsoft AD-Domänencontroller herstellen und auch keine Gruppenrichtlinien verarbeiten.

SMBv1 Clients funktionieren mit allen anderen SMBv1 kompatiblen Dateiservern, die Sie haben. AWS empfiehlt jedoch, dass Sie alle Ihre SMB-Server und -Clients auf SMBv2 oder eine neuere Version aktualisieren. [Weitere Informationen zur Deaktivierung SMBv1 und Aktualisierung auf neuere SMB-Versionen auf Ihren Systemen finden Sie in diesen Beiträgen auf Microsoft TechNet und in der Dokumentation. Microsoft](#)

Verfolgen von Remoteverbindungen SMBv1

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 Verbindungen hin. SMBv1 Im Folgenden finden Sie ein Beispiel für die Informationen, die Sie in einem dieser Protokolle finden können:

SMB1 Zugriff

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

Leitfaden:

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

Bewährte Methoden bei der Programmierung Ihrer Anwendungen für ein AWS verwaltetes Microsoft AD

Bevor Sie Ihre Anwendungen so programmieren, dass sie mit AWS Managed Microsoft AD funktionieren, sollten Sie Folgendes berücksichtigen:

Themen

- [Verwenden Sie den Windows DC Locator-Dienst](#)
- [Auslastungstests vor der Inbetriebnahme](#)
- [Effiziente LDAP-Abfragen verwenden](#)

Verwenden Sie den Windows DC Locator-Dienst

Verwenden Sie bei der Entwicklung von Anwendungen den Windows DC-Locator-Dienst oder den Dynamic DNS-Dienst (DDNS) Ihres AWS verwalteten Microsoft AD, um nach Domänencontrollern zu suchen (DCs). 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 festen DC binden und der DC gepatcht oder wiederhergestellt wird, verliert Ihre Anwendung den Zugriff auf den DC, anstatt einen der verbleibenden zu verwenden. DCs 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, testen Sie mit zusätzlichen Kapazitäten DCs und verteilen Sie gleichzeitig die Anfragen zwischen den DCs. Weitere Informationen finden Sie unter [Bereitstellung zusätzlicher Domänencontroller für Ihr AWS verwaltetes Microsoft AD](#).

Effiziente LDAP-Abfragen verwenden

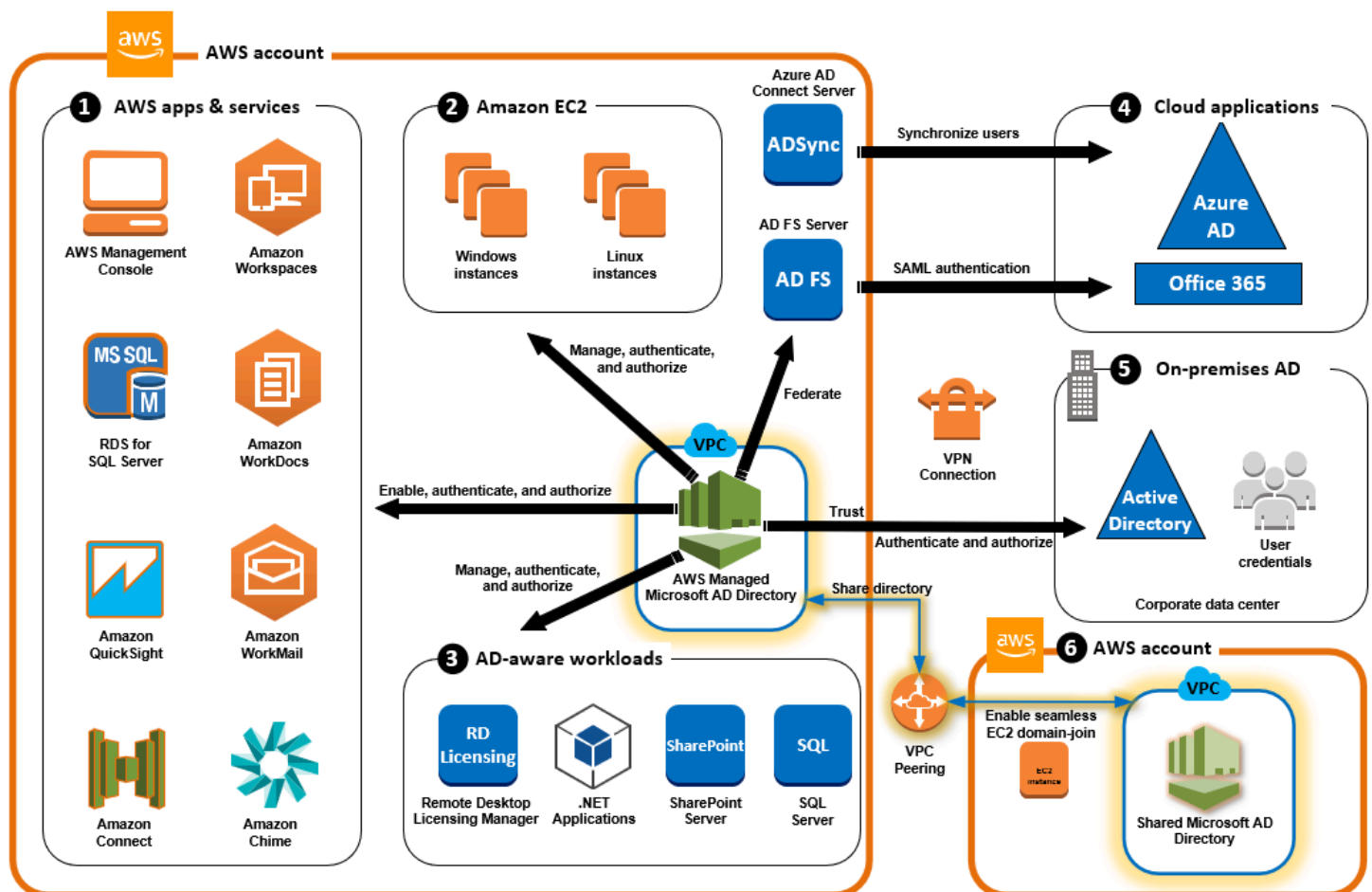
Umfassende LDAP-Abfragen für einen Domain-Controller bei tausenden von Objekten können umfangreiche CPU-Zyklen auf einem einzelnen DC verursachen und ein Hot Spotting nach sich

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 AWS IAM Identity Center Cloud-Anwendungen](#)
- [Anwendungsfall 5: Erweitern Sie Ihr lokales Active Directory auf AWS Cloud](#)
- [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-Managementkonsole](#), [Amazon Chime](#), [AWS IAM Identity Center](#), [Amazon Connect](#), [Amazon Quick FSx](#), [Amazon RDS for SQL Server WorkDocs](#), [WorkMail](#), [Amazon](#) aktivieren und [WorkSpaces](#) Ihr 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-Managementkonsole mit ihren Active Directory-Anmeldeinformationen bei anzumelden](#). Dazu aktivieren Sie das AWS-Managementkonsole 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-Managementkonsole, übernehmen sie eine IAM-Rolle zur Verwaltung von AWS Ressourcen. Auf diese Weise können Sie Ihren Benutzern ganz einfach Zugriff auf die AWS-Managementkonsole gewähren, ohne eine separate SAML-Infrastruktur konfigurieren und verwalten zu müssen.

Um das Benutzererlebnis weiter zu verbessern, können Sie [Single Sign-On-Funktionen](#) für aktivieren WorkDocs, sodass Ihre Benutzer WorkDocs von einem Computer aus zugreifen können, der mit dem Verzeichnis verbunden ist, 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 anmelden können, um AWS Ressourcen zu verwalten, indem sie den vorhandenen Benutzerkonten IAM-Rollen direkt zuweisen. AWS-Managementkonsole

FSx für die Windows File Server-Integration mit AWS Managed Microsoft AD

Die Integration FSx für Windows File Server mit AWS Managed Microsoft AD bietet ein vollständig verwaltetes systemeigenes 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 der Dateiserver FSx für Windows in ein selbstverwaltetes Microsoft Active Directory integriert werden kann, wird dieses Szenario hier nicht erörtert.

Allgemeine FSx Amazon-Anwendungsfälle und Ressourcen

Dieser Abschnitt enthält einen Verweis auf Ressourcen zu häufig verwendeten Anwendungsfällen FSx für Windows-Dateiserverintegrationen mit AWS verwaltetem Microsoft AD. Jeder der Anwendungsfälle in diesem Abschnitt beginnt mit einer grundlegenden Konfiguration FSx für AWS verwaltete Microsoft AD- und Windows-Dateiserver. 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

- [Wird FSx für Windows File Server als persistenter Speicher auf Windows-Containern verwendet](#)
- [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 WorkSpaces Applications stellt mithilfe von Amazon ein persönliches persistentes Speicherlaufwerk bereit FSx 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 WorkSpaces Anwendungen](#)

Unterstützung für Microsoft SQL Server

FSx für 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](#)
- [Vereinfachen Sie Ihre Hochverfügbarkeitsbereitstellungen von Microsoft SQL Server mithilfe von FSx Windows File Server](#)
- [Gruppenverwaltete Service-Konten](#)

Unterstützung von Stammordnern und Roaming-Benutzerprofilen

FSx für Windows File Server kann verwendet werden, um Daten aus den Basisordnern von Active Directory-Benutzern und dem Ordner Eigene Dateien 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](#)

- [Verwendung FSx für Windows File Server mit WorkSpaces](#)

Unterstützung für die Dateifreigaben im Netzwerk

Netzwerkfähige Dateifreigaben auf einem Dateiserver FSx für Windows bieten eine verwaltete und skalierbare Lösung für die gemeinsame Nutzung von Dateien. 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 FSx für 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 der Dateiserver FSx für Windows so konfiguriert werden, dass er alle Softwaredateien speichert, 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 Windows-Dateiserver anstelle des angehängten EBS-Volumes angeben.

Verwandte Elemente

- [Eine Wiederherstellung des Systemstatus Ihres Servers durchführen](#)

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

- [Teilen Sie Ihr AWS verwaltetes Microsoft AD](#)

- [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 unter:

- [Teilen Sie Ihr AWS verwaltetes Microsoft AD](#)
- [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 for SQL Server in eine grundlegende .NET-Anwendung integrieren und Managed Service Accounts (gMSAs) gruppieren. Weitere Informationen finden Sie unter [Wie AWS verwaltetes Microsoft AD dazu beiträgt, 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 Microsoft SharePoint und Microsoft SQL Server Always On in der Cloud](#) ausführen können. AWS Managed Microsoft AD hilft Ihnen auch dabei, die Sicherheit von Active Directory-integrierten .NET-Anwendungen zu vereinfachen und zu verbessern, indem Sie [Gruppenverwaltete Dienstkonten \(gMSAs\) und eingeschränkte Kerberos-Delegierung](#) (KCD) verwenden.

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

Sie können AWS Managed Microsoft AD verwenden, um AWS IAM Identity Center Dienste für Cloud-Anwendungen bereitzustellen. Sie können Microsoft Entra Connect (früher bekannt als Azure 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-Managementkonsole 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 AWS Cloud

Wenn Sie bereits über eine Active Directory-Infrastruktur verfügen und diese bei der Migration von Active Directory-fähigen Workloads auf die verwenden möchten AWS Cloud, 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-Managementkonsole 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 die betriebliche Belastung Ihrer Active Directory-Infrastruktur zu vermeiden, 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. Diese Funktion macht es einfacher und kostengünstiger, verzeichnisorientierte Workloads mit einem einzigen Verzeichnis für alle Konten und zu verwalten. VPCs Beispielsweise können Sie jetzt Ihre [Windows-Workloads](#), die in EC2-Instances bereitgestellt werden, über mehrere Konten hinweg und VPCs einfach verwalten, indem Sie ein einziges AWS verwaltetes Microsoft AD-Verzeichnis verwenden.

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 Manager](#) Ihre 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 [Teilen Sie Ihr AWS verwaltetes Microsoft AD](#).

Pflegen Sie Ihr AWS verwaltetes Microsoft AD

Sie können das verwenden AWS-Managementkonsole , um Ihr AWS Managed Microsoft AD zu verwalten und day-to-day administrative Aufgaben zu erledigen. Sie können Ihr Verzeichnis unter anderem auf folgende Weise verwalten:

- [Sehen Sie sich die Details Ihres AWS verwalteten Microsoft AD-Verzeichnisses](#) an, um Ihren AWS verwalteten Microsoft AD-Verzeichnistyp, Ihre Verzeichnis-ID, Ihren Verzeichnisstatus und Netzwerkdetails wie Amazon VPC, Subnetze und Availability Zones zu erfahren.
- [Stellen Sie Ihr AWS verwaltetes Microsoft AD mit Snapshots](#) wieder her. Sie können auch Snapshots erstellen und Snapshots löschen.
- [Stellen Sie zusätzliche Domänencontroller](#) bereit, um die Leistung und Verfügbarkeit von AWS Managed Microsoft AD zu verbessern.
- [Aktualisieren Sie Ihr AWS Managed Microsoft AD](#) von der Standard Edition auf die Enterprise Edition, die mehr Verzeichnisobjekte unterstützt.

- [Fügen Sie einen alternativen Benutzerprinzipalnamen \(UPN\)](#) hinzu, um die Benutzeranmeldung zu verbessern.
- [Benennen Sie den Namen Ihrer AWS verwalteten Microsoft AD-Site](#) um, um die Fähigkeit von AWS Managed Microsoft AD zu verbessern, Ihre vorhandenen Active Directory-Benutzer in Ihrem lokalen Verzeichnis zu finden und zu authentifizieren.
- [Löschen Sie Ihr AWS verwaltetes Microsoft AD](#), wenn Sie es nicht mehr benötigen.

AWS Verwaltete Microsoft AD-Verzeichnisinformationen anzeigen

Sie können den verwenden AWS-Managementkonsole , um Ihre AWS verwalteten Microsoft AD-Verzeichnisdetails wie folgt anzuzeigen:

- Verzeichnistyp
- Verzeichnis-ID
- Status des Verzeichnisses
- Netzwerkdetails für Ihr AWS verwaltetes Microsoft AD wie:
 - Amazon VPC
 - Subnets
 - Availability Zones
 - DNS-Adressen

Sie finden die folgenden Informationen zu Ihrem AWS Managed Microsoft AD:

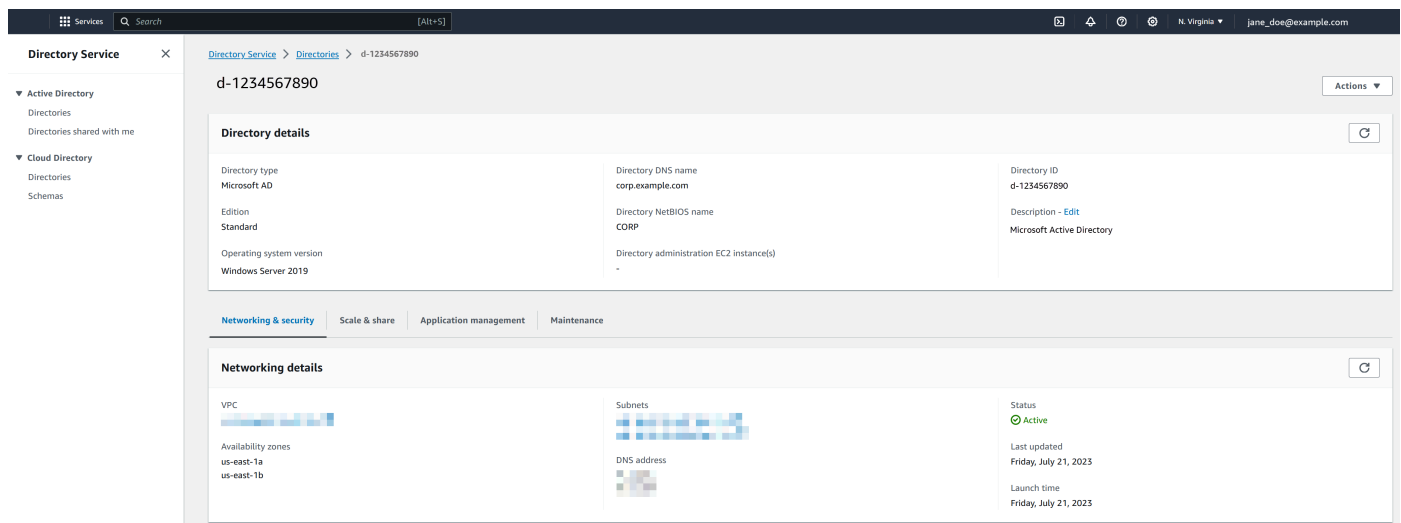
- Auf der Registerkarte Teilen und Teilen können Sie Ihr AWS verwaltetes Microsoft AD mit anderen teilen AWS-Konten und sich über die Netzwerkdetails für Ihre Domänencontroller informieren.
- Auf der Registerkarte Anwendungsverwaltung können Sie eine Anwendungszugriffs-URL für Ihr AWS verwaltetes Microsoft AD und AWS Anwendungen und Dienste für Ihr AWS verwaltetes Microsoft AD aktivieren.
- Auf der Registerkarte Wartung können Sie Amazon Simple Notification Service aktivieren, um Benachrichtigungen über Ihren AWS Managed Microsoft AD-Status zu erhalten und Snapshots Ihres AWS Managed Microsoft AD zu überprüfen.
- Weitere Informationen zum Feld Status finden Sie unter [Den Status Ihres AWS verwalteten Microsoft AD-Verzeichnisses verstehen](#).

Sie können AWS verwaltete Microsoft AD-Verzeichnisinformationen mit dem AWS-Managementkonsole AWS CLI, oder anzeigenPowerShell:

AWS-Managementkonsole

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

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. Informationen über das Verzeichnis werden auf der Seite Verzeichnisdetails angezeigt.



AWS CLI

Um detaillierte Verzeichnisinformationen anzuzeigen, verwenden Sie den AWS CLI

- Öffnen Sie das AWS CLI. Um Ihre AWS verwalteten Microsoft AD-Verzeichnisinformationen anzuzeigen, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

Weitere Informationen finden Sie unter [describe-directories](#).

PowerShell

Um detaillierte Verzeichnisinformationen anzuzeigen mit PowerShell

- Öffnen Sie PowerShell. Um Ihre AWS verwalteten Microsoft AD-Verzeichnisinformationen anzuzeigen, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

Weitere Informationen finden Sie unter [Get-DSDirectory](#).

Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots

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. Wenn Sie dieses Limit bereits erreicht haben, müssen Sie einen Ihrer vorhandenen manuellen Snapshots löschen, bevor Sie einen weiteren erstellen können. Sie können keine Snapshots von AD-Connector-Verzeichnissen erstellen.

Note

Snapshot ist eine globale Funktion von AWS Managed Microsoft AD. Wenn Sie [Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD](#) 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. Wenn Sie dieses Limit bereits erreicht haben, müssen Sie einen Ihrer vorhandenen manuellen Snapshots löschen, bevor Sie einen weiteren erstellen können.

Gehen Sie wie folgt vor, um einen manuellen Snapshot Ihres AWS verwalteten Microsoft AD mit dem AWS-Managementkonsole AWS CLI, oder zu erstellen PowerShell:

AWS-Managementkonsole

Um einen manuellen Snapshot zu erstellen in AWS-Managementkonsole

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.

AWS CLI

Um einen manuellen Snapshot zu erstellen mit AWS CLI

- Öffnen Sie das AWS CLI. Um einen Snapshot Ihres AWS verwalteten Microsoft AD zu erstellen, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

Weitere Informationen finden Sie unter [create-snapshot](#).

PowerShell

Um einen manuellen Snapshot zu erstellen mit PowerShell

- Öffnen Sie PowerShell. Um einen Snapshot Ihres AWS verwalteten Microsoft AD zu erstellen, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

Weitere Informationen finden Sie unter [New-DSSnapshot](#).

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 auf [der Website unter Nützliche Haltbarkeit einer Systemstatussicherung von Active Directory](#). Microsoft

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 wissen, dass alle DNS-Server DCs und DNS-Server, die dem Verzeichnis zugeordnet sind, offline sind, bis der Wiederherstellungsvorgang abgeschlossen ist.

Gehen Sie wie folgt vor, um Ihr Verzeichnis mithilfe von AWS-Managementkonsole AWS CLI, oder aus einem Snapshot wiederherzustellen PowerShell:

AWS-Managementkonsole

Um ein Verzeichnis aus einem Snapshot wiederherzustellen, finden Sie im AWS-Managementkonsole

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.

AWS CLI

Um ein Verzeichnis aus einem Snapshot wiederherzustellen mit AWS CLI

1. Öffnen Sie das AWS CLI. Um die Snapshots für Ihr AWS verwaltetes Microsoft AD aufzulisten, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

2. Um Ihr AWS Managed Microsoft AD aus einem Snapshot wiederherzustellen, können Sie den [restore-from-snapshot](#)Befehl verwenden. Stellen Sie sicher, dass Sie den snapshot-id Parameter durch die Snapshot-ID ersetzen, die Sie für die Wiederherstellung Ihres AWS verwalteten Microsoft AD verwenden möchten:

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

PowerShell

Um ein Verzeichnis aus einem Snapshot wiederherzustellen mit PowerShell

1. Öffnen Sie PowerShell. Um die Snapshots für Ihr AWS verwaltetes Microsoft AD aufzulisten, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

2. Um Ihr AWS Managed Microsoft AD aus einem Snapshot wiederherzustellen, können Sie den [Restore-DSFromSnapshot](#) Befehl verwenden. Stellen Sie sicher, dass Sie den `snapshot-id` Parameter durch die Snapshot-ID ersetzen, die Sie für die Wiederherstellung Ihres AWS verwalteten Microsoft AD verwenden möchten:

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

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

Gehen Sie wie folgt vor, um einen Snapshot Ihres AWS verwalteten Microsoft AD mit dem AWS-Managementkonsole AWS CLI, oder zu löschen PowerShell:

AWS-Managementkonsole

Um einen Snapshot zu löschen in AWS-Managementkonsole

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.

AWS CLI

Um einen Snapshot zu löschen mit AWS CLI

1. Öffne das AWS CLI. Um die Snapshots für Ihr AWS verwaltetes Microsoft AD aufzulisten, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

2. Um einen Snapshot Ihres AWS verwalteten Microsoft AD zu löschen, können Sie den [delete-snapshot](#) Befehl verwenden. Stellen Sie sicher, dass Sie den `snapshot-id` Parameter durch die Snapshot-ID des Snapshots ersetzen, den Sie löschen möchten:

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

PowerShell

Um einen Snapshot zu löschen mit PowerShell

1. Öffnen Sie PowerShell. Um die Snapshots für Ihr AWS verwaltetes Microsoft AD aufzulisten, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

2. Um Ihr AWS Managed Microsoft AD aus einem Snapshot wiederherzustellen, können Sie den [Remove-DSSnapshot](#) Befehl verwenden. Stellen Sie sicher, dass Sie den `snapshot-id` Parameter durch die Snapshot-ID des Snapshots ersetzen, den Sie löschen möchten:

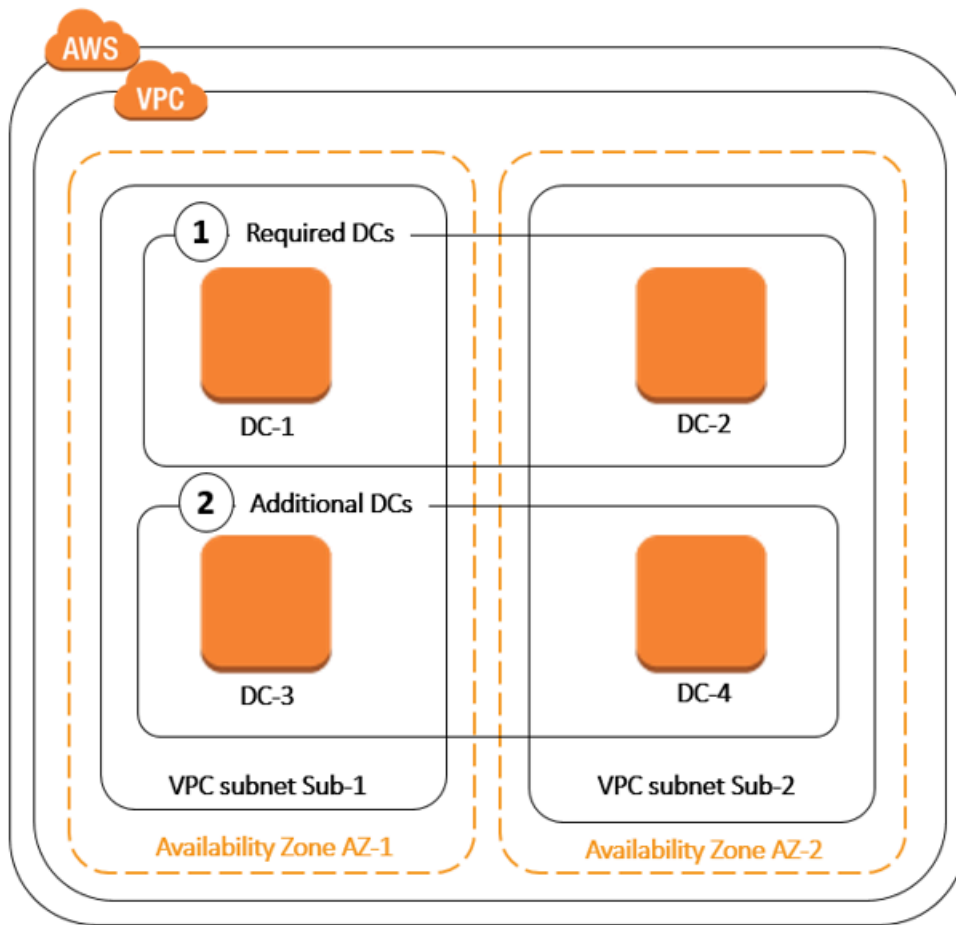
```
Remove-DSSnapshot -SnapshotId s-1234567890
```

Bereitstellung zusätzlicher Domänencontroller für Ihr AWS verwaltetes Microsoft AD

Durch die Bereitstellung zusätzlicher Domänencontroller für Ihr AWS Managed Microsoft AD wird die Redundanz erhöht, was zu noch größerer Ausfallsicherheit und höherer Verfügbarkeit führt. 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 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 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, geschäftskritische Active Directory-integrierte Workloads zu migrieren und auszuführen, AWS Cloud ohne Ihre eigene Active Directory-Infrastruktur bereitstellen und verwalten zu müssen.

Sie können eines der folgenden Tools verwenden, um zusätzliche Domänencontroller für Ihr AWS verwaltetes Microsoft AD bereitzustellen oder zu entfernen:

- [update-number-of-domain-controllers](#) AWS CLI Befehl
- [UpdateNumberOfDomainControllers](#)-API
- [Hinzufügen oder Entfernen zusätzlicher Domänencontroller mit dem AWS-Managementkonsole](#)

 Note

Zusätzliche Domänencontroller sind ein regionales Feature von AWS Managed Microsoft AD. Wenn Sie die [regionsübergreifende Replikation](#) verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter [Globale und regionale Features](#).

Hinzufügen oder Entfernen zusätzlicher Domänencontroller mit dem AWS-Managementkonsole

Sie können die AWS-Managementkonsole verwenden, um zusätzliche Domänencontroller zu Ihrem AWS verwalteten Microsoft AD hinzuzufügen oder zu entfernen.

Voraussetzungen

Bevor Sie Ihrem AWS verwalteten Microsoft AD weitere Domänencontroller hinzufügen oder entfernen, finden Sie hier weitere Informationen zu den Anforderungen an Domänencontroller:

- 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 [Secure LDAP oder LDAPS aktivieren](#).

Verfahren

Gehen Sie wie folgt vor, um zusätzliche Domänencontroller in Ihrem AWS verwalteten Microsoft AD mit der AWS-Managementkonsole, der AWS CLI, oder PowerShell bereitzustellen oder zu entfernen.

AWS-Managementkonsole

Um zusätzliche Domänencontroller hinzuzufügen oder zu entfernen, verwenden Sie die AWS-Managementkonsole.

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.

AWS CLI

Um zusätzliche Domain-Controller hinzuzufügen oder zu entfernen mit AWS CLI

1. Öffnen Sie das AWS CLI. Um die aktuelle Anzahl der Domänencontroller zu überprüfen, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

2. Um Domänencontroller hinzuzufügen oder zu entfernen, können Sie den [update-number-of-domain-controllers](#) Befehl verwenden. Sie können beispielsweise den folgenden Befehl verwenden, um die Gesamtzahl der Domänencontroller auf 4 festzulegen. Stellen Sie sicher, dass Sie die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den `desired-number` Parameter durch die Anzahl der Domänencontroller ersetzen, die Sie bereitstellen möchten.

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

PowerShell

Um zusätzliche Domänencontroller hinzuzufügen oder zu entfernen mit PowerShell

1. Öffnen Sie PowerShell. Um die aktuelle Anzahl der Domänencontroller zu überprüfen, führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

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

2. Um Domänencontroller hinzuzufügen oder zu entfernen, können Sie den [Set-DSDomainControllerCount](#) Befehl verwenden. Sie können beispielsweise den folgenden Befehl verwenden, um die Gesamtzahl der Domänencontroller auf 4 festzulegen. Stellen Sie sicher, dass Sie die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den DesiredNumber Parameter durch die Anzahl der Domänencontroller ersetzen, die Sie bereitstellen möchten.

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

Verwandter Blogartikel zum Thema AWS Sicherheit

- [So erhöhen Sie die Redundanz und Leistung Ihres Directory Service for AWS Managed Microsoft AD durch Hinzufügen von Domänencontrollern](#)

Ihr AWS verwaltetes Microsoft AD aktualisieren

Sie können Ihre Standard Edition AWS Managed Microsoft AD auf die Enterprise Edition aktualisieren. Im Folgenden werden die Unterschiede zwischen der Standard- und der Enterprise-Edition beschrieben:

- 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.

Um Ihre Standard Edition AWS Managed Microsoft AD auf Enterprise Edition zu aktualisieren, verwenden Sie [UpdateDirectorySetupupdate-directory-setup](#) von der API AWS CLI, von oder [Update-DSDirectory Setup](#) von AWS -Tools für PowerShell.

API

So aktualisieren Sie Ihre Standard Edition AWS Managed Microsoft AD auf die Enterprise Edition:

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

AWS CLI

So aktualisieren Sie Ihre Standard Edition AWS Managed Microsoft AD auf die Enterprise Edition:

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

PowerShell

So aktualisieren Sie Ihre Standard Edition AWS Managed Microsoft AD auf die Enterprise Edition:

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

`-DirectorySizeUpdateSettings_DirectorySize Large` **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)
- Asien-Pazifik (Mumbai)
- Asien-Pazifik (Osaka)
- Asien-Pazifik (Seoul)
- Asien-Pazifik (Singapur)
- Asien-Pazifik (Sydney)
- Asien-Pazifik (Thailand)
- Asien-Pazifik (Tokio)
- Canada (Central)
- China (Peking)
- China (Ningxia)
- Mexiko (Zentral)
- Europe (Frankfurt)
- Europa (Irland)
- Europa (London)
- Europe (Paris)
- Europa (Stockholm)
- Südamerika (São Paulo)
- AWS GovCloud (USA West)
- AWS GovCloud (US-Ost)

Bei der Aktualisierung Ihres AWS Managed Microsoft AD sind einige Einschränkungen zu beachten. Diese sind:

- Für das Upgrade fallen zusätzliche Kosten an. Weitere Informationen finden Sie unter [Directory Service -Preise](#).
- Sobald Ihr Active Directory aktualisiert wurde, kann es nicht mehr auf die vorherige Version zurückgesetzt werden.
- Frühere Snapshots können nicht verwendet werden, um das Active Directory wiederherzustellen, nachdem es aktualisiert wurde.
- Upgrades erfolgen an einem geplanten Datum und zu einer Uhrzeit, die mit Support Ihnen vereinbart wurden. 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.
- Während des Upgrade-Vorgangs wird der Hostname jeder Domain-Controller-Instanz geändert, ihre IP-Adressen bleiben jedoch unverändert.
- Wenn Sie LDAPS (Lightweight Directory Access Protocol over SSL) verwenden, benötigen die Domänencontroller neue Zertifikate.

Netzwerktyp des Verzeichnisses aktualisieren

Sie können den Netzwerktyp Ihres Directory Service Verzeichnisses von IPv4 auf Dual-Stack (IPv4 und IPv6) ändern. Wenn Sie den Netzwerktyp so aktualisieren, dass er IPv6 IP-Adressen einschließt, steht Ihnen ein größerer Adressraum zur Verfügung als IPv4. IPv4 und IPv6 Kommunikation sind unabhängig voneinander.

Einzelheiten finden Sie unter [Vergleichen IPv4 und IPv6](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Important

Dies ist ein unidirektionaler Vorgang, der nicht rückgängig gemacht werden kann. Testen Sie zuerst in einer Umgebung außerhalb der Produktionsumgebung.

Voraussetzungen

Bevor Sie den Netzwerktyp Ihres Verzeichnisses aktualisieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Ihre VPC und die zugehörigen Subnetze, in denen Ihr Verzeichnis derzeit existiert, müssen mit IPv6 CIDR-Bereichen konfiguriert sein. Einzelheiten finden Sie unter [IPv6 Support für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.
- Sie haben Administratorzugriff auf die AWS-Managementkonsole.
- Ihr Verzeichnis muss sich im Status Aktiv befinden.
- Sie verfügen über die entsprechenden IAM-Berechtigungen, um Directory Service Einstellungen zu ändern.

Um den Netzwerktyp des Verzeichnisses zu aktualisieren

Um Ihr Verzeichnis auf Dual-Stack-Netzwerke zu aktualisieren

Note

Wenn Ihr Verzeichnis in mehreren Regionen repliziert wird, führen Sie dieses Update in jeder Region durch.

1. Wählen Sie im Navigationsbereich der [AWS Directory Service -Konsole](#) Directories aus.
2. Wählen Sie das Zielverzeichnis aus.
3. Gehen Sie zur Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie IPv6 Support hinzufügen aus. Diese Option ist nur für Verzeichnisse verfügbar, die IPv4 nur diese Option enthalten.
5. Lesen Sie die Aktualisierungsinformationen und Preisdetails.
6. Wählen Sie Hinzufügen, um das Update zu bestätigen.

Nach dem Start des Updates ändert sich der Verzeichnisstatus während des Aktualisierungsvorgangs in Aktualisierung. Die Aktualisierung dauert in der Regel 15 bis 30 Minuten. Sobald der Vorgang abgeschlossen ist, wird der Verzeichnisstatus wieder auf Aktiv zurückgesetzt.

Hinzufügen alternativer UPN-Suffixe zu Ihrem AWS Managed Microsoft AD

Sie können die Verwaltung von Active Directory-Anmeldenamen (AD) vereinfachen und die Benutzeranmeldung verbessern, indem Sie Ihrem AWS verwalteten Microsoft AD-Verzeichnis alternative UPN-Suffixe (User Principal Name) 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 erstellt](#).

So fügen Sie alternative UPN-Suffixe hinzu

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Suchen Sie eine EC2 Amazon-Instance, die mit Ihrem AWS Managed Microsoft AD-Verzeichnis verknüpft 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.

Umbenennen des AWS Site-Namens Ihres verwalteten Microsoft AD-Verzeichnisses

Sie können den Standardnamen Ihres AWS verwalteten Microsoft AD-Verzeichnisses so umbenennen, dass er mit Ihren vorhandenen Microsoft Active Directory-Standortnamen (AD) übereinstimmt. Dadurch kann AWS Managed Microsoft AD Ihre vorhandenen AD-Benutzer in Ihrem lokalen Verzeichnis schneller finden und authentifizieren. Das Ergebnis ist eine bessere Benutzererfahrung, wenn sich Benutzer bei AWS Ressourcen wie [Amazon EC2 und Amazon RDS for SQL Server Server-Instances](#) anmelden, die Sie mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis verknüpft 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 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 den Namen der AWS verwalteten Microsoft AD-Site um

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Suchen Sie eine EC2 Amazon-Instance, die mit Ihrem AWS Managed Microsoft AD-Verzeichnis verknüpft 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).

Löschen Ihres AWS verwalteten Microsoft AD

Wenn ein AWS verwaltetes Microsoft AD-, Simple AD- oder Hybridverzeichnis 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.

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 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 bereitgestellt wird. Weitere Informationen finden Sie unter [Wählen einer Region](#).
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-Managementkonsole den Zugriff. Weitere Informationen finden Sie unter [Zugriff wird deaktiviert AWS-Managementkonsole](#).
 - Um Amazon zu deaktivieren WorkSpaces, müssen Sie den Service aus dem Verzeichnis in der WorkSpaces Konsole abmelden. Weitere Informationen finden Sie unter [Löschen eines Verzeichnisses](#) im WorkSpaces Amazon-Administratorhandbuch.
 - Um sie zu deaktivieren WorkDocs, müssen Sie die WorkDocs Site in der WorkDocs 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 for Windows File Server zu deaktivieren, müssen Sie das FSx Amazon-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter [Arbeiten mit Active Directory in FSx für Windows File Server](#) im Amazon FSx for Windows File 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 [Arbeiten mit Client VPN](#) im AWS Client VPN Administratorhandbuch.

- Zur Deaktivierung von Amazon Connect müssen Sie die Amazon Connect-Instance löschen. Weitere Informationen finden Sie unter [Löschen Ihrer Amazon Connect Connect-Instance](#) im Amazon Connect Connect-Administratorhandbuch.
- Um Amazon Quick zu deaktivieren, müssen Sie sich von Amazon Quick abmelden. Weitere Informationen finden Sie unter [Schließen Ihres Amazon Quick Kontos](#) in der Amazon-Kurzanleitung.

 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.

Schützen Sie Ihr AWS verwaltetes Microsoft AD

Sie können Kennwortrichtlinien, Funktionen wie Multi-Faktor-Authentifizierung (MFA) und Einstellungen verwenden, um Ihr AWS Managed Microsoft AD zu schützen. Zu den Möglichkeiten, Ihr Verzeichnis zu schützen, gehören:

- [Erfahren Sie, wie die Kennwortrichtlinien in Active Directory funktionieren](#), sodass sie auf AWS verwaltete Microsoft AD-Benutzer angewendet werden können. Sie können auch delegieren, welcher Benutzer Ihre AWS verwalteten Microsoft AD-Passwortrichtlinien verwalten kann.
- [Aktivieren Sie MFA](#), was Ihre AWS Managed Microsoft AD-Sicherheit erhöht.
- [>Aktivieren Sie das Lightweight Directory Access Protocol über Secure Socket Layer \(SSL\) / Transport Layer Security \(TLS\) \(LDAPS\)](#), sodass die Kommunikation über LDAP verschlüsselt wird und die Sicherheit verbessert wird.

- [Verwalten Sie Ihre AWS Managed Microsoft AD-Konformität](#) mit Standards wie dem Federal Risk and Authorization Management Program (FedRAMP) und dem Payment Card Industry (PCI) Data Security Standard (DSS).
- [Verbessern Sie Ihre AWS Managed Microsoft AD-Netzwerksicherheitskonfiguration](#), indem Sie die AWS Sicherheitsgruppe an Ihre Umgebungsanforderungen anpassen.
- [Bearbeiten Sie die Sicherheitseinstellungen Ihres AWS verwalteten Microsoft AD-Verzeichnisses](#) wie Certificate Base Authentication, Secure Channel Cipher und Protocol ganz nach Ihren Bedürfnissen.
- [Richten Sie AWS Private Certificate Authority Connector für AD](#) ein, damit Sie Zertifikate für Ihr AWS verwaltetes Microsoft AD mit ausstellen und verwalten können AWS Private CA.

Grundlegendes zu AWS verwalteten Microsoft AD-Kennwortrichtlinien

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 das Active Directory angewendet. 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

Note

- * Das maximale Kennwortalter von 42 Tagen beinhaltet das Admin-Passwort.

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.

Die folgenden Ressourcen bieten weitere Informationen zu den detaillierten Kennwortrichtlinien und Sicherheitsrichtlinien von Microsoft Active Directory:

- [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 Directory Administrative Center](#) verwenden. Informationen zu den ersten Schritten mit den Microsoft Richtlinientools finden Sie unter [Installation der Active Directory-Verwaltungstools für AWS verwaltetes Microsoft AD](#).

Wie werden Passwortrichtlinien angewendet

Je nachdem, ob das Passwort zurückgesetzt oder geändert wurde, gibt es Unterschiede bei der Anwendung der detaillierten Passwortrichtlinien. Domänenbenutzer können ihr eigenes Passwort ändern. Ein Active Directory-Administrator oder ein 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

Richtlinie	Passwort zurückgesetzt	Passwort ändern
Maximales Passwortalter	 Ja	 Ja
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.

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](#).

Richtliniename	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.

- Richtliniename
- [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 fehlgeschlagenen 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 resultierende 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.

Themen

- [Zuweisen von Kennwortrichtlinien zu Ihren AWS verwalteten Microsoft AD-Benutzern](#)
- [Delegieren, wer Ihre AWS verwalteten Microsoft AD-Passwortrichtlinien verwalten kann](#)

Verwandter Blogartikel zum Thema AWS Sicherheit

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

Zuweisen von Kennwortrichtlinien zu Ihren AWS verwalteten Microsoft AD-Benutzern

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 Passworrichtlinien zu

1. Starten Sie [das Active Directory-Verwaltungszentrum \(ADAC\)](#) 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](#).

Delegieren, wer Ihre AWS verwalteten Microsoft AD-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-Verwaltungszentrum \(ADAC\)](#) 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 erstellt](#).
3. Suchen Sie die Benutzergruppe AWS Delegated Fine Grained Password Policy Administrators. Fügen Sie dieser Gruppe Benutzer oder Gruppen aus Ihrer Domain hinzu.

Aktivierung der 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 auf unterstützte Amazon Enterprise-Anwendungen angeben. 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 client/server Industriestandardprotokoll, das Authentifizierung, Autorisierung und Kontoverwaltung ermöglicht, damit 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 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 [Multi-Faktor-Authentifizierung für AD Connector aktivieren](#).
- MFA ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie die [Multi-Region-Replikation](#) verwenden, können Sie MFA nur in der primären Region Ihres AWS verwalteten Microsoft AD verwenden.
- 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 [Support](#).
- Alle Amazon Enterprise IT-Anwendungen WorkSpaces, einschließlich Amazon WorkDocs WorkMail, Amazon Quick und Zugriff auf AWS IAM Identity Center und AWS-Managementkonsole

werden unterstützt, wenn AWS Managed Microsoft AD und AD Connector mit MFA verwendet werden. Diese AWS Anwendungen, die MFA verwenden, werden in mehreren Regionen nicht unterstützt.

Weitere Informationen finden Sie unter [So aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Dienste mithilfe von AWS verwaltetem Microsoft AD und lokalen Anmeldeinformationen](#).

- Informationen zur Konfiguration des grundlegenden Benutzerzugriffs auf Amazon Enterprise-Anwendungen, AWS Single Sign-On und deren AWS-Managementkonsole Verwendung Directory Service finden Sie unter [Zugriff auf AWS Anwendungen und Dienste von Ihrem AWS Managed Microsoft AD](#) und [AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren](#).
- Im folgenden AWS Sicherheits-Blogbeitrag erfahren Sie, wie Sie MFA für WorkSpaces Amazon-Benutzer in Ihrem AWS Managed Microsoft AD aktivieren, [So aktivieren Sie die Multi-Faktor-Authentifizierung für AWS Dienste mithilfe von AWS Managed Microsoft AD und lokalen Anmeldeinformationen](#)

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-Managementkonsole oder auf Amazon Enterprise-Anwendungen und -Services wie WorkSpaces Amazon Quick oder Amazon Chime. Amazon Enterprise-Anwendungen und -Services werden in der primären Region nur unterstützt, wenn die Multi-Region-Replikation für Ihr AWS Managed Microsoft AD konfiguriert ist. Es bietet keine MFA für Windows-Workloads, die auf EC2-Instances ausgeführt werden, oder für die Anmeldung bei einer EC2-Instance. 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 Push-Benachrichtigungen oder Authentifikator-Einmalkennwörter (OTP) für den Benutzer ausführt. 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 standardmäßigen RADIUS-Serverport (UDP:1812) von den Servern zulassen. 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.

Secure 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 kommerziellen oder eigenen LDAP-fähigen Anwendungen (fungieren als LDAP-Clients) und AWS Managed Microsoft AD (fungiert als LDAP-Server). Weitere Informationen finden Sie unter [Serverseitiges LDAPS mit AWS Managed Microsoft AD aktivieren](#).
- Das clientseitige LDAPS verschlüsselt die LDAP-Kommunikation zwischen AWS Anwendungen wie WorkSpaces (als LDAP-Clients) und Ihrem selbstverwalteten (lokalen) Active Directory (das als LDAP-Server fungiert). Weitere Informationen finden Sie unter [Aktivierung von clientseitigem LDAPS mit AWS Managed Microsoft AD](#).

[Weitere Informationen zu bewährten Methoden zur Sicherung Ihrer Active Directory-Implementierung finden Sie in der Dokumentation. MicrosoftCertificate ServicesMicrosoft](#)

Themen

- [Serverseitiges LDAPS mit AWS Managed Microsoft AD aktivieren](#)

- [Aktivierung von clientseitigem LDAPS mit AWS Managed Microsoft AD](#)

Serverseitiges LDAPS mit AWS Managed Microsoft AD aktivieren

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

Aktivieren Sie serverseitiges LDAPS mit AWS Private Certificate Authority

Ausführliche Anweisungen zur Einrichtung und Konfiguration serverseitiger LDAPS und Ihres CA-Servers (Certificate Authority) finden Sie unter AWS Private CA. [AWS Private CA Connector für AD für AWS Managed Microsoft AD einrichten](#)

Aktivieren Sie serverseitiges LDAPS mithilfe von CA Microsoft

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 AWS Cloud

Wenn Sie Ihre PKI Infrastruktur mithilfe von Automatisierung einrichten möchten, können Sie die [MicrosoftPublic Key Infrastructure auf AWS QuickStart Guide](#) verwenden. Insbesondere sollten Sie den Anweisungen in der Anleitung folgen, um die Vorlage für [Deploy MicrosoftPKI in eine bestehende VPC zu](#) laden AWS. Stellen Sie nach dem Laden der Vorlage sicher, dass Sie **AWSManaged** auswählen, wenn Sie zur Option Typ der Active-Directory-Domainservices gelangen. Wenn Sie die QuickStart Anleitung verwendet haben, können Sie direkt zu dieser wechseln [Schritt 3: Eine Zertifikatvorlage erstellen](#).

Themen

- [Schritt 1: Delegieren, wer LDAPS aktivieren kann](#)
- [Schritt 2: Ihre Zertifizierungsstelle einrichten](#)
- [Schritt 3: Eine Zertifikatvorlage erstellen](#)

- [Schritt 4: Sicherheitsgruppenregeln hinzufügen](#)

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. Mit diesem Zertifikat kann der LDAP Dienst auf den Domänencontrollern auf SSL Verbindungen von LDAP Clients warten und diese automatisch akzeptieren.

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:

- Einen untergeordneten Server erstellen Microsoft Enterprise CA — (empfohlen) Mit dieser Option können Sie einen untergeordneten Microsoft Enterprise CA Server in der Cloud bereitstellen. AWS Der Server kann Amazon EC2 verwenden, sodass er mit Ihrer vorhandenen Microsoft Root-CA funktioniert. Weitere Informationen zum Einrichten eines untergeordneten Microsoft Enterprise CA Verzeichnisses finden Sie unter Schritt 4: Hinzufügen eines Microsoft Enterprise CA zu Ihrem AWS Microsoft AD Verzeichnis in [So aktivieren Sie serverseitiges LDAPS für Ihr AWS verwaltetes Microsoft AD-Verzeichnis](#).

- **Root erstellen Microsoft Enterprise CA** — Mit dieser Option können Sie mithilfe von Amazon EC2 ein Root Microsoft Enterprise CA in der AWS Cloud erstellen und es 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 [Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD zu verbinden](#).

Schritt 3: Eine Zertifikatvorlage erstellen

Nachdem Sie Ihre Enterprise CA eingerichtet haben, können Sie die Vorlage für das Kerberos Authentifizierungszertifikat 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 die ZertifizierungsstelleOS, die Ihrer Zertifizierungsstelle 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 unterstützt von Windows Server 2019.

- 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 LDAPOverSSL-Zertifikatsvorlage (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 dann OK aus.

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 Ihrem herzustellenEnterprise CA, um ein Zertifikat anzufordern. Dazu fügen Sie Regeln für eingehenden Datenverkehr hinzu, sodass Sie eingehenden Datenverkehr von Ihren Domänencontrollern akzeptieren Enterprise CA können. Anschließend fügen Sie Regeln für ausgehenden Datenverkehr hinzu, um den Datenverkehr von Ihren Domänencontrollern zum zuzulassen. Enterprise CA

Sobald beide Regeln konfiguriert wurden, fordern Ihre Domänencontroller Enterprise CA automatisch ein Zertifikat von Ihnen an und aktivieren LDAPS für Ihr Verzeichnis. Der LDAP Dienst auf Ihren Domänencontrollern ist jetzt bereit, LDAPS-Verbindungen zu akzeptieren.

Konfigurieren von Sicherheitsgruppenregeln

1. Navigieren Sie zu Ihrer Amazon EC2 EC2-Konsole unter <https://console.aws.amazon.com/ec2> und melden Sie sich mit Administratoranmeldedaten 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 (z. B. sg-123456789) für Ihr Verzeichnis 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 für Ihre CA in das Feld neben Ziel ein.
 - Wählen Sie Speichern.

Mit dem LDP Tool können Sie die LDAPS-Verbindung zum AWS Managed Microsoft AD-Verzeichnis testen. Das LDP Tool wird mit dem Active Directory Administrative Tools geliefert. Weitere Informationen finden Sie unter [Installation der Active Directory-Verwaltungstools für AWS verwaltetes 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

Aktivierung von clientseitigem 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, Quick und Amazon Chime. Diese Verschlüsselung hilft Ihnen, die Identitätsdaten Ihres Unternehmens 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 dem selbstverwalteten Microsoft Active Directory](#)
- [Serverzertifikate in Active Directory bereitstellen](#)
- [Zertifikatsanforderungen der Zertifizierungsstelle](#)
- [Netzwerkanforderungen](#)

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

Zunächst müssen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und dem selbstverwalteten Microsoft Active Directory einrichten, um clientseitiges 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.

Zertifikatsanforderungen 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-Managementkonsole Methode verwenden. AWS CLI

Note

Clientseitiges LDAPS ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie die [regionsübergreifende 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 Directory Service](#)
- [Schritt 2: Den Registrierungsstatus überprüfen](#)
- [Schritt 3: Clientseitiges LDAPS aktivieren](#)
- [Schritt 4: Den LDAPS-Status überprüfen](#)

Schritt 1: Registrieren Sie ein Zertifikat in Directory Service

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

Methode 1: Um Ihr Zertifikat in Directory Service (AWS-Managementkonsole) 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 Directory Service (AWS CLI) zu registrieren

- Führen Sie den folgenden Befehl aus. Zeigen Sie für die Zertifikatsdaten auf den Speicherort der Zertifizierungsstellen-Zertifikatsdatei. 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 Directory Service (AWS-Managementkonsole) zu überprüfen

- Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
- Überprüfen Sie den aktuellen Status der Zertifikatsregistrierung, 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 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. 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 Directory Service AWS-Managementkonsole

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 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 zu überprüfen. Directory Service

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

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 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-Managementkonsole 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 Directory Service (AWS-Managementkonsole) 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: So zeigen Sie die Zertifikatsdetails in 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 zuerst LDAPS deaktivieren, bevor Sie das Zertifikat abmelden können.

Methode 1: Um die Registrierung eines Zertifikats in Directory Service () aufzuheben AWS-Managementkonsole

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 die Registrierung eines Zertifikats in () aufzuheben Directory Service AWS 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 das clientseitige LDAPS in () zu deaktivieren Directory Service AWS-Managementkonsole

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 Directory Service AWS 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. 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-konformen 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 [Grundlegendes zu AWS verwalteten Microsoft AD-Kennwortrichtlinien](#).

Verbesserung Ihrer AWS Managed Microsoft AD-Netzwerksicherheitskonfiguration

Die AWS Sicherheitsgruppe, die für das AWS verwaltete Microsoft AD-Verzeichnis bereitgestellt wird, ist mit den minimalen eingehenden Netzwerkports konfiguriert, die erforderlich sind, um alle bekannten Anwendungsfälle für Ihr AWS verwaltetes Microsoft AD-Verzeichnis zu unterstützen. Weitere Informationen zur bereitgestellten AWS Sicherheitsgruppe finden Sie unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#)

Um die Netzwerksicherheit Ihres AWS verwalteten Microsoft AD-Verzeichnisses weiter zu verbessern, können Sie die AWS Sicherheitsgruppe auf der Grundlage der folgenden häufigen Szenarien ändern.

Kundendomänencontroller CIDR — In diesem CIDR-Block befinden sich Ihre lokalen Domänencontroller.

Kunden-Client-CIDR — In diesem CIDR-Block authentifizieren sich Ihre Clients wie Computer oder Benutzer bei Ihrem AWS verwalteten Microsoft AD. Ihre AWS verwalteten Microsoft AD-Domänencontroller befinden sich ebenfalls in diesem CIDR-Block.

Szenarien

- [AWS Es werden nur Anwendungen unterstützt](#)
- [AWS Anwendungen nur mit Trust-Support](#)
- [AWS Unterstützung für Anwendungen und systemeigene Active Directory-Workloads](#)
- [AWS Unterstützung für Anwendungen und systemeigene Active Directory-Workloads mit Vertrauensunterstützung](#)

AWS Es werden nur Anwendungen unterstützt

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
- Schnell
- AWS IAM Identity Center

- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS-Managementkonsole

Sie können die folgende AWS Sicherheitsgruppenkonfiguration verwenden, um den gesamten unwichtigen Datenverkehr zu Ihren AWS verwalteten Microsoft AD-Domänencontrollern 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.

AWS Anwendungen nur mit Trust-Support

Alle Benutzerkonten werden in Ihrem AWS verwalteten Microsoft AD oder Ihrem vertrauenswürdigen Active Directory bereitgestellt und können mit unterstützten AWS Anwendungen verwendet werden, z. B. den folgenden:

- Amazon Chime
- Amazon Connect
- Schnell
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS-Managementkonsole

Sie können die Konfiguration der bereitgestellten AWS Sicherheitsgruppe ändern, um den gesamten unwichtigen Datenverkehr zu Ihren AWS verwalteten Microsoft AD-Domänencontrollern 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
- Bei dieser Konfiguration müssen Sie sicherstellen, dass das CIDR-Netzwerk der Kundendomänencontroller 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	Kundendomaincontroller (CIDR)	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauenstellungen
TCP und UDP	88	Kundendomaincontroller CIDR	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauenstellungen auf Gesamtstrukturebene
TCP und UDP	389	Kundendomaincontroller CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauenstellungen
TCP und UDP	464	Kundendomaincontroller CIDR	Kerberos Passwort ändern/einrichten	Replikation, Benutzer- und Computerauthentifizierung, Vertrauenstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	445	Kundendom änencontroller CIDR	SMB/CIFS	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien- Vertraue nsstellungen
TCP	135	Kundendom änencontroller CIDR	Replikation	RPC, EPM
TCP	636	Kundendom änencontroller CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	49152–65535	Kundendom änencontroller CIDR	RPC	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	3268 - 3269	Kundendom änencontroller CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
UDP	123	Kundendom änencontroller CIDR	Windows-Uhrzeit	Windows-U hrzeit, Vertrauen sstellungen

Regeln für ausgehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
Alle	Alle	Kundendom änencontroller CIDR	Gesamter Datenverkehr	

AWS Unterstützung für Anwendungen und systemeigene Active Directory-Workloads

Benutzerkonten werden nur in Ihrem AWS Managed Microsoft AD bereitgestellt, um sie mit unterstützten AWS Anwendungen wie den folgenden zu verwenden:

- Amazon Chime
- Amazon Connect
- Amazon EC2-Instances
- Amazon FSx

- Schnell
- Amazon RDS für MySQL
- Amazon RDS für Oracle
- Amazon RDS für PostgreSQL
- Amazon RDS für SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS-Managementkonsole

Sie können die Konfiguration der bereitgestellten AWS Sicherheitsgruppe ändern, um den gesamten unwichtigen Datenverkehr zu Ihren AWS verwalteten Microsoft AD-Domänencontrollern zu blockieren.

Note

- Active Directory-Vertrauensstellungen können nicht zwischen Ihrem AWS verwalteten Microsoft AD-Verzeichnis und den Kundendomänencontrollern CIDR erstellt und verwaltet werden.
- Sie müssen sicherstellen, dass das CIDR-Netzwerk für den Kundenclient 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	Datenverk ehrstyp	Verwendung von Active Directory
TCP und UDP	53	CIDR für Kunden	DNS	Benutzer- und Computera

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
				uthentifizierung, Namensauf lösung, Vertrauen sstellungen
TCP und UDP	88	Kunde Kunde CIDR	Kerberos	Benutzer- und Computera uthentifizierung, Vertrauen sstellungen auf Gesamtstr ukturebene
TCP und UDP	389	Kunde Kunde CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP und UDP	445	Kunde Kunde CIDR	SMB/CIFS	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien- Vertraue nsstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP und UDP	464	Kunde Kunde CIDR	Kerberos Passwort ändern/ei nrichten	Replikation, Benutzer- und Computera uthentifizierung, Vertrauen sstellungen
TCP	135	Kunde Kunde CIDR	Replikation	RPC, EPM
TCP	636	Kunde Kunde CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	49152–65535	Kunde Kunde CIDR	RPC	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	3268 - 3269	Kunde Kunde CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	9389	Kunde Kunde CIDR	SOAP	AD-DS-Web- Services
UDP	123	Kunde Kunde CIDR	Windows-Uhrzeit	Windows-U hrzeit, Vertrauen sstellungen
UDP	138	Kunde Kunde CIDR	DFSN und NetLogon	DFS, Gruppenri chtlinie

Regeln für ausgehenden Datenverkehr

Keine.

AWS Unterstützung für Anwendungen und systemeigene Active Directory-Workloads mit Vertrauensunterstützung

Alle Benutzerkonten werden in Ihrem AWS verwalteten Microsoft AD oder Ihrem vertrauenswürdigen Active Directory bereitgestellt und können mit unterstützten AWS Anwendungen verwendet werden, z. B. den folgenden:

- Amazon Chime
- Amazon Connect
- Amazon EC2-Instances

- Amazon FSx
- Schnell
- Amazon RDS für MySQL
- Amazon RDS für Oracle
- Amazon RDS für PostgreSQL
- Amazon RDS für SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS-Managementkonsole

Sie können die Konfiguration der bereitgestellten AWS Sicherheitsgruppe ändern, um den gesamten unwichtigen Datenverkehr zu Ihren AWS verwalteten Microsoft AD-Domänencontrollern zu blockieren.

 Note

- Dazu müssen Sie sicherstellen, dass die Netzwerke „Customer Domain Controller CIDR“ und „Customer Client CIDR“ sicher sind.
- TCP 445 mit den „Kundendomänencontrollern CIDR“ wird nur zur Vertrauensbildung verwendet und kann entfernt werden, nachdem die Vertrauensstellung hergestellt wurde.
- TCP 445 mit dem „Kunden-Client-CIDR“ sollte geöffnet bleiben, da es für die Gruppenrichtlinien-Verarbeitung 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	Datenverk ehrstyp	Verwendung von Active Directory
TCP und UDP	53	Domänencontroller des Kunden (CIDR)	DNS	Benutzer- und Computerauthentifizierung, Namensauflösung, Vertrauenstellungen
TCP und UDP	88	Kundendomänencontroller CIDR	Kerberos	Benutzer- und Computerauthentifizierung, Vertrauenstellungen auf Gesamtstrukturebene
TCP und UDP	389	Kundendomänencontroller CIDR	LDAP	Verzeichnis, Replikation, Benutzer- und Computerauthentifizierung, Gruppenrichtlinien, Vertrauenstellungen
TCP und UDP	464	Kundendomänencontroller CIDR	Kerberos Passwort ändern/einrichten	Replikation, Benutzer- und Computerauthentifizierung, Vertrauenstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	445	Kundendom änencontroller CIDR	SMB/CIFS	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien- Vertraue nsstellungen
TCP	135	Kundendom änencontroller CIDR	Replikation	RPC, EPM
TCP	636	Kundendom änencontroller CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	49152–65535	Kundendom änencontroller CIDR	RPC	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	3268 - 3269	Kundendom änencontroller CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
UDP	123	Kundendom änencontroller CIDR	Windows-Uhrzeit	Windows-U hrzeit, Vertrauen sstellungen
TCP und UDP	53	Kundendom änencontroller CIDR	DNS	Benutzer- und Computera uthentifizierung, Namensauf lösung, Vertrauen sstellungen
TCP und UDP	88	Kundendom änencontroller CIDR	Kerberos	Benutzer- und Computera uthentifizierung, Vertrauen sstellungen auf Gesamtstr ukturebene

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

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
TCP	636	Kundendom änencontroller CIDR	LDAP SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	49152–65535	Kundendom änencontroller CIDR	RPC	Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	3268 - 3269	Kundendom änencontroller CIDR	LDAP GC und LDAP GC SSL	Verzeichnis, Replikation, Benutzer- und Computera uthentifizierung, Gruppenri chtlinien, Vertrauen sstellungen
TCP	9389	Kunden-Do mänencontroller CIDR	SOAP	AD-DS-Web- Services

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
UDP	123	Kundendom änencontroller CIDR	Windows-Uhrzeit	Windows-U hrzeit, Vertrauen sstellungen
UDP	138	Kundendom änencontroller CIDR	DFSN und NetLogon	DFS, Gruppenri chtlinie

Regeln für ausgehenden Datenverkehr

Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp	Verwendung von Active Directory
Alle	Alle	Domänenco ntroller des Kunden (CIDR)	Gesamter Datenverkehr	

Sicherheitseinstellungen für AWS verwaltete Microsoft AD-Verzeichnisse bearbeiten

Sie können detaillierte Verzeichniseinstellungen für Ihr AWS verwaltetes Microsoft AD konfigurieren, um Ihre Compliance- und Sicherheitsanforderungen zu erfüllen, ohne die betriebliche Arbeitslast zu erhöhen. In den Verzeichniseinstellungen können Sie die Secure-Channel-Konfiguration für die in Ihrem Verzeichnis verwendeten Protokolle und Codes aktualisieren. Sie haben beispielsweise die Flexibilität, einzelne ältere Verschlüsselungen 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 Domänencontrollern in Ihrem Verzeichnis bereit, verwaltet Neustarts von Domänencontrollern und behält diese Konfiguration bei, wenn Sie sie skalieren oder weitere bereitstellen. AWS-Regionen 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 Management Console an und öffnen Sie die 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	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
Zertifikatsbasierte Authentifizierung	Certificate	CERTIFICATE_BACKDATING_COMPENSATION	Jahre: 0 bis 50	Geben Sie einen Wert an, der angibt, wie lange ein Zertifikat einem Benutzer in Active Directory vorausgehen kann und noch für die Authentifizierung
	Backdating	TING_COMPENSATION	Monate: 0 bis 11	
	Compensation		Tage: 0 bis 30	
			Stunden: 0 bis 23	
			Minuten: 0 bis 59	
			Sekunden: 0 bis 59	

Typ	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
				isierung 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	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
				Authentifizierung auf Windows-Domänencontrollern in der Microsoft-Supportdokumentation.

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

Typ	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
				andernfalls die Authentifizierung fehlschlägt. • Vollständige Durchsetzung (Standard): 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	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
				Weitere Informationen finden Sie unter KB5014754 — Änderungen der zertifikatsbasierten Authentifizierung auf Windows-Domänencontrollern in der Microsoft-Supportdokumentation.
Sicherer Kanal: Code	AES 128/128	AES_128_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie den AES-128/128-Verschlüsselungsscode für die Secure-Channel-Kommunikationen zwischen Domain-Controllern in Ihrem Verzeichnis.

Typ	Einstellungsname	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 die RC2 40/128-Verschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.

Typ	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
	RC2_56/128	RC2_56_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie die RC2 56/128-Verschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.
	RC2_128/128	RC2_128_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie die RC2 128/128-Verschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.

Typ	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
	RC4_40/128	RC4_40_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie die RC4 40/128-Verschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.
	RC4_56/128	RC4_56_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie die RC4 56/128-Verschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.

Typ	Einstellungsname	API-Name	Mögliche Werte	Beschreibung der Einstellung
	RC4_64/128	RC4_64_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie die RC4 64/128-Verschlüsselungsschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.
	RC4_128/128	RC4_128_128	Aktivieren, Deaktivieren	Aktivieren oder deaktivieren Sie die RC4 128/128-Verschlüsselungsschlüsselungsschlüssel für die sichere Kanalkommunikation zwischen Domänencontrollern in Ihrem Verzeichnis.

Typ	Einstellungsname	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	Einstellungsname	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	Einstellungsname	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.

Aktivieren Sie Public Key Cryptography for Initial Authentication (PKINIT) für Ihre AWS verwalteten Microsoft AD-Benutzer

AWS Verwaltete Microsoft AD-Verzeichnisse verwenden standardmäßig eine starke Zertifikatsbindung, was eine explizite Zuordnung zwischen Zertifikaten und AD-Objekten erfordert. Die folgenden Zuordnungen werden für AWS Managed Microsoft AD als stark angesehen:

- `altSecurityIdentitiesEmittent` und Seriennummer
- `altSecurityIdentitiesSchlüssel-ID` für den Betreff
- `altSecurityIdentities` SHA1 Hash des öffentlichen Schlüssels

Diese Attribute ermöglichen eine sichere Zertifikatszuweisung, die mehr Sicherheit für die zertifikatsbasierte Authentifizierung bietet, da explizite certificate-to-user Beziehungen erforderlich sind, die in Active Directory definiert werden müssen. Dies trägt dazu bei, zertifikatsbasierte Angriffe mit Rechteeskalation zu verhindern.

Sie können dieses Verfahren verwenden, um starke Zertifikatsbindungen zu konfigurieren, um Angriffe mit Rechteeskalation zu verhindern und gleichzeitig die Funktionalität der Zertifikatsauthentifizierung aufrechtzuerhalten.

Weitere Informationen finden Sie unter [Microsoft KB5014754: Änderungen der zertifikatsbasierten Authentifizierung auf Windows-Domänencontrollern](#)

Voraussetzungen

- Ein AWS verwaltetes Microsoft AD-Verzeichnis mit konfigurierter Zertifizierungsstelle
- Administratorzugriff auf Ihre Active Directory-Umgebung
- PowerShell mit installiertem Active Directory-Modul
- Das Zertifikat, das Sie dem AD-Objekt zuordnen möchten

AltSecurityIdentity Attribut zuordnen

1. Wählen Sie basierend auf Ihren Zertifikatsinformationen eine der folgenden `AltSecurityIdentity` Zuordnungsmethoden:
 - **SHA1 Hash** — Verwendet den SHA1 Hash des öffentlichen Schlüssels des Zertifikats

Extrahieren Sie für die SHA1 Hash-Zuordnung den Zertifikat-Hash und wenden Sie ihn auf das Benutzerobjekt an:

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

- **Aussteller und Seriennummer** — Verwendet den Namen und die Seriennummer des Zertifikats

Verwenden Sie für die Zuordnung von Aussteller und Seriennummer den Aussteller und die Seriennummer des Zertifikats:

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

- **Schlüssel-ID für den Betreff** — Verwendet die Erweiterung der Schlüssel-ID für den Betreff des Zertifikats

Verwenden Sie für die Zuordnung der Schlüssel-ID für den Betreff die Schlüssel-ID für den Betreff des Zertifikats:

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

2. Stellen Sie sicher, dass die Zuordnung erfolgreich angewendet wurde:

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

3. Warten Sie, bis die Active Directory-Replikation abgeschlossen ist (normalerweise 15-30 Sekunden), bevor Sie die Zertifikatsauthentifizierung testen.

Beispiel: Massenzertifikat, das das Attribut zuordnet AltSecurityIdentity

Das folgende Beispiel zeigt, wie AltSecurityIdentity Attribute für mehrere Benutzerzertifikate von einer Zertifizierungsstelle zugeordnet werden:

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

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

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



```
Write-Output "Adding $thumbprint to $User as altSecurityIdentity"
Set-ADUser -Identity $User -Add @{'altSecurityIdentities'=$SHA1PUKEY}
}
}
```

Nächste Schritte

- Testen Sie die zertifikatsbasierte Authentifizierung mit Ihren zugewiesenen Zertifikaten
- Konfigurieren Sie Ihre Anwendungen so, dass sie die zugewiesenen Zertifikate für die Authentifizierung verwenden
- [Überwachen Sie Ihr AWS verwaltetes Microsoft AD](#) für Authentifizierungsereignisse

AWS Private CA Connector für AD für AWS Managed Microsoft AD einrichten

Sie können Ihr AWS verwaltetes Microsoft AD mit [AWS Private Certificate Authority \(CA\)](#) integrieren, um Zertifikate für Ihre Active Directory-Domänencontroller, domänengebundenen Benutzer, Gruppen und Maschinen auszustellen und zu verwalten. AWS Private CA Connector for Active Directory ermöglicht es Ihnen, einen vollständig verwalteten AWS Private CA Drop-In-Ersatz für Ihr selbstverwaltetes Unternehmen zu verwenden, CAs 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 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 [Connector-Vorlage erstellen](#). In den folgenden Schritten erfahren Sie, wie Sie diese Integration von der Directory Service Konsole aus einrichten.

AWS Private CA Connector für AD einrichten

Um einen privaten CA-Connector für Active Directory zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die 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 Anwendungsverwaltung und im Bereich AWS Apps und Dienste die Option AWS Private CA Connector for AD aus.
4. Führen Sie auf der Seite Privates CA-Zertifikat für Active Directory erstellen die Schritte aus, um Ihren privaten CA for Active Directory-Connector zu erstellen.

Weitere Informationen finden Sie unter [Einen Konnektor erstellen](#).

AWS Private CA Connector für AD anzeigen

So zeigen Sie Details zum privaten CA-Connector an

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
 2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
 3. Sehen Sie sich auf der Registerkarte Anwendungsverwaltung und im Bereich AWS Apps und Dienste Ihre Private CA-Connectors und die zugehörige private CA an. Die folgenden Felder werden angezeigt:
 - a. AWS Private CA Connector-ID — Die eindeutige Kennung für einen AWS Private CA Connector. Wählen Sie es aus, um die Detailseite anzuzeigen.
 - b. AWS Private CA Betreff — Informationen zum eindeutigen Namen der CA. Wählen Sie es aus, um die Detailseite aufzurufen.
 - c. Status — Ergebnisse der Statusprüfung für den AWS Private CA Connector und AWS Private CA:
 - Aktiv — Beide Prüfungen bestehen
 - 1/2 Prüfungen fehlgeschlagen — Eine Prüfung schlägt fehl
 - Fehlgeschlagen — Beide Prüfungen schlagen fehl
- Einzelheiten zum Status „Fehlgeschlagen“ erhalten Sie, wenn Sie mit der Maus auf den Hyperlink zeigen, um zu sehen, welche Prüfung fehlgeschlagen ist.
- d. Registrierungsstatus für DC-Zertifikate — Statusüberprüfung für den Status des Domänencontroller-Zertifikats:
 - Aktiviert — Die Zertifikatsregistrierung ist aktiviert
 - Deaktiviert — Die Zertifikatsregistrierung ist deaktiviert

- e. Erstellungsdatum — Wann der AWS Private CA Connector erstellt wurde.

Weitere Informationen finden Sie unter [Konnektor-Details anzeigen](#).

Die folgende Tabelle zeigt die verschiedenen Status für die Registrierung von Domänencontroller-Zertifikaten für AWS Managed Microsoft AD mit AWS Private CA

DC-Registrierungsstatus	Description	Maßnahme erforderlich
Aktiviert	Domänencontroller-Zertifikate wurden erfolgreich in Ihrem Verzeichnis registriert.	Es ist keine Aktion erforderlich.
Fehlgeschlagen	Die Aktivierung oder Deaktivierung der Registrierung von Domänencontroller-Zertifikaten ist für Ihr Verzeichnis fehlgeschlagen.	Wenn Ihre Aktivierungsaktion fehlschlägt, versuchen Sie es erneut, indem Sie die Domänencontroller-Zertifikate deaktivieren und dann wieder einschalten. Wenn Ihre Deaktivierungsaktion fehlschlägt, versuchen Sie es erneut, indem Sie die Domänencontrollerzertifikate aktivieren und dann wieder ausschalten. Wenn der Wiederholungsversuch fehlschlägt, wenden Sie sich an den AWS Support.
Beeinträchtigt	Domänencontroller haben Probleme mit der Netzwerkkonnektivität bei der Kommunikation mit AWS Private CA Endpunkten.	Überprüfen Sie die AWS Private CA VPC-Endpunkt- und S3-Bucket-Richtlinien, um die Netzwerkkonnektivität mit Ihrem Verzeichnis zu ermöglichen. Weitere Informationen finden Sie unter Problembehandlung bei Ausnahmemeldungen AWS einer privaten Zertifizierungsstelle und Behebung von Problemen mit

DC-Registrierungsstatus	Description	Maßnahme erforderlich
		dem Widerruf von AWS Private CA Zertifikaten.
Disabled	Die Registrierung von Domänencontroller-Zertifikaten wurde für Ihr Verzeichnis erfolgreich deaktiviert.	Es ist keine Aktion erforderlich.
Deaktivieren	Die Deaktivierung der Registrierung von Domänencontroller-Zertifikaten ist im Gange.	Es ist keine Aktion erforderlich.
Aktivieren	Die Aktivierung der Registrierung von Domänencontroller-Zertifikaten ist im Gange.	Es ist keine Aktion erforderlich.

Konfiguration von AD-Richtlinien

AWS Private CA Connector für AD muss so konfiguriert sein, dass AWS verwaltete Microsoft AD-Domänencontroller und Objekte Zertifikate anfordern und empfangen können. Konfigurieren Sie Ihr Gruppenrichtlinienobjekt ([GPO](#)) so, dass Zertifikate für AWS verwaltete Microsoft AD-Objekte ausgestellt werden AWS Private CA können.

Konfiguration von Active Directory-Richtlinien für Domänencontroller

Aktivieren Sie Active Directory-Richtlinien für Domänencontroller

1. Öffnen Sie die Registerkarte Netzwerk und Sicherheit.
2. Wählen Sie AWS Private CA Connectors.
3. Wählen Sie einen Connector aus, der mit dem AWS Private CA Betreff verknüpft ist, der Domänencontroller-Zertifikate für Ihr Verzeichnis ausstellt.
4. Wählen Sie Aktionen, Domänencontroller-Zertifikate aktivieren aus.

 Important

Konfigurieren Sie eine gültige Domänencontroller-Vorlage, bevor Sie Domänencontrollerzertifikate aktivieren, um verzögerte Updates zu vermeiden.

Nachdem Sie die Registrierung von Domänencontroller-Zertifikaten aktiviert haben, fordern die Domänencontroller Ihres Verzeichnisses Zertifikate von AWS Private CA Connector for AD an und empfangen sie.

Um die Ausstellung von AWS Private CA Domänencontrollerzertifikaten AWS Private CA zu ändern, verbinden Sie die neuen Zertifikate zunächst über einen neuen AWS Private CA Connector für AD mit Ihrem Verzeichnis. Bevor Sie die Zertifikatsregistrierung auf dem neuen Gerät aktivieren AWS Private CA, deaktivieren Sie die Zertifikatsregistrierung auf dem vorhandenen Gerät:

Schalten Sie die Domänencontrollerzertifikate aus

1. Öffnen Sie die Registerkarte Netzwerk und Sicherheit.
2. Wählen Sie AWS Private CA Connectors.
3. Wählen Sie einen Connector aus, der mit dem AWS Private CA Betreff verknüpft ist, der Domänencontroller-Zertifikate für Ihr Verzeichnis ausstellt.
4. Wählen Sie Aktionen, Domänencontroller-Zertifikate deaktivieren.

Konfiguration von Active Directory-Richtlinien für Benutzer, Computer und Maschinen, die einer Domäne angehören

Gruppenrichtlinienobjekte konfigurieren

1. Connect zur AWS verwalteten Microsoft AD-Administratorinstanz her und öffnen Sie [Server Manager](#) im Startmenü.
2. Wählen Sie unter Tools die Option Group Policy Management aus.
3. Suchen Sie unter Gesamtstruktur und Domänen nach Ihrer Subdomänen-Organisationseinheit (OU) (dies corp ist beispielsweise Ihre Subdomänen-Organisationseinheit, wenn Sie die unter beschriebenen Verfahren befolgt haben [Ihr AWS verwaltetes Microsoft AD erstellen](#)) und klicken Sie mit der rechten Maustaste auf Ihre Subdomänen-Organisationseinheit. Wählen Sie Create a GPO in this domain aus, verknüpfen Sie es hier und geben Sie PCA GPO als Namen ein. Wählen Sie OK aus.

4. Das neu erstellte Gruppenrichtlinienobjekt wird hinter dem Namen Ihrer Subdomain angezeigt. Klicken Sie mit der rechten Maustaste darauf **PCA GPO** und wählen Sie Bearbeiten. Wenn ein Dialogfeld mit einer Warnmeldung geöffnet wird, die besagt, dass dies ein Link ist und dass Änderungen global verbreitet werden, bestätigen Sie die Meldung, indem Sie OK wählen, um fortzufahren. Das Fenster Group Policy Management Editor wird geöffnet.
5. Gehen Sie im Fenster des Gruppenrichtlinienverwaltungs-Editors zu Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel (wählen Sie den Ordner aus).
6. Wählen Sie unter Objekttyp die Option Certificate Services Client — Certificate Enrollment Policy aus.
7. Ändern Sie im Fenster Certificate Services Client — Certificate Enrollment Policy das Konfigurationsmodell auf Aktiviert.
8. Vergewissern Sie sich, dass die Active Directory-Registrierungsrichtlinie ausgewählt und aktiviert ist. Wählen Sie Hinzufügen aus.
9. Das Dialogfeld Certificate Enrollment Policy Server wird geöffnet. Geben Sie den Endpunkt des Zertifikatsregistrierungsrichtlinienservers, den Sie bei der Erstellung Ihres Connectors generiert haben, in das Feld Registrierungsserver-Richtlinien-URI eingeben ein. Belassen Sie den Authentifizierungstyp auf Windows integrated.
10. Wählen Sie „Validieren“. Nachdem die Validierung erfolgreich war, wählen Sie Hinzufügen.
11. Kehren Sie zum Dialogfeld Certificate Services Client — Certificate Enrollment Policy zurück und wählen Sie das Feld neben dem neu erstellten Connector aus, um sicherzustellen, dass es sich bei dem Connector um die Standardregistrierungsrichtlinie handelt.
12. Wählen Sie „Active Directory-Registrierungsrichtlinie“ und dann „Entfernen“.
13. Wählen Sie im Bestätigungsdialogfeld Ja aus, um die LDAP-basierte Authentifizierung zu löschen.
14. Klicken Sie im Fenster Certificate Services Client — Certificate Enrollment Policy auf Anwenden und anschließend auf OK. Schließen Sie dann das Fenster.
15. Wählen Sie unter Objekttyp für den Ordner Public Key Policies die Option Certificate Services Client — Auto-Enrollment aus.
16. Ändern Sie die Option „Konfigurationsmodell“ auf „Aktiviert“.
17. Vergewissern Sie sich, dass die Optionen Abgelaufene Zertifikate verlängern und Zertifikate aktualisieren ausgewählt sind. Lassen Sie die anderen Einstellungen unverändert.
18. Wählen Sie Anwenden und dann OK aus, und schließen Sie das Dialogfeld.

Konfigurieren Sie anschließend die Richtlinien für öffentliche Schlüssel für die Benutzerkonfiguration, indem Sie die Schritte 6 bis 17 im Abschnitt Benutzerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Richtlinien für öffentliche Schlüssel wiederholen.

Nachdem Sie die Konfiguration GPOs und die Richtlinien für öffentliche Schlüssel abgeschlossen haben, fordern Objekte in der Domäne Zertifikate von AWS Private CA Connector for AD an und erhalten Zertifikate, die von AWS Private CA ausgestellt wurden.

Bestätigung der AWS Private CA Ausstellung eines Zertifikats

Die Aktualisierung AWS Private CA zur Ausstellung von Zertifikaten für Ihr AWS Managed Microsoft AD kann bis zu 8 Stunden dauern.

Sie können einen der folgenden Schritte ausführen:

- Sie können diesen Zeitraum abwarten.
- Sie können die mit der AWS verwalteten Microsoft AD-Domäne verbundenen Maschinen neu starten, die für den Empfang von Zertifikaten von konfiguriert wurden AWS Private CA. Anschließend können Sie bestätigen, dass der Zertifikate für Mitglieder Ihrer AWS verwalteten Microsoft AD-Domäne ausgestellt AWS Private CA hat, indem Sie das in der [MicrosoftDokumentation beschriebene Verfahren befolgen](#).
- Sie können den folgenden PowerShell Befehl verwenden, um die Zertifikate für Ihr AWS verwaltetes Microsoft AD zu aktualisieren:

```
certutil -pulse
```

Überwachen Sie Ihr AWS verwaltetes Microsoft AD

Sie können Ihr AWS verwaltetes Microsoft AD optimal nutzen, indem Sie mehr über die verschiedenen Status von AWS Managed Microsoft AD und deren Bedeutung für Ihr AWS verwaltetes Microsoft AD erfahren. Sie können auch AWS Dienste wie Amazon Simple Notification Service und Amazon verwenden CloudWatch , um Ihr AWS Managed Microsoft AD zu überwachen. Amazon Simple Notification Service kann Ihnen Benachrichtigungen über den Status Ihres AWS verwalteten Microsoft AD-Verzeichnisses senden. Amazon CloudWatch kann die Leistung Ihrer AWS verwalteten Microsoft AD-Domain-Controller überwachen.

Aufgaben zur Überwachung Ihres AWS Managed Microsoft AD

- [Den Status Ihres AWS verwalteten Microsoft AD-Verzeichnisses verstehen](#)
- [Statusbenachrichtigungen für AWS verwaltete Microsoft AD-Verzeichnisse mit Amazon Simple Notification Service aktivieren](#)
- [Grundlegendes zu Ihren AWS verwalteten Microsoft AD-Verzeichnisprotokollen](#)
- [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#)
- [Wird verwendet CloudWatch , um die Leistung Ihrer AWS verwalteten Microsoft AD-Domänencontroller zu überwachen](#)
- [Deaktivieren der CloudWatch Amazon-Protokollweiterleitung für AWS Managed Microsoft AD](#)
- [Überwachen des DNS-Servers mit Microsoft Event Viewer](#)

Den Status Ihres AWS verwalteten Microsoft AD-Verzeichnisses verstehen

Im Folgenden sind die verschiedenen Zustandsangaben für ein Verzeichnis aufgeführt.

Aktiv

Das Verzeichnis funktioniert normal. 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 Verzeichnismvorgängen die volle Leistungskapazität erreicht. Es gibt viele mögliche Gründe dafür, dass sich das Verzeichnis in diesem Zustand befindet. Dazu gehören normale Wartungsaktivitäten wie Patchen oder EC2 Instanzrotation, temporäres Hotspotting durch eine Anwendung auf einem Ihrer Domänencontroller 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 bei normalen Wartungsproblemen diese Probleme 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 [Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots](#).

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.

Statusbenachrichtigungen für AWS verwaltete Microsoft AD-Verzeichnisse mit Amazon Simple Notification Service aktivieren

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“, um Nachrichten zu sammeln und zu verteilen. 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 Directory Service als Herausgeber hinzufügen. Wenn 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 Verzeichnisstatusmeldungen 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 die [regionsübergreifende Replikation](#) verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter [Globale und regionale Features](#).

Amazon SNS aktivieren

Im Folgenden erfahren Sie, wie Sie Amazon SNS für Ihr AWS verwaltetes Microsoft AD aktivieren können:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die [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 [DirectoryServiceFullAccess](#) verwaltete Richtlinie gilt, muss Ihr Themenname mit

"DirectoryMonitoring" beginnen. Wenn Sie Ihren Themennamen weiter anpassen möchten, benötigen Sie zusätzliche Rechte für SNS.

8. Wählen Sie Erstellen aus.

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.

Entfernen von Verzeichnisstatusmeldungen aus einem Amazon SNS SNS-Thema

Im Folgenden erfahren Sie, wie Sie die Statusmeldungen Ihres AWS verwalteten Microsoft AD-Verzeichnisses aus einem Amazon SNS SNS-Thema entfernen können:

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die [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 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.

Löschen eines Amazon SNS SNS-Themas

Wenn Sie das gesamte Thema löschen möchten, können Sie dies von der [Amazon SNS SNS-Konsole](#) aus tun.

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, wenn ein Verzeichnis das nächste Mal eine Benachrichtigung zu dem gelöschten Thema veröffentlicht. In diesem Fall würden Sie auf der Registerkarte Überwachung des Verzeichnisses einen aktualisierten Status sehen, der darauf hinweist, dass das Thema nicht gefunden werden konnte.

Um zu vermeiden, dass wichtige Verzeichnisstatusmeldungen übersehen werden, verknüpfen Sie Ihr Verzeichnis daher mit einem anderen Amazon SNS SNS-Thema Directory Service, bevor Sie ein Thema löschen, von dem Nachrichten empfangen werden.

Weitere Informationen zum Löschen eines Amazon SNS SNS-Themas finden Sie unter [Löschen eines Amazon SNS SNS-Themas und](#) -Abonnements.

Grundlegendes zu Ihren AWS verwalteten Microsoft AD-Verzeichnisprotokollen

Sicherheitsprotokolle von AWS verwalteten Microsoft AD-Domänencontroller-Instanzen werden für ein Jahr archiviert. Sie können Ihr AWS verwaltetes Microsoft AD-Verzeichnis auch so konfigurieren, dass Domain-Controller-Protokolle nahezu in Echtzeit an Amazon CloudWatch Logs weitergeleitet werden. Weitere Informationen finden Sie unter [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#).

AWS protokolliert die folgenden Ereignisse aus Compliance-Gründen.

Überwachungskategorie	Richtlinieneinstellung	Audit-Status
Kontoanmeldung	Audit Validierung Anmeldeinformationen	Erfolg, Fehler
	Andere Ereignisse bei der Kontoanmeldung prüfen	Erfolg, Fehler
	Überprüft den Kerberos-Authentifizierungsdienst	Erfolg, Fehler
Kontoverwaltung	Audit Computerkonten-Management	Erfolg, Fehler

Überwachungskategorie	Richtlinieneinstellung	Audit-Status
	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
	Prüfen Sie andere Logon/Logoff Ereignisse	Erfolg, Fehler
	Audit Spezielle Anmeldung	Erfolg, Fehler
Objektzugriff	Andere Objektzugriffsereignisse prüfen	Erfolg, Fehler
	Audit Wechseldatenträger	Erfolg, Fehler
	Audit Zentrales Zugriffsrichtlinien-Staging	Erfolg, Fehler

Überwachungskategorie	Richtlinieneinstellung	Audit-Status
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)	IPsec Treiber prüfen	Erfolg, Fehler
	Andere Weitere Systemereignisse	Erfolg, Fehler
	Audit Sicherheitsstatusänderung	Erfolg, Fehler
	Audit Sicherheitssystemerweiterung	Erfolg, Fehler
	Audit Systemintegrität	Erfolg, Fehler

Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD

Sie können entweder die Directory Service Konsole verwenden oder APIs um die Sicherheitsereignisprotokolle des Domain-Controllers an Amazon CloudWatch Logs für Ihr AWS verwaltetes Microsoft AD 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 Protokolle können diese Ereignisse auch an andere AWS Konten, AWS Dienste 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 verwenden, um die Daten aus der Protokollgruppe abzurufen, die Sie bei der Aktivierung des Dienstes angegeben haben. Diese Protokollgruppe enthält die Sicherheitsprotokolle aus Ihren Domain-Controllern.

Weitere Informationen zu Protokollgruppen und zum Lesen ihrer Daten finden Sie unter [Arbeiten mit Protokollgruppen und Protokollströmen](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

Note

Die Protokollweiterleitung ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie die [regionsübergreifende Replikation](#) verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter [Globale und regionale Features](#).

Nach der Aktivierung beginnt die Protokollweiterleitungsfunktion mit der Übertragung von Protokollen von Ihren Domänencontrollern an die angegebene CloudWatch Protokollgruppe. Alle Protokolle, die vor der Aktivierung der Protokollweiterleitung erstellt wurden, werden nicht in die CloudWatch Protokollgruppe übertragen.

Themen

- [Verwenden von AWS-Managementkonsole , um die Amazon CloudWatch Logs-Protokollweiterleitung zu aktivieren](#)
- [Verwenden der CLI oder PowerShell um die Amazon CloudWatch Logs-Protokollweiterleitung zu aktivieren](#)

Verwenden von AWS-Managementkonsole , um die Amazon CloudWatch Logs-Protokollweiterleitung zu aktivieren

Sie können die Amazon CloudWatch Logs-Protokollweiterleitung für Ihr AWS Managed Microsoft AD in der aktivieren AWS-Managementkonsole.

1. Wählen Sie im Navigationsbereich der [Directory Service -Konsole](#) Directories aus.
2. Wählen Sie die Verzeichnis-ID des AWS verwalteten Microsoft AD-Verzeichnisses, das Sie teilen 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 CloudWatch Dialogfeld Protokollweiterleitung aktivieren für eine der folgenden Optionen:
 - a. Wählen Sie Neue CloudWatch Protokollgruppe erstellen aus und geben Sie unter Name der CloudWatch Protokollgruppe einen Namen an, auf den Sie unter CloudWatch Protokolle verweisen können.
 - b. Wählen Sie Eine bestehende CloudWatch Protokollgruppe auswählen und wählen Sie unter Bestehende CloudWatch Protokollgruppen eine Protokollgruppe aus dem Menü aus.
6. Prüfen Sie die Preisinformationen und die Verknüpfung und wählen Sie dann Enable aus.

Verwenden der CLI oder PowerShell um die Amazon CloudWatch Logs-Protokollweiterleitung zu aktivieren

Bevor Sie den [ds create-log-subscription](#) Befehl verwenden können, müssen Sie zunächst eine CloudWatch Amazon-Protokollgruppe und dann eine IAM-Ressourcenrichtlinie erstellen, die dieser Gruppe die erforderlichen Berechtigungen erteilt. Gehen Sie wie folgt vor PowerShell, um die Protokollweiterleitung mit der CLI oder zu aktivieren.

Schritt 1: Erstellen Sie eine Protokollgruppe in CloudWatch Logs

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

CLI Command

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-1111111111'
```

PowerShell Command

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-1111111111'
```

Anweisungen zum Erstellen einer CloudWatch Logs-Gruppe finden Sie unter [Erstellen einer Protokollgruppe in CloudWatch Logs](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

Schritt 2: Erstellen Sie eine CloudWatch Logs-Ressourcenrichtlinie in IAM

Erstellen Sie eine CloudWatch Protokoll-Ressourcenrichtlinie, die 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 auf andere Protokollgruppen zu beschränken Directory Service, oder einen Platzhalter verwenden, um alle Protokollgruppen einzubeziehen. Die folgende Beispielrichtlinie verwendet die Platzhaltermethode, um zu ermitteln, dass alle Protokollgruppen, die mit /aws/directoryservice/ dem AWS Konto beginnen, in dem sich Ihr Verzeichnis befindet, eingeschlossen werden.

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

CLI Command

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

PowerShell Command

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

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

Schritt 3: Erstellen Sie ein Directory Service Protokollabonnement

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

CLI Command

```
aws ds create-log-subscription --directory-id 'd-1111111111' --log-group-name '/aws/directoryservice/d-1111111111'
```

PowerShell Command

```
New-DSLogSubscription -DirectoryId 'd-1111111111' -LogGroupName '/aws/directoryservice/d-1111111111'
```

Wird verwendet CloudWatch , um die Leistung Ihrer AWS verwalteten Microsoft AD-Domänencontroller zu überwachen

Directory Service ist in Amazon integriert CloudWatch , um Ihnen wichtige Leistungskennzahlen für jeden Domain-Controller in Ihrem Active Directory zur Verfügung zu stellen. 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 der Domänencontroller in Ihrem Active Directory zu erhöhen.

Weitere Informationen zur Überwachung Ihrer Domain-Controller finden Sie unter [Feststellen, wann Domänencontroller mit CloudWatch Metriken hinzugefügt werden sollen](#).

Im Zusammenhang mit Amazon fallen Gebühren an CloudWatch. Weitere Informationen finden Sie unter [CloudWatch Abrechnung und Kosten](#).

Important

Die Leistungsmetriken für Domänencontroller mit CloudWatch sind in der Region Kanada West (Calgary) nicht verfügbar.

Informationen zur Aktivierung finden Sie CloudWatch unter [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#).

Leistungsmetriken für Domänencontroller finden Sie in 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-Managementkonsole 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.

Feststellen, wann Domänencontroller mit CloudWatch Metriken hinzugefügt werden sollen

Der Lastenausgleich zwischen all Ihren Domänencontrollern ist wichtig für die Stabilität und Leistung Ihres Active 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 Ihr Active Directory im Laufe der Zeit, um Ihre durchschnittliche und maximale Active Directory-Auslastung zu ermitteln. Nachdem Sie Ihren Ausgangswert festgelegt haben, können Sie diese Messwerte regelmäßig überwachen, um zu bestimmen, wann ein Domänencontroller zu Ihrem Active Directory hinzugefügt werden sollte.

Die folgenden Metriken sollten Sie regelmäßig überwachen. Eine vollständige Liste der verfügbaren Messwerte für Domänencontroller finden Sie unter [AWS Verwaltete Microsoft AD-Leistungsindikatoren](#). CloudWatch

- 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 Domain-Controllern finden Sie unter [Kapazitätsplanung für Active Directory Domain Services](#) 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

Metrik-Kategorie	Metrikname
DirectoryServices (NTDS)	Durchschnittliche Latenz von I/O-Datenbank-Lesevorgängen
	I/O Database Reads/sec
	Durchschnittliche Latenz von I/O-Protokollschreibvorgängen
	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.
LogicalDisk	Durchschn. Länge der Datenträgerwarteschlange
	% freier Speicherplatz
Arbeitsspeicher	% übertragene Bytes im Gebrauch
	Langfristige durchschnittliche Standby-Cache-Lebensdauer (S)
Netzwerkschnittstelle	Gesendete Byte/Sek.

Metrik-Kategorie	Metrikname
NTDS	Empfangene Bytes/Sek.
	Aktuelle Bandbreite
	Geschätzte Verzögerung in der ATQ-Warteschlange
	ATQ-Anforderungslatenz
	Lesevorgänge pro Sekunde im DS-Verzeichnis
	DS-Verzeichnis-Suchen/Sek
	Schreibvorgänge im DS-Verzeichnis pro Sekunde
	LDAP-Clientsitzungen
	LDAP-Suchen/Sekunde
Prozessor	Erfolgreiche LDAP-Bindungen/Sekunde
	% Prozessorzeit
Systemweite Sicherheitsstatistiken	Kerberos-Authentifizierungen
	NTLM-Authentifizierungen

Deaktivieren der CloudWatch Amazon-Protokollweiterleitung für AWS Managed Microsoft AD

Sie können die Weiterleitung von CloudWatch Logs Log für Ihr AWS Managed Microsoft AD im deaktivieren AWS-Managementkonsole. Weitere Informationen zur Protokollweiterleitung finden Sie unter [the section called “Wird CloudWatch zur Überwachung Ihres Verzeichnisses verwendet”](#).

1. Wählen Sie im Navigationsbereich der [Directory Service -Konsole](#) Directories aus.

2. Wählen Sie die Verzeichnis-ID des AWS verwalteten Microsoft AD-Verzeichnisses, das Sie teilen 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. Nachdem Sie die Informationen im Dialogfeld „Protokollweiterleitung deaktivieren“ gelesen haben, wählen Sie „Deaktivieren“.

Überwachen des DNS-Servers mit Microsoft Event Viewer

Sie können Ihre AWS verwalteten Microsoft AD-DNS-Ereignisse überprüfen, um DNS-Probleme leichter zu identifizieren und zu beheben. 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 erstellt](#).

So greifen Sie auf die Ereignisanzeige für Ihr AWS verwaltetes Microsoft AD-DNS zu

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Suchen Sie eine EC2 Amazon-Instance, die mit Ihrem AWS Managed Microsoft AD-Verzeichnis verknüpft ist. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Sobald Sie mit der EC2 Amazon-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 den Namen oder die IP-Adresse eines Ihrer AWS verwalteten Microsoft AD DNS-Server ein, und wählen Sie 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.

Zugriff auf AWS Anwendungen und Dienste von Ihrem AWS Managed Microsoft AD

Sie können Ihren AWS verwalteten Microsoft AD-Benutzern Zugriff auf AWS Anwendungen und Dienste gewähren. Einige dieser AWS Anwendungen und Dienste umfassen:

- Amazon Chime
- Amazon EC2
- Schnell
- AWS-Managementkonsole
- Amazon WorkSpaces

Sie können Access URLs und Single Sign-On auch mit Ihrem AWS Managed Microsoft AD verwenden.

Aufgaben für den Zugriff auf AWS Anwendungen und Dienste von AWS Managed Microsoft AD

- [Anwendungskompatibilität für AWS Managed Microsoft AD](#)
- [Aktivieren des Zugriffs auf AWS Anwendungen und Dienste für Ihr AWS Managed Microsoft AD](#)
- [AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren](#)
- [Zugriffs-URL für AWS Managed Microsoft AD erstellen](#)
- [Single Sign-On für AWS Managed Microsoft AD aktivieren](#)

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
- Amazon Connect
- Amazon EC2
- Schnell
- Amazon RDS
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS IAM Identity Center
- AWS License Manager
- AWS-Managementkonsole
- FSx für Windows-Dateiserver
- WorkSpaces

Weitere Informationen finden Sie unter [Aktivieren des Zugriffs auf AWS Anwendungen und Dienste für Ihr 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 als Azure 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 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 zu Ihrer Organisationseinheit finden Sie unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#).

- Schemaänderungen während des Installations-Workflows – Einige Active Directory-Anwendungen erfordern Änderungen am standardmäßigen Active Directory-Schema. Möglicherweise versuchen sie auch, diese Änderungen im Rahmen des Anwendungsinstallations-Workflows zu installieren. Aufgrund des privilegierten Charakters von Schemaerweiterungen AWS ist dies möglich, indem LDIF-Dateien (Lightweight Directory Interchange Format) nur über die 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. 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

Aktivieren des Zugriffs auf AWS Anwendungen und Dienste für Ihr AWS Managed Microsoft AD

Benutzer können AWS Managed Microsoft AD autorisieren, AWS Anwendungen und Diensten wie Amazon WorkSpaces Zugriff auf Ihr 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 unter Verbindung mit Active Directory herstellen.
Amazon Connect	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Connect .
Amazon EC2	Weitere Informationen finden Sie unter Möglichkeiten, eine Amazon EC2 EC2-Instanz mit Ihrem AWS Managed Microsoft AD zu verbinden .
Amazon FSx für Windows-Dateiserver	Weitere Informationen finden Sie unter Amazon FSx mit AWS Directory Service für Microsoft Active Directory verwenden.
Schnell	Weitere Informationen finden Sie unter Active Directory mit Quick Enterprise Edition verwenden .
Amazon Relational Database Service	Weitere Informationen finden Sie hier: • Kerberos-Authentifizierung für MySQL verwenden • Verwenden der Kerberos-Authentifizierung mit Amazon RDS for Oracle • Verwenden der Kerberos-Authentifizierung mit Amazon RDS for PostgreSQL

AWS Anwendung/Dienst	Weitere Informationen ...
	• Arbeiten mit AWS Managed Microsoft AD mit Amazon RDS for SQL Server
Amazon WorkDocs	Weitere Informationen finden Sie unter Amazon WorkDocs für AWS Managed Microsoft AD aktivieren .
Amazon WorkMail	Weitere Informationen finden Sie unter Organisation erstellen .
Amazon WorkSpaces	Sie können direkt von Simple AD, AWS Managed Microsoft AD oder AD Connector aus erstellen WorkSpaces. Starten Sie einfach Advanced Setup bei der Erstellung Ihres Workspace. Weitere Informationen finden Sie unter Registrieren eines vorhandenen Directory Service Verzeichnisses mit WorkSpaces Personal.
AWS Client VPN	Weitere Informationen finden Sie unter Active Directory-Authentifizierung in Client VPN .
AWS IAM Identity Center	Weitere Informationen finden Sie im Verzeichnis is Connect to a Microsoft AD .
AWS License Manager	Weitere Informationen finden Sie unter Benutzerbasierte Abonnements im License Manager verwalten .
AWS-Managementkonsole	Weitere Informationen finden Sie unter AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren .

AWS Anwendung/Dienst	Weitere Informationen ...
AWS Private Certificate Authority	Weitere Informationen finden Sie unter AWS Private CA Connector für Active Directory .
AWS Transfer Family	Weitere Informationen finden Sie unter Konfiguration eines SFTP-, FTPS- oder FTP-Serverendpunkts .

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.

Suchen Sie nach AWS Anwendungen und Diensten

Gehen Sie wie folgt vor, um die zuvor in der Directory Service Konsole beschriebenen AWS Anwendungen und Dienste zu finden.

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 Directory Service. [Autorisierung für AWS Anwendungen und Dienste, die Directory Service](#)

AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren

Directory Service ermöglicht es Ihnen, Mitgliedern Ihres Verzeichnisses Zugriff auf die zu gewähren AWS-Managementkonsole. Standardmäßig haben Ihre Verzeichnismitglieder keinen Zugriff auf AWS Ressourcen. Sie weisen Ihren Verzeichnismitgliedern IAM-Rollen zu, um ihnen Zugriff auf die verschiedenen AWS Dienste und Ressourcen zu gewähren. 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 [AWS Verwaltete Microsoft AD-Verzeichnisinformationen anzeigen](#). Weitere Informationen zum Erstellen einer Zugriffs-URL finden Sie unter [Zugriffs-URL für AWS Managed Microsoft AD erstellen](#).

Weitere Informationen zum Erstellen von IAM-Rollen und zum Zuweisen dieser Rollen zu den Mitgliedern Ihres Verzeichnisses finden Sie unter [Benutzern und Gruppen von AWS verwaltetem Microsoft AD Zugriff auf AWS Ressourcen mit IAM-Rollen gewähren](#).

Themen

- [Zugriff aktivieren AWS-Managementkonsole](#)
- [Zugriff wird deaktiviert AWS-Managementkonsole](#)
- [Länge der AWS-Managementkonsole Anmeldesitzung festlegen](#)

Verwandter Blogartikel zum Thema AWS Sicherheit

- [So greifen Sie AWS-Managementkonsole mithilfe von AWS verwaltetem Microsoft AD und Ihren lokalen Anmeldeinformationen auf](#)

Verwandter Artikel AWS re:Post

- [Wie kann ich lokalen Active Directory-Benutzern Zugriff auf die gewähren? AWS-Managementkonsole](#)

Note

Der Zugriff auf AWS-Managementkonsole ist eine regionale Funktion von AWS Managed Microsoft AD. Wenn Sie die [regionsübergreifende Replikation](#) verwenden, müssen die folgenden Verfahren in jeder Region separat angewendet werden. Weitere Informationen finden Sie unter [Globale und regionale Features](#).

Zugriff aktivieren AWS-Managementkonsole

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 Replikation mehrerer Regionen mehrere Regionen angezeigt werden, wählen Sie die Region aus, für die Sie den Zugriff aktivieren möchten AWS-Managementkonsole, und klicken Sie dann auf 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-Managementkonsole die Option Aktivieren aus. Der Konsolenzugriff ist jetzt für Ihr Verzeichnis aktiviert.

Important

Bevor sich Benutzer mit Ihrer Zugriffs-URL an der Konsole anmelden können, müssen Sie zuerst Ihre Benutzer zur IAM-Rolle hinzufügen. Weitere Informationen zum Zuweisen von Benutzern zu IAM-Rollen finden Sie unter [Zuweisen von Benutzern oder Gruppen zu einer vorhandenen IAM-Rolle](#). Nachdem die IAM-Rollen zugewiesen wurden, können die entsprechenden Benutzer über die Zugriffs-URL auf die Konsole zugreifen. Wenn Ihre Verzeichniszugriffs-URL beispielsweise lautet `example-corp.awsapps.com`, lautet die URL für den Zugriff auf die Konsole `https://example-corp.awsapps.com/console/`

Zugriff wird deaktiviert AWS-Managementkonsole

Gehen Sie wie folgt vor, um den AWS-Managementkonsole Zugriff für Ihre AWS verwalteten Microsoft AD-Verzeichnisbenutzer und -gruppen zu deaktivieren:

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 Replikation mehrerer Regionen mehrere Regionen angezeigt werden, wählen Sie die Region aus, für die Sie den Zugriff deaktivieren möchten AWS-Managementkonsole, und klicken Sie dann auf 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-Managementkonsole 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.

Länge der AWS-Managementkonsole Anmeldesitzung festlegen

Standardmäßig haben Benutzer nach erfolgreicher Anmeldung eine Stunde Zeit, um ihre Sitzung zu nutzen, AWS-Managementkonsole 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.

Um die Länge der AWS-Managementkonsole Anmeldesitzung festzulegen

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 Weiter aus.
- 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.

Zugriffs-URL für AWS Managed Microsoft AD erstellen

Eine Zugriffs-URL wird mit AWS Anwendungen und Diensten wie Amazon verwendet WorkDocs, um zu einer Anmeldeseite zu gelangen, die mit Ihrem Verzeichnis verknüpft ist. Folgen Sie der Anleitung unten, um eine Zugriffs-URL für Ihr Verzeichnis zu erstellen.

Überlegungen

- Die URL muss global eindeutig sein.
- Die Zugriffs-URL kann nur von der primären Region aus konfiguriert werden, wenn Sie Verzeichnisse mit mehreren Regionen verwenden.
- Sobald Sie eine Anwendungszugriffs-URL für dieses Verzeichnis erstellt haben, 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. 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` angezeigt. Standardmäßig werden Sie über diese URL zur Anmeldeseite für weitergeleitet. WorkDocs

Single Sign-On für AWS Managed Microsoft AD aktivieren

AWS Directory Service bietet die Möglichkeit, Ihren Benutzern den Zugriff 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 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 zu aktivieren oder zu deaktivieren mit 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 zu aktivieren. WorkDocs

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 [Zugriffs-URL für AWS Managed Microsoft AD erstellen](#).

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 zu einem späteren Zeitpunkt 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 zugelassenen 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](#)
- [Manuelles Update für Single Sign-On in OS X](#)
- [Gruppenrichtlinieneinstellungen für Single Sign-On](#)

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 [AuthServerAllowlist](#)Richtlinie 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 [AuthServerAllowlist](#)Richtlinie 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 *<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-Baumstruktur zu 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-Baumstruktur zu 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>) zur Liste der zugelassenen 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](https://support.mozilla.org/en-US/questions/939037).

Benutzern und Gruppen von AWS verwalteten Microsoft AD Zugriff auf AWS Ressourcen mit IAM-Rollen gewähren

AWS Directory Service bietet die Möglichkeit, Ihren AWS Managed Microsoft AD-Benutzern 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 gewähren [Identitätsbasierte 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-Managementkonsole. [AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren](#)

Themen

- [Eine neue IAM-Rolle erstellen](#)
- [Bearbeiten der Vertrauensbeziehung für eine bestehende IAM-Rolle](#)
- [Zuweisen von Benutzern oder Gruppen zu einer vorhandenen IAM-Rolle](#)
- [Anzeigen von Benutzern und Gruppen, die einer Rolle zugewiesen sind](#)
- [Einen Benutzer oder eine Gruppe aus einer IAM-Rolle entfernen](#)
- [Verwenden AWS verwalteter Richtlinien mit Directory Service](#)

Eine neue IAM-Rolle erstellen

Wenn Sie eine neue IAM-Rolle für die Verwendung mit erstellen müssen 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 Directory Service Konsole sehen können. Weitere Informationen finden Sie unter [Bearbeiten der Vertrauensbeziehung für eine bestehende IAM-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 \(AWS-Managementkonsole\)](#) 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. Amazon EC2 FullAccess), die Sie auf Ihre Verzeichnisbenutzer anwenden möchten, und wählen Sie dann Weiter aus.
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-Managementkonsole erstellen

Die folgende Checkliste enthält ein Beispiel für die Aufgaben, die Sie ausführen müssen, um eine neue IAM-Rolle zu erstellen, die bestimmten AWS Managed Microsoft AD-Benutzern Zugriff auf die Amazon EC2 EC2-Konsole gewährt.

1. Erstellen Sie eine Rolle mit der IAM-Konsole mit dem oben beschriebenen Verfahren. Wenn Sie nach einer Richtlinie gefragt werden, wählen Sie Amazon EC2 FullAccess.
2. Folgen Sie den Schritten unter [Bearbeiten der Vertrauensbeziehung für eine bestehende IAM-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-Managementkonsole im nächsten Schritt den Zugriff auf die aktiviert haben.
3. Folgen Sie den Anweisungen unter [AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren](#), um den allgemeinen Zugriff auf die AWS-Managementkonsole zu konfigurieren.

4. Folgen Sie den Anweisungen unter [Zuweisen von Benutzern oder Gruppen zu einer vorhandenen IAM-Rolle](#), um der neuen Rolle Benutzer hinzuzufügen, die Vollzugriff auf EC2-Ressourcen benötigen.

Bearbeiten der Vertrauensbeziehung für eine bestehende IAM-Rolle

Sie können Ihre vorhandenen IAM-Rollen Ihren Directory Service Benutzern und Gruppen zuweisen. Dazu muss die Rolle jedoch eine Vertrauensbeziehung mit Directory Service haben. Wenn Sie eine Rolle mithilfe des unter beschriebenen Verfahrens erstellen [Eine neue IAM-Rolle erstellen](#), wird diese Vertrauensstellung automatisch eingerichtet. Directory Service

Note

Sie müssen diese Vertrauensstellung nur für IAM-Rollen einrichten, die nicht von Directory Service erstellt wurden.

Um eine Vertrauensbeziehung für eine bestehende IAM-Rolle einzurichten, gehen Sie wie folgt vor Directory Service

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
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.

JSON

```
{
  "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 IAM-Rolle

Sie können einem AWS verwalteten Microsoft AD-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 IAM-Benutzer](#) oder [eine IAM-Gruppe](#).
- [Erstellen Sie eine Rolle](#), zu der eine Vertrauensbeziehung besteht. Directory Service Für bestehende IAM-Rollen müssen Sie [die Vertrauensbeziehung für eine bestehende Rolle bearbeiten](#).

Important

Der Zugriff für AWS verwaltete Microsoft AD-Benutzer in verschachtelten Gruppen innerhalb Ihres Verzeichnisses wird nicht unterstützt. Mitglieder übergeordneter Gruppen haben Konsolenzugriff, Mitglieder untergeordneter Gruppen nicht.

So weisen Sie AWS verwaltete Microsoft AD-Benutzer oder -Gruppen einer vorhandenen IAM-Rolle 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:
 - a. Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.
 - b. 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-ManagementkonsoleAbschnitt und 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-Managementkonsole benötigen. Weitere Informationen zum Konfigurieren einer vertrauenswürdigen Gesamtstruktur finden Sie unter [Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer selbstverwalteten Active Directory-Domäne](#).
8. Wählen Sie unter Specify, which users or groups to add (Angabe, 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 AWS verwalteten Microsoft AD-Benutzer und -Gruppen anzuzeigen, die einer IAM-Rolle zugewiesen sind.

Voraussetzungen

- [Erstellen Sie ein AWS verwaltetes Microsoft AD.](#)
- [Erstellen Sie einen IAM-Benutzer](#) oder [eine IAM-Gruppe](#).
- [Erstellen Sie eine Rolle](#), zu der eine Vertrauensbeziehung besteht. Directory Service Für bestehende IAM-Rollen müssen Sie [die Vertrauensbeziehung für eine bestehende Rolle bearbeiten](#).
- [Weisen Sie Ihre Benutzer oder Gruppen einer vorhandenen IAM-Rolle zu.](#)

So zeigen Sie AWS verwaltete Microsoft AD-Benutzer und Gruppen an, die einer IAM-Rolle zugewiesen sind

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:
 - a. 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](#).
 - b. Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.
4. Scrollen Sie nach unten zum AWS-ManagementkonsoleAbschnitt. Der Status sollte Aktiviert sein. Wenn nicht, wählen Sie Aktionen und Aktivieren. Weitere Informationen finden Sie unter [AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren](#).

Note

Sie werden keine Gruppen oder Benutzer sehen, wenn das deaktiviert AWS-Managementkonsole ist.

5. Wählen Sie im Abschnitt Delegate Console Access den Hyperlink der IAM-Rolle aus, die Sie anzeigen möchten. Alternativ können Sie Richtlinie in IAM anzeigen auswählen, um die IAM-Richtlinie in der IAM-Konsole anzuzeigen.

6. Auf der Seite Ausgewählte Rolle können Sie im Abschnitt Benutzer und Gruppen für diese Rolle verwalten die Benutzer und Gruppen anzeigen, die der IAM-Rolle zugewiesen sind.

Einen Benutzer oder eine Gruppe aus einer IAM-Rolle entfernen

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer oder eine verwaltete Microsoft AD-Gruppe aus einer IAM-Rolle zu entfernen.

So entfernen Sie einen Benutzer oder eine Gruppe aus einer IAM-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:
 - a. 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](#).
 - b. Wenn Sie unter Multi-Region-Replikation keine Regionen angezeigt bekommen, wählen Sie die Registerkarte Anwendungsverwaltung.
4. Wählen Sie im AWS-ManagementkonsoleAbschnitt die IAM-Rolle aus, aus der Sie Benutzer und Gruppen entfernen 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.

Note

Informationen zum Löschen einer Rolle finden Sie unter [Rollen oder Instanzprofile löschen](#).

Verwenden AWS verwalteter Richtlinien mit Directory Service

Directory Service bietet die folgenden AWS verwalteten Richtlinien, um Ihren Benutzern und Gruppen Zugriff auf AWS Dienste und Ressourcen zu gewähren, z. B. Zugriff auf die Amazon EC2 EC2-

Konsole. Sie müssen sich an der AWS-Managementkonsole anmelden, bevor Sie diese Richtlinien anzeigen können.

- [Schreibgeschützter Zugriff](#)
- [Power User Access](#)
- [Directory Service voller Zugriff](#)
- [Directory Service Nur-Lese-Zugriff](#)
- [AWS Vollzugriff auf Verzeichnisdienstdaten](#)
- [AWS Schreibgeschützter Zugriff auf Verzeichnisdienstdaten](#)
- [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](#)
- [AWS CloudTrail voller Zugriff](#)
- [AWS CloudTrail Nur-Lese-Zugriff](#)
- [CloudWatch Voller Zugriff auf Amazon](#)
- [Amazon hat nur CloudWatch Lesezugriff](#)
- [Amazon CloudWatch Logs Vollzugriff](#)
- [Amazon CloudWatch Logs nur Lesezugriff](#)

Weitere Informationen zum Erstellen eigener Richtlinien finden Sie unter [Beispielrichtlinien für die Verwaltung von AWS Ressourcen](#) im IAM-Benutzerhandbuch.

Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD

Die regionsübergreifende Replikation kann verwendet werden, um Ihre AWS verwalteten Microsoft AD-Verzeichnisdaten automatisch über mehrere zu replizieren. AWS-Regionen Diese Replikation kann die Leistung für Benutzer 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 Replikation mehrerer Regionen 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 Replikation mehrerer Regionen ist in Opt-in-Regionen nicht verfügbar. Bei den folgenden Regionen handelt es sich um optionale Regionen:

- 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
- Asien-Pazifik (Thailand) ap-southeast-7
- Kanada West (Calgary) ca-west-1
- Europa (Mailand) eu-south-1
- Europa (Spanien) eu-south-2
- Europa (Zürich) eu-central-2
- Zentral-Israel (Tel Aviv)
- Naher Osten (Bahrain) me-south-1
- Naher Osten (VAE) me-central-1
- Mexiko (Zentral) mx-central-1

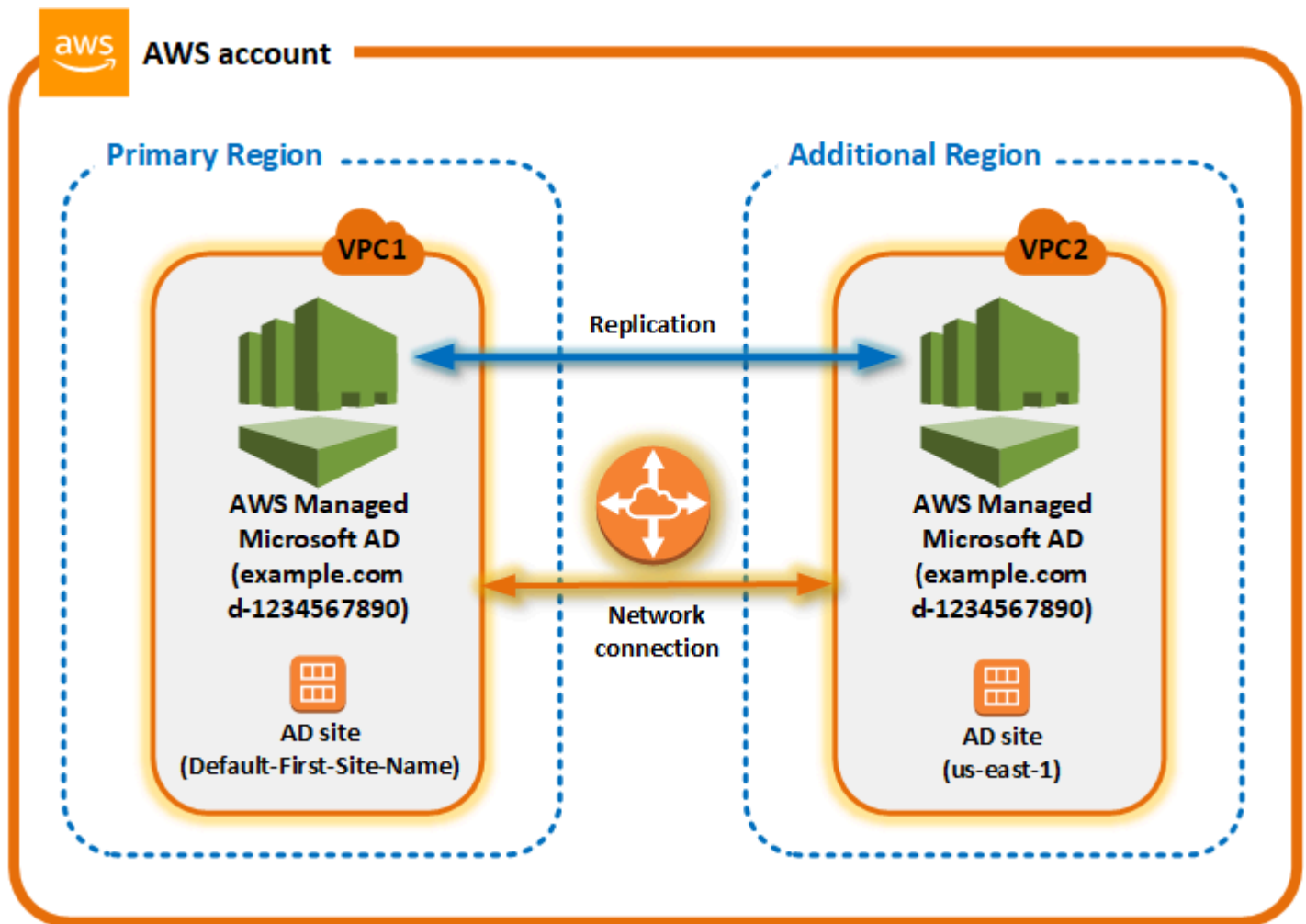
Weitere Informationen über Opt-in-Regionen und wie Sie sie aktivieren können, finden Sie unter [Festlegen, welche AWS-Regionen Ihr Konto verwenden kann](#) im AWS - Kontenverwaltung -Leitfaden.

So funktioniert die regionsübergreifende Replikation

Mit der Multi-Region-Replikationsfunktion macht AWS Managed Microsoft AD den undifferenzierten Aufwand der Verwaltung einer globalen Active Directory-Infrastruktur überflüssig. Wenn konfiguriert, AWS repliziert es alle Kundenverzeichnisdaten, einschließlich Benutzer, Gruppen, Gruppenrichtlinien und Schemas, über mehrere AWS-Regionen

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

- AWS Managed Microsoft AD erstellt zwei Domänencontroller in der ausgewählten VPC und stellt sie in der neuen Region mit demselben 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 den gleichen 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 regionsübergreifende 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 Dienste

AWS Dienste wie Amazon RDS for SQL Server und Amazon FSx stellen eine Verbindung zu den lokalen Instances des globalen Verzeichnisses her. Auf diese Weise können sich Ihre Benutzer einmalig bei Active Directory-fähigen Anwendungen anmelden, die in einer beliebigen AWS Region ausgeführt werden, AWS sowie bei AWS Diensten wie Amazon RDS for SQL Server. Dazu benötigen Benutzer Anmeldeinformationen von AWS Managed Microsoft AD oder lokalem Active Directory, wenn Sie Ihr AWS Managed Microsoft AD als vertrauenswürdig eingestuft haben.

Sie können die folgenden AWS Dienste mit der Replikationsfunktion für mehrere Regionen verwenden.

- Amazon EC2
- Amazon FSx für Windows-Dateiserver
- Amazon Relational Database Service 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 Domänencontroller in einer Region ausgefallen sind, stellt AWS Managed Microsoft AD die Domänencontroller wieder her und repliziert die Verzeichnisdaten automatisch. In der Zwischenzeit bleiben die Domain-Controller in anderen Regionen betriebsbereit.

Vorteile der Replikation in mehreren Regionen

Bei der Replikation mehrerer Regionen in AWS Managed Microsoft AD verwenden Active Directory-fähige Anwendungen das Verzeichnis lokal, um eine hohe Leistung zu erzielen, und die Multiregion-Funktion für mehr Stabilität. Sie können die regionsübergreifende Replikation mit Active Directory-fähigen Anwendungen wie SharePoint SQL Server Always On sowie mit AWS Diensten wie Amazon RDS for SQL Server und FSx für Windows File Server verwenden. Im Folgenden finden Sie weitere Vorteile der Multi-Region-Replikation.

- Damit können Sie schnell eine einzige AWS verwaltete Microsoft AD-Instanz global bereitstellen und die aufwändige Selbstverwaltung einer globalen Active Directory-Infrastruktur entfällt.
- Es macht es für Sie einfacher und kostengünstiger, Windows- und Linux-Workloads in mehreren AWS Regionen bereitzustellen und zu verwalten. Die automatisierte Replikation in mehreren Regionen ermöglicht eine optimale Leistung Ihrer globalen Active Directory-fähigen Anwendungen. Alle in Windows- oder Linux-Instances bereitgestellten Anwendungen 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. AWS Managed Microsoft AD wird in der hochverfügbaren AWS verwalteten Infrastruktur bereitgestellt und kümmert sich um 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](#)
- [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#)
- [Hinzufügen einer replizierten Region für AWS Managed Microsoft AD](#)
- [Löschen einer replizierten Region für AWS Managed Microsoft AD](#)

Globale und regionale Features

Wenn Sie Ihrem Verzeichnis mithilfe der Multiregions-Replikation eine AWS Region hinzufügen, wird der Umfang aller Funktionen Directory Service erweitert, sodass sie regionsabhängig werden. Diese Features sind auf verschiedenen Registerkarten der Detailseite aufgeführt, die angezeigt wird, wenn Sie die ID eines Verzeichnisses in der 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 Replikation mehrerer Regionen 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 Replikation mehrerer Regionen verwendet AWS Managed Microsoft AD die folgenden zwei Arten von Regionen, um zu unterscheiden, wie globale oder regionale Funktionen in Ihrem Verzeichnis angewendet werden sollten.

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 [Hinzufügen einer replizierten Region für AWS Managed Microsoft AD](#).

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.

Hinzufügen einer replizierten Region für AWS Managed Microsoft AD

Wenn Sie mithilfe der [Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD](#) Funktion eine Region hinzufügen, erstellt AWS Managed Microsoft AD zwei Domain-Controller in der ausgewählten AWS Region, Amazon Virtual Private Cloud (VPC) und im Subnetz. AWS Managed Microsoft AD erstellt auch die zugehörigen Sicherheitsgruppen, die es Windows-Workloads ermöglichen, eine Verbindung zu Ihrem Verzeichnis in der neuen Region herzustellen. Außerdem werden diese Ressourcen mit demselben AWS -Konto erstellt, auf dem Ihr Verzeichnis bereits bereitgestellt wurde. Dazu wählen Sie die Region aus, geben die VPC an und geben die Konfigurationen für die neue Region an.

Die Replikation mehrerer Regionen 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, das Amazon VPC-Setup und das Subnetz-Setup in der neuen Region verfügen, in die Sie das Verzeichnis replizieren möchten.
- Wenn Sie Ihre vorhandenen lokalen Active Directory-Anmeldeinformationen verwenden möchten, um auf Active Directory-fähige Workloads zuzugreifen und diese zu verwalten AWS, müssen Sie eine Active Directory-Vertrauensstellung zwischen AWS Managed Microsoft AD und Ihrer lokalen AD-Infrastruktur einrichten. Weitere Informationen über Vertrauensstellungen finden Sie unter [Connect AWS Managed Microsoft AD mit Ihrer vorhandenen Active Directory-Infrastruktur](#).
- Wenn Sie über eine bestehende Vertrauensstellung zwischen Ihrem lokalen Active Directory verfügen und eine replizierte Region hinzufügen möchten, müssen Sie sicherstellen, dass Sie in der neuen Region, in die Sie das Verzeichnis replizieren möchten, über die erforderliche Amazon VPC- und Subnetzkonfiguration verfügen.

Sie können auch eine Vertrauensstellung zwischen Ihrem AWS verwalteten Microsoft AD und der lokalen AD-Infrastruktur einrichten, sodass Sie vorhandene lokale Active Directory-Anmeldeinformationen verwenden können, um AD-fähige Workloads zu verwalten. Weitere Informationen finden Sie unter [Connect AWS Managed Microsoft AD mit Ihrer vorhandenen Active Directory-Infrastruktur](#).

Eine Region hinzufügen

Gehen Sie wie folgt vor, um eine replizierte Region für Ihr AWS verwaltetes Microsoft AD-Verzeichnis 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 für den Domänencontroller 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 [Hinzufügen oder Entfernen zusätzlicher Domänencontroller mit dem AWS-Managementkonsole](#).

Note

Wenn Sie Ihrem AWS verwalteten Microsoft AD ein AWS-Region Replikat hinzufügen, werden standardmäßig zwei Domänencontroller erstellt. Dies ist die Mindestanzahl von Domänencontrollern, die für Fehlertoleranz und Hochverfügbarkeit erforderlich ist.

- Teilen Sie Ihr Verzeichnis mit mehr AWS Konten pro Region. Konfigurationen für die Verzeichnisfreigabe werden nicht automatisch von der primären Region repliziert. Weitere Informationen finden Sie unter [Teilen Sie Ihr AWS verwaltetes Microsoft AD](#).

Note

Konfigurationen für die gemeinsame Nutzung von Verzeichnissen werden in der AWS-Region Primärversion nicht automatisch repliziert.

- Aktivieren Sie die Protokollweiterleitung, um die Sicherheitsprotokolle Ihres Verzeichnisses mithilfe von 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 [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#).

Note

Wenn Sie die Protokollweiterleitung aktivieren, müssen Sie einen Namen für die Protokollgruppe in jeder AWS-Region Protokollgruppe angeben, in die Sie Ihr Verzeichnis repliziert haben.

- 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 [Statusbenachrichtigungen für AWS verwaltete Microsoft AD-Verzeichnisse mit Amazon Simple Notification Service aktivieren](#).

Löschen einer replizierten Region für AWS Managed Microsoft AD

Gehen Sie wie folgt vor, um eine Region für Ihr AWS verwaltetes Microsoft AD-Verzeichnis 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 aus.

Note

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

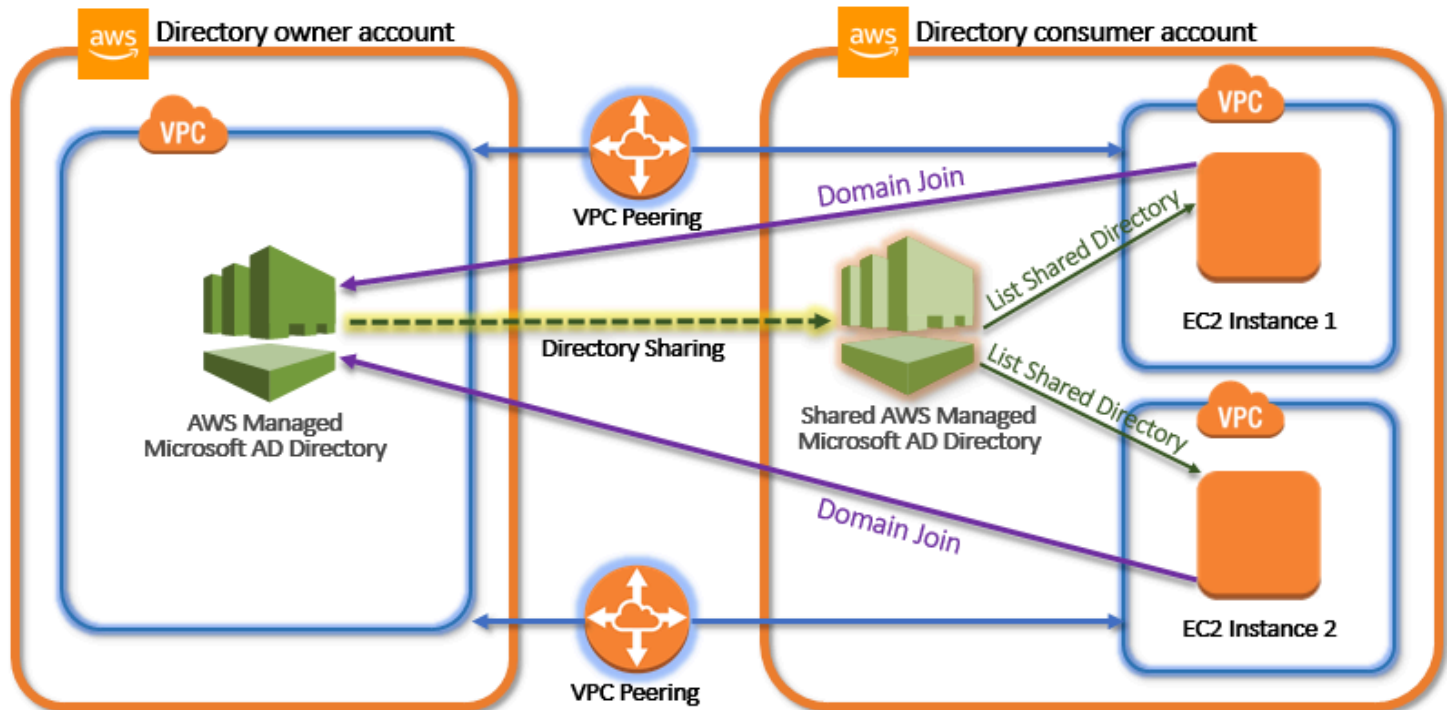
Teilen Sie Ihr AWS verwaltetes Microsoft AD

AWS Managed Microsoft AD ist eng in Microsoft AD integriert AWS Organizations , um eine nahtlose gemeinsame Nutzung von Verzeichnissen durch mehrere zu ermöglichen AWS-Konten. Sie können ein einzelnes Verzeichnis mit anderen vertrauenswürdigen Personen AWS-Konten innerhalb derselben Organisation teilen oder das Verzeichnis mit anderen Personen AWS-Konten außerhalb

Ihrer Organisation gemeinsam nutzen. Sie können Ihr Verzeichnis auch dann teilen, wenn Sie AWS-Konto derzeit kein Mitglied einer Organisation sind.

Schlüsselkonzepte der Verzeichnisfreigabe

Sie werden mehr aus der Funktion zur gemeinsamen Nutzung von Verzeichnissen herausholen, wenn Sie sich mit den folgenden Schlüsselkonzepten vertraut machen.



Konto des Verzeichniseigentümers

Ein Verzeichnisbesitzer ist der AWS-Konto Inhaber, dem das ursprüngliche Verzeichnis in der Beziehung zum gemeinsamen Verzeichnis gehört. Ein Administrator dieses Kontos initiiert den Workflow zur gemeinsamen Nutzung von Verzeichnissen, indem er angibt, AWS-Konten für wen das Verzeichnis freigegeben werden soll. Verzeichniseigentümer können auf der Registerkarte **Scale & Share** (Skalieren und Freigeben) für ein bestimmtes Verzeichnis in der 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 zwei Methoden zur gemeinsamen Nutzung von Verzeichnissen:

- **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 Methode der gemeinsamen Nutzung vereinfacht Ihre Einrichtung, da die Verzeichnisnutzerkonten nicht erforderlich sind, um Ihre Anfrage zur gemeinsamen Nutzung von Verzeichnissen anzunehmen. In der Konsole wird diese Methode AWS-Konten innerhalb Ihrer Organisation als „Dieses Verzeichnis teilen“ bezeichnet.
- **Handshake** — Diese Methode ermöglicht die gemeinsame Nutzung von Verzeichnissen, wenn Sie sie nicht verwenden AWS Organizations. 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.

Netzwerkverbindbarkeit

Netzwerkverbindbarkeit ist eine Grundvoraussetzung für die Nutzung einer Beziehung zur gemeinsamen Nutzung von Verzeichnissen zwischen AWS-Konten. AWS [unterstützt viele Verbindungslösungen VPCs, darunter VPC-Peering, Transit Gateway und VPN](#). Um zu beginnen, sehen Sie sich [Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt](#) an.

Überlegungen

Im Folgenden finden Sie einige Überlegungen bei der Verwendung von Directory Share mit Ihrem AWS verwalteten Microsoft AD:

Preisgestaltung

- AWS erhebt eine zusätzliche Gebühr für die gemeinsame Nutzung von Verzeichnissen. Derjenige AWS-Konto, der das gemeinsam genutzte AWS Managed Microsoft AD verwendet, ist das Konto, für das die Sharing-Gebühren berechnet wurden. Weitere Informationen finden Sie auf der Seite mit den [Preisen](#) auf der Directory Service Website.
- Durch die gemeinsame Nutzung von Verzeichnissen ist AWS Managed Microsoft AD eine kostengünstigere Möglichkeit der Integration mit Amazon EC2 in mehreren Konten und VPCs.

Verfügbarkeit in Regionen

- Die gemeinsame Nutzung von Verzeichnissen ist in allen [AWS Regionen verfügbar, in denen AWS Managed Microsoft AD](#) angeboten wird.
- In AWS China (Ningxia) ist diese Funktion nur verfügbar, wenn Sie [AWS Systems Manager](#) (SSM) verwenden, um Ihre Amazon EC2 EC2-Instances nahtlos zu verbinden.

Weitere Informationen zur gemeinsamen Nutzung von Verzeichnissen und zur Erweiterung der Reichweite Ihres AWS verwalteten Microsoft AD-Verzeichnisses über AWS Kontogrenzen hinweg finden Sie in den folgenden Themen.

Themen

- [Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt](#)
- [Die Freigabe Ihres Verzeichnisses aufheben](#)

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

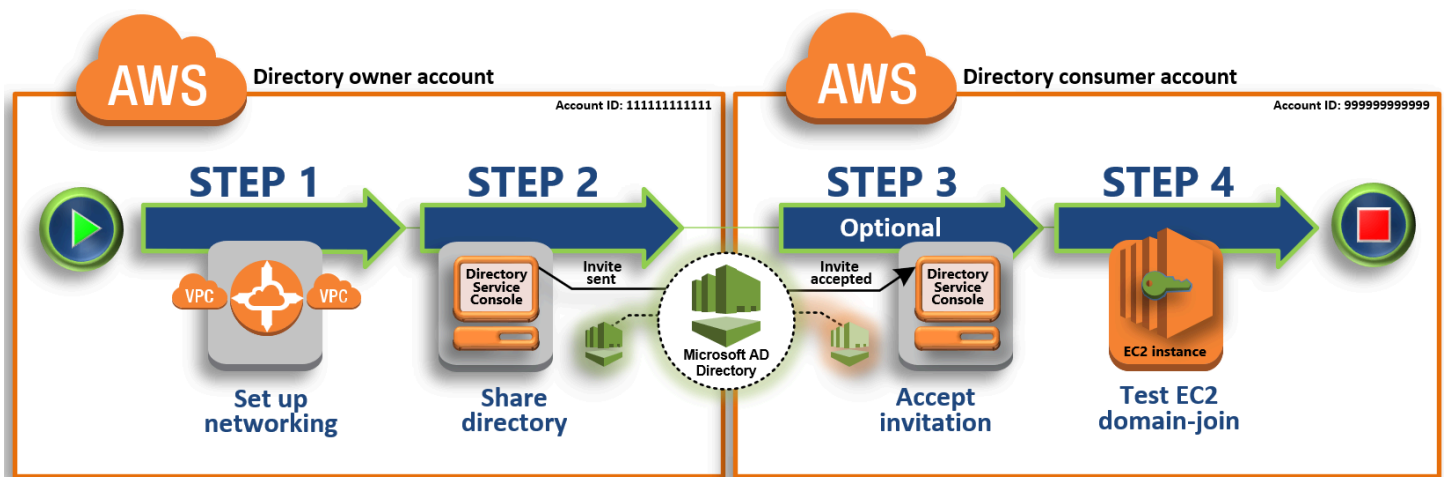
Dieses Tutorial zeigt Ihnen, wie Sie Ihr AWS verwaltetes Microsoft AD-Verzeichnis (das Verzeichnisbesitzerkonto) mit einem anderen AWS-Konto (dem Verzeichnisverbraucherkonto) teilen können. Sobald die Netzwerkvoraussetzungen erfüllt sind, teilen Sie sich ein Verzeichnis für zwei

Personen AWS-Konten. Anschließend erfahren Sie, wie Sie eine EC2-Instance nahtlos mit einer Domain im Directory-Benutzerkonto verbinden können.

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](#).

Der Prozess für die gemeinsame Nutzung Ihres Verzeichnisses hängt davon ab, ob Sie das Verzeichnis mit einem anderen AWS-Konto in derselben AWS Organisation oder mit einem Konto außerhalb der AWS Organisation teilen. 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 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 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 aus VPCs mit einem einzigen AWS verwalteten Microsoft AD-Verzeichnis](#)

Schritt 1: Ihre Netzwerkumgebung einrichten

Sie müssen eine Amazon VPC-Peering-Verbindung einrichten, um Ihr AWS verwaltetes Microsoft AD-Verzeichnis (Verzeichniskontoinhaber) mit einem anderen AWS-Konto (Directory-Consumer-Konto) zu teilen. In den folgenden Verfahren finden Sie Schritte zum Einrichten Ihrer Netzwerkumgebung für ein gemeinsam genutztes AWS verwaltetes Microsoft AD.

Voraussetzungen

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 ein AWS verwaltetes Microsoft AD.](#)
- Beim Erstellen einer VPC-Peering-Verbindung benötigen sowohl der Besitzer des Verzeichniskontos als auch das Verzeichnisverbraucherkonto die erforderlichen Berechtigungen, um die Peering-Verbindung herzustellen und zu akzeptieren. Weitere Informationen finden Sie unter [Beispiel: Eine VPC-Peering-Verbindung erstellen](#) und [Beispiel: Eine VPC-Peering-Verbindung akzeptieren](#).

 Note

Es gibt zwar viele Möglichkeiten, den Verzeichnisbesitzer und das Directory-Benutzerkonto zu verbinden VPCs, in diesem Tutorial wird jedoch die VPC-Peering-Methode verwendet. Weitere VPC-Konnektivitätsoptionen finden Sie unter [Netzwerk-konnektivität](#).

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

Die VPC-Peering-Verbindung, die Sie erstellen, besteht zwischen dem Verzeichnisverbraucher und dem Verzeichnisbesitzer. VPCs Führen Sie die folgenden Schritte zum Konfigurieren einer VPC-Peering-Verbindung für Konnektivität mit dem Verzeichniskonsumentenkonto durch. Mit dieser Verbindung können Sie den Verkehr zwischen beiden VPCs mithilfe 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/>. Stellt sicher, dass Sie sich als Benutzer mit Administratoranmeldedaten im Verzeichnisbesitzerkonto anmelden und über die erforderlichen Berechtigungen verfügen, um eine VPC-Peering-Verbindung herzustellen. Weitere Informationen finden Sie unter [Voraussetzungen](#).
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.

So akzeptieren Sie die Peering-Anfrage im Namen des Verzeichniskonsumentenkontos

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>. Stellt sicher, dass Sie sich als Benutzer mit den erforderlichen Berechtigungen anmelden, um die Peering-Anfrage anzunehmen. Weitere Informationen finden Sie unter [Voraussetzungen](#).
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.

Fügen Sie Active Directory-Protokolle und -Ports zu den ausgehenden Regeln für Sicherheitsgruppen in Directory Consumer hinzu. VPCs 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 die [regionsübergreifende 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-Managementkonsole mit Administratoranmeldedaten im Konto des Verzeichnisbesitzers an und öffnen Sie die [AWS Directory Service Konsole](https://console.aws.amazon.com/directoryservicev2/) 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) und 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, 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 im Feld AWS-Konto ID (s) alle Namen ein AWS-Konto IDs , mit denen Sie das Verzeichnis teilen möchten, und 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-Managementkonsole 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 an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole 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 heruntergeladen. 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:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

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-Instance-Profil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien Amazon SSMManaged InstanceCore und Amazon SSMDirectory ServiceAccess zugeordnet 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 unter Berechtigungen hinzufügen in der Liste der Richtlinien die SSMDirectory ServiceAccess Richtlinien von Amazon SSMManged InstanceCore und Amazon aus. Geben Sie im Suchfeld **SSM** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

 Note

Amazon SSMDirectory ServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einem Active Directory, das von verwaltet wird Directory Service. Amazon SSMManged InstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des AWS Systems Manager Dienstes erforderlich sind. 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 Domain-Join mit AWS Systems Manager

Verwenden Sie diese Schritte im Konto des Verzeichnisverbrauchs. Um dieses Verfahren abzuschließen, benötigen Sie einige Informationen über das Konto des Verzeichnisbesitzers, z. B. 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 Amazon SSMManged InstanceCore und Amazon SSMDirectory ServiceAccess 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 unter <https://console.aws.amazon.com/systems-manager/>.
2. Wählen Sie im Navigationsbereich unter Knotenverwaltung die Option Befehl ausführen.
3. Wählen Sie 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 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 für Verzeichnis-ID den Namen des AWS Managed 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 AWS verwalteten Microsoft AD-Verzeichnisses 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 AWS verwalteten Microsoft AD-Verzeichnisses 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: Geben Sie Ihr Verzeichnis frei, um Amazon EC2-Instances kontenübergreifend AWS nahtlos mit einer Domain zu verbinden](#)
- [AWS Blogartikel zum Thema Sicherheit: So verbinden Sie Amazon EC2 EC2-Instances von mehreren Konten aus VPCs mit einem einzigen AWS verwalteten Microsoft AD-Verzeichnis](#)
- [Kontenübergreifendes Verbinden Ihrer Amazon-RDS-DB-Instances mit einer einzelnen freigegebenen Domain](#)

Migration von Active Directory-Benutzern zu AWS Managed Microsoft AD

Sie können den 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.

Ausführliche Anweisungen finden Sie im AWS Sicherheitsblog unter [So migrieren Sie Ihre lokale Domäne mithilfe von ADMT zu AWS Managed Microsoft AD](#).

Connect AWS Managed Microsoft AD mit Ihrer vorhandenen Active Directory-Infrastruktur

In diesem Abschnitt wird beschrieben, wie Sie Vertrauensbeziehungen zwischen AWS Managed Microsoft AD und Ihrer vorhandenen Active Directory-Infrastruktur konfigurieren.

Aufgaben zum Verbinden Ihres AWS Managed Microsoft AD mit Ihrem vorhandenen Active Directory:

- [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#)

- [Hinzufügen von IP-Routen bei der Verwendung öffentlicher IP-Adressen mit Ihrem AWS verwalteten Microsoft AD](#)
- [Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer selbstverwalteten Active Directory-Domäne](#)
- [Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen zwei AWS verwalteten Microsoft AD-Domänen](#)

Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD

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 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: Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer selbstverwalteten Active Directory-Domäne](#).

Für AWS Unternehmens-Apps wie Amazon Chime, Amazon Connect, Quick,, Amazon, Amazon und die ist eine bidirektionale Vertrauensstellung WorkSpaces erforderlich. AWS IAM Identity Center WorkDocs WorkMail AWS-Managementkonsole AWS Managed Microsoft AD muss in der Lage sein, die Benutzer und Gruppen in Ihrem selbstverwalteten Active Directory abzufragen.

Sie können die selektive Authentifizierung aktivieren, sodass nur das AWS anwendungsspezifische Dienstkonto Ihr selbstverwaltetes Active Directory abfragen kann. Weitere Informationen finden Sie unter [Verbessern Sie die Sicherheit Ihrer AWS App-Integration mit AWS Managed Microsoft AD](#).

Amazon EC2, Amazon RDS und Amazon FSx arbeiten 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 Quick zu verwenden, müssen Sie Port 9389 zulassen. Weitere Informationen zu Active Directory-Ports und -Protokollen finden Sie in der [Dokumentation unter Serviceübersicht und Anforderungen an Netzwerkports](#). 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 Ihres Verzeichnisses vertraut](#).
6. Wählen Sie Speichern aus.

Kerberos-Vorabauthentifizierung aktivieren

Auf Ihren Benutzerkonten muss die Kerberos-Vorabauthentifizierung aktiviert sein. Weitere Informationen zu dieser Einstellung finden Sie unter [Vorabauthentifizierung](#) bei Microsoft TechNet.

DNS-bedingte Weiterleitung 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-Managementkonsole 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 [Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD](#) 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 Vertrauentyps, 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 selbstveraltetes 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 unidirektionale Vertrauensstellung in der „eingehenden Richtung“ verfügen und anschließend eine weitere Vertrauensstellung in der „ausgehenden Richtung“ einrichten möchten, müssen Sie die bestehende Vertrauensstellung löschen und eine neue „bidirektionale“ Vertrauensstellung 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 aus.

Hinzufügen von IP-Routen bei der Verwendung öffentlicher IP-Adressen mit Ihrem AWS verwalteten Microsoft AD

Sie können den AWS Directory Service für Microsoft Active Directory verwenden, um viele leistungsstarke Active Directory-Funktionen zu nutzen, einschließlich der 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 [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#).

In ähnlicher Weise müssen Sie auch die IP-Adressinformationen eingeben, wenn Sie den Datenverkehr von Ihrem AWS verwalteten Microsoft AD AWS an eine AWS Peer-VPC weiterleiten, wenn die VPC öffentliche IP-Bereiche verwendet.

Wenn Sie die IP-Adressen wie in [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#) 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 Ihres Verzeichnisses vertraut](#).

Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer selbstverwalteten Active Directory-Domäne

Dieses Tutorial führt Sie durch alle Schritte, die zum Einrichten einer Vertrauensstellung zwischen dem AWS Directory Service für Microsoft Active Directory und Ihrem selbstverwalteten (lokalen) Microsoft Active Directory erforderlich sind. Eine Vertrauensstellung zu erstellen, erfordert nur wenige Schritte, jedoch müssen Sie zuerst die folgenden vorbereitenden Schritte ausführen.

Themen

- [Voraussetzungen](#)
- [Schritt 1: Selbstverwaltete AD-Domain vorbereiten](#)
- [Schritt 2: Bereiten Sie Ihr AWS verwaltetes Microsoft AD vor](#)
- [Schritt 3: Eine Vertrauensstellung einrichten](#)

Weitere Informationen finden Sie auch unter:

[Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#)

Voraussetzungen

In dieser praktischen Anleitung wird davon ausgegangen, dass Sie bereits über folgende Elemente verfügen:

Note

AWS Managed Microsoft AD unterstützt kein Vertrauen in [Single-Label-Domains](#).

- Ein AWS verwaltetes Microsoft AD-Verzeichnis, das am erstellt wurde AWS. Weitere Informationen hierzu finden Sie unter [Erste Schritte mit AWS Managed Microsoft AD](#).

- Eine laufende EC2-Instanz Windows wurde zu diesem AWS Managed Microsoft AD hinzugefügt. Weitere Informationen hierzu finden Sie unter [Hinzufügen einer Amazon EC2 Windows-Instanz zu Ihrem AWS verwalteten Microsoft AD Active Directory](#).

 Important

Das Administratorkonto für Ihr AWS verwaltetes Microsoft AD muss Administratorzugriff auf diese Instanz haben.

- Die folgenden Windows Servertools sind auf dieser Instanz installiert:
 - AD DS- und AD LDS-Tools
 - DNS

Weitere Informationen hierzu finden Sie unter [Installation der Active Directory-Verwaltungstools für AWS verwaltetes Microsoft AD](#).

- Ein selbstverwaltetes (On-Premises) Microsoft Active Directory

Sie müssen Administratorzugriff auf dieses Verzeichnis haben. Dieselben Windows Servertools wie oben aufgeführt müssen auch für dieses Verzeichnis verfügbar sein.

- Eine aktive Verbindung zwischen Ihrem selbstverwalteten Netzwerk und der VPC, die Ihr AWS verwaltetes 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 [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#).

Praktische Anleitung zur Konfiguration

Für dieses Tutorial haben wir bereits ein AWS verwaltetes 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 Verwaltetes Microsoft AD läuft auf AWS

- Domänenname (FQDN): MyManaged AD.Example.com
- NetBIOS-Name: AD MyManaged
- DNS-Adressen: 10.0.10.246, 10.0.20.121
- VPC-CIDR: 10.0.0.0/16

Das AWS verwaltete Microsoft AD befindet sich in der VPC-ID: vpc-12345678.

Selbstverwaltete oder AWS verwaltete 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 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 Quick verwenden möchten.)

 Note

SMBv1 wird nicht mehr unterstützt.

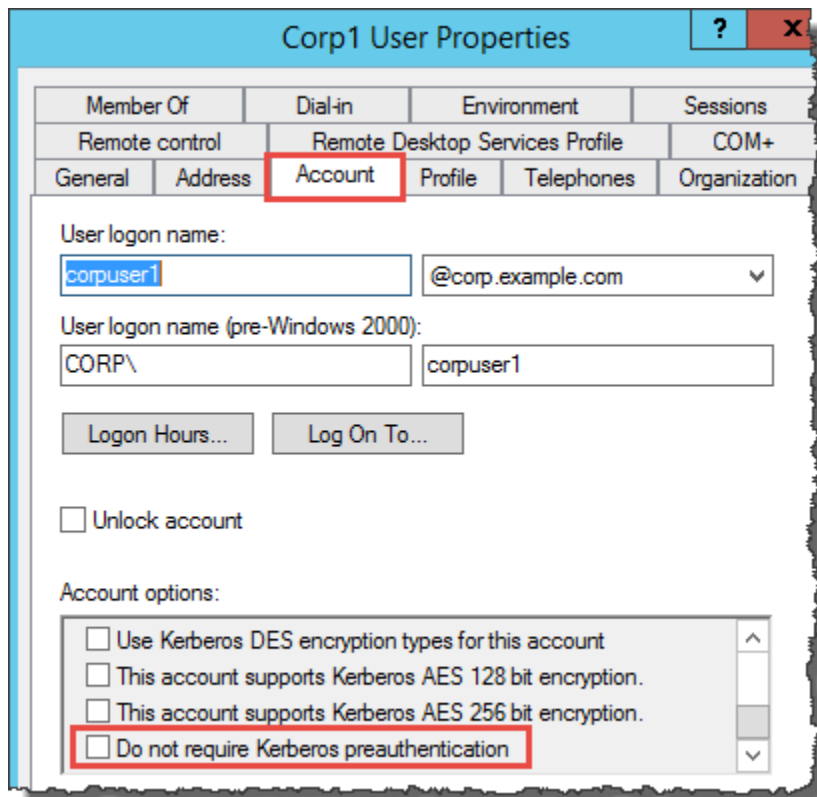
Dies sind die minimalen Ports, die für die Verbindung der VPC mit dem selbstverwalteten Verzeichnis notwendig sind. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports.

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-Managementkonsole 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 CN7 VJ0 WIN-5V70 .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 Domännennamen (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.

New Conditional Forwarder

DNS Domain:
MyManagedAD.example.com

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add a...>		
10.0.10.246	<Unable to resolve>	A timeout occurred duri...
10.0.20.121	<Unable to resolve>	A timeout occurred duri...

☒ Store this conditional forwarder in Active Directory, and replicate it as follows:
All DNS servers in this domain

This will not replicate to DNS Servers that are pre-Windows Server 2003 Domain Controllers

Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

OK Cancel

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: Bereiten Sie Ihr AWS verwaltetes Microsoft AD vor](#)

Schritt 2: Bereiten Sie Ihr AWS verwaltetes Microsoft AD vor

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 mit den Subnetzen, die für die Bereitstellung Ihres AWS verwalteten Microsoft AD verwendeten Subnetzes ACLs verknüpft sind, 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

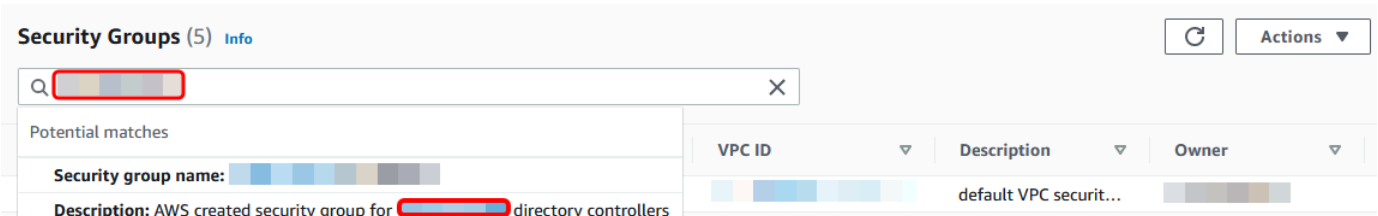
- ALL

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 Ihre ausgehenden und eingehenden 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 Ihres Verzeichnisses vertraut](#).

6. Wählen Sie Regel speichern aus.

Edit outbound rules^{info}

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules^{info}

Security group rule ID	Type ^{info}	Protocol ^{info}	Port range ^{info}	Destination ^{info}	Description - optional ^{info}
	All traffic	All	All	Anywhere...	

0.0.0.0/0 X

Add rule

Cancel Preview changes Save rules

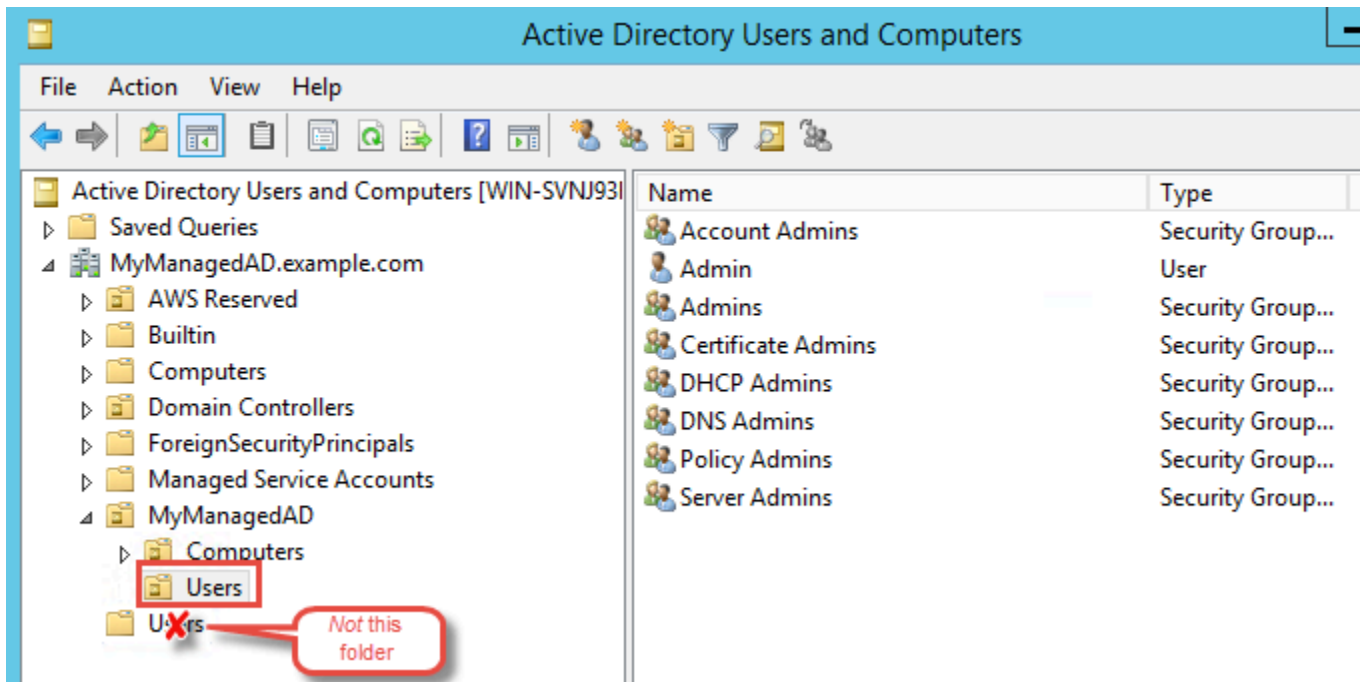
Sicherstellen, dass Kerberos-Vorauthentifizierung aktiviert ist

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 [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#) 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 [Installation der Active Directory-Verwaltungstools für AWS verwaltetes 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 das Vertrauen für Ihre selbstverwaltete Domain und dann schließlich für Ihr AWS verwaltetes 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 eine unidirektionale, ausgehende Vertrauensstellung für Ihre selbstverwaltete Domain einrichten, müssen Sie eine unidirektionale, eingehende Vertrauensstellung für Ihr AWS verwaltetes Microsoft AD einrichten.

 Note

AWS Managed Microsoft AD unterstützt auch externe Vertrauensstellungen. Für dieses Tutorial erstellen Sie jedoch eine bidirektionale Gesamtstruktur-Vertrauensstellung.

Um die Vertrauensstellung in Ihrem selbstverwalteten Active Directory zu konfigurieren

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 Ihres AWS verwalteten Microsoft AD ein und wählen Sie Weiter.
4. Wählen Sie Forest trust. Wählen Sie Weiter aus.
5. Wählen Sie Two-way. Wählen Sie Weiter aus.
6. Wählen Sie This domain only. Wählen Sie Weiter aus.
7. Wählen Sie Forest-wide authentication. Wählen Sie Weiter aus.
8. Geben Sie ein Trust password ein. Denken Sie daran, sich dieses Passwort zu merken, da Sie es benötigen, wenn Sie den Trust für Ihr AWS Managed Microsoft AD einrichten.
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 aus.
11. Wählen Sie No, do not confirm the incoming trust. Wählen Sie Weiter aus.

Konfigurieren Sie die Vertrauensstellung in Ihrem AWS verwalteten Microsoft AD-Verzeichnis

Schließlich konfigurieren Sie die Gesamtstrukturvertrauensstellung mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis. Da Sie für die selbstverwaltete Domäne eine bidirektionale Gesamtstrukturvertrauensstellung eingerichtet haben, erstellen Sie auch eine bidirektionale Vertrauensstellung mithilfe Ihres AWS verwalteten Microsoft AD-Verzeichnisses.

 Note

Vertrauensbeziehungen sind eine globale Funktion von AWS Managed Microsoft AD. Wenn Sie [Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD](#) 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 AWS verwalteten Microsoft AD-Verzeichnis

1. Kehren Sie zur [AWS Directory Service -Konsole](#) zurück.
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 Vertrauensstellung hinzufügen den Vertrauentyp 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 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 beispielsweise 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 [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#).

Tutorial: Erstellen Sie eine Vertrauensbeziehung zwischen zwei AWS verwalteten Microsoft AD-Domänen

Dieses Tutorial führt Sie durch alle Schritte, die zum Einrichten einer Vertrauensstellung zwischen zwei AWS Directory Service für Microsoft Active Directory-Domänen erforderlich sind.

Themen

- [Schritt 1: Bereiten Sie Ihr AWS verwaltetes Microsoft AD vor](#)
- [Schritt 2: Erstellen Sie die Vertrauensbeziehung mit einer anderen AWS verwalteten Microsoft AD-Domäne](#)

Weitere Informationen finden Sie auch unter:

[Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#)

Schritt 1: Bereiten Sie Ihr AWS verwaltetes Microsoft AD vor

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: Erstellen Sie eine Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und Ihrer selbstverwalteten Active Directory-Domäne](#) 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 mit den

Subnetzen, die für die Bereitstellung Ihres AWS verwalteten Microsoft AD verwendeten Subnetzes ACLs verknüpft sind, 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 Mindestports, die erforderlich sind, um VPCs von beiden AWS verwalteten Microsoft ADs aus eine Verbindung herstellen zu können. Ihre spezifische Konfiguration erfordert möglicherweise die Öffnung zusätzlicher Ports. Weitere Informationen finden Sie

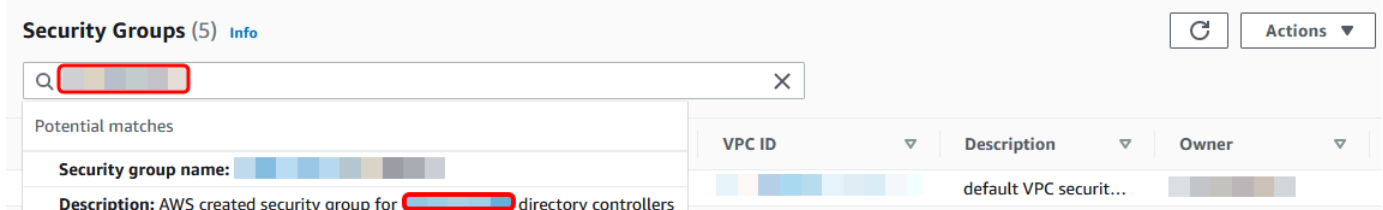
unter [Konfigurieren einer Firewall für Active-Directory-Domains und -Vertrauensstellungen](#) auf der Website von Microsoft.

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 Ihres Verzeichnisses vertraut](#).
6. Wählen Sie Speichern aus.

Edit outbound rules^{info}

Outbound rules control the outgoing traffic that's allowed to leave the instance.

Outbound rules

Security group rule ID	Type	Protocol	Port range	Destination	Description - optional
	All traffic	All	All	Anywhere...	

0.0.0.0/0 X

Add rule

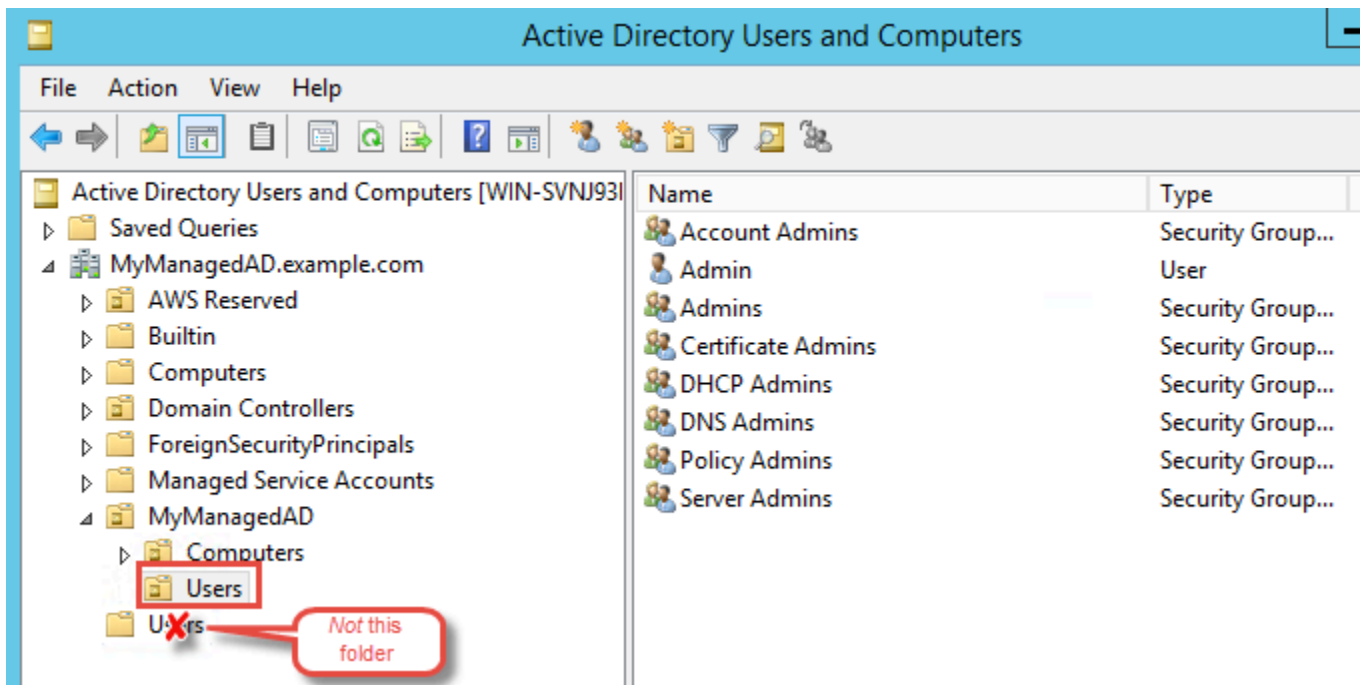
Cancel Preview changes Save rules

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 [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#) 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 [Installation der Active Directory-Verwaltungstools für AWS verwaltetes 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: Erstellen Sie die Vertrauensbeziehung mit einer anderen AWS verwalteten Microsoft AD-Domäne

Schritt 2: Erstellen Sie die Vertrauensbeziehung mit einer anderen AWS verwalteten Microsoft AD-Domäne

Nachdem die Vorbereitungsarbeiten abgeschlossen sind, bestehen die letzten Schritte darin, die Vertrauensstellungen zwischen Ihren beiden AWS verwalteten Microsoft AD-Domänen herzustellen. Wenn während der Erstellung von Vertrauensstellungen Probleme auftreten, finden Sie weitere Informationen unter [Gründe für den Status der Vertrauensstellung](#).

Konfigurieren Sie das Vertrauen in Ihrer ersten AWS verwalteten Microsoft AD-Domain

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 für diese erste Domäne eine unidirektionale, ausgehende Vertrauensstellung einrichten, müssen Sie eine unidirektionale, eingehende Vertrauensstellung für Ihre zweite AWS verwaltete Microsoft AD-Domäne einrichten.

 Note

AWS Managed Microsoft AD unterstützt auch externe Vertrauensstellungen. Für dieses Tutorial erstellen Sie jedoch eine bidirektionale Gesamtstruktur-Vertrauensstellung.

So konfigurieren Sie das Vertrauen in Ihrer ersten AWS verwalteten Microsoft AD-Domäne

1. Öffnen Sie die [AWS Directory Service -Konsole](#).
2. Wählen Sie auf der Seite Verzeichnisse Ihre erste 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 Vertrauensstellung hinzufügen den FQDN Ihrer zweiten AWS verwalteten Microsoft AD-Domäne ein. Denken Sie daran, sich dieses Passwort zu merken, da Sie es benötigen, wenn Sie den Trust für Ihr zweites AWS Managed Microsoft AD einrichten. Geben Sie die Richtung an. In diesem Fall wählen wir Zwei-Wege aus.
6. Geben Sie im Feld Conditional Forwarder die IP-Adresse Ihres zweiten AWS verwalteten Microsoft AD DNS-Servers ein.
7. (Optional) Wählen Sie Weitere IP-Adresse hinzufügen und geben Sie eine zweite IP-Adresse für Ihren zweiten AWS verwalteten Microsoft AD DNS-Server ein. Sie können insgesamt bis zu vier DNS-Server angeben.
8. Wählen Sie Hinzufügen aus. Die Vertrauensstellung wird an dieser Stelle fehlschlagen, was zu erwarten ist, bis wir die andere Seite der Vertrauensstellung erstellen.

Konfigurieren Sie das Vertrauen in Ihrer zweiten AWS verwalteten Microsoft AD-Domain

Jetzt konfigurieren Sie die Gesamtstrukturvertrauensstellung mit Ihrem zweiten AWS verwalteten Microsoft AD-Verzeichnis. Da Sie eine bidirektionale Gesamtstrukturvertrauensstellung für die erste AWS verwaltete Microsoft AD-Domäne erstellt haben, erstellen Sie auch eine bidirektionale Vertrauensstellung mithilfe dieser AWS verwalteten Microsoft AD-Domäne.

So konfigurieren Sie das Vertrauen in Ihrer zweiten AWS verwalteten Microsoft AD-Domäne

1. Kehren Sie zur [AWS Directory Service -Konsole](#) zurück.
2. Wählen Sie auf der Seite Verzeichnisse Ihre zweite 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 Vertrauensstellung hinzufügen den FQDN Ihrer ersten AWS verwalteten Microsoft AD-Domäne 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 AWS verwalteten Microsoft AD DNS-Server ein. Sie können insgesamt bis zu vier DNS-Server angeben.
8. Wählen Sie 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 Vertrauensbeziehung zwischen Ihren beiden AWS verwalteten Microsoft AD-Domänen. Zwischen diesen beiden Domains kann nur eine

Vertrauensstellung eingerichtet werden. Wenn Sie beispielsweise statt einer bidirektionalen eine unidirektionale Vertrauensstellung nutzen möchten, müssen Sie die bestehende Vertrauensstellung löschen und eine neue erstellen.

Erweitern Sie Ihr AWS verwaltetes Microsoft AD-Schema

AWS Managed Microsoft AD verwendet Schemas, um die Speicherung von Verzeichnisdaten zu organisieren und durchzusetzen. Das Hinzufügen von Definitionen zum Schema wird als „Erweiterung des Schemas“ bezeichnet. Schemaerweiterungen ermöglichen es Ihnen, das Schema Ihres AWS verwalteten Microsoft AD-Verzeichnisses mithilfe einer gültigen LDIF-Datei (LDAP Data Interchange Format) zu ändern. Weitere Informationen über AD-Schemas und darüber, wie Sie Ihr Schema erweitern, finden Sie unter nachfolgenden Themen.

Wann Sie Ihr AWS Managed Microsoft AD-Schema erweitern sollten

Sie können Ihr AWS verwaltetes Microsoft AD-Schema erweitern, indem Sie neue Objektklassen und Attribute hinzufügen. 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 kann besonders nützlich sein, wenn Sie Unternehmensanwendungen, die von AWS Managed Microsoft AD abhängig sind, in die AWS Cloud migrieren müssen.

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.

Um zu beginnen, sehen Sie sich [Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas](#) an.

Verwandte Themen

- [Erweitern Sie Ihr AWS verwaltetes Microsoft AD-Schema](#)
- [Schemaelemente](#)

Themen

- [Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas](#)

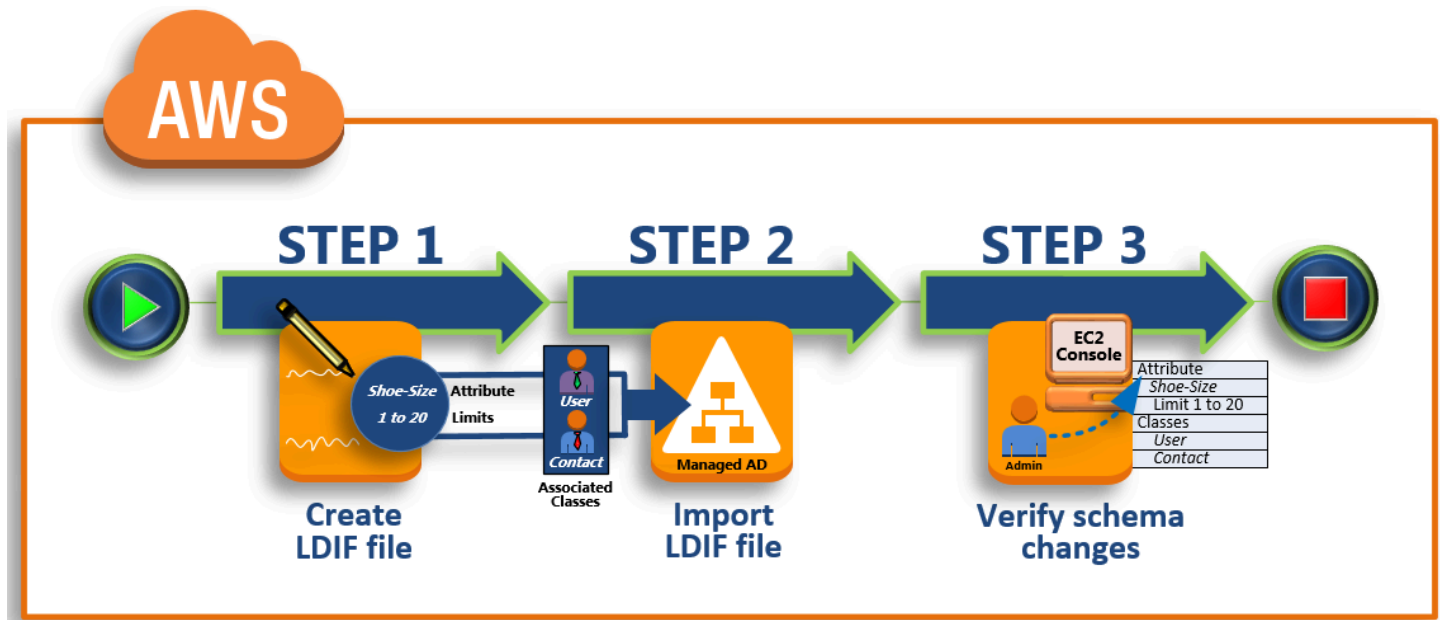
Tutorial: Erweitern Ihres AWS verwalteten Microsoft AD-Schemas

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 Sie Ihr AWS Managed Microsoft AD-Schema erweitern sollten](#).

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 wird es für Sie hilfreich sein, die LDIF-Skriptsyntax zu 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 IDs, Objekte 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 in der Struktur des Active Directory-Objekts und muss die Domänenkomponenten für Ihr Verzeichnis enthalten. Die Domainkomponenten für das Verzeichnis in diesem Tutorial lauten beispielsweise `DC=example,DC=com`.

Der DN muss den allgemeinen Namen (CN) des Active Directory-Objekts enthalten. Der erste CN-Eintrag steht für den Attribut- oder Klassennamen. Um das Active Directory-Schema zu erweitern, verwenden Sie `CN=Schema,CN=Configuration`. Denken Sie daran, dass Sie den Inhalt von Active Directory-Objekten nicht ändern können. Es folgt das allgemeine DN-Format.

```
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 Sie also einen Fehler machen und nicht aus einer Sicherungskopie wiederherstellen möchten, können Sie 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 dazu, wie Sie dies mit der Schemaerweiterung tun können APIs, 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: Sobald Sie eine neue Klasse oder ein neues Attribut erstellt haben, können Sie es in Active Directory nicht mehr 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 [Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD](#) 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 kein Schemaupdate in der Produktionsumgebung an, ohne es zuerst 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 von Ihnen DCs und wendet die Updates in der LDIF-Datei auf den isolierten DC an. Anschließend wählt es eines Ihrer DCs Schemas als primäres Schema aus, entfernt diesen DC aus der Verzeichnisreplikation und wendet Ihre LDIF-Datei mithilfe von `an.Ldifde.exe`
4. Die Replikation erfolgt für alle. 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 mithilfe des Active Directory-Schema-Snap-Ins and/or PowerShell überprüft, 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 [TechNet](#) Website.
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. Beispiel:

```
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 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 EC2 InstanceID-Wert hinzu.

```
PS C:\> set-adcomputer -Identity computer name -add @{example-  
EC2InstanceID = 'EC2 instance ID'}
```

2. Sie können überprüfen, ob der EC2 InstanceID-Wert dem Computerobjekt hinzugefügt wurde, indem Sie den folgenden Befehl ausführen:

```
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](#)

Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD zu verbinden

Sie können eine Amazon EC2 EC2-Instance nahtlos mit Ihrer Active Directory-Domain verbinden, wenn die Instance gestartet wird. Weitere Informationen finden Sie unter [Hinzufügen einer Amazon](#)

[EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#). [Mit Automation können Sie auch direkt von der Directory Service Konsole aus eine EC2-Instance starten und sie einer Active Directory-Domain hinzufügen](#). [AWS Systems Manager](#)

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

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 einer Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory](#)
- [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#)
- [Hinzufügen einer Amazon EC2 Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#)
- [Hinzufügen einer Amazon EC2 Mac-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#)
- [Delegieren von Verzeichnisbeitrittsberechtigungen für AWS Managed Microsoft AD](#)
- [Einen DHCP-Optionssatz für AWS Managed Microsoft AD erstellen oder ändern](#)

Starten einer 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-Managementkonsole verwendet. Sie können dies auch erreichen, indem Sie die Option [Automation AWS>Create DSManagement Instance direkt](#) in der AWS Systems Manager Automation-Konsole ausführen.

Weitere Informationen finden Sie unter den folgenden Links:

- [Vereinfachung des Active Directory-Domänenbeitritts mit AWS Systems Manager](#)

- [Wie verwende ich AWS Systems Manager , um laufende Windows EC2-Instances mit meiner Directory Service Domain zu verbinden?](#)

Voraussetzungen

Die folgenden Voraussetzungen sind erforderlich, um dieses Tutorial abzuschließen:

- Sie müssen es einrichten AWS Systems Manager. Weitere Informationen finden Sie unter [Einrichten AWS Systems Manager](#).
- Sie benötigen eine [IAM-Instanzprofilrolle](#), die Systems Manager und AWS Managed Microsoft AD zulässt.
 - Weitere Informationen zu Systems Manager finden [Sie unter Konfigurieren der für Systems Manager erforderlichen Instanzberechtigungen](#).
 - Die IAM-Instanzrolle benötigt die folgenden AWS verwalteten Richtlinien, damit Ihre Windows EC2-Verzeichnisverwaltungsinstanz Ihrem AWS verwalteten Microsoft AD der Domäne beitreten kann:
 - **AmazonSSMManagedInstanceCore**
 - **AmazonSSMDirectoryServiceAccess**
- Die mit Ihrem AWS Managed Microsoft AD verbundene VPC muss den Zugriff auf öffentliche Directory Service Endpunkte ermöglichen. Weitere Informationen finden Sie unter [Voraussetzungen für die Erstellung eines AWS verwalteten Microsoft AD](#).
- Sie müssen die folgenden Berechtigungen in Ihrem Konto aktiviert haben, um eine EC2-Instance für die Verzeichnisverwaltung von der Konsole aus zu starten:
 - `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`

Starten einer EC2-Instanz für die Verzeichnisverwaltung in der AWS-Managementkonsole

1. Melden Sie sich bei der [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-Instanz 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-Instanz für die Verzeichnisverwaltung starten aus.
6. Füllen Sie auf der Seite EC2-Instanz für die Verzeichnisverwaltung starten unter Eingabeparameter alle Felder aus.
 - a. (Optional) Sie können ein key pair für die Instanz 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.

Anzeige der EC2-Instanz für die Verzeichnisverwaltung

Wenn Sie keine EC2-Instances für ein Verzeichnis gestartet haben, wird ein Bindestrich (-) unter EC2-Instanz 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-Instanz eine oder alle Ihre Instances aus, die Sie anzeigen möchten.
3. Wenn Sie eine Instanz auswählen, werden Sie zur EC2-Seite Mit Instanz verbinden weitergeleitet, um einen Remote-Desktop mit Ihrer Instanz zu verbinden.

Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory

Sie können eine Amazon EC2 Windows EC2-Instance starten und mit einem AWS Managed Microsoft AD verbinden. Alternativ können Sie eine vorhandene Windows EC2-Instance manuell mit einem AWS verwalteten Microsoft AD verbinden.

Seamlessly join EC2 Windows instance

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 unter [Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt](#). Mehr Informationen zu Amazon EC2 finden Sie unter [Was ist Amazon EC2?](#).

Voraussetzungen

Für einen nahtlosen Domänenbeitritt zu einer EC2-Instance müssen Sie die folgenden Schritte ausführen:

- Haben Sie ein AWS verwaltetes Microsoft AD. Weitere Informationen hierzu finden Sie unter [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Sie benötigen die folgenden IAM-Berechtigungen, um einer Windows EC2-Instance problemlos beitreten zu können:
 - IAM-Instanzprofil mit den folgenden IAM-Berechtigungen:
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - Die Benutzerdomäne, die EC2 nahtlos mit dem AWS Managed Microsoft AD verbindet, benötigt die folgenden IAM-Berechtigungen:
 - Directory Service Berechtigungen:
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Amazon VPC-Berechtigungen:
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"

- "ec2:CreateNetworkInterface"
- "ec2:AttachNetworkInterface"
- EC2-Berechtigungen:
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
- AWS Systems Manager Berechtigungen:
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Wenn Ihr AWS verwaltetes Microsoft AD erstellt wird, wird eine Sicherheitsgruppe mit Regeln für eingehenden und ausgehenden Datenverkehr erstellt. Weitere Informationen zu diesen Regeln und Ports finden Sie unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#). Für einen nahtlosen Domänenbeitritt zu einer Windows EC2-Instance sollte Ihre VPC, in der Sie Ihre Instance starten, dieselben Ports zulassen, die in den eingehenden und ausgehenden Regeln Ihrer AWS Managed Microsoft AD-Sicherheitsgruppe zulässig sind.

- Abhängig von Ihren Netzwerksicherheits- und Firewall-Einstellungen müssen Sie möglicherweise zusätzlichen ausgehenden Datenverkehr zulassen. Dieser Datenverkehr würde über HTTPS (Port 443) zu den folgenden Endpunkten erfolgen:

Endpoint	Rolle
ec2messages. <i>region</i> .amazonaws.com	Erstellt und löscht Sitzungskanäle mit dem Session Manager-Dienst. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .

Endpoint	Rolle
<code>ssm.region.amazonaws.com</code>	Endpoint für AWS Systems Manager Session Manager. Weitere Informationen finden Sie unter AWS Systems Manager - Endpunkte und -Kontingente .
<code>ssmmessages.region.amazonaws.com</code>	Erstellt und löscht Sitzungskanäle mit dem Session Manager-Dienst. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .
<code>ds.region.amazonaws.com</code>	Endpoint für Directory Service. Weitere Informationen finden Sie unter Verfügbarkeit in der Region für Directory Service .

- Wir empfehlen, einen DNS-Server zu verwenden, der Ihren AWS verwalteten Microsoft AD-Domainnamen auflöst. Zu diesem Zweck können Sie einen DHCP-Optionssatz erstellen. Weitere Informationen finden Sie unter [Einen DHCP-Optionssatz für AWS Managed Microsoft AD erstellen oder ändern](#).
- Wenn Sie sich dafür entscheiden, keinen DHCP-Optionssatz zu erstellen, sind Ihre DNS-Server statisch und werden von Ihrem AWS verwalteten Microsoft AD entsprechend konfiguriert.

Um einer Amazon EC2 Windows EC2-Instance nahtlos beizutreten

1. Melden Sie sich bei der AWS-Managementkonsole an und öffnen Sie die Amazon EC2 EC2-Konsole 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 Schlüsselpaar-Typ 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 heruntergeladen. 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:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

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-Instance-Profil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien Amazon SSMManged InstanceCore und Amazon SSMDirectory ServiceAccess zugeordnet 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 unter Berechtigungen hinzufügen in der Liste der Richtlinien die Amazon SSMManged InstanceCore - und SSMDirectoryServiceAccessAmazon-Richtlinien aus. Geben Sie im Suchfeld **SSM** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

 Note

Amazon SSMDirectory ServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einem Active Directory, das von verwaltet wird Directory Service. Amazon SSMManged InstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des AWS Systems Manager Dienstes erforderlich sind. 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.

Manually join EC2 Windows instance

Um eine bestehende Amazon EC2 Windows EC2-Instance manuell mit einem AWS Managed Microsoft AD Active Directory zu verbinden, muss die Instance mit den unter angegebenen Parametern gestartet werden. [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten 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.

The screenshot shows the AWS Directory Service console. On the left, the 'Directory Service' sidebar is visible with 'Active Directory' and 'Cloud Directory' sections. The 'Directories' link under 'Active Directory' is highlighted with a red box. The main content area shows the details for directory 'd-1234567890'. The 'Directory details' section is highlighted with a red box and contains the following information:

Property	Value
Directory type	Microsoft AD
Edition	Standard
Operating system version	Windows Server 2019
Directory DNS name	corp.example.com
Directory NetBIOS name	corp
Directory administration EC2 instance(s)	-

Below the details, there are tabs for 'Networking & security', 'Scale & share', 'Application management', and 'Maintenance'. The 'Networking & security' tab is selected and highlighted with a red box. It shows 'VPC' and 'Subnets' sections. The 'DNS address' is highlighted with a red box and shows the values 192.0.2.1 and 198.51.100.1.

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 das IPv4 TCP/-Eigenschaftendialogfeld auf der Instanz.
 - a. Öffnen Sie Network Connections.

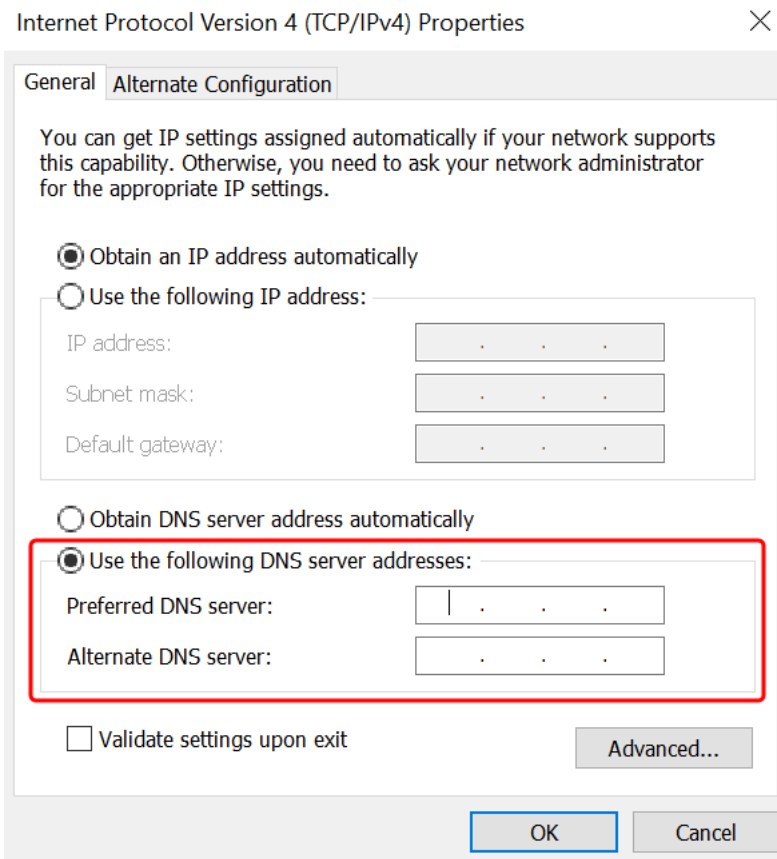
Tip

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, 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 Verzeichnisbeitrittsberechtigungen 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 [Installation der Active Directory-Verwaltungstools für AWS verwaltetes 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](#).

Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory

Sie können eine EC2-Linux-Instance starten und mit Ihrem AWS Managed Microsoft AD in der AWS-Managementkonsole verbinden. Sie können die EC2-Linux-Instance auch manuell mit Ihrem AWS

Managed Microsoft AD verbinden. Tools wie Winbind können auch verwendet werden, damit Sie eine EC2-Linux-Instance mit Ihrem AWS verwalteten Microsoft AD domänenverbinden können.

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

Distributionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 und 8 unterstützen die Funktion zum nahtlosen Domänenbeitritt nicht.

Möglichkeiten zum Domänenbeitritt zu einer EC2-Linux-Instance:

- [Nahtloses Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#)
- [Nahtloses Verbinden einer Amazon EC2 EC2-Linux-Instance mit einem gemeinsam genutzten AWS Managed Microsoft AD](#)
- [Manuelles Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#)
- [Manuelles Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory mithilfe von Winbind](#)

Nahtloses Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory

Dieses Verfahren verbindet eine Amazon EC2 Linux-Instance nahtlos mit Ihrem AWS verwalteten Microsoft AD Active Directory. Um dieses Verfahren abzuschließen, müssen Sie ein AWS Secrets Manager Geheimnis erstellen, was zusätzliche Kosten verursachen kann. Weitere Informationen finden Sie unter [AWS Secrets Manager – Preise](#).

Wenn Sie einen nahtlosen Domänenbeitritt über mehrere AWS Konten hinweg durchführen möchten, 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

Distributionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 und 8 unterstützen die Funktion zum nahtlosen Domänenbeitritt 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 EC2-Linux-Instance einrichten können, müssen Sie die Verfahren in diesen Abschnitten abschließen.

Netzwerkvoraussetzungen für einen nahtlosen Domänenbeitritt

Für einen nahtlosen Domänenbeitritt zu einer EC2-Linux-Instance müssen Sie die folgenden Schritte ausführen:

- Sie benötigen die folgenden IAM-Berechtigungen, um einer EC2-Linux-Instance nahtlos beizutreten:
 - Haben Sie ein AWS verwaltetes Microsoft AD. Weitere Informationen hierzu finden Sie unter [Ihr AWS verwaltetes Microsoft AD erstellen](#).

- Sie benötigen die folgenden IAM-Berechtigungen, um einer Windows EC2-Instance problemlos beitreten zu können:
 - IAM-Instanzprofil mit den folgenden IAM-Berechtigungen:
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - Die Benutzerdomäne, die EC2 nahtlos mit dem AWS Managed Microsoft AD verbindet, benötigt die folgenden IAM-Berechtigungen:
 - Directory Service Berechtigungen:
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Amazon VPC-Berechtigungen:
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - EC2-Berechtigungen:
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
 - AWS Systems Manager Berechtigungen:
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"
- Wenn Ihr AWS verwaltetes Microsoft AD erstellt wird, wird eine Sicherheitsgruppe mit Regeln für eingehenden und ausgehenden Datenverkehr erstellt. Weitere Informationen zu diesen Regeln und Ports finden Sie unter: [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#). Für einen nahtlosen Domänenbeitritt zu einer EC2-Linux-Instance sollte Ihre VPC, auf der Sie Ihre Instance

starten, dieselben Ports zulassen, die in den eingehenden und ausgehenden Regeln Ihrer AWS Managed Microsoft AD-Sicherheitsgruppe zulässig sind.

- Abhängig von Ihren Netzwerksicherheits- und Firewall-Einstellungen müssen Sie möglicherweise zusätzlichen ausgehenden Datenverkehr zulassen. Dieser Datenverkehr würde über HTTPS (Port 443) zu den folgenden Endpunkten erfolgen:

Endpoint	Rolle
ec2messages. <i>region</i> .amazonaws.com	Erstellt und löscht Sitzungskanäle mit dem Session Manager-Dienst. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .
ssm. <i>region</i> .amazonaws.com	Endpunkt für AWS Systems Manager Session Manager. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .
ssmmessages. <i>region</i> .amazonaws.com	Erstellt und löscht Sitzungskanäle mit dem Session Manager-Dienst. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .
ds. <i>region</i> .amazonaws.com	Endpunkt für Directory Service. Weitere Informationen finden Sie unter Verfügbarkeit in der Region für Directory Service .
secretsmanager. <i>region</i> .amazonaws.com	Endpunkt für AWS Secrets Manager. Weitere Informationen finden Sie unter AWS Secrets Manager -Endpunkte und -Kontingente .

- Wir empfehlen, einen DNS-Server zu verwenden, der Ihren AWS verwalteten Microsoft AD-Domainnamen auflöst. Zu diesem Zweck können Sie einen DHCP-Optionssatz erstellen. Weitere Informationen finden Sie unter [Einen DHCP-Optionssatz für AWS Managed Microsoft AD erstellen oder ändern](#).
- Wenn Sie sich dafür entscheiden, keinen DHCP-Optionssatz zu erstellen, sind Ihre DNS-Server statisch und werden von Ihrem AWS verwalteten Microsoft AD entsprechend konfiguriert.

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 [Installation der Active Directory-Verwaltungstools für AWS verwaltetes 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 Standardcomputercontainer 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. Weitere Informationen finden Sie unter [Create an AWS Secrets Manager Secret](#).

 Note

Für Secrets Manager fallen Gebühren an. Weitere Informationen finden Sie unter [Preise](#) im AWS Secrets Manager Benutzerhandbuch.

So erstellen Sie Secrets und speichern die Kontoinformationen des Domainservices

1. Melden Sie sich bei der an AWS-Managementkonsole 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.

The screenshot shows the AWS Secrets Manager console interface. The breadcrumb navigation is [AWS Secrets Manager](#) > [Secrets](#) > Store a new secret. The left sidebar shows the steps: Step 1: Choose secret type (active), Step 2: Configure secret, Step 3 - optional: Configure rotation, and Step 4: Review. The main content area is titled 'Choose secret type'. It has three sections: 'Secret type' with four radio button options (Credentials for Amazon RDS database, Credentials for Amazon DocumentDB database, Credentials for Amazon Redshift cluster, and Other type of secret - which is selected and highlighted with a red box), 'Key/value pairs' with a table showing one row with the key 'awsSeamlessDomainUsername' (highlighted with a red box) and an empty value field, and 'Encryption key' with a dropdown menu showing 'aws/secretsmanager' and a refresh button. At the bottom right are 'Cancel' and 'Next' buttons.

- 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.
- 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 **d-xxxxxxxx** ersetzen Sie ihn durch Ihre Verzeichnis-ID:

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

Dies wird verwendet, um Secrets in der Anwendung abzurufen.

 Note

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

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

Secret name must contain only alphanumeric characters and the characters / _ + = . @ -

Description - optional

Maximum 250 characters.

Tags - optional
No tags associated with the secret.

Resource permissions - optional [Info](#)
Add or edit a resource policy to access secrets across AWS accounts.

Replicate secret - optional
Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

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.

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 EC2 DomainJoin Linux-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-Managementkonsole als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Öffnen Sie dann die IAM-Konsole unter <https://console.aws.amazon.com/iam/>
2. Wählen Sie im Navigationsbereich Access Management die Option Policies 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:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/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-xxxxxxxx-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 EC2 DomainJoin Linux-Rolle

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

Um die EC2 DomainJoin Linux-Rolle zu erstellen

1. Melden Sie sich AWS-Managementkonsole als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Öffnen Sie dann 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.

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected, which is described as 'Allows EC2 instances to call AWS services on your behalf.' Other options include 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'.

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

Amazon SSMDirectory ServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einem Active Directory, das von verwaltet wird Directory Service. Amazon SSMManged InstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des AWS Systems Manager Dienstes erforderlich sind. 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

Um Ihrer Linux-Instanz nahtlos beizutreten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie aus der Regionsauswahl 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 Linux EC2-Instance verwenden möchten.

5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüssel-Wert-Paare hinzuzufügen, um den Zugriff für diese EC2-Instance zu organisieren, zu verfolgen oder zu kontrollieren.
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 einer Active Directory-Domäne hinzugefügt wird. Das Plugin ändert den Hostnamen für die Linux-Instanzen in das Format EC2 AMAZ-**XXXXXXX**. Weitere Informationen `aws:domainJoin` dazu finden Sie in der [Plugin-Referenz zum AWS Systems Manager Befehlsdokument](#) im AWS Systems Manager Benutzerhandbuch.

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 heruntergeladen. 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:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

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: Linux-Rolle erstellen. EC2 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.

Nahtloses Verbinden einer Amazon EC2 EC2-Linux-Instance mit einem gemeinsam genutzten AWS Managed Microsoft AD

In diesem Verfahren verbinden Sie eine Amazon EC2 EC2-Linux-Instance nahtlos mit einem gemeinsam genutzten AWS Managed Microsoft AD. Dazu erstellen Sie eine AWS Secrets Manager IAM-Leserichtlinie in der EC2-Instance-Rolle des Kontos, in dem Sie die EC2-Linux-Instance starten möchten. Dies wird in diesem Verfahren als Account 2 bezeichnet. Diese Instanz verwendet das AWS verwaltete Microsoft AD, das von dem anderen Konto gemeinsam genutzt wird, das als Account 1 bezeichnet wird.

Voraussetzungen

Bevor Sie eine Amazon EC2 Linux-Instance nahtlos mit einem gemeinsam genutzten AWS Managed Microsoft AD verbinden können, müssen Sie die folgenden Schritte ausführen:

- Schritte 1 bis 3 im Tutorial, [Tutorial: Teilen Ihres AWS verwalteten Microsoft AD-Verzeichnisses für einen nahtlosen EC2-Domänenbeitritt](#). Dieses Tutorial führt Sie durch die Einrichtung Ihres Netzwerks und die gemeinsame Nutzung Ihres AWS Managed Microsoft AD.

- Das Verfahren wird in beschrieben [Nahtloses Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#).

Schritt 1. Erstellen Sie die EC2 DomainJoin Linux-Rolle in Konto 2

In diesem Schritt verwenden Sie die IAM-Konsole, um die IAM-Rolle zu erstellen, die Sie für den Domänenbeitritt Ihrer EC2-Linux-Instance verwenden, während Sie angemeldet sind. Account 2

Erstellen Sie die Linux-Rolle EC2 DomainJoin

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Access Management die Option Rollen aus.
3. Klicken Sie auf der Seite Roles (Rollen) auf Create role (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
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. Nachdem Sie diese Richtlinien hinzugefügt haben, wählen Sie Rolle erstellen aus.

Note

AmazonSSMDirectoryServiceAccess bietet die Berechtigungen zum Hinzufügen von Instanzen zu einem Active Directory, das von verwaltet wird Directory Service. AmazonSSMManagedInstanceCore stellt die Mindestberechtigungen bereit, die zur Verwendung erforderlich sind AWS Systems Manager. Weitere Informationen zum Erstellen einer Rolle mit diesen Berechtigungen und Informationen zu anderen Berechtigungen und Richtlinien, die Sie Ihrer IAM-Rolle zuweisen können, finden Sie unter [Konfigurieren der für Systems Manager erforderlichen Instanzberechtigungen](#) 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 unter 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.

Schritt 2. Richten Sie kontenübergreifenden Zugriff auf Ressourcen ein, um Geheimnisse zu teilen AWS Secrets Manager

Der nächste Abschnitt enthält zusätzliche Anforderungen, die erfüllt werden müssen, um EC2-Linux-Instances nahtlos mit einem gemeinsam genutzten AWS verwalteten Microsoft AD zu verbinden. Zu diesen Anforderungen gehören die Erstellung von Ressourcenrichtlinien und deren Verknüpfung mit den entsprechenden Diensten und Ressourcen.

Um Benutzern in einem Konto den Zugriff auf AWS Secrets Manager geheime Daten in einem anderen Konto zu ermöglichen, müssen Sie den Zugriff sowohl in einer Ressourcenrichtlinie als auch in einer Identitätsrichtlinie zulassen. Diese Art des Zugriffs wird als [kontoübergreifender Ressourcenzugriff](#) bezeichnet.

Diese Art des Zugriffs unterscheidet sich von der Gewährung des Zugriffs auf Identitäten in demselben Konto wie das Secrets Manager Manager-Geheimnis. Außerdem müssen Sie der Identität die Verwendung des [AWS Key Management Service](#)(KMS-Schlüssels) gestatten, mit dem das Geheimnis verschlüsselt ist. Diese Berechtigung ist erforderlich, da Sie den AWS verwalteten Schlüssel (aws/secretsmanager) nicht für den kontoübergreifenden Zugriff verwenden können. Stattdessen verschlüsseln Sie Ihr Geheimnis mit einem von Ihnen erstellten KMS-Schlüssel und fügen ihm dann eine Schlüsselrichtlinie hinzu. Informationen zum Ändern des Verschlüsselungsschlüssels für ein Geheimnis finden Sie unter [Ändern eines AWS Secrets Manager Geheimnisses](#).

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 Von AWS verwalteter 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 – Preise](#).

Mit den folgenden Schritten können Sie die Ressourcenrichtlinien erstellen, damit Benutzer eine EC2-Linux-Instance nahtlos mit einem gemeinsam genutzten AWS verwalteten Microsoft AD verbinden können.

Fügen Sie dem Secret in Konto 1 eine Ressourcenrichtlinie hinzu

1. Öffnen Sie die Secrets Manager Manager-Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
2. Wählen Sie aus der Liste der Geheimnisse Ihr Geheimnis aus, das Sie während des erstellt haben [Voraussetzungen](#).
3. Scrollen Sie auf der Detailseite des Geheimnisses unter dem Tab Übersicht nach unten zu Ressourcenberechtigungen.
4. Wählen Sie Berechtigungen bearbeiten aus.
 - Geben Sie im Richtlinienfeld die folgende Richtlinie ein. Die folgende Richtlinie ermöglicht Linux EC2 DomainJoin in den Account 2 Zugriff auf das Secret in Account 1. Ersetzen Sie den ARN-Wert durch den ARN-Wert für Ihre LinuxEC2DomainJoin Rolle Account 2, die Sie in [Schritt 1](#) erstellt haben. Informationen zur Verwendung dieser Richtlinie finden Sie unter [Anhängen einer Berechtigungsrichtlinie an ein AWS Secrets Manager Geheimnis](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/LinuxEC2DomainJoin"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

Fügen Sie der Schlüsselrichtlinie für den KMS-Schlüssel in Konto 1 eine Erklärung hinzu

1. Öffnen Sie die Secrets Manager Manager-Konsole unter <https://console.aws.amazon.com/secretsmanager/>.
2. Wählen Sie im linken Navigationsbereich vom Kunden verwaltete Schlüssel aus.
3. Wählen Sie auf der Seite Vom Kunden verwaltete Schlüssel den Schlüssel aus, den Sie erstellt haben.
4. Navigieren Sie auf der Seite mit den Schlüsseldetails zu Schlüsselrichtlinie und wählen Sie Bearbeiten aus.
5. Die folgende wichtige Richtlinienanweisung ermöglicht ApplicationRole die Verwendung des KMS-Schlüssels in Account 1, um den geheimen Schlüssel in Account 1 zu entschlüsseln. Account 2 Um diese Anweisung zu verwenden, fügen Sie sie der Schlüsselrichtlinie für Ihren KMS-Schlüssel hinzu. Weitere Informationen finden Sie unter [Changing a key policy \(Ändern einer Schlüsselrichtlinie\)](#).

```
{
  {
    "Effect": "Allow",
    "Principal": {
      "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
    },
    "Action": [
      "kms:Decrypt",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  }
}
```

Erstellen Sie eine Identitätsrichtlinie für die Identität in Konto 2

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im linken Navigationsbereich unter Zugriffsverwaltung die Option Richtlinien aus.
3. Wählen Sie Create Policy (Richtlinie erstellen). Wählen Sie im Richtlinien-Editor JSON aus.

4. Die folgende Richtlinie ermöglicht ApplicationRole den Account 2 Zugriff auf den geheimen Wert Account 1 und die Entschlüsselung des Geheimwerts mithilfe des ebenfalls enthaltenen Verschlüsselungsschlüssels. Account 1 Sie finden den ARN für Ihr Secret in der Secrets Manager-Konsole auf der Seite Secret Details unter Secret ARN. Alternativ können Sie [describe-secret](#) aufrufen, um den ARN des Secrets zu identifizieren. Ersetzen Sie den Ressourcen-ARN durch den Ressourcen-ARN für den geheimen ARN und Account 1. Informationen zur Verwendung dieser Richtlinie finden Sie unter [Anhängen einer Berechtigungsrichtlinie an ein AWS Secrets Manager Geheimnis](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:us-east-1:111122223333:secret:secretName-AbCdEf"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:Describekey"
      ],
      "Resource": "arn:aws:kms:us-east-1:111122223333:key/Your_Encryption_Key"
    }
  ]
}
```

5. Wählen Sie Weiter und dann Änderungen speichern aus.
6. Suchen Sie die Rolle, die Sie Account 2 in erstellt haben, und wählen Sie sie aus [Attach a resource policy to the secret in Account 1](#).
7. Wählen Sie unter Berechtigungen hinzufügen die Option Richtlinien anhängen aus.
8. Suchen Sie in der Suchleiste nach der Richtlinie, in der Sie sie erstellt haben, [Add a statement to the key policy for the KMS key in Account 1](#) und wählen Sie das Feld aus, um die Richtlinie der Rolle hinzuzufügen. Wählen Sie dann Berechtigungen hinzufügen aus.

Schritt 3. Treten Sie Ihrer Linux-Instanz nahtlos bei

Sie können jetzt das folgende Verfahren verwenden, um Ihre EC2-Linux-Instance nahtlos mit Ihrem gemeinsam genutzten AWS verwalteten Microsoft AD zu verbinden.

Um Ihrer Linux-Instance nahtlos beizutreten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie aus der Regionsauswahl 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 Linux EC2-Instance verwenden möchten.
5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüssel-Wert-Paare hinzuzufügen, um den Zugriff für diese EC2-Instance zu organisieren, zu verfolgen oder zu kontrollieren.
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 einer Active Directory-Domäne hinzugefügt wird. Das Plugin ändert den Hostnamen für die Linux-Instanzen in das Format EC2 AMAZ-**XXXXXXX**. Weitere Informationen `aws:domainJoin` dazu finden Sie in der [Plugin-Referenz zum AWS Systems Manager Befehlsdokument](#) im AWS Systems Manager Benutzerhandbuch.

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 heruntergeladen. 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:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

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: Linux-Rolle erstellen. EC2 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

Neben Amazon EC2 Windows EC2-Instances können Sie auch bestimmte Amazon EC2 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 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* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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.)

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. 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* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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. 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

Der AMAccounts-Name für ein Konto in der *example.com* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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 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 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

Der AMAccount s-Name in der *example.com* Domäne, die 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 Verzeichnisbeitrittsberechtigungen 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 `auto` ein Home-Verzeichnis 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/sss/sssd_be --domain example.com --uid 0 --gid 0 --
  logger=files
          ##548 /usr/lib/sss/sssd_nss --uid 0 --gid 0 --logger=files
          ##549 /usr/lib/sss/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 Instanz her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der bereitgestellten DNS-Server verwendet. Directory Service Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instanz 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-Instanz zu?](#) eine Anleitung, um den persistenten DNS-Server für Ihre Linux-Distribution und -Version festzulegen.
3. Stellen Sie sicher, dass Ihre Ubuntu - 64bit-Instanz auf dem neuesten Stand ist.

```
sudo apt-get update  
sudo apt-get -y upgrade
```

4. Installieren Sie die erforderlichen Ubuntu-Pakete auf Ihrer Linux-Instanz.

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

Der AMAccounts-Name für ein Konto in der *example.com* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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. Beispiel:

```
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 lautet der Gruppenname. *admins*

ou

Dies ist die Organisationseinheit, in der sich die oben genannte Gruppe befindet. In diesem Beispiel ist die Organisationseinheit *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/sss/sss.conf` hinzufügen.

Öffnen Sie die Datei `/etc/sss/sss.conf` in einem Text-Editor.

```
sudo vi /etc/sss/sss.conf
```

Danach sieht `sss.conf` wie folgt aus:

```
[sss]
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.

Beispiel:

```
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 lautet der Gruppenname *admins*.

ou

Dies ist die Organisationseinheit, in der sich die oben genannte Gruppe befindet. In diesem Beispiel ist die Organisationseinheit *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/sss/sss.conf` hinzufügen.

1. Öffnen Sie die Datei `/etc/sss/sss.conf` in einem Text-Editor.

```
sudo vi /etc/sss/sss.conf
```

2. Danach sieht `sss.conf` wie folgt aus:

```
[sss]
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 `sss`-Service neu starten:

```
sudo systemctl restart sss.service
```

Alternativ können Sie:

```
sudo service sss 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. Diese Methoden sind:

1. Zentralisiert
2. Verteilt

Note

Für die zentrale Zuordnung von Benutzeridentitäten in Active Directory ist ein Portable Operating System Interface oder POSIX erforderlich.

Zentralisierte Zuordnung von Benutzeridentitäten

Active Directory oder ein anderer LDAP-Dienst (Lightweight Directory Access Protocol) stellt den Linux-Benutzern UID und GID zur Verfügung. In Active Directory werden diese Bezeichner in den Benutzerattributen gespeichert, wenn die POSIX-Erweiterung konfiguriert ist:

- 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 aus Active Directory zu konfigurieren, 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 Active Directory eine UID, UID-Nummer und GID-Nummer hinzugefügt haben.

Zuordnung verteilter Benutzeridentitäten

Wenn Active Directory nicht über die POSIX-Erweiterung verfügt 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.

Häufige Probleme

Wenn Sie dies festlegen `ldap_id_mapping = False`, schlägt das Starten des SSSD-Dienstes manchmal fehl. Der Grund für diesen Fehler liegt darin, dass Änderungen von IDs nicht unterstützt werden. Wir empfehlen Ihnen, den SSSD-Cache zu löschen, wenn Sie von ID-Zuordnung zu POSIX-Attributen oder von POSIX-Attributen zu ID-Zuordnung wechseln. Weitere Informationen zur ID-Zuordnung und den `ldap_id_mapping`-Parametern finden Sie in der Manpage `sssd-ldap (8)` in der Linux-Befehlszeile.

Connect zur Linux-Instanz her

Wenn ein Benutzer die Verbindung zur Instanz 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. Auf diese Weise 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 Instanz nicht erreichbar oder unbrauchbar machen. Aus diesem Grund empfehlen wir dringend, eine Sicherung anzufertigen oder einen Snapshot der Instanz zu machen, bevor diese Verfahren ausgeführt werden.

So fügen Sie Ihrem Verzeichnis eine Linux-Instanz hinzu

Folgen Sie den Schritten für Ihre spezifische Linux-Instanz unter Verwendung einer der folgenden Registerkarten:

Amazon Linux/CENTOS/REDHAT

1. Stellen Sie über einen SSH-Client eine Verbindung zur Instanz her.
2. Konfigurieren Sie die Linux-Instanz so, dass sie die DNS-Server-IP-Adressen der Directory Service-bereitgestellten DNS-Server verwendet. Das können Sie entweder in den DHCP-Optionen der VPC oder manuell auf der Instanz einrichten. Wenn Sie ihn manuell einrichten möchten, finden Sie im AWS Knowledge Center unter [Wie weise ich einer privaten Amazon EC2 EC2-Instanz 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-Instanz auf dem aktuellen Stand ist.

```
sudo yum -y update
```

4. Installieren Sie die erforderlichen Samba-/Winbind-Pakete auf Ihrer Linux-Instanz.

```
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
```

- 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
```

- 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* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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 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 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

Der AMAccount s-Name in der *example.com* Domäne, die 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 Verzeichnisbeitrittsberechtigungen 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 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 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* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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%
```

Hinzufügen einer Amazon EC2 Mac-Instance zu 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 [Einen DHCP-Optionssatz für AWS Managed Microsoft AD erstellen oder ändern](#).

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](#).

Manuelles Beitreten zu einer Mac-Instance

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 den *ec2-user* Account:

```
sudo passwd ec2-user
```

3. Wenn Sie in der Befehlszeile dazu aufgefordert werden, geben Sie ein Passwort für das *ec2-user* Konto 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 *dsconfigad* Befehl, um Ihre Mac-Instanz mit der AWS verwalteten Microsoft AD Active Directory-Domäne zu verbinden. Stellen Sie sicher, dass Sie den Domännennamen, 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 Verzeichnisbeitrittsberechtigungen für AWS Managed Microsoft AD

Um einen Computer mit Ihrem AWS verwalteten Microsoft AD hinzuzufügen, benötigen Sie ein Konto, das über die Rechte verfügt, Computer mit dem Verzeichnis zu verbinden.

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

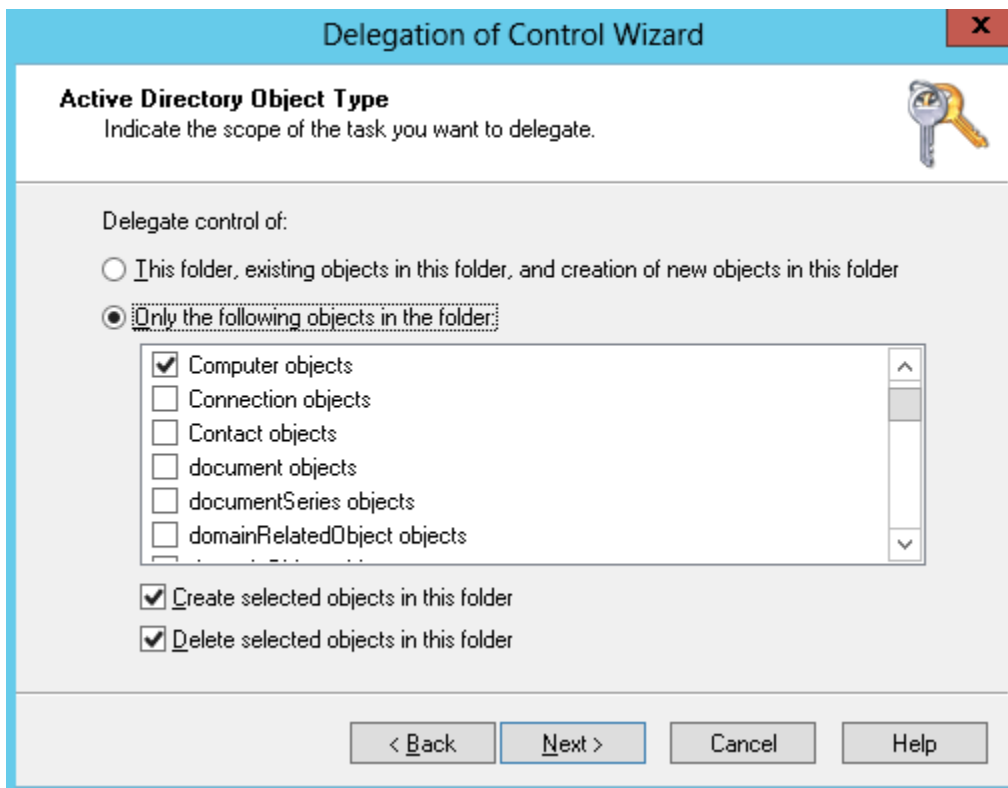
1. Öffnen Sie Active Directory User and Computers und wählen Sie die Organisationseinheit (Organizational Unit – OU) mit Ihrem NetBIOS-Namen in der Navigationsstruktur aus. Klicken Sie dann auf die OU Users.

Important

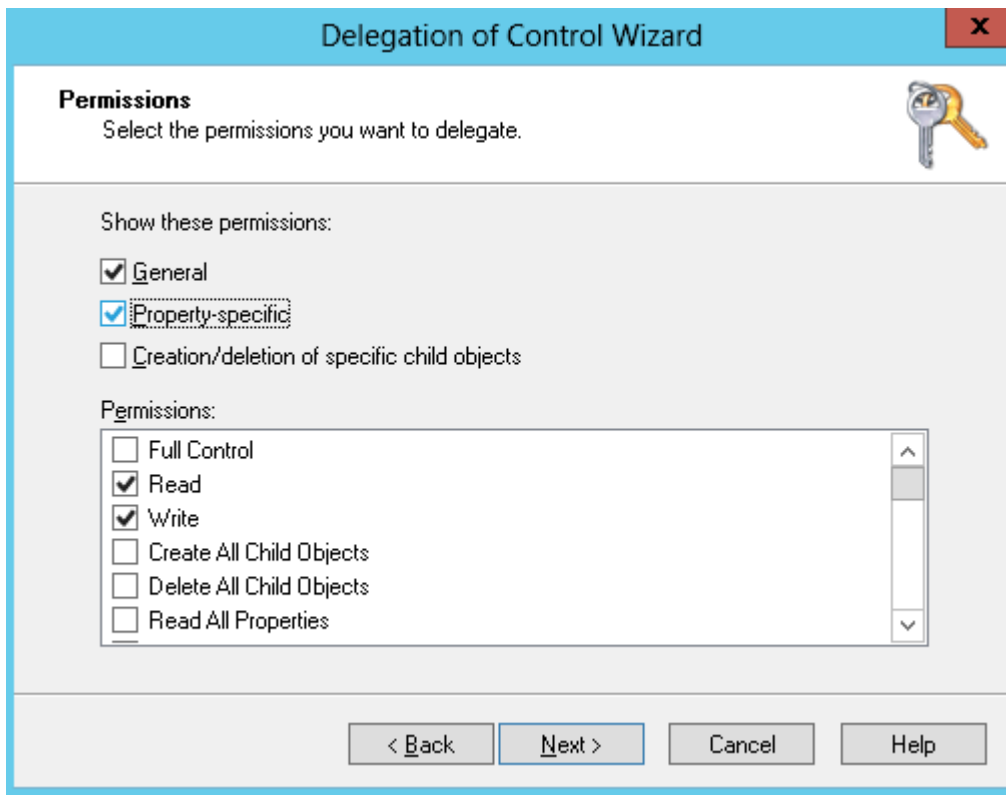
Wenn Sie einen AWS Directory Service für Microsoft Active Directory starten, AWS wird eine Organisationseinheit (OU) erstellt, die alle Objekte Ihres Verzeichnisses enthält. Diese OU erhält den NetBIOS-Namen, den Sie beim Erstellen des Verzeichnisses eingegeben haben, und befindet sich im Domainstamm. 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. Klicken Sie anschließend auf 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.

Einen DHCP-Optionssatz für AWS Managed Microsoft AD erstellen oder ändern

AWS empfiehlt, dass Sie einen DHCP-Optionssatz für Ihr 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 des neuen Satzes von DHCP-Optionen (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 Ihr aus. VPCs
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 Gruppenverwaltung in AWS Managed Microsoft AD

Sie können Benutzer und Gruppen in AWS Managed Microsoft AD verwalten. Sie erstellen einen Benutzer, der eine Person oder Entität repräsentiert, die auf Ihr Verzeichnis zugreifen kann. Sie können auch eine Gruppe erstellen, um mehr als einem Benutzer gleichzeitig Berechtigungen zu erteilen oder zu verweigern. Sie können nicht nur Benutzer zu einer Gruppe hinzufügen, sondern auch Gruppen zu einer Gruppe. Wenn Sie einen Benutzer zu einer Gruppe hinzufügen, erbt der Benutzer die Rollen und Berechtigungen, die der Gruppe zugewiesen sind. Wenn Sie einer Gruppe eine Gruppe hinzufügen, teilen sich die Gruppen eine Eltern-Kind-Beziehung, in der die untergeordnete Gruppe die Rollen und Berechtigungen erbt, die der übergeordneten Gruppe zugewiesen sind. Sie können auch die Gruppenmitgliedschaften eines Benutzers in einen anderen Benutzer kopieren.

Sie können Benutzer und Gruppen mit [the section called “Verzeichnisdienstdaten”](#) den folgenden Methoden verwalten:

- [AWS-Managementkonsole](#)
- [AWS CLI](#)

- [AWS Verzeichnisdienst-Daten-API](#)
- [AWS Tools for Windows PowerShell](#)

Eine Demonstration der AWS Directory Service Data CLI finden Sie im folgenden YouTube Video.

[Benutzer und Gruppen in AWS Managed Microsoft AD mithilfe von CRUD verwalten APIs](#)

Alternativ können Sie eine Instanz verwenden, die in eine [Domäne eingebunden](#) ist.

Verwalten Sie Benutzer und Gruppen mit dem AWS-Managementkonsole

Sie können Benutzer und Gruppen AWS-Managementkonsole mit den AWS Verzeichnisdienstdaten verwalten. Directory Service Data ist eine Erweiterung von Directory Service , die Ihnen die Möglichkeit bietet, integrierte Objektverwaltungsaufgaben auszuführen. Einige dieser Aufgaben umfassen das Erstellen von Benutzern und Gruppen und das Hinzufügen von Benutzern zu Gruppen sowie Gruppen zu einer Gruppe.

Weitere Informationen finden Sie unter [Verwalten von AWS verwalteten Microsoft AD-Benutzern und -Gruppen mit dem AWS-Managementkonsole](#).

Note

Um diese Funktion verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Benutzer- und Gruppenverwaltung aktivieren](#).

Sie können Benutzer und Gruppen nur mit dem AWS-Managementkonsole aus dem Primärverzeichnis AWS-Region für Ihr Verzeichnis verwalten. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).

Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).

Verwalten Sie Benutzer und Gruppen mit dem AWS CLI

Sie können Benutzer und Gruppen mit der AWS CLI über die [AWS Directory Service Data API](#) verwalten. Directory Service Data ist eine Erweiterung von Directory Service, die Ihnen die Möglichkeit bietet, integrierte Objektverwaltungsaufgaben mithilfe des ds-data Namespace auszuführen. Einige dieser Aufgaben umfassen das Erstellen von Benutzern und Gruppen und das Hinzufügen von Benutzern zu Gruppen sowie von Gruppen zu einer Gruppe.

Erstellen Sie einen Benutzer mit AWS Directory Service Data CLI

Im Folgenden finden Sie einen AWS CLI Beispielfehl, der den ds-data Namespace verwendet, um einen Benutzer zu erstellen.

```
aws ds-data create-user --directory-id d-1234567890 --sam-account-name "jane.doe" --  
region your-Primary-Region-name
```

Note

Um diesen zu verwenden AWS CLI, muss er aktiviert sein. Weitere Informationen finden Sie unter [Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten aktivieren oder deaktivieren](#).

Sie können Benutzer und Gruppen nur mit der AWS Directory Service Data CLI von der Primärschnittstelle AWS-Region für Ihr Verzeichnis aus verwalten. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).

Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#). Weitere Informationen finden Sie unter [Bewährte IAM-Methoden](#).

Weitere Informationen finden Sie unter [Verwalten von AWS verwalteten Microsoft AD-Benutzern und -Gruppen mit dem AWS CLI](#).

Verwalten Sie Benutzer und Gruppen mit AWS -Tools für PowerShell

Das [AWS -Tools für PowerShell](#) bietet zwei separate Module für die Verwaltung AWS Directory Service: `AWS.Tools.DirectoryService` (DS) und `AWS.Tools.DirectoryServiceData` (DSD). Stellen Sie bei der Arbeit mit sicher AWS Directory Service, dass Sie das richtige Modul für Ihren beabsichtigten Betrieb verwenden.

- Das `DirectoryService` Modul enthält Cmdlets zur Verwaltung der Konfiguration und Verwaltung des Verzeichnisdienstes, einschließlich Cmdlets wie `Enable-DSDirectoryDataAccess`, und `Disable-DSDirectoryDataAccess` `Reset-DSUserPassword`
- Das `DirectoryServiceData` Modul enthält Cmdlets für die Ausführung von Vorgängen innerhalb eines Verzeichnisses, die sich speziell auf die Benutzer- und Gruppenverwaltung konzentrieren. Diese DSD-Cmdlets umfassen Benutzerverwaltungsvorgänge (`New-DSDUser`, `Remove-DSDUser`) `Get-DSDUserUpdate-DSDUser`, Gruppenverwaltungsvorgänge (`Get-DSDGroup`, `Update-DSDGroup`, `Remove-DSDGroup`) `New-DSDGroup` `Get-DSDGroup`, die Verwaltung von Gruppenmitgliedschaften (`Add-DSDGroupMember`, `Remove-DSDGroupMember`) und Suchfunktionen (`Search-DSDUser` `Search-DSDGroup`)

Benutzer und Gruppen mit einer lokalen Instance oder Amazon EC2 EC2-Instance verwalten

Wenn die AWS Verzeichnisdienstdaten Ihren Anwendungsfall nicht unterstützen, empfehlen wir, Benutzer und Gruppen mit einer lokalen oder EC2-Instanz zu verwalten.

Um Benutzer und Gruppen in einem AWS verwalteten Microsoft AD zu erstellen, können Sie jede Instanz (entweder lokal oder EC2) verwenden, die Ihrem AWS Managed Microsoft AD hinzugefügt wurde. Sie müssen als Benutzer angemeldet sein, der über Rechte zum Erstellen von Benutzern und Gruppen verfügt. Sie müssen auch die Active Directory-Tools auf Ihrer Instanz installieren, damit Sie Ihre Benutzer und Gruppen mit dem Tool Active Directory-Benutzer und -Computer hinzufügen können.

- Sie können eine vorkonfigurierte EC2-Instanz mit vorinstallierten Active Directory-Verwaltungstools von der Managementkonsole aus Directory Service bereitstellen. Weitere Informationen finden Sie unter [Starten einer Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory](#).
- Informationen dazu, wie Sie eine selbstverwaltete EC2-Instanz 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.](#)

Themen

- [AWS Verwaltete Microsoft AD-Benutzer und -Gruppen mit dem AWS-Managementkonsole, AWS CLI, oder verwalten AWS -Tools für PowerShell](#)
- [Benutzer und Gruppen mit einer EC2 Amazon-Instance verwalten](#)

AWS Verwaltete Microsoft AD-Benutzer und -Gruppen mit dem AWS-Managementkonsole, AWS CLI, oder verwalten AWS -Tools für PowerShell

Sie können das AWS-Managementkonsole, oder verwenden AWS CLI, AWS -Tools für PowerShell um Ihre AWS verwalteten Microsoft AD-Benutzer und -Gruppen mit zu verwalten [AWS Verzeichnisdienstdaten](#). Die AWS Directory Service Data CLI verwendet den ds-data Namespace. Weitere Informationen zu finden Sie AWS CLI unter [Erste Schritte mit AWS CLI](#). Weitere Informationen zu AWS -Tools für PowerShell finden Sie im [AWS -Tools für PowerShell Benutzerhandbuch](#).

In den folgenden Verfahren finden Sie weitere Informationen zum Erstellen, Anzeigen, Aktualisieren und Löschen von AWS verwalteten Microsoft AD-Benutzern und -Gruppen.

Verfahren zur Benutzer- und Gruppenverwaltung

- [Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten aktivieren oder deaktivieren](#)
- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#)
- [Einen AWS verwalteten Microsoft AD-Benutzer anzeigen und aktualisieren](#)
- [Löschen eines AWS verwalteten Microsoft AD-Benutzers](#)
- [Deaktivieren eines AWS verwalteten Microsoft AD-Benutzers](#)
- [Das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen und aktivieren](#)
- [Eine AWS verwaltete Microsoft AD-Gruppe erstellen](#)
- [Details einer AWS verwalteten Microsoft AD-Gruppe anzeigen und aktualisieren](#)
- [Löschen einer AWS verwalteten Microsoft AD-Gruppe](#)
- [Hinzufügen und Entfernen von AWS verwalteten Microsoft AD-Mitgliedern zu Gruppen und Gruppen zu Gruppen](#)

- [Kopieren von AWS verwalteten Microsoft AD-Gruppenmitgliedschaften in AWS-Managementkonsole](#)

Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten aktivieren oder deaktivieren

Um die Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten verwenden zu können, muss sie aktiviert sein. Nach der Aktivierung können Sie Benutzer und Gruppen über AWS-Managementkonsole AWS CLI, oder verwalten AWS -Tools für PowerShell.

Important

- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Eine Liste der Regionen, die AWS Directory Service Data unterstützen, finden Sie unter [Unterstützt AWS-Regionen für Verzeichnisdienstdaten](#).
- Die Zugriffskontrollen für AWS Directory Service Data unterscheiden sich von den Zugriffskontrollen für AWS-Services Amazon WorkSpaces, Amazon Quick und Amazon WorkMail. Weitere Informationen finden Sie unter [AWS Anwendungsautorisierung mit Directory Service Data](#).

AWS Verzeichnisdienstdaten aktivieren

Gehen Sie wie folgt vor, um die Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten für ein vorhandenes AWS verwaltetes Microsoft AD entweder mit AWS-Managementkonsole AWS CLI, oder zu aktivieren AWS -Tools für PowerShell.

AWS-Managementkonsole

Sie können die Benutzer- und Gruppenverwaltung mit dem aktivieren AWS-Managementkonsole.

Um die Benutzer- und Gruppenverwaltung zu aktivieren

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.

2. Wählen Sie auf der Seite mit den Verzeichnisdetails die Option Aktivieren aus, um die Benutzer- und Gruppenverwaltung zu aktivieren.
3. Wählen Sie im Dialogfeld Benutzer- und Gruppenverwaltung aktivieren die Option Aktivieren aus.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung formatiert wird, die die AWS Directory Service Data CLI aktiviert. Sie müssen Ihre Verzeichnis-ID-Nummer in Ihrer Anfrage angeben.

Note

Die CLI-Befehle enable AWS Directory Service Data verwenden `aws ds`.

So aktivieren Sie AWS Directory Service Data CLI

- Öffnen Sie den AWS CLI und führen Sie den folgenden Befehl aus, wobei Sie die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID ersetzen:

```
aws ds enable-directory-data-access --directory-id d-1234567890
```

AWS -Tools für PowerShell

So aktivieren Sie Directory Service Data mit Tools für PowerShell

- Öffnen Sie den folgenden Befehl PowerShell, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

```
Enable-DSDirectoryDataAccess -DirectoryId d-1234567890
```

AWS Verzeichnisdienstdaten deaktivieren

Gehen Sie wie folgt vor, um die Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten für ein vorhandenes AWS verwaltetes Microsoft AD entweder mit AWS-Managementkonsole AWS CLI, oder zu deaktivieren AWS -Tools für PowerShell.

AWS-Managementkonsole

Sie können die Benutzer- und Gruppenverwaltung mit der deaktivieren AWS-Managementkonsole.

Um die Benutzer- und Gruppenverwaltung zu deaktivieren

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie auf der Seite mit den Verzeichnisdetails die Option Deaktivieren aus, um die Benutzer- und Gruppenverwaltung zu deaktivieren.
3. Wählen Sie im Dialogfeld Benutzer- und Gruppenverwaltung deaktivieren die Option Deaktivieren aus.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung formatiert wird, die die AWS Directory Service Data CLI deaktiviert. Sie müssen Ihre Verzeichnis-ID-Nummer in Ihrer Anfrage angeben.

Note

Die CLI-Befehle zum Deaktivieren von AWS Directory Service Data verwenden `aws ds`.

So deaktivieren Sie AWS Directory Service Data CLI

- Öffnen Sie den AWS CLI und führen Sie den folgenden Befehl aus, wobei Sie die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID ersetzen:

```
aws ds disable-directory-data-access --directory-id d-1234567890
```

AWS -Tools für PowerShell

So deaktivieren Sie Verzeichnisdienstdaten mit Tools für PowerShell

- Öffnen Sie den folgenden Befehl PowerShell, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID:

```
Disable-DSDirectoryDataAccess -DirectoryId d-123456789
```

Einen AWS verwalteten Microsoft AD-Benutzer erstellen

Gehen Sie wie folgt vor, um einen neuen AWS verwalteten Microsoft AD-Benutzer mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder zu erstellen AWS -Tools für PowerShell.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).

AWS-Managementkonsole

Sie können ein neues AWS verwaltetes Microsoft AD-Benutzerkonto in der erstellen AWS-Managementkonsole. Wenn Sie ein neues Benutzerkonto erstellen, geben Sie die Details des neuen Benutzers an und legen fest, ob Sie den neuen Benutzer zu einer Gruppe hinzufügen oder die Gruppenmitgliedschaften eines anderen Benutzers in den neuen Benutzer kopieren möchten.

Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

Um einen AWS verwalteten Microsoft AD-Benutzer mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.

2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie auf der Seite mit den Verzeichnisdetails im Abschnitt Benutzer die Option Benutzerkonto erstellen aus.
5. Die Seite „Benutzerdetails angeben“ wird geöffnet. Geben Sie im Abschnitt Erforderliche Informationen einen Benutzeranmeldenamen und ein Kennwort ein. Benutzeranmeldenamen müssen die folgenden Bedingungen erfüllen:
 - Muss ein eindeutiger Anmeldename sein
 - Kann bis zu 20 Zeichen lang sein
 - Kann nur alphanumerische Zeichen enthalten
 - ~!@#\$%^&* _-+=`|\\(){}[]:;'"<>,.?/
 - Das Passwort muss den Anforderungen Ihrer Passwortrichtlinie entsprechen. Wenden Sie sich an Ihren AWS Administrator, um weitere Informationen zu erhalten.

 Warning

Der Anmeldename des Benutzers kann nicht geändert werden, nachdem der Benutzer erstellt wurde.

- a. (Optional) Im Abschnitt Primäre Informationen können Sie einen Vor- und Nachnamen für den Benutzer eingeben. Sie können auch einen Anzeigenamen und eine Beschreibung für den Benutzer eingeben.
- b. (Optional) Im Abschnitt Kontaktmethoden können Sie eine E-Mail-Adresse und Telefonnummern für den Benutzer eingeben.
- c. (Optional) Im Bereich Berufsbezogene Informationen können Sie eine Abteilung, einen Manager, ein Büro und eine Firma für den Benutzer eingeben.
- d. (Optional) Im Bereich Adresse können Sie eine Adresse für den Benutzer eingeben.
- e. (Optional) Im Abschnitt Kontoeinstellungen können Sie Notizen, eine bevorzugte Sprache und den Dienstprinzipalnamen für den Benutzer eingeben.

Weitere Informationen zu Benutzerattributen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und in der [MicrosoftDokumentation](#).

6. Wählen Sie Weiter, sobald Sie die Benutzerkontodetails eingegeben haben.
7. Auf der Seite Benutzer zu Gruppen hinzufügen — optional können Sie den Benutzer zu einer neuen Gruppe oder zu einer bestehenden Gruppe hinzufügen. Sie können auch die Gruppenmitgliedschaft eines vorhandenen Benutzers auf den neuen Benutzer kopieren. Wenn Sie keinen Benutzer zu einer Gruppe hinzufügen möchten, wählen Sie Weiter. Fahren Sie mit Schritt 12 fort, um dieses Verfahren fortzusetzen.
8. (Optional) Informationen zum Erstellen einer neuen Gruppe finden Sie unter [Erstellen einer AWS verwalteten Microsoft AD-Gruppe](#).
9. (Optional) So fügen Sie einer vorhandenen Gruppe einen neuen Benutzer hinzu:
 - Wählen Sie im Abschnitt Gruppen die Gruppe aus, zu der Sie den neuen Benutzer hinzufügen möchten. Um Gruppen zu finden, geben Sie den Gruppennamen in das Suchfeld ein.
10. (Optional) Um die Gruppenmitgliedschaft eines vorhandenen Benutzers auf einen neuen Benutzer zu kopieren:
 - a. Wählen Sie die Registerkarte Gruppenmitgliedschaft von Benutzer kopieren aus. Um einen Benutzer mit einer Gruppenmitgliedschaft zu finden, die Sie kopieren möchten, geben Sie den Benutzeranmeldenamen in das Suchfeld unter dem Abschnitt Benutzer ein.
 - b. Wählen Sie im Abschnitt Ausgewählte Gruppen die Gruppen aus, denen der neue Benutzer beitreten soll.
11. Wählen Sie Weiter, wenn Sie bereit sind, das neue Benutzerkonto zu erstellen.
12. Überprüfen Sie auf der Seite Benutzer überprüfen und erstellen alle von Ihnen getroffenen Entscheidungen. Wählen Sie Create user (Benutzer erstellen) aus.
13. Nachdem der Benutzer konfiguriert wurde, gelangen Sie zur Detailseite des neuen Benutzers. Es wird ein Banner angezeigt, das besagt, dass der Benutzer erfolgreich erstellt wurde.

 Important

Wenn Sie eine Fehlermeldung erhalten, die Ihnen mitteilt, dass Sie nicht berechtigt sind, einen Benutzer zu erstellen, folgen Sie den Anweisungen in der Fehlermeldung, um Ihren Administrator aufzufordern, Ihnen Zugriff zu gewähren.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung, die ein neues AWS verwaltetes Microsoft AD-Benutzerkonto erstellt, mit der AWS Directory Service Data CLI formatiert wird. Sie müssen Ihre Verzeichnis-ID-Nummer und einen Benutzeranmeldenamen in Ihrer Anfrage angeben. Sie können dem `DisplayName` Attribut auch andere Attribute hinzufügen, z. B. einen Benutzeranzeigenamen. Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

So erstellen Sie einen AWS verwalteten Microsoft AD-Benutzer mit AWS CLI

- Öffnen Sie den folgenden Befehl AWS CLI, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen und den Anzeigenamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und die gewünschten Anmeldeinformationen:

```
aws ds-data create-user \  
  --directory-id d-1234567890 \  
  --sam-account-name "jane.doe" \  
  --other-attributes '{  
    "DisplayName" : { "S": "jane.doe"},  
    "Department":{ "S": "Legal"}  
  }'
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, die ein neues AWS verwaltetes Microsoft AD-Benutzerkonto mit erstellt AWS -Tools für PowerShell. Sie müssen Ihre Verzeichnis-ID-Nummer und einen Benutzeranmeldenamen in Ihrer Anfrage angeben. Sie können dem `DisplayName` Attribut auch andere Attribute hinzufügen, z. B. einen Benutzeranzeigenamen. Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

So erstellen Sie einen AWS verwalteten Microsoft AD-Benutzer mit Tools für PowerShell

- Öffnen Sie den folgenden Befehl PowerShell, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen und den Anzeigenamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und die gewünschten Anmeldeinformationen:

```
New-DSDUser `
  -DirectoryId d-1234567890 `
  -SAMAccountName "jane.doe" `
  -OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'jane.doe' }
    Department = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'Legal' }
  }
```

Einen AWS verwalteten Microsoft AD-Benutzer anzeigen und aktualisieren

Gehen Sie wie folgt vor, um die Details eines AWS verwalteten Microsoft AD-Benutzers mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder anzuzeigen oder zu aktualisieren AWS -Tools für PowerShell.

Details eines AWS verwalteten Microsoft AD-Benutzers anzeigen

Sie können die Details eines Benutzers im AWS-Managementkonsole oder anzeigen AWS CLI. Zu den Benutzerdetails gehören Profil- und Kontoinformationen sowie die Gruppenmitgliedschaft.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre

Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).

- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#).

AWS-Managementkonsole

Sie können die Details eines AWS verwalteten Microsoft AD-Benutzers in der einsehen AWS-Managementkonsole.

Um die Details und Kontodetails eines AWS verwalteten Microsoft AD-Benutzers mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Users (Benutzer) aus. Auf der Registerkarte wird eine Liste der Benutzer in Ihrem Verzeichnis angezeigt.
5. Wählen Sie einen Benutzer aus. Sie werden zum Bildschirm mit den Benutzerdetails weitergeleitet. Auf dem Bildschirm mit den Benutzerdetails werden die folgenden Informationen angezeigt:
 - Gruppen, in denen der Benutzer Mitglied ist (Gruppenmitgliedschaften)
 - Profildetails (wie Primärinformationen wie Benutzeranmeldename, Vorname, Nachname usw.)
 - Kontoeinstellungen (wie Kontoinformationen wie Benutzerprinzipalname, Dienstprinzipalname, definierter Name usw.)
 - Kontostatus

Weitere Informationen zu Benutzerattributen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und in der [MicrosoftDokumentation](#).

AWS CLI

Mit dem AWS CLI können Sie die Details eines Benutzers einsehen, darunter Profil- und Kontoinformationen sowie Gruppenmitgliedschaften.

Um das Profil und die Kontodetails eines AWS verwalteten Microsoft AD-Benutzers mit dem AWS CLI

Im Folgenden wird beschrieben, wie Sie die Details eines AWS verwalteten Microsoft AD-Benutzers mit der AWS Directory Service Data CLI anzeigen.

- Um die Details eines Benutzers anzuzeigen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Benutzernamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen:

```
aws ds-data describe-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Um die Gruppenmitgliedschaften eines Benutzers anzuzeigen

Im Folgenden wird beschrieben, wie Sie die Gruppenmitgliedschaft eines AWS verwalteten Microsoft AD-Benutzers mit der AWS Directory Service Data CLI anzeigen.

- Um die Gruppenmitgliedschaften eines Benutzers anzuzeigen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Benutzernamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen:

```
aws ds-data list-groups-for-member --directory-id d-1234567890 --sam-account-name "jane.doe"
```

Weitere Informationen zu Benutzerattributen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und in der [MicrosoftDokumentation](#).

AWS -Tools für PowerShell

Mit Tools für PowerShell können Sie die Details eines Benutzers anzeigen, darunter Profil- und Kontoinformationen sowie Gruppenmitgliedschaften.

So zeigen Sie das Profil und die Kontodetails eines AWS verwalteten Microsoft AD-Benutzers mit Tools für an PowerShell

Im Folgenden wird beschrieben, wie Sie die Details eines AWS verwalteten Microsoft AD-Benutzers mit den Tools für anzeigen PowerShell.

- Um die Details eines Benutzers anzuzeigen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Benutzernamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen:

```
Get-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Um die Gruppenmitgliedschaften eines Benutzers anzuzeigen

Im Folgenden wird beschrieben, wie Sie die Gruppenmitgliedschaft eines AWS verwalteten Microsoft AD-Benutzers mit den Tools für anzeigen PowerShell.

- Um die Gruppenmitgliedschaften eines Benutzers anzuzeigen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Benutzernamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen:

```
(Get-DSDGroupsForMemberList -DirectoryId d-1234567890 -SAMAccountName "jane.doe") .Groups
```

Weitere Informationen zu Benutzerattributen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und in der [MicrosoftDokumentation](#).

Aktualisierung der Daten eines AWS verwalteten Microsoft AD-Benutzers

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten in einem der AWS-Managementkonsole, AWS CLI, zu aktualisieren AWS -Tools für PowerShell.

Note

Die Mindestlänge eines Attributs ist 1.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#).

AWS-Managementkonsole

Sie können die Details eines AWS verwalteten Microsoft AD-Benutzers in der aktualisieren AWS-Managementkonsole.

Um die Details eines AWS verwalteten Microsoft AD-Benutzers mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Users (Benutzer) aus. Auf der Registerkarte wird eine Liste der Benutzer in Ihrem Verzeichnis angezeigt.

5. Wählen Sie einen Benutzer aus. Um einen Benutzer zu suchen, geben Sie den Benutzeranmeldenamen in das Suchfeld unter dem Abschnitt Benutzer ein. Sie werden zum Bildschirm mit den Benutzerdetails weitergeleitet.
6. Um Gruppen zu bearbeiten, in denen der Benutzer Mitglied ist, wählen Sie Gruppen. Auf dieser Registerkarte können Sie den Benutzer zu Gruppen hinzufügen und daraus entfernen. Weitere Informationen finden [Sie unter Hinzufügen eines AWS verwalteten Microsoft AD-Mitglieds zu einer Gruppe](#).
7. Um die Profildetails des Benutzers zu bearbeiten, wählen Sie Profil und dann Bearbeiten aus. Oder wählen Sie Aktionen und dann Benutzer bearbeiten aus. Nehmen Sie Ihre Aktualisierungen vor, überprüfen Sie sie und wählen Sie dann Speichern.

 Warning

Der Anmelde-name des Benutzers kann nicht geändert werden, nachdem der Benutzer erstellt wurde.

8. Um die Kontoeinstellungen des Benutzers zu bearbeiten, wählen Sie Benutzerkontoeinstellungen. Oder wählen Sie Aktionen und dann Benutzer bearbeiten. Nehmen Sie Ihre Aktualisierungen vor, überprüfen Sie sie und wählen Sie dann Speichern.

Weitere Informationen zu Benutzerattributen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und in der [MicrosoftDokumentation](#).

AWS CLI

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, mit der die Details eines AWS verwalteten Microsoft AD-Benutzers mit AWS Directory Service Data CLI aktualisiert werden.

Wenn Sie ein Benutzerkonto aktualisieren, müssen Sie Ihre Verzeichnis-ID-Nummer und Ihren Benutzeranmeldenamen angeben. Sie müssen auch den Aktualisierungstyp und das Attribut, die Sie aktualisieren möchten, in Ihrer Anfrage angeben, z. B. den Nachnamen eines Benutzers mit dem Surname Parameter. Weitere Informationen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#).

- Um die Details eines Benutzers zu aktualisieren, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen, den Benutzertyp und den Attributwert durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Ihren Benutzernamen und den gewünschten Benutzertyp und Attributwert:


```
aws ds-data update-user --directory-id d-1234567890 --sam-account-name "jane.doe" --  
update-type "REPLACE" --surname "Doe"
```

Note

Wenn Sie Benutzerattribute mit dem CLI-Befehl [update-user](#) entfernen, müssen Sie das Attribut und den genauen Wert angeben, der entfernt werden soll. Verwenden Sie den Befehl [describe-user](#), um Benutzerattribute zu ermitteln.

[Weitere Informationen zu Benutzerattributen finden Sie unter AWS Verzeichnisdienst-Datenattribute und Microsoft in der Dokumentation.](#)

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, mit der die Details eines AWS verwalteten Microsoft AD-Benutzers aktualisiert AWS -Tools für PowerShell werden.

Wenn Sie ein Benutzerkonto aktualisieren, müssen Sie Ihre Verzeichnis-ID-Nummer und Ihren Benutzeranmeldenamen angeben. Sie müssen auch den Aktualisierungstyp und das Attribut, die Sie aktualisieren möchten, in Ihrer Anfrage angeben, z. B. den Nachnamen eines Benutzers mit dem Surname Parameter. Weitere Informationen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#).

- Um die Details eines Benutzers zu aktualisieren, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen, den Benutzertyp und den Attributwert durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Ihren Benutzernamen und den gewünschten Benutzertyp und Attributwert:

```
Update-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe" -UpdateType  
"REPLACE" -Surname "Doe"
```

Weitere Informationen zu Benutzerattributen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und in der [MicrosoftDokumentation](#).

Löschen eines AWS verwalteten Microsoft AD-Benutzers

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole, AWS CLI, zu löschen AWS -Tools für PowerShell.

Important

Wenn Sie ein Benutzerkonto aus einem Verzeichnis löschen, werden alle Informationen über den Benutzer entfernt, einschließlich aller Berechtigungen, über die der Benutzer für den Zugriff auf sein Konto und seine Anwendungen verfügt.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#).

AWS-Managementkonsole

Sie können ein AWS verwaltetes Microsoft AD-Benutzerkonto in der löschen AWS-Managementkonsole.

Um ein AWS verwaltetes Microsoft AD-Benutzerkonto mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Users (Benutzer) aus. Auf der Registerkarte wird eine Liste der Benutzer in Ihrem Verzeichnis angezeigt.
5. Wählen Sie den Benutzer aus, dessen Konto Sie löschen möchten. Um einen Benutzer zu finden, geben Sie den Benutzeranmeldenamen in das Suchfeld unter dem Abschnitt Benutzer ein. Sie werden zum Bildschirm mit den Benutzerdetails weitergeleitet.
6. Wählen Sie Aktionen. Wählen Sie dann Benutzerkonto löschen und erneut Benutzerkonto löschen.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung, mit der das Konto eines AWS verwalteten Microsoft AD-Benutzers gelöscht wird, mit der AWS Directory Service Data CLI formatiert wird.

Um ein AWS verwaltetes Microsoft AD-Benutzerkonto zu löschen mit AWS CLI

- Öffnen Sie den AWS CLI und führen Sie den folgenden Befehl aus, wobei Sie die Verzeichnis-ID und den Benutzernamen durch Ihre AWS Managed Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen ersetzen:

```
aws ds-data delete-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, mit AWS -Tools für PowerShell der das Konto eines AWS verwalteten Microsoft AD-Benutzers gelöscht wird.

Um ein AWS verwaltetes Microsoft AD-Benutzerkonto zu löschen mit AWS -Tools für PowerShell

- Öffnen Sie den folgenden Befehl PowerShell, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Benutzernamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen:

```
Remove-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

Deaktivieren eines AWS verwalteten Microsoft AD-Benutzers

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder zu deaktivieren AWS -Tools für PowerShell.

Important

Wenn Sie das Konto eines Benutzers deaktivieren, verliert der Benutzer alle Zugriffsberechtigungen für sein Konto und seine Anwendungen.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#).

AWS-Managementkonsole

Sie können ein AWS verwaltetes Microsoft AD-Benutzerkonto in der deaktivieren AWS-Managementkonsole.

Um ein AWS verwaltetes Microsoft AD-Benutzerkonto mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Users (Benutzer) aus. Auf der Registerkarte wird eine Liste der Benutzer in Ihrem Verzeichnis angezeigt.
5. Wählen Sie den Benutzer aus, dessen Konto Sie deaktivieren möchten. Sie werden zum Bildschirm mit den Benutzerdetails weitergeleitet.
6. Wählen Sie Aktionen. Wählen Sie dann Benutzerkonto deaktivieren und erneut Benutzerkonto deaktivieren.

Note

Um Ihr Benutzerkonto wieder zu aktivieren, müssen Sie das Benutzerkennwort zurücksetzen. Weitere Informationen finden Sie unter [Das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen und aktivieren](#).

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung, die ein AWS verwaltetes Microsoft AD-Benutzerkonto deaktiviert, mit der AWS Directory Service Data CLI formatiert wird.

Um ein AWS verwaltetes Microsoft AD-Benutzerkonto mit dem AWS CLI

- Öffnen Sie den AWS CLI und führen Sie den folgenden Befehl aus, wobei Sie die Verzeichnis-ID und den Benutzernamen durch Ihre AWS Managed Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen ersetzen:

```
aws ds-data disable-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

 Note

Um Ihr Benutzerkonto wieder zu aktivieren, müssen Sie das Benutzerkennwort zurücksetzen. Weitere Informationen finden Sie unter [Das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen und aktivieren](#).

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, die ein AWS verwaltetes Microsoft AD-Benutzerkonto mit AWS -Tools für PowerShell deaktiviert.

Um ein AWS verwaltetes Microsoft AD-Benutzerkonto zu deaktivieren mit AWS -Tools für PowerShell

- Öffnen Sie PowerShell, und führen Sie den folgenden Befehl aus, wobei Sie die Verzeichnis-ID und den Benutzernamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und Ihren Benutzernamen ersetzen:

```
Disable-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

 Note

Um Ihr Benutzerkonto wieder zu aktivieren, müssen Sie das Benutzerkennwort zurücksetzen. Weitere Informationen finden Sie unter [Das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen und aktivieren](#).

Das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen und aktivieren

Gehen Sie wie folgt vor, um das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurückzusetzen, um sein Konto mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienst Daten in einem der AWS-Managementkonsole, AWS CLI, zu aktivieren AWS -Tools für PowerShell.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#).

AWS-Managementkonsole

Sie können das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen, um sein Konto in der zu aktivieren AWS-Managementkonsole. Sie können diese Aufgabe entweder im Fenster Verzeichnisse oder im Fenster mit den Verzeichnisdetails ausführen.

Verzeichnisse

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie Aktionen und dann Benutzerpasswort zurücksetzen und Konto aktivieren.
 - a. Geben Sie unter Benutzeranmeldename den Benutzeranmeldenamen für den Benutzer ein, dessen Passwort Sie zurücksetzen möchten.
 - b. Geben Sie unter Neues Passwort das neue Passwort des Benutzers ein.
 - c. Geben Sie unter Passwort bestätigen erneut das neue Passwort des Benutzers ein.

4. Nachdem Sie das neue Passwort des Benutzers bestätigt haben, wählen Sie Passwort zurücksetzen und Konto aktivieren.

Angaben zum Verzeichnis

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrer anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Users (Benutzer) aus. Auf der Registerkarte wird eine Liste der Benutzer in Ihrem Verzeichnis angezeigt.
5. Wählen Sie den Benutzer aus, dessen Passwort Sie zurücksetzen möchten.
6. Wählen Sie Aktionen und dann Benutzerkennwort zurücksetzen und Konto aktivieren.
 - a. Geben Sie unter Neues Passwort das neue Passwort des Benutzers ein.
 - b. Geben Sie unter Passwort bestätigen erneut das neue Passwort des Benutzers ein.
7. Nachdem Sie das neue Passwort des Benutzers bestätigt haben, wählen Sie Passwort zurücksetzen und Konto aktivieren.

AWS CLI

Sie können das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen, um sein Konto mit der AWS Directory Service Data CLI zu aktivieren.

Note

Der Befehl zum Zurücksetzen des Benutzerkennworts verwendet `aws ds`.

Um das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurückzusetzen mit dem AWS CLI

- Um das Passwort eines Benutzers zurückzusetzen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen und das Passwort durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Ihren Benutzernamen und die gewünschten Anmeldeinformationen:

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

AWS -Tools für PowerShell

Sie können das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurücksetzen, um sein Konto mit zu aktivieren AWS -Tools für PowerShell.

Um das Passwort eines AWS verwalteten Microsoft AD-Benutzers zurückzusetzen mit AWS -Tools für PowerShell

- Um das Passwort eines Benutzers zurückzusetzen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen und das Passwort durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Ihren Benutzernamen und die gewünschten Anmeldeinformationen:

```
Reset-DSUserPassword -DirectoryId d-1234567890 -UserName "jane.doe" -NewPassword "your-password"
```

Eine AWS verwaltete Microsoft AD-Gruppe erstellen

Gehen Sie wie folgt vor, um eine AWS verwaltete Microsoft AD-Gruppe mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder zu erstellen AWS -Tools für PowerShell.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen.](#)

- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).

AWS-Managementkonsole

Sie können eine neue AWS verwaltete Microsoft AD-Gruppe in der erstellen AWS-Managementkonsole. Wenn Sie eine neue Gruppe erstellen, geben Sie die Details der Gruppe an und bestimmen den [Typ und den Umfang der Gruppe](#). Sie haben auch die Möglichkeit, Ihrer neuen Gruppe Benutzer und untergeordnete Gruppen hinzuzufügen oder Ihre neue Gruppe einer übergeordneten Gruppe hinzuzufügen.

Um eine AWS verwaltete Microsoft AD-Gruppe mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Gruppe. Die Registerkarte zeigt eine Liste der Gruppen in Ihrem AWS-Region.
5. Wählen Sie Create group (Gruppe erstellen) aus. Sie werden zu einem Verfahren weitergeleitet, in dem Sie die Erstellung Ihrer neuen Gruppe abschließen.
6. Die Seite „Gruppendetails angeben“ wird geöffnet. Geben Sie einen Gruppennamen ein. Gruppennamen müssen die folgenden Bedingungen erfüllen:

- Muss ein eindeutiger Gruppenname sein
- Kann bis zu 64 Zeichen lang sein
- Kann nur alphanumerische Zeichen enthalten
- ~!@#\$%^&* _-+=`|()\{\}[]:;'"<>,.?/

 Warning

Der Gruppenname kann nach der Erstellung der Gruppe nicht geändert werden.

7. Wählen Sie den Gruppentyp aus einer der folgenden Optionen aus:
 - Sicherheit
 - Verteilung
 - Weitere Informationen hierzu finden Sie unter [the section called “Group type \(Gruppentyp\)”](#).
8. Wählen Sie den Gruppenbereich aus einer der folgenden Optionen aus:
 - Domäne: lokal
 - Universell
 - Global
 - Sie können die Option Bereiche vergleichen aktivieren, um ein Diagramm mit den Ähnlichkeiten und Unterschieden zwischen Gruppenbereichen anzuzeigen. Weitere Informationen hierzu finden Sie unter [the section called “Group scope \(Gruppenumfang\)”](#).
9. Nachdem Sie die wichtigsten Informationen und Kontaktmethoden angegeben haben, wählen Sie Weiter.
10. Die Seite Benutzer zur Gruppe hinzufügen — optional wird geöffnet, und Sie können der neuen Gruppe Benutzer hinzufügen. Um einen Benutzer zu finden, der der Gruppe hinzugefügt werden soll, geben Sie den Benutzeranmeldenamen in das Suchfeld unter dem Abschnitt Benutzer ein. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und klicken Sie auf Weiter.
11. Die Seite „Untergeordnete Gruppen hinzufügen — optional“ wird geöffnet, auf der Sie der neuen Gruppe vorhandene Gruppen hinzufügen können. Die vorhandenen Gruppen werden zu untergeordneten Gruppen der neu erstellten Gruppe. Wenn Sie Ihrer Gruppe eine untergeordnete Gruppe hinzufügen, wird Ihre Gruppe zur übergeordneten Gruppe, und die

untergeordnete Gruppe erbt alle Rollen und Berechtigungen Ihrer Gruppe. Um Gruppen zum Hinzufügen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Untergeordnete Gruppen hinzufügen ein. Wählen Sie die Kindergruppen aus, die Sie der neuen Gruppe hinzufügen möchten, und klicken Sie auf Weiter.

12. Die Seite „Elterngruppen hinzufügen — optional“ wird geöffnet, auf der Sie die neue Gruppe zu bestehenden Gruppen hinzufügen können. Die neue Gruppe wird zur übergeordneten Gruppe der vorhandenen Gruppen. Wenn Sie Ihre Gruppe zu einer übergeordneten Gruppe hinzufügen, wird Ihre Gruppe zur untergeordneten Gruppe und erbt alle Rollen und Berechtigungen der übergeordneten Gruppe. Um Gruppen zum Hinzufügen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Übergeordnete Gruppen hinzufügen ein. Wählen Sie die übergeordneten Gruppen aus, die Sie der neuen Gruppe hinzufügen möchten, und klicken Sie auf Weiter.
13. Überprüfen Sie auf der Seite Gruppe überprüfen und erstellen Ihre Auswahl und wählen Sie dann Gruppe erstellen aus.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung, die eine AWS verwaltete Microsoft AD-Gruppe erstellt, mit der AWS Directory Service Data CLI formatiert wird. Wenn Sie eine neue Gruppe erstellen, müssen Sie Ihre Verzeichnis-ID-Nummer und einen Gruppennamen angeben. Sie können dem DisplayName Attribut auch andere Attribute hinzufügen, z. B. einen Gruppenanzeigenamen. Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

Um eine AWS verwaltete Microsoft AD-Gruppe mit dem AWS CLI

- Öffnen Sie den folgenden Befehl AWS CLI, und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen und den Gruppenanzeigenamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Ihren Benutzernamen und den gewünschten Gruppenanzeigenamen:

```
aws ds-data create-group \
  --directory-id d-1234567890 \
  --sam-account-name "your-group-name" \
  --other-attributes '{
    "DisplayName": { "S": "myGroupDisplayName" }
    "Description": { "S": "myGroupDescription" }
```

```
}'
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, mit der eine AWS verwaltete Microsoft AD-Gruppe erstellt wird AWS -Tools für PowerShell. Wenn Sie eine neue Gruppe erstellen, müssen Sie Ihre Verzeichnis-ID-Nummer und einen Gruppennamen angeben. Sie können dem `DisplayName` Attribut auch andere Attribute hinzufügen, z. B. einen Gruppenanzeigenamen. Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

Um eine AWS verwaltete Microsoft AD-Gruppe zu erstellen mit AWS -Tools für PowerShell

- Öffnen Sie den folgenden Befehl PowerShell, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, den Benutzernamen und den Gruppenanzeigenamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Ihren Benutzernamen und den gewünschten Gruppenanzeigenamen:

```
New-DSGroup `
  -DirectoryId d-1234567890 `
  -SAMAccountName "your-group-name" `
  -OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'myGroupDisplayName' }
    Description = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'myGroupDescription' }
  }
```

Details einer AWS verwalteten Microsoft AD-Gruppe anzeigen und aktualisieren

Gehen Sie wie folgt vor, um die Details einer AWS verwalteten Microsoft AD-Gruppe mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder anzuzeigen oder zu aktualisieren AWS -Tools für PowerShell.

Details einer AWS verwalteten Microsoft AD-Gruppe anzeigen

Sie können die Details einer Gruppe im AWS-Managementkonsole AWS CLI, oder anzeigen oder aktualisieren AWS -Tools für PowerShell.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen einer AWS verwalteten Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können die Details einer AWS verwalteten Microsoft AD-Gruppe in der einsehen AWS-Managementkonsole.

Um die Details der AWS verwalteten Microsoft AD-Gruppe anzuzeigen mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Gruppe. Die Registerkarte zeigt eine Liste der Gruppen in Ihrem AWS-Region.
5. Wählen Sie eine Gruppe aus. Um Gruppen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Sie werden zum Bildschirm mit den

Gruppendetails weitergeleitet. Auf dem Bildschirm mit den Gruppendetails werden die folgenden Informationen angezeigt:

- Auf der Registerkarte „Mitglieder“ werden die Benutzer und untergeordneten Gruppen aufgeführt, die Mitglieder Ihrer Gruppe sind.
- Auf der Registerkarte „Übergeordnete Gruppen“ werden die übergeordneten Gruppen aufgeführt, in denen Ihre Gruppe Mitglied ist.
- Auf der Registerkarte „Eigenschaften“ werden die Gruppeneigenschaften aufgeführt (z. B. Hauptinformationen wie Gruppenname, Anzeigename der Gruppe usw.).

AWS CLI

Sie können die Details einer AWS verwalteten Microsoft AD-Gruppe mit der AWS Directory Service Data CLI anzeigen.

Um die Details einer AWS verwalteten Microsoft AD-Gruppe mit dem AWS CLI

Im Folgenden wird beschrieben, wie Sie die Details einer AWS verwalteten Microsoft AD-Gruppe mit dem anzeigen AWS CLI.

- Um die Details einer Gruppe anzuzeigen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Gruppennamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den Gruppennamen:

```
aws ds-data describe-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

So zeigen Sie die Gruppenmitglieder einer AWS verwalteten Microsoft AD-Gruppe mit dem AWS CLI

Im Folgenden wird beschrieben, wie Sie die Mitglieder einer AWS verwalteten Microsoft AD-Gruppe mit dem anzeigen AWS CLI.

- Um die Details einer Gruppe anzuzeigen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Gruppennamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den Gruppennamen:

```
aws ds-data list-group-members --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS -Tools für PowerShell

Sie können die Details einer AWS verwalteten Microsoft AD-Gruppe mit anzeigen AWS -Tools für PowerShell.

Um die Details einer AWS verwalteten Microsoft AD-Gruppe anzuzeigen mit AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie die Details einer AWS verwalteten Microsoft AD-Gruppe mit den Tools für anzeigen PowerShell.

- Um die Details einer Gruppe anzuzeigen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Gruppennamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den Gruppennamen:

```
Get-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Um die Gruppenmitglieder einer AWS verwalteten Microsoft AD-Gruppe anzuzeigen mit AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie die Mitglieder einer AWS verwalteten Microsoft AD-Gruppe mit den Tools für anzeigen PowerShell.

- Um die Details einer Gruppe anzuzeigen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Gruppennamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den Gruppennamen:

```
(Get-DSDGroupMemberList -DirectoryId d-1234567890 -SAMAccountName "your-group-name").Members
```

Aktualisierung der Details einer AWS verwalteten Microsoft AD-Gruppe

Gehen Sie wie folgt vor, um die Details einer AWS verwalteten Microsoft AD-Gruppe mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder zu aktualisieren AWS -Tools für PowerShell.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen einer AWS verwalteten Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können die Details einer Gruppe mit dem aktualisieren AWS-Managementkonsole. Weitere Informationen finden Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#)

Um die Details einer AWS verwalteten Microsoft AD-Gruppe zu aktualisieren mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Gruppe. Die Registerkarte zeigt eine Liste der Gruppen in Ihrem AWS-Region.

5. Wähle eine Gruppe. Um Gruppen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet.
6. Um Benutzer und untergeordnete Gruppen zu bearbeiten, die Mitglieder Ihrer Gruppe sind, wählen Sie Mitglieder. Auf dieser Registerkarte können Sie Benutzer und Kindergruppen zu Ihrer Gruppe hinzufügen und daraus entfernen. Weitere Informationen finden Sie unter [Mitglieder zu Gruppen und Gruppen zu Gruppen hinzufügen und entfernen](#).
7. Um übergeordnete Gruppen zu bearbeiten, in denen Ihre Gruppe Mitglied ist, wählen Sie Übergeordnete Gruppen. Auf dieser Registerkarte können Sie Ihre Gruppe zu übergeordneten Gruppen hinzufügen und daraus entfernen. Weitere Informationen finden Sie unter [Mitglieder zu Gruppen und Gruppen zu Gruppen hinzufügen und entfernen](#).
8. Um Ihre Gruppeneigenschaften zu bearbeiten, wählen Sie Eigenschaften und dann Bearbeiten. Oder wählen Sie Aktionen und dann Gruppe bearbeiten aus. Nehmen Sie Ihre Aktualisierungen vor, überprüfen Sie sie und wählen Sie dann Speichern.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anfrage, die die Details einer AWS verwalteten Microsoft AD-Gruppe aktualisiert, mit der AWS Directory Service Data CLI formatiert wird.

Wenn Sie eine Gruppe aktualisieren, müssen Sie Ihre Verzeichnis-ID-Nummer und Ihren Gruppennamen angeben. Sie müssen auch den Aktualisierungstyp und das Attribut, das Sie aktualisieren möchten, in Ihrer Anfrage angeben, z. B. eine Gruppen-E-Mail-Adresse mit dem `EmailAddress` Parameter. Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

- Um die Details einer AWS verwalteten Microsoft AD-Gruppe zu aktualisieren mit dem AWS CLI

Um die Details einer Gruppe zu aktualisieren, öffnen Sie den folgenden Befehl AWS CLI, und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, den Gruppennamen, den Aktualisierungstyp und das Attribut durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, den Gruppennamen und den gewünschten Aktualisierungstyp und das gewünschte Attribut:

```
aws ds-data update-group --directory-id d-1234567890 --sam-account-name "your-group-name" --update-type "REPLACE" --group-scope "global"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, mit der die Details einer AWS verwalteten Microsoft AD-Gruppe aktualisiert AWS -Tools für PowerShell werden.

Wenn Sie eine Gruppe aktualisieren, müssen Sie Ihre Verzeichnis-ID-Nummer und Ihren Gruppennamen angeben. Sie müssen auch den Aktualisierungstyp und das Attribut, das Sie aktualisieren möchten, in Ihrer Anfrage angeben, z. B. eine Gruppen-E-Mail-Adresse mit dem `EmailAddress` Parameter. Weitere Informationen erhalten Sie unter [AWS Verzeichnisdienst-Datenattribute](#) und [Gruppentyp und Gruppenumfang](#).

- Um die Details einer AWS verwalteten Microsoft AD-Gruppe zu aktualisieren mit AWS -Tools für PowerShell

Um die Details einer Gruppe zu aktualisieren, öffnen Sie den folgenden Befehl PowerShell, und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, den Gruppennamen, den Aktualisierungstyp und das Attribut durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, den Gruppennamen und den gewünschten Aktualisierungstyp und das gewünschte Attribut:

```
Update-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name" -  
UpdateType "REPLACE" -GroupScope "global"
```

Löschen einer AWS verwalteten Microsoft AD-Gruppe

Gehen Sie wie folgt vor, um eine AWS verwaltete Microsoft AD-Gruppe mit Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten im AWS-Managementkonsole AWS CLI, oder zu löschen AWS -Tools für PowerShell.

Important

Wenn Sie eine Gruppe löschen, werden alle Informationen über die Gruppe entfernt, einschließlich aller Berechtigungen, die Gruppenmitglieder erben.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen Sie eine AWS verwaltete Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können eine AWS verwaltete Microsoft AD-Gruppe in der löschen AWS-Managementkonsole.

Um eine AWS verwaltete Microsoft AD-Gruppe mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Wählen Sie Gruppe. Die Registerkarte zeigt eine Liste der Gruppen in Ihrem AWS-Region.
5. Wählen Sie die Gruppe aus, die Sie löschen möchten. Um nach Gruppen zu suchen, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet.
6. Wählen Sie Delete group (Gruppe löschen) aus. Es erscheint ein Dialogfeld, in dem Sie Bestätigen wählen können, um die Gruppe zu löschen.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anforderung, die eine AWS verwaltete Microsoft AD-Gruppe löscht, mit der AWS Directory Service Data CLI formatiert wird.

Um eine AWS verwaltete Microsoft AD-Gruppe mit dem AWS CLI

- Öffnen Sie den folgenden Befehl AWS CLI, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Gruppennamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den Gruppennamen:

```
aws ds-data delete-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, die eine AWS verwaltete Microsoft AD-Gruppe löscht, mit dem AWS -Tools für PowerShell.

Um eine AWS verwaltete Microsoft AD-Gruppe mit dem AWS -Tools für PowerShell

- Öffnen Sie den folgenden Befehl PowerShell, und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID und den Gruppennamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID und den Gruppennamen:

```
Remove-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

Hinzufügen und Entfernen von AWS verwalteten Microsoft AD-Mitgliedern zu Gruppen und Gruppen zu Gruppen

Mit der [AWS Directory Service Data API](#) kann ein Mitglied ein Benutzer, eine Gruppe oder ein Computer sein. Ein Benutzer steht für eine Person oder Entität, die auf Ihr Verzeichnis zugreifen kann. Gruppen ermöglichen es Ihnen, mehr als einem Benutzer gleichzeitig Berechtigungen zu erteilen oder zu verweigern.

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer zu einer Gruppe oder eine Gruppe zu einer anderen Gruppe hinzuzufügen oder zu entfernen, wobei Benutzer- und

Gruppenverwaltung oder AWS Verzeichnisdienstdaten entweder im AWS-Managementkonsole AWS CLI, oder enthalten sind AWS -Tools für PowerShell.

Einen Benutzer zu einer Gruppe hinzufügen

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer zu einer Gruppe hinzuzufügen, deren Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten entweder im AWS-Managementkonsole AWS CLI, oder enthalten sind AWS -Tools für PowerShell.

 Important

Wenn Sie einer Gruppe einen AWS verwalteten Microsoft AD-Benutzer hinzufügen, erbt der Benutzer die Rollen und Berechtigungen, die der Gruppe zugewiesen sind. Diese Rollen und Berechtigungen sind Teil der Gruppenmitgliedschaften des Benutzers.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen Sie einen AWS verwalteten Microsoft AD-Benutzer](#).
- [Erstellen Sie eine AWS verwaltete Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können ein AWS verwaltetes Microsoft AD-Mitglied zu einer Gruppe mit dem hinzufügen AWS-Managementkonsole.

Um einen AWS verwalteten Microsoft AD-Benutzer zu einer Gruppe hinzuzufügen mit AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Um nach Gruppen zu suchen, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Auf der Registerkarte wird eine Liste der Gruppen in Ihrem angezeigt AWS-Region.
5. Wählen Sie eine Gruppe aus. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet.
6. Wählen Sie Mitglieder aus. Auf der Registerkarte wird eine Liste der Benutzer und untergeordneten Gruppen nach Mitgliedstyp in Ihrer Gruppe angezeigt.
7. Wählen Sie auf der Registerkarte Mitglieder die Option Mitglied hinzufügen aus.
8. Wählen Sie unter Mitglieder den Benutzer aus, den Sie zu Ihrer Gruppe hinzufügen möchten, und klicken Sie dann auf Mitglied zur Gruppe hinzufügen. Um nach Mitgliedern zu suchen, geben Sie den Benutzeranmeldenamen für Benutzer und den Gruppennamen für Gruppen in das Suchfeld unter dem Abschnitt Mitglieder ein.

AWS CLI

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, die ein AWS verwaltetes Microsoft AD-Mitglied zu einer Gruppe mit der AWS Directory Service Data CLI hinzufügt.

Um einen AWS verwalteten Microsoft AD-Benutzer zu einer Gruppe hinzuzufügen mit AWS CLI

- Um einen Benutzer zu einer Gruppe hinzuzufügen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und

Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID sowie Gruppen- und Mitgliedsnamen:

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, mit der ein AWS verwaltetes Microsoft AD-Mitglied zu einer Gruppe mit hinzugefügt wird AWS -Tools für PowerShell.

Um einen AWS verwalteten Microsoft AD-Benutzer zu einer Gruppe hinzuzufügen mit AWS -Tools für PowerShell

- Um einen Benutzer zu einer Gruppe hinzuzufügen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID sowie Gruppen- und Mitgliedsnamen:

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

Einen Benutzer aus einer Gruppe entfernen

Mit der [AWS Directory Service Data API](#) kann ein Mitglied ein Benutzer, eine Gruppe oder ein Computer sein. Ein Benutzer steht für eine Person oder Entität, die auf Ihr Verzeichnis zugreifen kann. Gruppen ermöglichen es Ihnen, mehr als einem Benutzer gleichzeitig Berechtigungen zu erteilen oder zu verweigern.

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer aus einer Gruppe zu entfernen, deren Benutzer- und Gruppenverwaltung oder AWS Verzeichnisdienstdaten entweder im AWS-Managementkonsole AWS CLI, oder enthalten sind AWS -Tools für PowerShell.

 Important

Wenn Sie einen AWS verwalteten Microsoft AD-Benutzer aus einer Gruppe entfernen, verliert der Benutzer den Zugriff auf die Rollen und Berechtigungen, die der Gruppe zugewiesen sind. Diese Rollen und Berechtigungen sind Teil der Gruppenmitgliedschaften.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen Sie einen AWS verwalteten Microsoft AD-Benutzer](#).
- [Erstellen Sie eine AWS verwaltete Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können ein AWS verwaltetes Microsoft AD-Mitglied aus einer Gruppe mit dem entfernen AWS-Managementkonsole.

Um einen AWS verwalteten Microsoft AD-Benutzer aus einer Gruppe mit dem zu entfernen AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.

2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Auf der Registerkarte wird eine Liste der Gruppen in Ihrem angezeigt AWS-Region.
5. Wähle eine Gruppe. Um Gruppen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet.
6. Wählen Sie Mitglieder aus. Auf der Registerkarte wird eine Liste der Benutzer und untergeordneten Gruppen nach Mitgliedstyp in Ihrer Gruppe angezeigt.
7. Wählen Sie den Benutzer aus, den Sie aus Ihrer Gruppe entfernen möchten, und klicken Sie dann auf Entfernen. Um nach Benutzern zu suchen, geben Sie den Benutzeranmeldenamen in das Suchfeld im Bereich Mitglieder ein.
8. Bestätigen Sie, dass Sie den Benutzer aus Ihrer Gruppe entfernen möchten, und wählen Sie dann erneut Entfernen.

AWS CLI

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, die ein AWS verwaltetes Microsoft AD-Mitglied mit der AWS Directory Service Data CLI aus einer Gruppe entfernt.

Um einen AWS verwalteten Microsoft AD-Benutzer aus einer Gruppe zu entfernen mit AWS CLI

- Um einen Benutzer aus einer Gruppe zu entfernen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Gruppen- und Mitgliedsnamen:

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, mit der ein AWS verwaltetes Microsoft AD-Mitglied aus einer Gruppe mit entfernt wird AWS -Tools für PowerShell.

Um einen AWS verwalteten Microsoft AD-Benutzer aus einer Gruppe zu entfernen mit AWS -Tools für PowerShell

- Um einen Benutzer aus einer Gruppe zu entfernen, öffnen Sie den PowerShell folgenden Befehl und führen Sie ihn aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Gruppen- und Mitgliedsnamen:

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -  
MemberName "jane.doe"
```

Eine Gruppe zu einer Gruppe hinzufügen

Wenn Sie eine AWS verwaltete Microsoft AD-Gruppe zu einer anderen Gruppe hinzufügen, teilen sich die Gruppen eine Eltern-Kind-Beziehung. Die untergeordnete Gruppe erhält Zugriff auf die Rollen und Berechtigungen, die der übergeordneten Gruppe zugewiesen sind. Sie können Ihrer Gruppe eine untergeordnete Gruppe und Ihre Gruppe einer übergeordneten Gruppe hinzufügen.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie:](#)

[AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).

- [Erstellen Sie eine AWS verwaltete Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können eine AWS verwaltete Microsoft AD-Gruppe zu einer Gruppe mit dem hinzufügen AWS-Managementkonsole.

Um Ihrer Gruppe eine untergeordnete Gruppe hinzuzufügen mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Auf der Registerkarte wird eine Liste der Gruppen in Ihrem angezeigt AWS-Region.
5. Wähle eine Gruppe. Um Gruppen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet.
6. Wählen Sie Mitglieder aus. Auf der Registerkarte wird eine Liste der Benutzer und untergeordneten Gruppen nach Mitgliedstyp in Ihrer Gruppe angezeigt.
7. Wählen Sie Mitglied hinzufügen aus.
8. Wählen Sie unter Mitglieder die untergeordneten Gruppen aus, die Sie zu Ihrer Gruppe hinzufügen möchten, und wählen Sie dann Mitglied zur Gruppe hinzufügen aus.

Um eine übergeordnete Gruppe zu einer Gruppe hinzuzufügen, verwenden Sie AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.

2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Auf der Registerkarte wird eine Liste der Gruppen in Ihrem angezeigt AWS-Region.
5. Wähle eine Gruppe. Um Gruppen zu finden, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet.
6. Wählen Sie Übergeordnete Gruppen aus. Auf der Registerkarte wird eine Liste der Gruppen angezeigt, in denen Ihre Gruppe Mitglied ist.
7. Wählen Sie Übergeordnete Gruppen hinzufügen aus.
8. Wählen Sie unter Gruppen die Gruppe (n) aus, zu der Sie Ihre Gruppe hinzufügen möchten, und wählen Sie dann erneut Übergeordnete Gruppen hinzufügen aus.

AWS CLI

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, die eine AWS verwaltete Microsoft AD-Gruppe zu einer Gruppe mit der AWS Directory Service Data CLI hinzufügt.

Um Ihrer Gruppe eine untergeordnete Gruppe hinzuzufügen, verwenden Sie AWS CLI

- Um einer übergeordneten Gruppe eine untergeordnete Gruppe hinzuzufügen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Gruppen- und Mitgliedsnamen:

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, mit der eine AWS verwaltete Microsoft AD-Gruppe zu einer Gruppe mit hinzugefügt wird AWS -Tools für PowerShell.

Um Ihrer Gruppe eine untergeordnete Gruppe hinzuzufügen mit AWS -Tools für PowerShell

- Um einer übergeordneten Gruppe eine untergeordnete Gruppe hinzuzufügen, öffnen Sie den PowerShell folgenden Befehl und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Gruppen- und Mitgliedsnamen:

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -  
MemberName "child-group-name"
```

Eine Gruppe aus einer Gruppe entfernen

Wenn Sie eine AWS verwaltete Microsoft AD-Gruppe aus einer anderen Gruppe entfernen, besteht zwischen den Gruppen keine Eltern-Kind-Beziehung mehr. Die untergeordnete Gruppe verliert den Zugriff auf die Rollen und Berechtigungen, die der übergeordneten Gruppe zugewiesen sind. Sie können eine untergeordnete Gruppe aus Ihrer Gruppe und Ihre Gruppe aus einer übergeordneten Gruppe entfernen.

Bevor Sie mit einem der beiden Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen Sie eine AWS verwaltete Microsoft AD-Gruppe](#).

AWS-Managementkonsole

Sie können eine AWS verwaltete Microsoft AD-Gruppe zu einer Gruppe mit dem entfernen AWS-Managementkonsole.

Um eine untergeordnete Gruppe aus Ihrer Gruppe zu entfernen, verwenden Sie den AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Auf der Registerkarte wird eine Liste der Gruppen in Ihrem angezeigt AWS-Region.
5. Wähle eine Gruppe. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet. Um nach Gruppen zu suchen, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein.
6. Wählen Sie Mitglieder aus. Auf der Registerkarte wird eine Liste der Benutzer und untergeordneten Gruppen nach Mitgliedstyp in Ihrer Gruppe angezeigt.
7. Wählen Sie die Kindergruppe (n) aus, die Sie aus Ihrer Gruppe entfernen möchten, und klicken Sie dann auf Entfernen.
8. Bestätigen Sie die Kindergruppe (n), die Sie aus Ihrer Gruppe entfernen möchten, und wählen Sie dann erneut Entfernen aus.

Um Ihre Gruppe aus einer übergeordneten Gruppe zu entfernen, verwenden Sie AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.

3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Auf der Registerkarte wird eine Liste der Gruppen in Ihrer AWS-Region angezeigt.
5. Wählen Sie eine Gruppe. Sie werden zum Bildschirm mit den Gruppendetails weitergeleitet. Um nach Gruppen zu suchen, geben Sie den Gruppennamen in das Suchfeld unter dem Abschnitt Gruppen ein.
6. Wählen Sie Übergeordnete Gruppen aus. Auf der Registerkarte wird eine Liste der Gruppen angezeigt, in denen Ihre Gruppe Mitglied ist.
7. Wählen Sie die übergeordnete Gruppe aus, aus der Sie Ihre Gruppe entfernen möchten, und wählen Sie dann Übergeordnete Gruppen entfernen aus.
8. Bestätigen Sie die übergeordnete Gruppe, aus der Sie Ihre Gruppe entfernen möchten, und wählen Sie dann erneut Übergeordnete Gruppen entfernen aus.

AWS CLI

Im Folgenden wird beschrieben, wie Sie eine Anfrage formatieren, die eine AWS verwaltete Microsoft AD-Gruppe in eine Gruppe mit der AWS Directory Service Data CLI entfernt.

- Um eine untergeordnete Gruppe aus einer übergeordneten Gruppe zu entfernen, verwenden Sie den AWS CLI

Um eine untergeordnete Gruppe hinzuzufügen oder aus einer übergeordneten Gruppe zu entfernen, öffnen Sie den AWS CLI folgenden Befehl und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Gruppen- und Mitgliedsnamen:

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS -Tools für PowerShell

Im Folgenden wird beschrieben, wie eine Anfrage formatiert wird, mit der eine AWS verwaltete Microsoft AD-Gruppe in eine Gruppe mit entfernt wird AWS -Tools für PowerShell.

- Um eine untergeordnete Gruppe aus einer übergeordneten Gruppe zu entfernen mit AWS - Tools für PowerShell

Um eine untergeordnete Gruppe hinzuzufügen oder aus einer übergeordneten Gruppe zu entfernen, öffnen Sie den PowerShell folgenden Befehl und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei die Verzeichnis-ID, Gruppen- und Mitgliedsnamen durch Ihre AWS verwaltete Microsoft AD-Verzeichnis-ID, Gruppen- und Mitgliedsnamen:

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -  
MemberName "child-group-name"
```

Kopieren von AWS verwalteten Microsoft AD-Gruppenmitgliedschaften in AWS-Managementkonsole

Sie können Gruppenmitgliedschaften von einem AWS verwalteten Microsoft AD-Benutzer in einen anderen Benutzer in der AWS-Managementkonsole kopieren. Gruppenmitgliedschaften sind die Rollen und Berechtigungen, die ein Benutzer erbt, wenn Sie ihn zu einer Gruppe hinzufügen.

Bevor Sie mit diesem Verfahren beginnen, müssen Sie die folgenden Schritte ausführen:

- [Ihr AWS verwaltetes Microsoft AD erstellen](#).
- Um die Benutzer- und Gruppenverwaltung oder die AWS Directory Service Data CLI verwenden zu können, muss sie aktiviert sein. Weitere Informationen finden Sie unter [Aktivieren der Benutzer- und Gruppenverwaltung oder unter Verzeichnisdienstdaten](#).
- Sie können diese Funktion nur von der Primärseite aus AWS-Region für Ihr Verzeichnis aktivieren. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).
- Sie benötigen die erforderlichen IAM-Berechtigungen, um AWS Directory Service Data verwenden zu können. Weitere Informationen finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#). Um mit der Gewährung von Berechtigungen für Ihre Benutzer und Workloads zu beginnen, können Sie AWS verwaltete Richtlinien wie [AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess](#) oder verwenden. [AWS verwaltete Richtlinie: AWSDirectoryServiceDataReadOnlyAccess](#) Weitere Informationen finden Sie unter [Bewährte Sicherheitsmethoden in IAM](#).
- [Erstellen Sie eine AWS verwaltete Microsoft AD-Gruppe](#).

Um AWS verwaltete Microsoft AD-Gruppenmitgliedschaften mit dem AWS-Managementkonsole

1. Öffnen Sie die Directory Service Konsole unter. <https://console.aws.amazon.com/directoryservicev2/>
2. Wählen Sie im Navigationsbereich Active Directory und dann Directories aus. Sie werden zum Fenster Verzeichnisse weitergeleitet, auf dem Sie eine Liste der Verzeichnisse in Ihrem anzeigen können AWS-Region.
3. Wählen Sie ein Verzeichnis aus. Sie werden zum Bildschirm mit den Verzeichnisdetails weitergeleitet.
4. Klicken Sie auf Groups (Gruppen). Auf der Registerkarte wird eine Liste der Gruppen in Ihrem angezeigt AWS-Region.
5. Wählen Sie den Benutzer aus, dessen Konto Sie dessen Gruppenmitgliedschaft kopieren möchten. Um einen Benutzer zu finden, geben Sie den Anmeldenamen des Benutzers in das Suchfeld im Abschnitt Benutzer ein. Sie werden zum Bildschirm mit den Benutzerdetails weitergeleitet.
6. Wähle Alle Gruppenmitgliedschaften kopieren aus. Sie werden zu einem Verfahren weitergeleitet, in dem Sie angeben können, welche Gruppen Sie kopieren möchten.
 - a. Wählen Sie unter Zu kopierende Gruppen überprüfen unter Zu kopierende Gruppen die Gruppen mit Rollen und Berechtigungen aus, die Sie kopieren möchten, und klicken Sie dann auf Weiter.
 - b. Wählen Sie für Zielkonto auswählen unter Kontotyp die Option Bestehendes Benutzerkonto aus, um Gruppenmitgliedschaften in ein vorhandenes Benutzerkonto zu kopieren. Wählen Sie alternativ Neues Benutzerkonto aus, um einen neuen Benutzer zu erstellen und Gruppenmitgliedschaften in das neue Benutzerkonto zu kopieren. Um eine Gruppe zu finden, geben Sie den Namen der Gruppe in das Suchfeld im Abschnitt Ausgewählte Gruppen ein.
 - i. (Optional) Wenn Sie Bestehendes Benutzerkonto wählen, wählen Sie die Zielkonten aus, in die Sie die Rollen und Berechtigungen kopieren möchten, und klicken Sie dann auf Weiter.
 - ii. (Optional) Wenn Sie Neues Benutzerkonto wählen, schließen Sie den Vorgang ab und wählen Sie dann Weiter. Informationen zum Erstellen eines Benutzers finden Sie unter [Erstellen eines Benutzers](#).
 - c. Überprüfen Sie unter Gruppenmitgliedschaften überprüfen und kopieren Ihre Auswahl und wählen Sie dann Gruppenmitgliedschaft kopieren aus.

Benutzer und Gruppen mit einer EC2 Amazon-Instance verwalten

Dieser Abschnitt enthält Verfahren zur Verwaltung von Benutzern und Gruppen mit einer EC2 Amazon-Instance, die mit Ihrem AWS verwalteten Microsoft AD verknüpft ist.

Wir empfehlen, Benutzer und Gruppen mit einer EC2 Amazon-Instance zu verwalten, wenn die Directory Service Data API Ihren Anwendungsfall nicht unterstützt. Weitere Informationen finden Sie in der [AWS Directory Service Data API-Referenz](#).

Note

Bevor Sie eines der Verfahren in den folgenden Themen ausführen, müssen Sie die Active Directory-Verwaltungstools installieren. Weitere Informationen finden [Sie unter Installieren der Active Directory-Verwaltungstools](#).

Themen

- [Installation der Active Directory-Verwaltungstools für AWS verwaltetes Microsoft AD](#)
- [Einen AWS verwalteten Microsoft AD-Benutzer erstellen](#)
- [Löschen Sie das Konto eines Benutzers mit einer EC2 Amazon-Instance](#)
- [Zurücksetzen eines AWS verwalteten Microsoft AD-Benutzerkennworts](#)
- [Eine AWS verwaltete Microsoft AD-Gruppe erstellen](#)
- [Hinzufügen eines AWS verwalteten Microsoft AD-Benutzers zu einer Gruppe](#)

Installation der Active Directory-Verwaltungstools für AWS verwaltetes Microsoft AD

Sie können Ihr AWS verwaltetes Microsoft AD Active Directory mit verwaltenActive Directory Domain Services and Active Directory Lightweight Directory Services Tools. Um sie verwenden zu könnenActive Directory Domain Services and Active Directory Lightweight Directory Services Tools, müssen Sie sie installieren. Die folgenden Verfahren führen Sie durch die Installation dieser Tools auf einer Amazon EC2 Windows Server-Instance oder mit einem PowerShell Befehl. Alternativ können Sie eine EC2-Instance für die Verzeichnisverwaltung starten, auf der diese Tools bereits installiert sind.

EC2 Windows Server instance

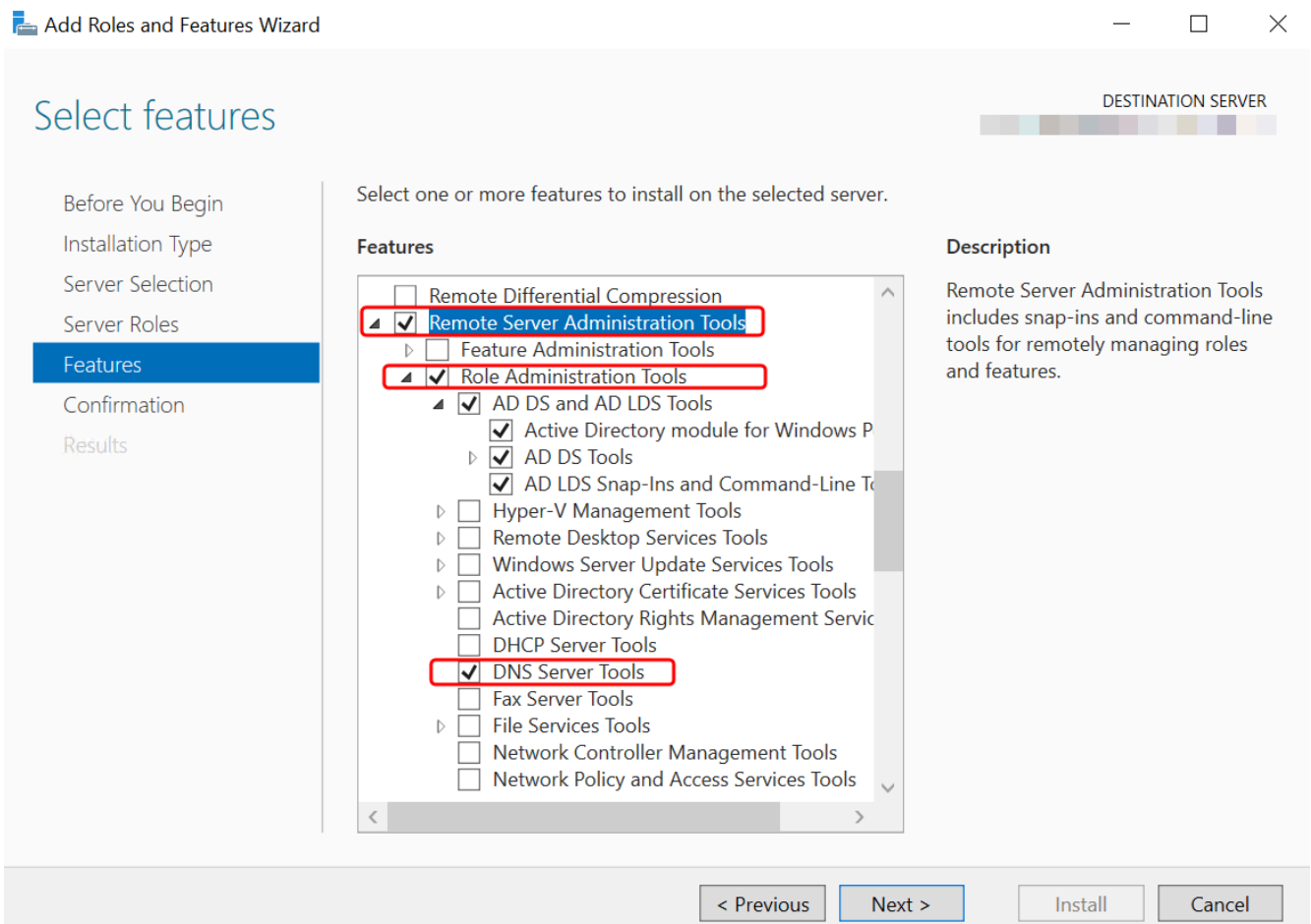
Bevor Sie mit diesem Verfahren beginnen können, gehen Sie wie folgt vor:

1. Erstellen Sie ein AWS verwaltetes Microsoft AD Active Directory. Weitere Informationen finden Sie unter [Ihr AWS verwaltetes Microsoft AD erstellen](#).
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: **AmazonSSManagedInstanceCore** und **AmazonSSMDirectoryServiceAccess**. Weitere Informationen erhalten Sie unter [Starten einer Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory](#) und [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#).
3. Sie benötigen die Anmeldeinformationen für Ihren Active Directory-Domänenadministrator. Diese Anmeldeinformationen wurden bei der Erstellung von AWS Managed Microsoft AD erstellt. Wenn Sie das Verfahren unter [Ihr AWS verwaltetes Microsoft AD erstellen](#) befolgt haben, enthält Ihr Administrator-Benutzername Ihren NetBIOS-Namen, **corp\admin**.

Installation der Active Directory-Verwaltungstools auf einer EC2 Server-Instanz Windows

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 würden [Ihr AWS verwaltetes Microsoft AD erstellen](#).
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, sind das Active Directory-Modul für PowerShell, die AD DS-Tools und die 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.

PowerShell

Sie können die Active Directory-Verwaltungstools mithilfe von installieren PowerShell. Sie können die Active Directory-Remoteverwaltungstools beispielsweise von einer PowerShell Eingabeaufforderung aus mit installieren `Install-WindowsFeature RSAT-ADDS`. Weitere Informationen finden [Sie unter Install- WindowsFeature](#) auf der Microsoft-Website.

Directory administration instance

Sie können eine EC2-Instanz für die Verzeichnisverwaltung in der Datei starten, auf der bereits AWS-Managementkonsole die Active Directory-Domänendienste und die Active Directory Lightweight Directory Services Tools installiert sind, indem Sie die Verfahren unter befolgen. [Starten einer Verzeichnisverwaltungsinstanz in Ihrem AWS verwalteten Microsoft AD Active Directory](#)

Einen AWS verwalteten Microsoft AD-Benutzer erstellen

Sie können AWS verwaltete Microsoft AD-Benutzer mit den Active Directory-Verwaltungstools und erstellen PowerShell. Bevor Sie Benutzer mit den Active Directory-Verwaltungstools erstellen können, müssen Sie das Verfahren unter abschließen [Installation der Active Directory-Verwaltungstools für AWS verwaltetes Microsoft AD](#).

Active Directory Administration Tools

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer mit den Active Directory-Verwaltungstools zu erstellen.

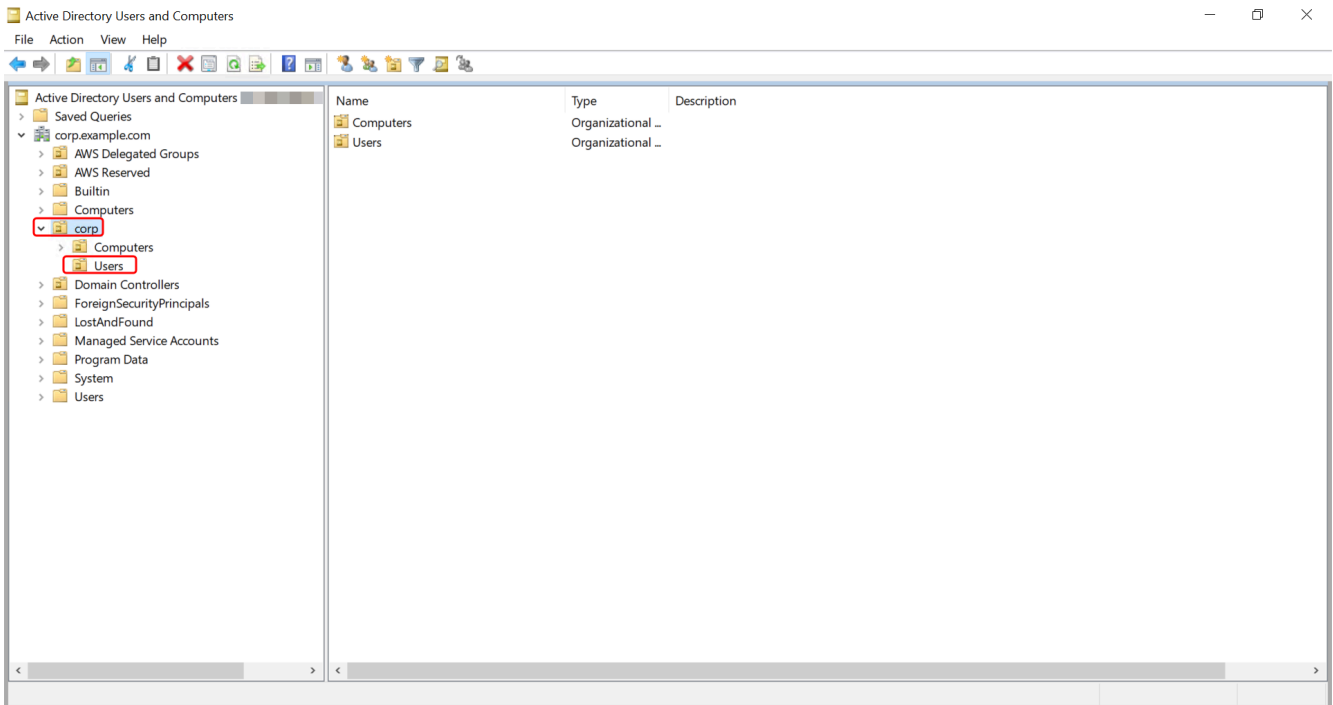
1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool „Active Directory-Benutzer und -Computer“ im Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

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
```

- 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 unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#).



- Wählen Sie im Menü Aktionen die Option Neu und wählen Sie dann Benutzer, um den Assistenten für neue Benutzer zu öffnen.
- 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
- 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.

- 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.

PowerShell

Gehen Sie wie folgt vor, um einen AWS verwalteten Microsoft AD-Benutzer mit zu erstellenPowerShell.

- Stellen Sie als Active Directory-Administrator eine Connect zu der Instanz her, die zu Ihrer Active Directory-Domäne gehört.
- Öffnen Sie PowerShell.
- Geben Sie den folgenden Befehl ein **jane.doe** und ersetzen Sie den Benutzernamen durch den Benutzernamen des Benutzers, den Sie erstellen möchten. Sie werden aufgefordertPowerShell, 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 ADUser Befehl New- finden Sie in der [MicrosoftDokumentation](#).

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

Löschen Sie das Konto eines Benutzers mit einer EC2 Amazon-Instance

Sie können das folgende Verfahren verwenden, um einen Benutzer mit einer EC2 Amazon-Instance zu löschen, die Ihrem AWS verwalteten Microsoft AD beigetreten ist.

Note

Bevor Sie dieses Verfahren abschließen, müssen Sie die Active Directory-Verwaltungstools installieren. Weitere Informationen finden [Sie unter Installieren der Active Directory-Verwaltungstools](#).

So löschen Sie einen Benutzer

1. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Es gibt eine Verknüpfung zu diesem Tool im Ordner Windows-Verwaltungstools.

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
```

2. Wählen Sie in der Verzeichnisstruktur die OU aus, die den Benutzer enthält, den Sie löschen möchten (z. B. Corp\Users).
3. Wählen Sie den Benutzer aus, den Sie löschen möchten. Wählen Sie im Menü Aktionen die Option Löschen.
4. Es erscheint ein Dialogfeld, in dem Sie bestätigen müssen, dass Sie den Benutzer löschen möchten. Wählen Sie Ja, um den Benutzer zu löschen.

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 Microsoft-Blog „Ask the Directory Services Team“.

Zurücksetzen eines AWS verwalteten Microsoft AD-Benutzerkennworts

Benutzer müssen sich an die im Active Directory definierten Kennwortrichtlinien halten. 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, 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 Directory Service Ressourcen](#).

Sie können das Passwort für jeden Benutzer in Ihrem Active Directory zurücksetzen, 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 [Ihr AWS verwaltetes Microsoft AD erstellen](#) Ihrem NetBIOS-Namen befolgt haben, wäre der Name CORP und die Benutzerkennwörter, die Sie zurücksetzen könnten, wären Mitglieder von Corp/Users OU.
- 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 unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#).

Weitere Informationen darüber, wie die Kennwortrichtlinien angewendet werden, wenn ein Passwort in AWS Managed Microsoft AD zurückgesetzt wird, finden Sie unter [Wie werden Passwortrichtlinien angewendet](#).

Sie können eines der folgenden Tools verwenden, um ein AWS verwaltetes Microsoft AD-Benutzerkennwort zurückzusetzen:

- AWS-Managementkonsole
- AWS CLI
- PowerShell

AWS-Managementkonsole

Gehen Sie wie folgt vor, um ein AWS verwaltetes Microsoft AD-Benutzerkennwort mit dem zurückzusetzen AWS-Managementkonsole.

1. Wählen Sie im Navigationsbereich der [Directory Service Konsole](#) unter Active Directory die Option Verzeichnisse aus, und wählen Sie dann in der Liste das Active Directory 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 Kennwort geändert werden muss.
4. Geben Sie ein Passwort unter Neues Passwort und Passwort bestätigen ein und wählen Sie dann Passwort zurücksetzen.

AWS CLI

Gehen Sie wie folgt vor, um ein AWS verwaltetes Microsoft AD-Benutzerkennwort mit dem zurückzusetzen 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 Kennwort **P@ssw0rd** durch Ihre Active Directory-Verzeichnis-ID und die gewünschten Anmeldeinformationen. Weitere Informationen finden Sie [reset-user-password](#) in der AWS CLI Befehlsreferenz.

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

PowerShell

Gehen Sie wie folgt vor, um ein AWS verwaltetes Microsoft AD-Benutzerkennwort mit dem zurückzusetzen PowerShell.

1. Stellen Sie als Active Directory-Administrator eine Connect zu der Instanz her, die zu Ihrer Active Directory-Domäne gehört.
2. Öffnen Sie PowerShell.
3. Geben Sie den folgenden Befehl ein und ersetzen Sie den Benutzernamen **jane.doe**, die Verzeichnis-ID und das Kennwort **P@ssw0rd** durch Ihre Active Directory-Verzeichnis-ID und die gewünschten Anmeldeinformationen. Weitere Informationen finden Sie [unter DSUser Reset-Password-Cmdlet](#).

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

Eine AWS verwaltete Microsoft AD-Gruppe erstellen

Sie können Gruppen in Ihrem AWS Managed Microsoft AD erstellen. Gehen Sie wie folgt vor, um eine Sicherheitsgruppe mit einer EC2 Amazon-Instanz zu erstellen, die mit Ihrem AWS verwalteten

Microsoft AD-Verzeichnis verknüpft ist. Bevor Sie Sicherheitsgruppen erstellen können, müssen Sie die Verfahren unter [Installation der Active-Directory-Verwaltungstools](#) abschließen.

Active Directory Administration Tools

Gehen Sie wie folgt vor, um eine AWS verwaltete Microsoft AD-Gruppe mit den Active Directory-Verwaltungstools zu erstellen.

So erstellen Sie eine Gruppe

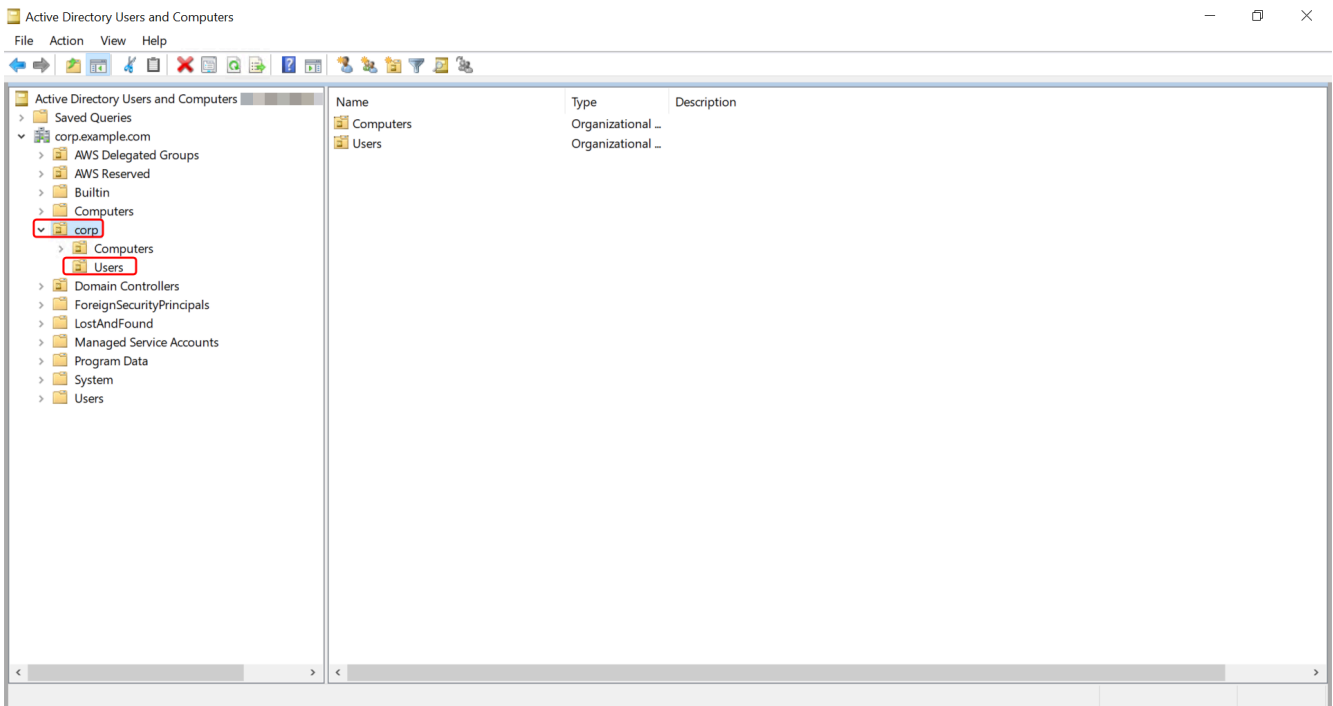
1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

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 unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt.](#)



4. Klicken Sie im Menü Action 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.

PowerShell

Sie können PowerShell Befehle verwenden, um Gruppen zu erstellen. Weitere Informationen finden Sie ADGroup in der PowerShell Dokumentation [zu Windows Server 2022 unter Neu](#).

Hinzufügen eines AWS verwalteten Microsoft AD-Benutzers zu einer Gruppe

Sie können AWS verwaltete Microsoft AD-Benutzer zu einer Gruppe hinzufügen. Gehen Sie wie folgt vor, um einen Benutzer zu einer Sicherheitsgruppe mit einer EC2 Amazon-Instance hinzuzufügen, die mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis verknüpft ist.

Active Directory Administration Tools

So fügen Sie einer Gruppe einen Benutzer hinzu

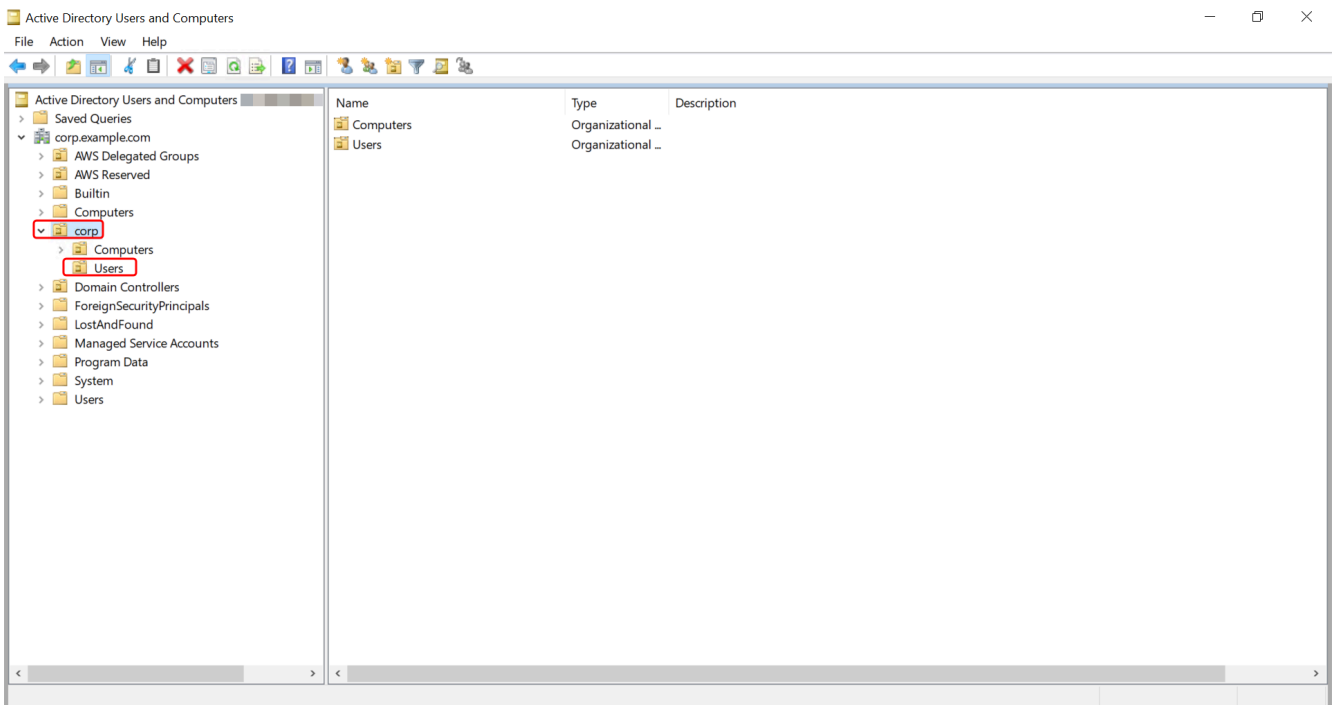
1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

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.

AWS Verzeichnisdienstdaten

AWS Directory Service Data ist eine Erweiterung von AWS Directory Service. Sie können Active Directory-Benutzer, -Gruppen und -Mitgliedschaften von einem Directory Service für Microsoft Active Directory aus erstellen, lesen, aktualisieren und Active AWS Directory (AD) aktualisieren, ohne dedizierte AD-Management-Instances auf einer EC2 Amazon-Instance bereitzustellen. Sie können auch integrierte Objektverwaltungsaufgaben verzeichnisübergreifend ohne direkte Netzwerkkonnektivität ausführen. Dies vereinfacht die Bereitstellung und das Zugriffsmanagement und ermöglicht so vollautomatische Bereitstellungen. Weitere Informationen finden Sie in der [AWS Directory Service Data API-Referenz](#).

Directory Service Data unterstützt Benutzer- und Gruppenschreibvorgänge wie `CreateUser` und innerhalb des AWS verwalteten Microsoft AD `CreateGroup`, das sich in Ihrer Organisationseinheit (OU) befindet. Directory Service Data unterstützt Lesevorgänge wie `ListUsers` und `ListGroups` für alle Benutzer, Gruppen und Gruppenmitgliedschaften innerhalb von AWS Managed Microsoft AD und in vertrauenswürdigen Bereichen. Directory Service Data unterstützt das Hinzufügen und Entfernen von Gruppenmitgliedern aus Gruppen in Ihrer Organisationseinheit und der Organisationseinheit AWS Delegated Groups, sodass Sie Berechtigungen delegieren können, indem Sie Benutzer zu bestimmten delegierten Gruppenobjekten hinzufügen. Weitere Informationen finden Sie unter [Benutzer- und Gruppenverwaltung in AWS Managed Microsoft AD](#).

Note

Verzeichnisdienstdaten sind nur in Ihrer Hauptregion verfügbar. Weitere Informationen finden Sie unter [Primäre Regionen im Vergleich zu zusätzlichen Regionen](#).

Themen

- [Replikation und Konsistenz](#)
- [AWS Verzeichnisdienst-Datenattribute](#)
- [Gruppentyp und Gruppenumfang](#)

Replikation und Konsistenz

Die Directory Service Data API stellt eine Verbindung zu Ihren AWS verwalteten Microsoft AD-Domänencontrollern her, um Operationen an den zugrunde liegenden Verzeichnisobjekten durchzuführen. Active Directory ist eine letztlich konsistente Plattform, und die Replikation findet kontinuierlich zwischen Directory Service Verzeichnisdomänencontrollern statt. Standardmäßig wird jedes Directory Service Verzeichnis mit zwei Domänencontrollern erstellt.

Directory Service Data versucht, eine konsistente Benutzererfahrung aufrechtzuerhalten, indem für alle Anfragen derselbe Domänencontroller verwendet wird. Falls ein Domänencontroller nicht verfügbar ist, wechselt Directory Service Data zu einem alternativen Domänencontroller. Während dieser Ereignisse stellen Sie möglicherweise fest, dass die einzelnen Domänencontroller einheitlich sind, während Objekte auf allen Domänencontrollern repliziert werden.

Die Verzeichnislimits variieren je nach AWS Managed Microsoft AD-Edition:

- Standard Edition — Unterstützt 8 Transaktionen pro Sekunde für Lesevorgänge und 4 TPS für Schreibvorgänge pro Verzeichnis.
- Enterprise Edition — Unterstützt 16 Transaktionen pro Sekunde für Lesevorgänge und 8 TPS für Schreibvorgänge pro Verzeichnis.

Note

Sowohl für die Standard- als auch für die Enterprise-Edition gilt ein Parallelitätslimit von 10 gleichzeitigen Anfragen.

- AWS-Konto— Unterstützt insgesamt 100 Transaktionen pro Sekunde für Directory Service Data-Operationen in allen Verzeichnissen.

AWS Verzeichnisdienst-Datenattribute

In diesem Thema wird beschrieben, wie Sie mit Attributen in der [AWS Directory Service Data API-Referenz](#) arbeiten.

Anforderungsattribute

Die folgenden Attribute müssen in den Parametern des Anforderungstexts definiert werden. Ein Beispiel für die Definition dieser Attribute finden Sie [CreateGroup](#) in der AWS Directory Service Data API-Referenz.

Name des Verzeichnisdienst-Datenattributs	LDAP-Anzeigename	AWS-Managementconsole	PowerShell Alias	Access type (Art des Zugriffs)	Objekttyp	Wert des Attributs	Durchsuchbar
DistinguishedName	distinguishedName	Definiert den Namen (Distinguished Name)	Keine	ReadOnly	Benutzer, Gruppe	Zeichenfolge	Nein
EmailAddress	Post	E-Mail-Adresse	EmailAddress	Erstellbar	Benutzer	Zeichenfolge	Ja
Aktiviert	Keine	Aktiviert	Aktiviert	Mutable	Benutzer	Boolesch	Nein
GivenName	givenName	Vorname	GivenName	Erstellbar	Benutzer	Zeichenfolge	Ja
GroupScope	GroupScope	Group scope (Gruppenumfang)	Keine	Erstellbar	Group (Gruppieren)	Enum	Nein

Name des Verzeichnisdienst-Datenattributs	LDAP-Anzeigename	AWS-Managementkonsole	PowerShell Alias	Access type (Art des Zugriffs)	Objekttyp	Wert des Attributs	Durchsuchbar
GroupType	Gruppentyp	Group type (Gruppentyp)	Keine	Erstellbar	Group (Gruppieren)	Enum	Nein
SamAccountName	Ein AMAccountName	Benutzeranmeldename	sAMAccountName	Erstellbar	Benutzer, Gruppe	Zeichenfolge	Ja
SID	Objekt-ID	Sicherheits-ID (SID) für Benutzer und Gruppe	SID	ReadOnly	Benutzer, Gruppe	Zeichenfolge	Nein
Nachname	sn	Nachname	Nachname	Erstellbar	Benutzer	Zeichenfolge	Ja
UserPrincipalName	userPrincipalName	Prinzipalname des Benutzers	UserPrincipalName	ReadOnly	Benutzer	Zeichenfolge	Nein

Weitere Attribute

Die folgenden Attribute müssen in definiert sein `OtherAttributes` und dürfen keinen Anforderungstextparametern zugeordnet werden. Wenn Sie in Ihren Anfragen andere Attribute definieren, müssen Sie den Attributnamen, den Datentyp und den Wert für jedes Attribut angeben.

Ein Beispiel für die Definition dieser Attribute finden Sie [CreateUser](#) in der AWS Directory Service Data API-Referenz.

 Note

Bei den Namen dieser Attribute wird nicht zwischen Groß - und Kleinschreibung unterschieden, wenn sie als Eingabe angegeben werden. Sie entsprechen dem LDAP-Anzeigenamen.

Name des Verzeichnisdienst-Datenattributs	LDAP-Anzeigename	AWS-Managementkonsole	PowerShell Alias	Access type (Art des Zugriffs)	Objekttyp	Wert des Attributs	Durchsuchbar
Assistent in	assistant	Assistent	Keine	ReadOnly	Benutzer	Zeichenfolge	Nein
Kann	cn	Common Name	Keine	ReadOnly	Benutzer, Gruppe	Zeichenfolge	Nein
Co	co	Land/Region	Land	Mutable	Benutzer	Zeichenfolge	Nein
Firma	company	Unternehmen	Unternehmen	Kreierbar	Benutzer	Zeichenfolge	Nein
Abteilung	Abteilung	Department	Department	Erstellbar	Benutzer	Zeichenfolge	Nein
Beschreibung	description	Description	Description	Erstellbar	Benutzer, Gruppe	Zeichenfolge	Nein
DirectReports	Direkte Berichte	Direkt unterstellte	Keine	ReadOnly	Benutzer	Zeichenkettensatz	Nein

Name des Verzeichnisdienst-Datenattributs	LDAP-Anzeigename	AWS-Managementkonsole	PowerShell Alias	Access type (Art des Zugriffs)	Objekttyp	Wert des Attributs	Durchsuchbar
Display Name	displayName	Anzeigename	DisplayName	Erstellbar	Benutzer, Gruppe	Zeichenfolge	Ja
Facsimile Telephone Number	facsimileTelephoneNumber	Fax	Fax	Erstellbar	Benutzer, Gruppe	Zeichenfolge	Nein
HomePhone	homePhone	Private Telefonnummer	HomePhone	Erstellbar	Benutzer	Zeichenfolge	Nein
Info	info	Hinweise	Keine	Mutable	Benutzer, Gruppe	Zeichenfolge	Nein
Initialen	Initialen	Initialen	Initialen	Mutable	Benutzer	Zeichenfolge	Nein
IpPhone	IP-Telefon	IP-Telefon	Keine	Mutable	Benutzer	Zeichenfolge	Nein
L	l	Ort	Ort	Erstellbar	Benutzer	Zeichenfolge	Ja
Managerin	manager	Manager	Manager	Mutable	Benutzer	Zeichenfolge	Nein
Post	Post	E-Mail-Adresse	EmailAddress	Mutable	Group (Gruppieren)	Zeichenfolge	Ja
Mobil	mobile	Handynummer	MobilePhone	Mutable	Benutzer	Zeichenfolge	Nein

Name des Verzeichnisdienst-Datenattributs	LDAP-Anzeigename	AWS-Managementkonsole	PowerShell Alias	Access type (Art des Zugriffs)	Objekttyp	Wert des Attributs	Durchsuchbar
ObjectClass	Objektklasse	Benutzer/Gruppe	Keine	ReadOnly	Group (Gruppieren)	Zeichenfolge	Nein
ObjectGUID	Objekt-GUID	Globaler eindeutiger Bezeichner (GUID)	Keine	ReadOnly	Benutzer, Gruppe	Zeichenfolge	Nein
Pager	Funkrufempfänger	Pager	Keine	Mutable	Benutzer	Zeichenfolge	Nein
PhysicalDeliveryOfficeName	physicalDeliveryOfficeName	Office	Keine	Erstellbar	Benutzer	Zeichenfolge	Ja
PostalCode	postalCode	PLZ/PLZ	PostalCode	Erstellbar	Benutzer	Zeichenfolge	Nein
PreferredLanguage	Bevorzugte Sprache	Bevorzugte Sprache	Keine	Mutable	Benutzer	Zeichenfolge	Nein
ProxyAddresses	Proxy-Adressen	Proxy-Adresse	Keine	ReadOnly	Benutzer, Gruppe	Zeichenfolge mit mehreren Werten	Ja

Name des Verzeichnisdienst-Datenattributs	LDAP-Anzeigename	AWS-Managementkonsole	PowerShell Alias	Access type (Art des Zugriffs)	Objekttyp	Wert des Attributs	Durchsuchbar
ServicePrincipalName	servicePrincipalName	Service-Principalname	ServicePrincipalName	Mutable	Benutzer	Mehrwertige Zeichenfolge	Nein
State	st	Bundesstaat/Provinz	Status	Erstellbar	Benutzer	Zeichenfolge	Nein
StreetAddress	Straße/Adresse	Adresse der Straße	StreetAddress	Erstellbar	Benutzer	Zeichenfolge	Nein
TelephoneNumber	Telefonnummer	Telefonnummer	OfficePhone	Erstellbar	Benutzer	Zeichenfolge	Nein
Title	Titel	Auftragstitel	Title	Mutable	Benutzer	Zeichenfolge	Nein
WhenChanged	Wann geändert	Letzte Aktualisierung	Keine	ReadOnly	Benutzer, Gruppe	Zeichenfolge	Nein
WWWHomePage	eine WWWHome Seite	URL der Startseite	WWWHomePage	Mutable	Benutzer, Gruppe	Zeichenfolge	Nein

Gruppentyp und Gruppenumfang

Gruppen in AWS Managed Microsoft AD haben sowohl einen Gruppentyp als auch einen Gruppenbereich. In den folgenden Abschnitten finden Sie weitere Informationen zu den einzelnen Abschnitten.

Themen

- [Group type \(Gruppentyp\)](#)
- [Group scope \(Gruppenumfang\)](#)

Group type (Gruppentyp)

Der Gruppentyp bestimmt, auf welche gemeinsam genutzten Ressourcen innerhalb des Active Directory die Gruppenmitglieder zugreifen können. Es gibt zwei Gruppentypen:

- Sicherheit — Sie können diesen Gruppen Berechtigungen zuweisen, sodass Gruppenmitglieder auf gemeinsam genutzte Active Directory-Ressourcen zugreifen können.
- Verteilung — Sie können diesen Typ verwenden, um E-Mail-Verteilerlisten zu erstellen. Diese Gruppenmitglieder können nicht auf gemeinsam genutzte Active Directory-Ressourcen zugreifen.

Beim Wechsel zwischen Gruppentypen gibt es keine Einschränkungen.

Weitere Informationen zu Gruppentypen finden Sie in der [Microsoft-Dokumentation](#).

Group scope (Gruppenumfang)

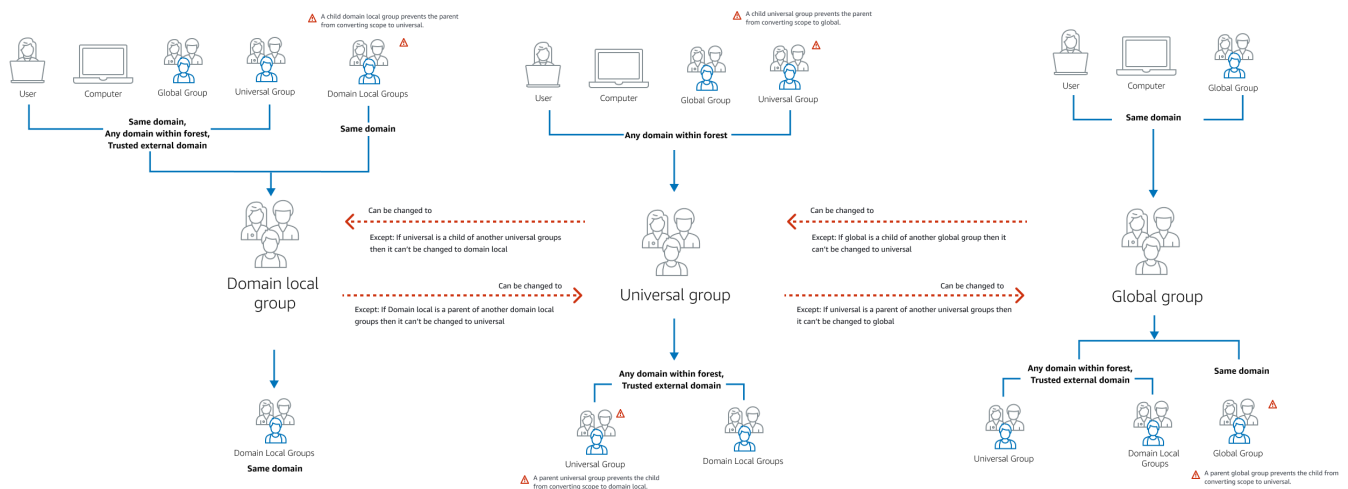
Der Gruppenbereich bestimmt, wie Gruppenmitglieder in der Domänenstruktur oder Gesamtstruktur definiert werden. Es gibt drei Gruppenbereiche:

- Lokale Domäne — um Gruppenmitgliedern, die sich in derselben Domäne befinden, Berechtigungen zuzuweisen.
- Universell — um Gruppenmitgliedern in einer beliebigen Domain Berechtigungen zuzuweisen.
- Global — um Gruppenmitgliedern in einer beliebigen Domäne oder Gesamtstruktur Berechtigungen zuzuweisen.

Bei der Änderung eines Gruppenbereichs gibt es Einschränkungen. In der folgenden Liste und in der folgenden Abbildung werden diese Einschränkungen dargestellt.

- Ändern des Gruppenbereichs von Domain Local auf Universal — Ja
 - Es sei denn, die lokale Domänengruppe ist einer anderen lokalen Domänengruppe übergeordnet.
- Gruppenbereich von Universal auf Domain Local ändern — Ja
 - Es sei denn, die universelle Gruppe ist eine untergeordnete Gruppe einer anderen universellen Gruppe.
- Änderung des Gruppenbereichs von Universal auf Global — Ja
 - Es sei denn, die universelle Gruppe ist einer anderen universellen Gruppe übergeordnet.
- Änderung des Gruppenbereichs von Global auf Universal — Ja
 - Es sei denn, die globale Gruppe ist einer anderen globalen Gruppe untergeordnet.

Weitere Informationen zu Gruppenbereichen finden Sie in der [MicrosoftDokumentation](#).



Verbinden Sie Ihr AWS verwaltetes Microsoft AD mit Microsoft Entra Connect Sync

Dieses Tutorial führt Sie durch die notwendigen Schritte zur Installation, [Microsoft Entra Connect Sync](#)um Ihr mit Ihrem AWS verwaltetes Microsoft AD [Microsoft Entra ID](#) zu 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 verwendet 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 “Ihr AWS verwaltetes Microsoft AD erstellen”](#).
- Eine Amazon EC2 Windows Server-Instance, die mit Ihrem AWS Managed Microsoft AD verbunden ist. Weitere Informationen finden Sie unter [Einer Windows-Instance beitreten](#).
- Ein Windows EC2-Server mit Administration Tools installiertem Active Directory zur Verwaltung Ihres AWS verwalteten Microsoft AD. Weitere Informationen finden Sie unter [the section called “Installation der AD-Verwaltungstools”](#).

Erstellen Sie einen Active Directory-Domänenbenutzer

In diesem Tutorial wird davon ausgegangen, dass Sie bereits eine AWS verwaltete Microsoft AD- sowie eine Windows EC2-Serverinstanz mit Active Directory Administration Tools installiert haben. Weitere Informationen finden Sie unter [the section called “Installation der AD-Verwaltungstools”](#).

1. Connect zu der Instanz her, auf der das Active Directory installiert Administration Tools wurde.
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 unter[the section called “Erstellen eines Benutzers”](#).

Herunterladen von 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.

PowerShellSkript ausführen

- [Öffnen Sie PowerShell als Administrator](#) und führen Sie das folgende Skript aus.

Während das Skript ausgeführt wird, werden Sie aufgefordert, den [AMAccountName](#)s für den neu erstellten Domänenbenutzer aus Schritt 1 einzugeben.

i Note

Im Folgenden finden Sie weitere Informationen zur Ausführung des Skripts:

- Sie können das Skript mit der ps1 Erweiterung in einem Ordner wie **temp** speichern. Anschließend können Sie den folgenden PowerShell Befehl verwenden, um das Skript zu laden:

```
import-module "c:\temp\entra.ps1"
```

- Nach dem Laden des Skripts können Sie den folgenden Befehl verwenden, um die erforderlichen Berechtigungen für die Ausführung des Skripts festzulegen, und ihn durch den Namen Ihres Entra Dienstkontos *Entra_Service_Account_Name* ersetzen:

```
Set-EntraConnectSvcPerms -ServiceAccountName Entra_Service_Account_Name
```

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

```
try {  
    # Attempt to import the module  
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
```

```
Import-Module $modulePath -ErrorAction Stop
Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    Try {
        $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
Stop | Select-Object -ExpandProperty 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get service account DN $_"
    }

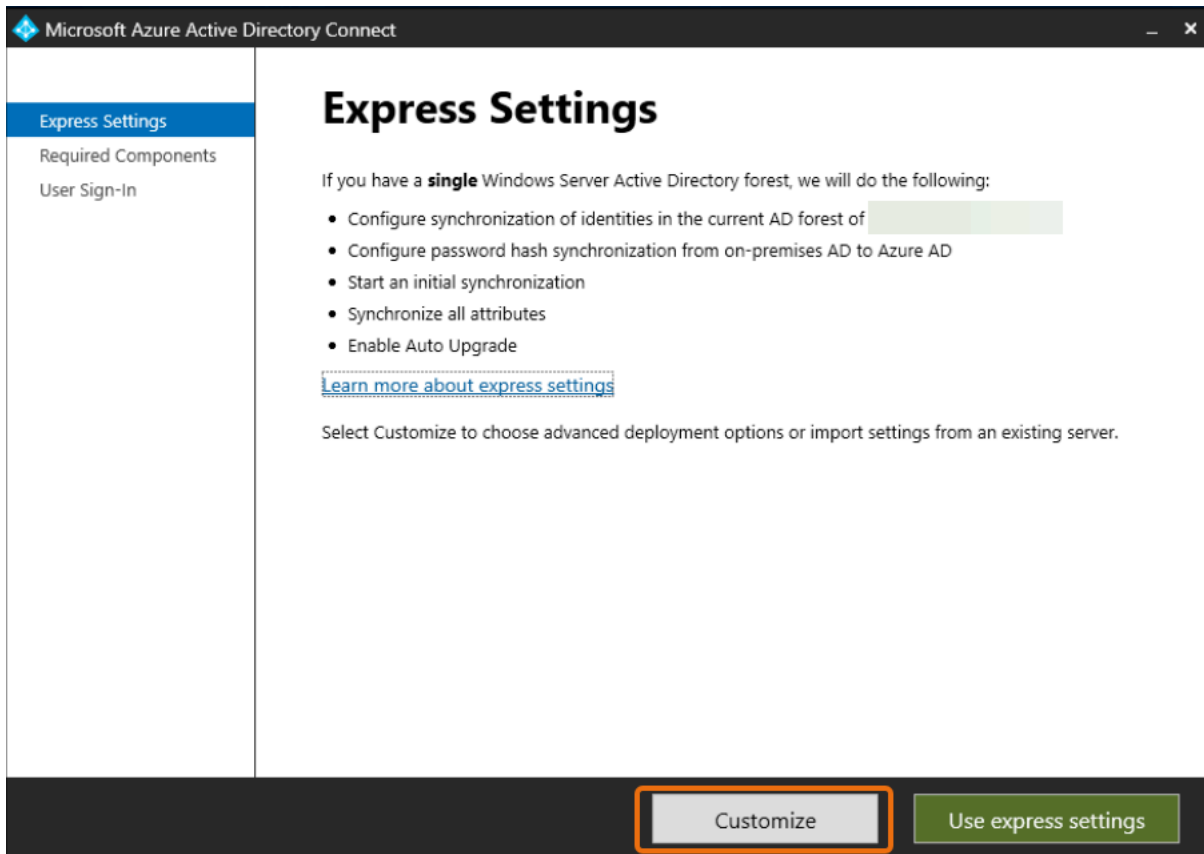
    Foreach ($OU in $OUs) {
        try {
            Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
$ADConnectorAccountDN -ADObjectDN $OU -Confirm:$false -ErrorAction Stop
        }
    }
}
```

```
Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

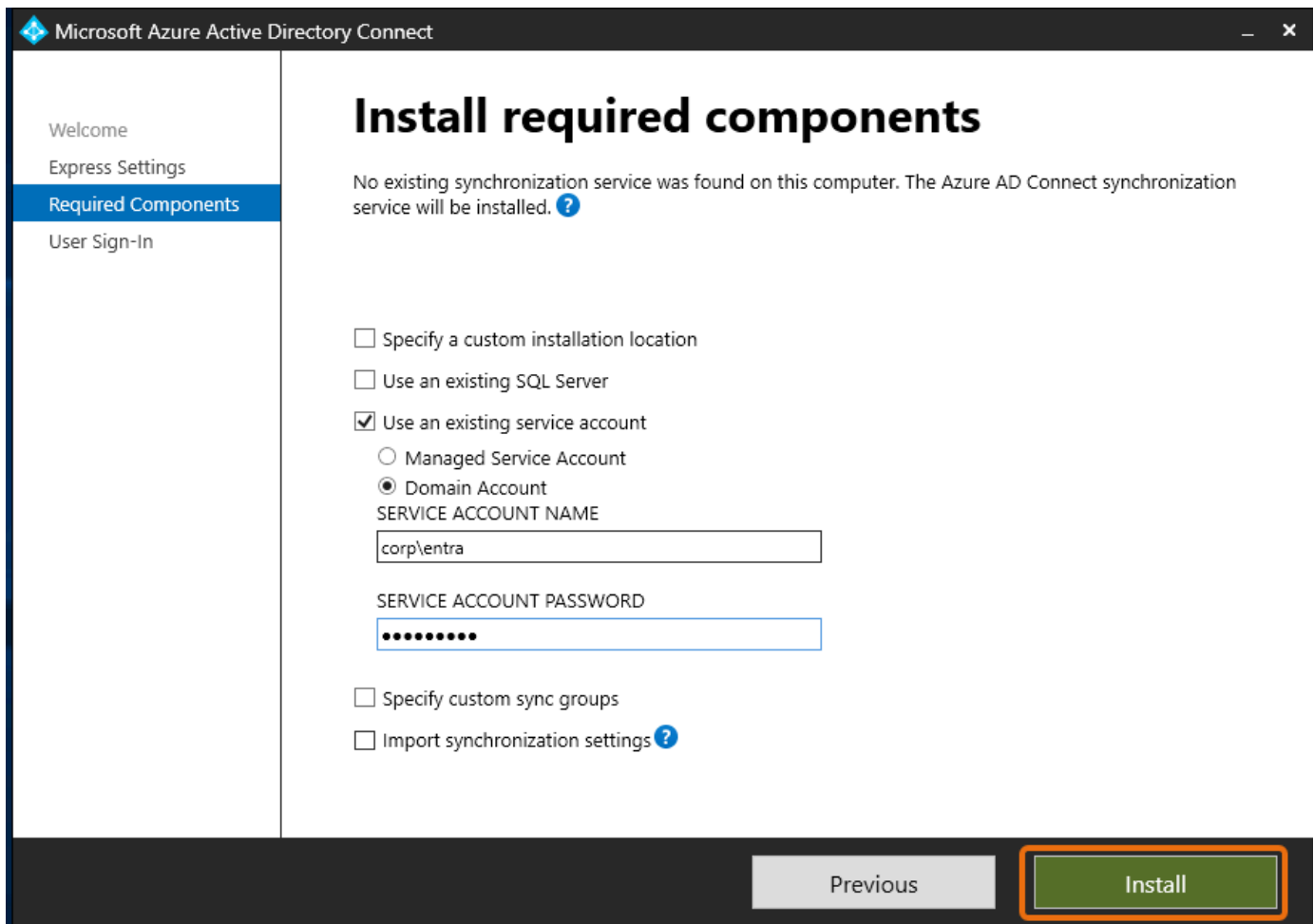
Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADObjectDN $OU -Confirm:$false -ErrorAction Stop
Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
on OU $OU"
}
catch {
Write-Host "An error occurred while setting permissions for
$ADConnectorAccountDN on OU $OU : $_"
}
}
}
```

Installieren Entra Connect Sync

1. Sobald das Skript abgeschlossen ist, können Sie die heruntergeladene Microsoft Entra Connect (früher bekannt als Azure 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 mit den Express-Einstellungen die Option Anpassen aus.



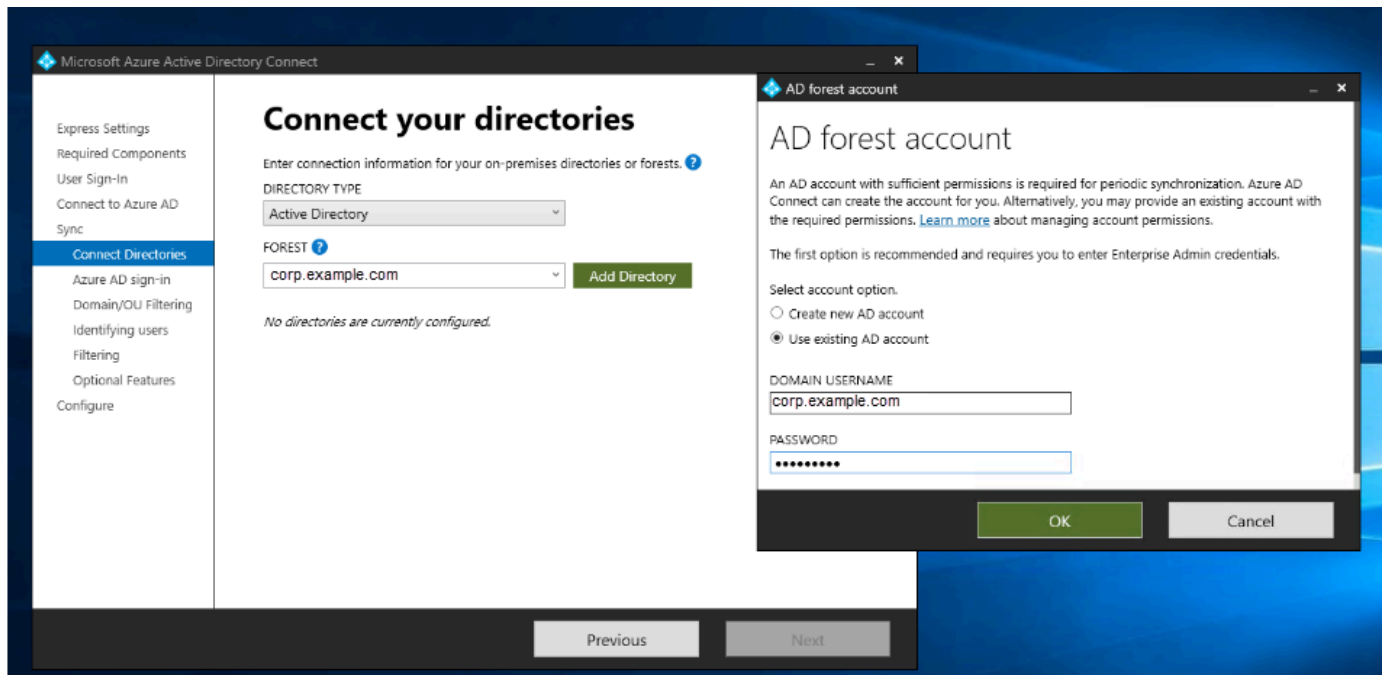
3. Aktivieren Sie im Fenster Erforderliche Komponenten installieren das Kontrollkästchen Bestehendes Dienstkonto verwenden. Geben Sie in den Feldern DIENSTKONTONAME und KENNWORT FÜR DAS DIENSTKONTO den AD DS Connector account Namen und das Passwort für den Benutzer ein, den Sie in Schritt 1 erstellt 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 bei Ihrem Active Directory 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 Sie im Fenster Ihre Verzeichnisse verbinden die Option Active Directory 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-Feld, 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 aus.



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.

AWS Tutorials für verwaltete Microsoft AD-Testlabore

Dieser Abschnitt enthält eine Reihe von geführten Tutorials, die Ihnen helfen, eine Testlabumgebung einzurichten, AWS in der Sie mit AWS Managed Microsoft AD experimentieren können.

Themen

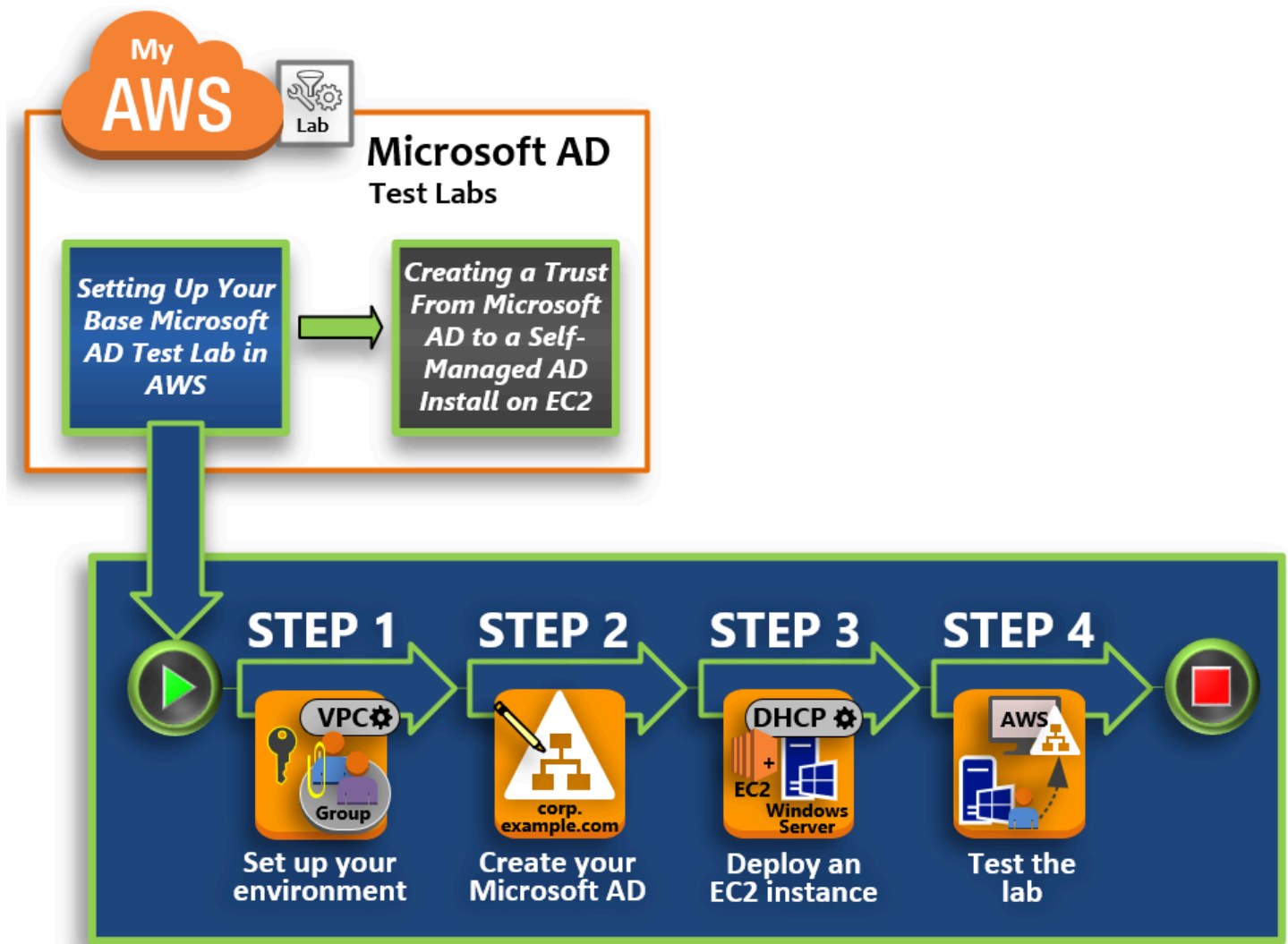
- [Tutorial: Einrichten Ihres AWS Managed Microsoft AD-Basis-Testlabors in AWS](#)

- [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 \(AWS-Managementkonsole\)](#).
- 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 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 neueste Version von From herunter <https://aws.amazon.com/powershell/>, installieren Sie sie und führen Sie dann den folgenden Befehl AWS Tools for Windows PowerShell 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 an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole 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 heruntergeladen. Der Dateiname ist der Name, den Sie beim Erstellen Ihres Schlüsselpaares mit der Erweiterung .pem angegeben haben. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

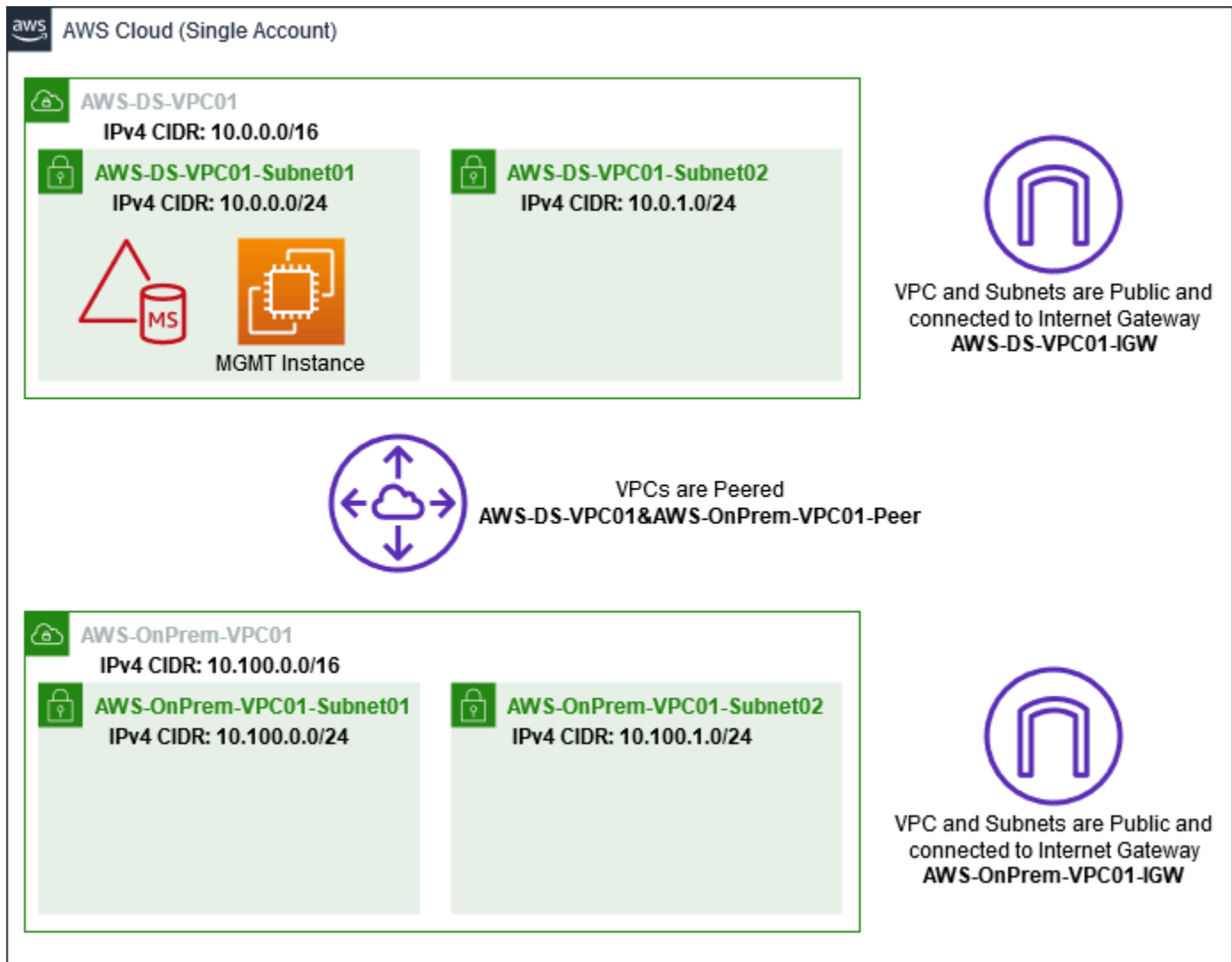
Important

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 erstellen, konfigurieren und miteinander verbinden VPCs

Wie in der folgenden Abbildung dargestellt, haben Sie bis zum Abschluss dieses mehrstufigen Prozesses zwei öffentliche VPCs, zwei öffentliche Subnetze pro VPC, ein Internet Gateway pro VPC und eine VPC-Peering-Verbindung zwischen den erstellt und konfiguriert. VPCs Aus Gründen der Einfachheit und der Kosten haben wir uns für öffentliche Netze VPCs und Subnetze entschieden.

Für Produktions-Workloads empfehlen wir, private Workloads zu verwenden. VPCs 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: Erstellen Sie zwei VPCs

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 [Teilen Sie Ihr AWS verwaltetes Microsoft AD](#) 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.

Informationen zur verwalteten Active Directory-VPC	On-Premises-VPC-Informationen
Namenskürzel: AWS-DS- VPC01	Namenskürzel: AWS- - OnPrem VPC01
IPv4 CIDR-Block: 10.0.0.0/16	IPv4 CIDR-Block: 10.100.0.0/16
IPv6 CIDR-Block: Kein CIDR-Block IPv6	IPv6 CIDR-Block: Kein CIDR-Block IPv6
Tenancy: Standard	Tenancy: Standard

Detaillierte Anweisungen finden Sie unter [Erstellen einer VPC](#).

Schritt 2: Zwei Subnetzen pro VPC erstellen

Nachdem Sie das erstellt haben, müssen VPCs Sie zwei Subnetze pro VPC mit den angegebenen Parametern in der folgenden Tabelle erstellen. 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 [Voraussetzungen für die Erstellung eines AWS verwalteten Microsoft AD](#).

AWS-DS- Subnetzinformationen: VPC01	AWS- OnPrem - Subnetzinformationen VPC01
Namenskürzel: AWS-DS- -Subnet01 VPC01	Namenskürzel: - - -Subnet01 AWS OnPrem VPC01
VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx -DS-VPC01	VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx - - OnPrem VPC01
Availability Zone: us-west-2a	Availability Zone: us-west-2a
IPv4 CIDR-Block: 10.0.0.0/24	IPv4 CIDR-Block: 10.100.0.0/24
Namenskürzel: -DS- -Subnet02 AWS VPC01	Namenskürzel: - - -Subnet02 AWS OnPrem VPC01
VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx -DS-VPC01	

AWS-DS- Subnetzinformationen: VPC01	AWS- OnPrem - Subnetzinformationen VPC01
Availability Zone: us-west-2b	VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx - - OnPrem VPC01
IPv4 CIDR-Block: 10.0.1.0/24	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: Erstellen Sie ein Internet Gateway und schließen Sie es an Ihr VPCs

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.

AWS-DS- VPC01 Internet-Gateway-Informationen	AWS- OnPrem - VPC01 Internet-Gateway-Informationen
Namenskürzel: AWS-DS- VPC01 -IGW	Namenskürzel: - - AWS-IGW OnPrem VPC01
VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx -DS- VPC01	VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx - - OnPrem VPC01

Detaillierte Anweisungen finden Sie unter [Internet-Gateways](#).

Schritt 4: Konfigurieren Sie eine VPC-Peering-Verbindung zwischen AWS-DS- VPC01 und - - AWS OnPrem VPC01

Da Sie bereits VPCs zuvor zwei erstellt haben, müssen Sie sie mithilfe von VPC-Peering miteinander vernetzen. Es gibt zwar viele Möglichkeiten VPCs, Ihre zu verbinden, aber in diesem Tutorial wird VPC Peering verwendet. [AWS Managed Microsoft AD unterstützt viele Verbindungslösungen. VPCs Einige davon umfassen VPC-Peering, Transit Gateway und VPN.](#)

Namensschild für die Peering-Verbindung: AWS-DS- VPC01 & - - -Peer AWS OnPrem VPC01

VPC (Antragsteller): AWS vpc-xxxxxxxxxxxxxxxxxxxxx -DS- VPC01

Konto: Mein Konto

Region: Diese Region

VPC (Akzeptierer): AWS vpc-xxxxxxxxxxxxxxxxxxx - - OnPrem VPC01

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: Fügen Sie der Hauptroutentabelle jeder VPC zwei Routen hinzu

Damit die in den vorherigen Schritten erstellten Internet-Gateways und die VPC-Peering-Verbindung funktionieren, müssen Sie die Haupt-Routing-Tabelle von beiden VPCs mithilfe der in der folgenden Tabelle angegebenen Parameter 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 AWS- -OnPrem) filtern. VPC01

AWS-DS- Informationen zu Route 1 VPC01	AWS-DS- Informationen zur VPC01 Route 2	AWS- OnPrem - Informationen VPC01 zur Route 1	AWS- OnPrem - Informationen zur VPC01 Route 2
Ziel: 0.0.0.0/0	Ziel: 10.100.0.0/16	Ziel: 0.0.0.0/0	Ziel: 10.0.0.0/16
Ziel: igw-xxxxxx xxxxxxxxxxxxx AWS- DS- -IGW VPC01	Ziel: pcx-xxxxxx xxxxxxxxxxxxx -DS- & - - -Peer AWS VPC01 AWS OnPrem VPC01	Ziel: igw-xxxxxx xxxxxxxx AWS-Onpre m- VPC01	Ziel: pcx-xxxxxx xxxxxxxxxxxxx -DS- & - - -Peer AWS VPC01 AWS OnPrem VPC01

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- Informationen zur VPC01 Sicherheitsgruppe:

Name der Sicherheitsgruppe: AWS DS Test Lab Security Group

Beschreibung: AWS DS Test Lab Sicherheitsgruppe

VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxxx -DS- VPC01

Sicherheitsgruppenregeln für eingehende Zugriffe für -DS- AWS VPC01

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverk ehrstyp
Zielbereich	TCP	3389	Meine IP	Remotedesktop
Gesamter Datenverkehr	Alle	Alle	10.0.0.0/16	Gesamter lokaler VPC-Verkehr

Regeln für ausgehende Sicherheitsgruppen für -DS- AWS VPC01

Typ	Protocol (Protokoll)	Port-Bereich	Ziel	Datenverk ehrstyp
Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	Gesamter Datenverkehr

AWS- OnPrem - Informationen VPC01 zur Sicherheitsgruppe:

Name der Sicherheitsgruppe: AWS OnPrem Test Lab Security Group.

AWS- OnPrem - Informationen VPC01 zur Sicherheitsgruppe:

Beschreibung: AWS OnPrem Test Lab Security Group.

VPC: AWS vpc-xxxxxxxxxxxxxxxxxxxx - - OnPrem VPC01

Sicherheitsgruppenregeln für eingehenden Datenverkehr für - - AWS OnPrem VPC01

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
Zielbereich	TCP	464	10.0.0.0/16	Kerberos Passwort ändern/ei nrichten
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

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Datenverkehrstyp
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
Gesamter Datenverkehr	Alle	Alle	10.100.0.0/16	Gesamter lokaler VPC-Verkehr

Regeln für ausgehende Sicherheitsgruppen für AWS- - OnPrem VPC01

Typ	Protocol (Protokoll)	Port-Bereich	Ziel	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-Managementkonsole 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-Managementkonsole)

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 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- beginnt VPC01 und mit (10.0.0.0/16) endet.
 - Für Subnetze wählen Sie die öffentlichen Subnetze 10.0.0.0/24 und 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 (PowerShell) (optional)

1. Öffnen Sie PowerShell.
2. Geben Sie den folgenden Befehl ein: Stellen Sie sicher, dass Sie die in Schritt 4 des vorherigen AWS-Managementkonsole Verfahrens angegebenen Werte verwenden.

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd  
-Description "AWS DS Managed" - VpcSettings_VpcId vpc-xxxxxxx -  
VpcSettings_SubnetId subnet-xxxxxxx, subnet-xxxxxxx
```

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-Managementkonsole 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-  
xxxxxxx,SubnetIds= subnet-xxxxxxx, subnet-xxxxxxx
```

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 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 in AWS-DS- VPC01 einen DHCP-Optionssatz 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 Directory Service Verzeichnisse auf und wählen Sie dann die entsprechende Verzeichnis-ID aus. Identifizieren und verwenden Sie auf der Seite „Details“ IPs die in der DNS-Adresse angezeigten Adressen.

Sie können diese Adressen auch finden, indem Sie die Directory Service - Seite Verzeichnisse aufrufen und die entsprechende Verzeichnis-ID auswählen. Wählen Sie dann Skalieren und freigeben. Identifizieren und verwenden Sie unter Domänencontroller IPs die, 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 des neuen Satzes von DHCP-Optionen (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 Ihr aus. VPCs
7. Wählen Sie in der Liste von VPCs AWS DS VPC, Aktionen und dann DHCP-Optionssatz 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 [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#).

So konfigurieren Sie EC2, um Windows-Instances mit Ihrer Domain zu verbinden

1. Öffnen Sie unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
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 Amazon SSMManged InstanceCore verwalteten Richtlinie aus. Diese Richtlinie enthält die erforderlichen Mindestberechtigungen zum Verwenden des Systems-Managers-Dienstes.
 - Markieren Sie das Kästchen neben „Von Amazon SSMDirectory ServiceAccess verwaltete Richtlinie“. Die Richtlinie enthält die Berechtigungen zum Verbinden von Instances mit einem von 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 mit einer Domain zu verbinden, z. EC2DomainJoinB.
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 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 die **xxxxxxxxxxxxxxxxxxxxxx** Option Select aus.

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 Network die VPC aus, die mit AWS-DS- endet VPC01 (z. B. vpc-
xxxxxxxxxxxxxxxxxxxx | AWS-DS-). VPC01
 - Wählen Sie als Subnetz Public Subnet 1 aus, das für Ihre bevorzugte Availability Zone
vorkonfiguriert sein sollte (z. B. subnet - | -DS- -Subnetz01 |). **xxxxxxxxxxxxxxxxxxxx** AWS
VPC01 *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 die Option corp.example.com (d-) aus. **xxxxxxxxxx**
 - Wählen Sie für die IAM-Rolle den Namen aus, den Sie Ihrer Instance-Rolle gegeben haben, z.
B. [Erstellen Sie eine Rolle, um Windows-Instanzen mit Ihrer AWS verwalteten Microsoft AD-
Domäne zu verbinden](#) EC2DomainJoin
 - 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 PowerShell verwenden.

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 die Option Get Password aus, um Ihr Passwort abzurufen, falls Sie das noch nicht getan haben, und wählen Sie dann Remote Desktop-Datei herunterladen.
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 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 (PowerShell) (optional)

1. Starten 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. Sie sollten corp.example.com mit allen Standard OUs - und Konten, die mit einer neuen Domäne verknüpft sind, angezeigt werden. 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.

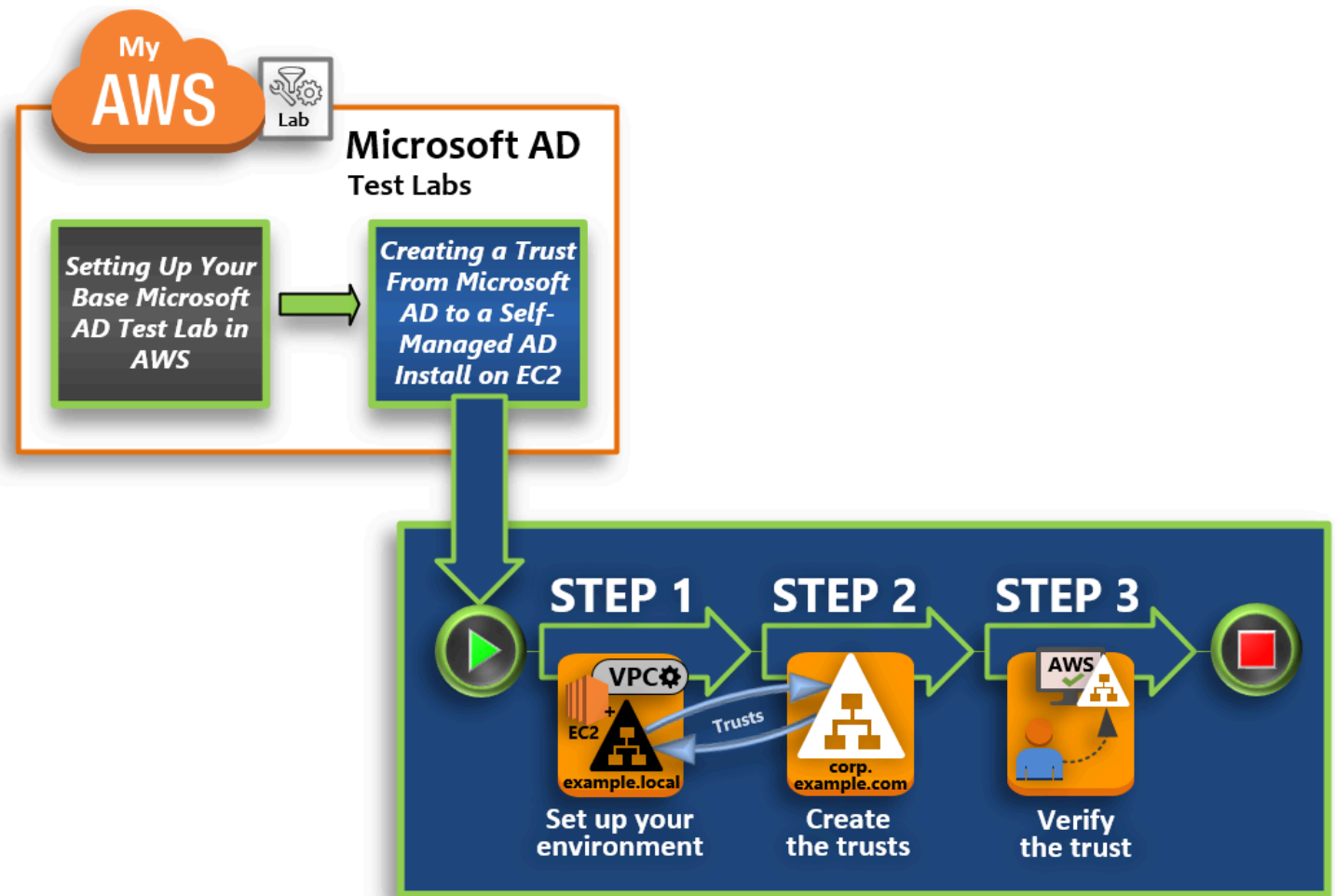
Herzlichen Glückwunsch! Ihre AWS verwaltete Microsoft AD-Basis-Testlabumgebung wurde jetzt konfiguriert. Sie können jetzt die nächsten Testumgebungen der Serie hinzufügen.

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

Bevor Sie Vertrauensstellungen zwischen einer neuen Active-Directory-Gesamtstruktur und der im [Basis-Tutorial](#) erstellten Gesamtstruktur von AWS Managed Microsoft AD einrichten können, müssen Sie Ihre Amazon-EC2-Umgebung vorbereiten. Dazu erstellen Sie zunächst einen Windows-Server-2019-Server, befördern diesen Server zu einem Domain-Controller und konfigurieren dann Ihre VPC entsprechend.

Schritt 2: Vertrauensstellungen erstellen

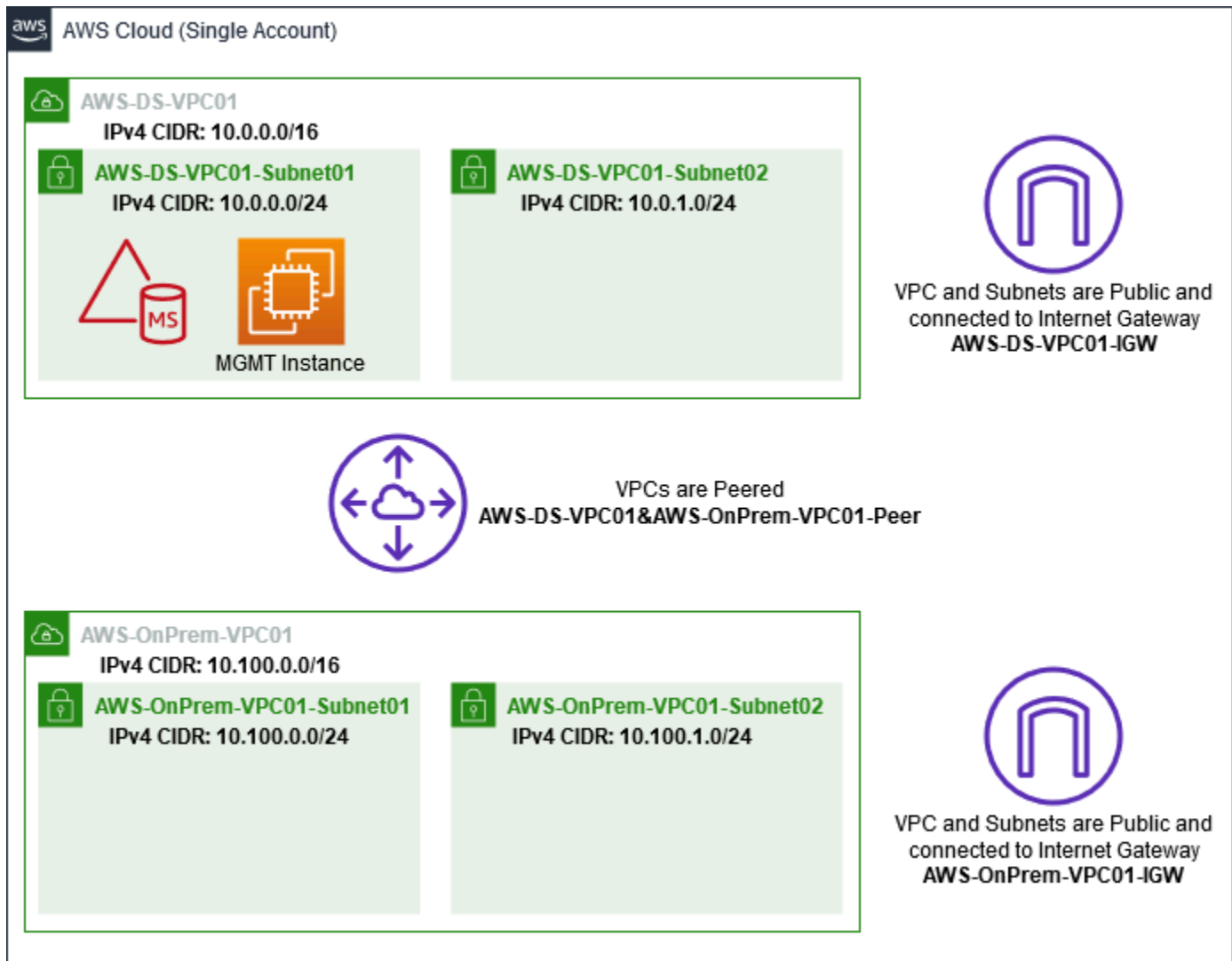
In diesem Schritt erstellen Sie eine bidirektionale Gesamtstruktur-Vertrauensstellung zwischen Ihrer neu erstellten Active Directory-Gesamtstruktur, die in Amazon EC2 gehostet wird, und Ihrer AWS verwalteten Microsoft AD-Gesamtstruktur in AWS.

Schritt 3: Die Vertrauensstellung überprüfen

Schließlich verwenden Sie als Administrator die Directory Service Konsole, um zu überprüfen, ob die neuen Trusts betriebsbereit sind.

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 **xxxxxxxxxxxxxxxxxxxx** in der Liste nach Microsoft Windows Server 2019 Base - ami-. 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- **xxxxxxxxxxxxxxxxxxxx** AWS- OnPrem - aus VPC01 (die Sie zuvor im [Base-Tutorial](#) eingerichtet haben).
 - Wählen Sie für Subnetz subnet - **xxxxxxxxxxxxxxxxxxxx** | AWS- - -Subnet01 | OnPrem - VPC01 - aus. AWS OnPrem VPC01
 - 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 AWS , der sich mit Ihrem lokalen Netzwerk repliziert, 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 angegeben sowohl DNS-Server als auch Global Catalog (GC) ausgewählt sind.
 - Geben Sie ein DSRM-Passwort (Directory Services Restore Mode) ein und bestätigen Sie es. Klicken Sie anschließend auf 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 aus, die Sicherheitsgruppe für **xxxxxx** D-Directory-Controller AWS erstellt wurde.

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 aus.

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-Domäne 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 sich die für den Server IPv4 angegebene Adresse. 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 [Konfiguration der regionsübergreifenden Replikation für AWS Managed Microsoft AD](#) 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 Vertrauentyp die Option Gesamtstruktur-Vertrauensstellung aus.

 Note

Stellen Sie sicher, dass der Vertrauentyp, den Sie hier auswählen, mit dem gleichen Vertrauentyp 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.

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 (Standard und Enterprise Edition)	20
AWS Verwaltete Microsoft AD-Verzeichnisse (Hybrid Edition)	5

Ressource	Standardkontingent
Manuelle Snapshots (Standard- und Enterprise-Edition) *	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.***	25
Freigegebene Domains pro Enterprise Microsoft AD-***	500
Gemeinsam genutzte Domänen pro Hybrid Microsoft AD ****	125
Maximale Anzahl registrierter Zertifizierungssertifikate (CA) pro Verzeichnis	5
Maximale Gesamtanzahl von 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 [Bewährte Methoden bei der Programmierung Ihrer Anwendungen für ein AWS verwaltetes Microsoft AD](#).

Informationen zu den Kontingenten für Speicher und Objekte finden Sie in der Vergleichstabelle auf der Seite zu [AWS Directory Service-Preisen](#).

Problembehandlung bei AWS verwaltetem Microsoft AD

Im Folgenden können Sie einige häufig auftretende Probleme beheben, die bei der Erstellung oder Verwendung Ihres AWS verwalteten Microsoft AD Active Directory auftreten können.

Probleme mit Ihrem AWS Managed Microsoft AD

Einige Aufgaben zur Problembehandlung können nur bis abgeschlossen werden Support. Hier sind einige der Aufgaben:

- Starten Sie Ihre von Ihnen Directory Service bereitgestellten Domänencontroller neu.
- [Ihr AWS verwaltetes Microsoft AD aktualisieren](#).

Informationen zum Erstellen eines Supportfalls finden Sie unter [Supportanfragen erstellen und Fallmanagement](#).

Probleme mit Netlogon und sicherer Kanalkommunikation

Als Gegenmaßnahme gegen [CVE-2020-1472](#) Microsoft wurde ein Patching veröffentlicht, das die Art und Weise ändert, wie die sichere Netlogon-Kanalkommunikation durch Domänencontroller 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 Ereignis IDs 5827 (für Probleme im

Zusammenhang mit der Geräteauthentifizierung) oder 5828 (für Probleme im Zusammenhang mit der AD-Vertrauensvalidierung). Informationen zu CloudWatch in AWS Managed Microsoft AD finden Sie unter [Aktivierung der Amazon CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#).

Weitere Informationen zur Risikominderung gegen CVE-2020-1472 finden Sie auf der Website unter [So verwalten Sie die Änderungen an sicheren Netlogon-Kanalverbindungen im Zusammenhang mit CVE-2020-1472](#). Microsoft

Sie erhalten die Fehlermeldung „Antwortstatus: 400 Bad Request“, wenn Sie versuchen, das Passwort eines Benutzers zurückzusetzen

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 unter [Problembehandlung bei Verzeichnisdaten](#).

Wiederherstellen des Passworts

Wenn ein Benutzer ein Passwort vergisst oder Probleme hat, sich bei Ihrem AWS Managed Microsoft AD-Verzeichnis anzumelden, können Sie sein Passwort entweder mit der AWS-Managementkonsole, PowerShell oder dem AWS CLI zurücksetzen.

Weitere Informationen finden Sie unter [Zurücksetzen eines AWS verwalteten Microsoft AD-Benutzerkennworts](#).

Weitere Ressourcen

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit AWS helfen.

- [AWS Knowledge Center](#) — Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, 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

- [Fehler beim Domänenbeitritt der Amazon EC2 EC2-Linux-Instance](#)
- [AWS Managed Microsoft AD, geringer verfügbarer Speicherplatz](#)
- [Fehler in Zusammenhang mit Schemaerweiterungen](#)
- [Gründe für den Status der Vertrauensstellung](#)

Fehler beim Domänenbeitritt der Amazon EC2 EC2-Linux-Instance

Im Folgenden können Sie einige Fehlermeldungen beheben, die beim Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem AWS Managed Microsoft AD-Verzeichnis 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
```

keine solche Identität:/Users/username/.ssh/id_ed25519: Keine solche Datei oder kein solches Verzeichnis

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 EC2 AMAZ- LSMWq T sshd [23832]: Fehlgeschlagenes Passwort für user@corp.example.com von xxx.xxx.xxx.xxx Port 18309 ssh2

31. Juli 00:05:00 EC2 AMAZ- T sshd [23832]: pam_winbind (sshd:auth): Passwort abrufen (0x00000390) LSMWq

31. Juli EC2 00:05:00 AMAZ- T sshd [23832]: pam_winbind (sshd:auth): pam_get_item hat ein Passwort zurückgegeben LSMWq

31. Juli 00:05:00 EC2 AMAZ- LSMWq T 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 EC2 AMAZ- LSMWq T 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
```

AWS Managed Microsoft AD, 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 [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. Bei diesen nicht unbedingt erforderlichen Dateien kann es sich um EXEs MSIs, oder jede andere Datei handeln, deren Verarbeitung durch Gruppenrichtlinien nicht unbedingt erforderlich ist. Die wichtigsten Objekte, die von Gruppenrichtlinien verarbeitet werden müssen, sind Gruppenrichtlinienobjekte, Logon/off Skripts 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](#) eine Option für verwaltete Dateiserver an FSx.

Um nicht benötigte Dateien zu entfernen, können Sie über den UNC-Pfad (Universal Naming Convention) auf die SYSVOL-Freigabe zugreifen. Wenn der vollqualifizierte Domänenname (FQDN) Ihrer Domain beispielsweise example.com lautet, wäre 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 [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 Gruppenverwaltung in AWS Managed Microsoft AD](#).

```
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 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 [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 [Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots](#). 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 es länger oder kürzer machen möchten, ersetzen Sie „30“ durch eine beliebige 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 bei der Behebung einiger Fehlermeldungen helfen, die bei der Erweiterung des Schemas für Ihr AWS verwaltetes Microsoft AD-Verzeichnis 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 ist: 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 ist: 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 der Attributkonvertierung, 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 ist: 0000208D: NameErr: DSID-03100238, Problem 2001 (NO_OBJECT), Daten 0, beste Übereinstimmung mit: 'CN=Schema, CN=Configuration, 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 die Vertrauensbildung für AWS Managed Microsoft AD fehlschlägt, enthält die Statusmeldung zusätzliche Informationen. Im Folgenden können Sie besser verstehen, was diese Meldungen bedeuten.

Zugriff verweigert

Der Zugriff wurde verweigert, wenn Sie versuchen, die Vertrauensstellung zu erstellen. Entweder ist das Vertrauenskennwort falsch oder die Sicherheitseinstellungen der Remotedomäne lassen die Konfiguration einer Vertrauensstellung nicht zu. Weitere Informationen zu Vertrauensstellungen finden Sie unter [Verbesserung der Vertrauenseffizienz durch Site-Namen und DCLocator](#). Versuchen Sie Folgendes, um dieses Problem zu beheben:

- 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) in dem `NullSessionPipesRegistrierungsschlüssel` vorhanden sind, der sich im Registrierungspfad `HKLM\SYSTEM\services\CurrentControlSet\Parameters` befindet. LanmanServer 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 SMB-Signatureeinstellung (Server Message Block) in der Standardrichtlinie für Domänencontroller. Diese Einstellungen finden Sie unter `Computerkonfiguration > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien/ Sicherheitsoptionen`. Sie sollten den folgenden Einstellungen entsprechen:
 - `MicrosoftNetzwerkclient: Kommunikation digital signieren (immer)`: Standard: Aktiviert

- MicrosoftNetzwerkserver: Kommunikation digital signieren (immer): Aktiviert

Verbesserung der Vertrauenseffizienz durch Site-Namen und DCLocator

Der erste Site-Name Default-First-Site-Name ist keine Voraussetzung für den Aufbau von Vertrauensbeziehungen zwischen Domänen. Durch die Abstimmung von Standortnamen zwischen Domänen kann jedoch die Effizienz des Domain Controller Locator (DCLocator) -Prozesses erheblich verbessert werden. Diese Ausrichtung verbessert die Vorhersage und Steuerung der Auswahl von Domänencontrollern in den Trusts der Gesamtstruktur.

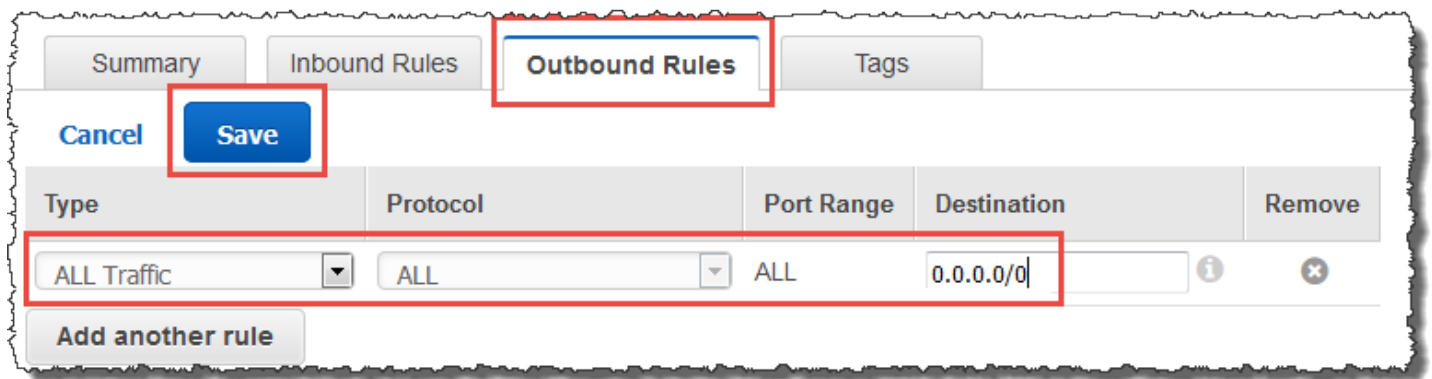
Dieser DCLocator Prozess ist entscheidend für die Suche nach Domänencontrollern in verschiedenen Domänen und Gesamtstrukturen. Weitere Informationen zu diesem DCLocator Prozess finden Sie in der [MicrosoftDokumentation](#). Eine effiziente Standortkonfiguration ermöglicht eine schnellere und genauere Ortung des Domänencontrollers, was zu einer besseren Leistung und Zuverlässigkeit bei gesamtstrukturübergreifenden Vorgängen führt.

Weitere Informationen zur Interaktion zwischen Site-Namen und DCLocator Prozessen finden Sie in den folgenden Artikeln: Microsoft

- [Wie sich Domänencontroller in verschiedenen Trusts befinden](#)
- [Domänen-Locator für alle Gesamtstrukturen](#)

Der angegebene Domain-Name ist nicht vorhanden oder konnte nicht hergestellt werden

Um dieses Problem zu lösen, stellen Sie sicher, dass die Sicherheitsgruppeneinstellungen für Ihre Domain und die Zugriffskontrollliste (ACL) für Ihre VPC korrekt sind und Sie die Informationen für Ihren Conditional Forwarder korrekt eingegeben haben. AWS konfiguriert die Sicherheitsgruppe so, dass nur die Ports geöffnet werden, 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: Bereiten Sie Ihr AWS verwaltetes Microsoft AD vor](#).



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 erhalten Sie unter [Eine Vertrauensbeziehung erstellen, überprüfen oder löschen](#) und [Voraussetzungen](#).

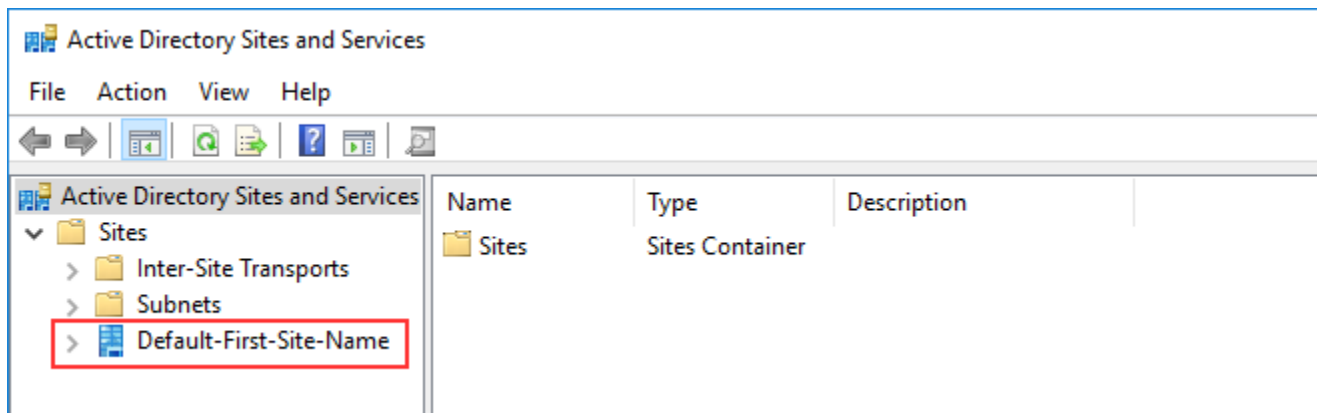
Die Internet Assigned Numbers Authority (IANA) hat die folgenden drei Blöcke der IP-Adressumgebung für private Internetdienste reserviert:

- 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-Site-Name für Ihr AWS verwaltetes Microsoft AD mit dem Standard-AD-Site-Namen in Ihrer lokalen 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 dazu, wie das funktioniert, finden Sie auf Microsoft der [Website unter Domain Locator Across a Forest Trust](#).



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](#).
- Gemäß RFC 1123 (<https://tools.ietf.org/html/rfc1123>) sind die einzigen Zeichen, die in DNS-Labels 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“ (Net-, Host-, Gateway- oder Domainname) eine Textzeichenfolge mit bis zu 24 Zeichen aus dem Alphabet (A-Z), Ziffern (0-9), Minuszeichen (-) und 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 Website](#). Microsoft

Standard-Tools für das Testen von Vertrauensstellungen

Im Folgenden finden Sie Tools, mit denen Sie verschiedene Probleme im Zusammenhang mit Vertrauensstellungen beheben können.

AWS Tool zur Problembehebung bei Systems Manager Automation

[Support Automation Workflows \(SAW\)](#) nutzen AWS Systems Manager Automation, um Ihnen ein vordefiniertes Runbook für Directory Service zur Verfügung zu stellen. Das [AWS Support-TroubleshootDirectoryTrust](#) Runbook-Tool hilft Ihnen bei der Diagnose häufiger Probleme bei der Vertrauensbildung zwischen AWS verwaltetem Microsoft AD und einem lokalen Microsoft Active Directory.

DirectoryServicePortTest Tool

Das [DirectoryServicePortTest](#) Testtool kann bei der Behebung von Problemen bei der Vertrauensbildung zwischen AWS Managed Microsoft AD und lokalem 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 auf der Website unter [Netdom](#) und [NLTEST](#). Microsoft

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 zwischenspeichern. 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 ziehen [Teilen Sie Ihr AWS verwaltetes Microsoft AD](#). AD Connector ist auch nicht Multi-VPC-fähig, was bedeutet, dass AWS Anwendungen wie in derselben VPC wie Ihr AD Connector bereitgestellt [WorkSpaces](#) werden müssen.

Nach der Einrichtung von AD Connector profitieren Sie von folgenden Vorteilen:

- Ihre Endbenutzer und IT-Administratoren können ihre vorhandenen Unternehmensanmeldedaten verwenden, um sich bei AWS Anwendungen wie WorkSpaces WorkDocs, oder Amazon anzumelden WorkMail.
- Sie können AWS Ressourcen wie EC2 Amazon-Instances oder Amazon S3-Buckets über den rollenbasierten IAM-Zugriff auf die verwalten. AWS-Managementkonsole
- 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](#)
- [Bewährte Methoden für AD Connector](#)
- [Ihr AD-Connector-Verzeichnis verwalten](#)
- [Ihr AD-Connector-Verzeichnis sichern](#)
- [Ihr AD-Connector-Verzeichnis überwachen](#)
- [Zugriff auf AWS Anwendungen und Dienste über AD Connector](#)
- [Möglichkeiten, eine EC2 Amazon-Instance mit Ihrem Active Directory zu verbinden](#)
- [Kontingente für AD Connector](#)
- [Fehlerbehebung in AD Connector](#)

Erste Schritte mit AD Connector

Mit AD Connector können Sie eine Verbindung Directory Service zu Ihrem vorhandenen Active Directory Ihres Unternehmens herstellen. Bei Verbindung mit Ihrem vorhandenen Verzeichnis bleiben alle Ihre Verzeichnisdaten auf Ihren Domain-Controllern. Directory Service repliziert keine Ihrer Verzeichnisdaten.

Themen

- [AD-Connector-Voraussetzungen](#)
- [Einen AD Connector erstellen](#)
- [Was wird mit Ihrem AD Connector erstellt](#)

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 der Subnetze muss sich in einer anderen Availability Zone befinden und denselben Netzwerktyp haben.

Sie können es IPv6 für Ihre VPC verwenden. Weitere Informationen finden Sie unter [IPv6 Support für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

- Die VPC muss mit Ihrem vorhandenen Netzwerk über ein VPN (Virtual Private Network) oder Direct Connect verbunden sein.
- Die VPC muss über Standard-Hardware-Tenancy verfügen.

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 zu AWS Direct Connect finden Sie im [AWS Direct Connect Benutzerhandbuch](#).

Vorhandenes Active Directory

Sie müssen eine Verbindung zu einem vorhandenen Netzwerk mit einer Active Directory-Domäne herstellen.

Note

AD Connector unterstützt [Single Label Domains](#) nicht.

Die Funktionsebene dieser Active Directory-Domäne muss Windows Server 2003 mindestens sein. 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.

Dienstkonto

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 Sie Seamless Domain Join verwenden 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-Domänencontroller umleiten kann, muss die Firewall für Ihr vorhandenes Netzwerk die folgenden Ports 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 `Disable VLVSsupport LDAP` für Ihre Domain-Controller auf 0 gesetzt werden. Dies ist die Standardeinstellung für die Domain-Controller. AD Connector kann keine Benutzer im Verzeichnis abfragen, wenn das Attribut `Disable VLVSsupport LDAP` 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-Domäne innerhalb der VPC befinden, müssen die mit diesen Servern verknüpften Sicherheitsgruppen die oben genannten Ports 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-Vorabauthentifizierung aktiviert ist](#). Allgemeine Informationen zu dieser Einstellung finden Sie unter [Vorabauthentifizierung](#) 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 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. 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 [Multi-Faktor-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 `erstellenConnectors`, die erforderlichen Rechte delegieren, die für die Verbindung mit Directory Service dieser Gruppe erforderlich sind, und dann 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

Feld	Wert/Auswahl
Group type (Gruppentyp)	Sicherheit

4. Wählen Sie in der Navigationsstruktur „Active Directory-Benutzer und -Computer“ die Option Identifizieren Sie die Organisationseinheit (OU) aus, in der die Computerkonten erstellt werden sollen. Wählen Sie im Menü Action und dann Delegate Control. Sie können eine übergeordnete Organisationseinheit bis zur Domäne auswählen, da die Berechtigungen auf das untergeordnete OUs Unternehmen übertragen werden. 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. Klicken Sie anschließend auf Weiter.

Delegation of Control Wizard

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

☐ This folder, existing objects in this folder, and creation of new objects in this folder

☒ Only the following objects in the folder:

- ☐ Site Settings objects
- ☐ Sites Container objects
- ☐ Subnet objects
- ☐ Subnets Container objects
- ☐ Trusted Domain objects
- ☒ User objects

☒ Create selected objects in this folder

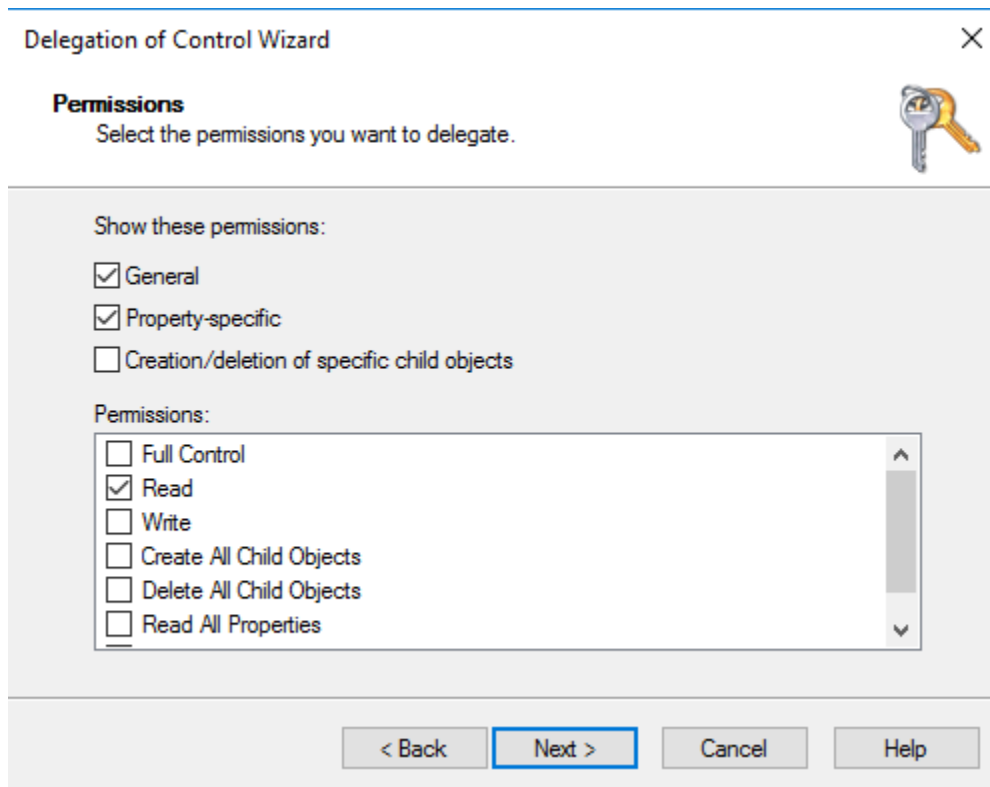
☒ Delete selected objects in this folder

< Back **Next >** Cancel Help

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 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 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 Testanwendung herunter und entpacken Sie sie. [DirectoryServicePortTest](#) 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.WriteLine("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\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.WriteLine("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 eine Netzwerkverbindung 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.

Weitere Informationen darüber, was mit Ihrem AD Connector erstellt wird, finden Sie unter [Was wird mit Ihrem AD Connector erstellt](#).

Was wird mit Ihrem AD Connector erstellt

Wenn Sie einen AD Connector erstellen, erstellt er Directory Service automatisch ein elastic network interface (ENI) und ordnet es jeder Ihrer AD Connector-Instanzen zu. Jedes dieser Elemente ENIs ist für die Konnektivität zwischen Ihrer VPC und Directory Service AD Connector unerlässlich und sollte niemals gelöscht werden. Sie können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, Directory Service anhand der Beschreibung identifizieren: "Netzwerkschnittstelle für Verzeichnis-ID AWS wurde 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.

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

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 Managed 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 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 einfaches 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 Directory Service Optionen finden Sie unter [Welche sollte man auswählen](#).

Stellen Sie sicher, dass Ihre VPCs und Instances korrekt konfiguriert sind

Um eine Verbindung zu Ihren Verzeichnissen herzustellen, sie zu verwalten und zu verwenden, müssen Sie die Verzeichnisse, VPCs denen die Verzeichnisse zugeordnet sind, ordnungsgemäß konfigurieren. Weitere Informationen über die Anforderungen zur VPC-Sicherheit und Netzwerken finden Sie unter [Voraussetzungen für die Erstellung eines AWS verwalteten 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 [Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD zu verbinden](#) 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 Ihres Verzeichnisses vertraut

AWS erstellt eine [Sicherheitsgruppe](#) und fügt sie den [elastischen Netzwerkschnittstellen](#) Ihres Verzeichnisses hinzu, auf die von Ihrem Peering aus zugegriffen werden kann oder deren Größe geändert wurde. [VPCs](#) AWS konfiguriert die Sicherheitsgruppe so, dass unnötiger Datenverkehr zum Verzeichnis blockiert wird, und lässt notwendigen Datenverkehr zu.

Ändern der Verzeichnissicherheitsgruppe

Um die Sicherheit Ihrer Sicherheitsgruppenverzeichnisse zu ändern, 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, die Sicherheitsgruppe des Verzeichnisses mit anderen von Ihnen erstellten EC2-Instances zu verknüpfen. 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.

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

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 WorkDocs WorkMail, Amazon oder Quick verwendet werden. 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 [Aktualisierung der Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos in AWS-Managementkonsole](#).

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 kompatibel ist und bleibt mit Directory Service. Weitere Informationen zu Ihren Verantwortlichkeiten finden Sie in unserem [Modell für übergreifende Verantwortlichkeit](#).

Ihr AD-Connector-Verzeichnis verwalten

Sie können den verwenden AWS-Managementkonsole , um Ihren AD Connector zu verwalten und day-to-day administrative Aufgaben zu erledigen. Sie können Ihr Verzeichnis unter anderem wie folgt verwalten:

- [Sehen Sie sich Details zu Ihrem AD Connector](#) an.
- [Aktualisieren Sie die DNS-Adresse, auf die Ihr AD Connector](#) verweist.
- [Löschen Sie Ihren AD Connector](#), wenn er nicht mehr benötigt wird.

AD Connector Connector-Verzeichnisinformationen anzeigen

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

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. Informationen über das Verzeichnis werden auf der Seite Verzeichnisdetails angezeigt.

Weitere Informationen zum Feld Status finden Sie unter [Erläuterungen zum Verzeichnisstatus](#).

Netzwerktyp des Verzeichnisses aktualisieren

Sie können den Netzwerktyp Ihres Directory Service Verzeichnisses von IPv4 auf Dual-Stack (IPv4 und IPv6) ändern. Wenn Sie den Netzwerktyp so aktualisieren, dass er IPv6 IP-Adressen einschließt, steht Ihnen ein größerer Adressraum zur Verfügung als IPv4. IPv4 und IPv6 Kommunikation sind unabhängig voneinander.

Einzelheiten finden Sie unter [Vergleichen IPv4 und IPv6](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Important

Dies ist ein unidirektionaler Vorgang, der nicht rückgängig gemacht werden kann. Testen Sie zuerst in einer Umgebung außerhalb der Produktionsumgebung.

Voraussetzungen

Bevor Sie den Netzwerktyp Ihres Verzeichnisses aktualisieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Ihre VPC muss mit IPv6 CIDR-Bereichen konfiguriert sein. Einzelheiten finden Sie unter [IPv6 Support für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.
- Sie haben Administratorzugriff auf die AWS-Managementkonsole.
- Ihr Verzeichnis muss sich im Status Aktiv befinden.
- Sie verfügen über die entsprechenden IAM-Berechtigungen, um Directory Service Einstellungen zu ändern.

Um den Netzwerktyp des Verzeichnisses zu aktualisieren

Um Ihr Verzeichnis auf Dual-Stack-Netzwerke zu aktualisieren

Note

Wenn Ihr Verzeichnis in mehreren Regionen repliziert wird, führen Sie dieses Update in jeder Region durch.

1. Wählen Sie im Navigationsbereich der [AWS Directory Service -Konsole](#) Directories aus.
2. Wählen Sie das Zielverzeichnis aus.
3. Gehen Sie zur Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie IPv6 Support hinzufügen aus. Diese Option ist nur für Verzeichnisse verfügbar, die IPv4 nur diese Option enthalten.
5. Lesen Sie die Aktualisierungsinformationen und Preisdetails.
6. Wählen Sie Hinzufügen, um das Update zu bestätigen.

Nach dem Start des Updates ändert sich der Verzeichnisstatus während des Aktualisierungsvorgangs in Aktualisierung. Die Aktualisierung dauert in der Regel 15 bis 30 Minuten. Sobald der Vorgang abgeschlossen ist, wird der Verzeichnisstatus wieder auf Aktiv zurückgesetzt.

Aktualisierung der DNS-Adresse für Ihren AD Connector

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 für Sie aktualisiert WorkSpace sind. Weitere Informationen finden Sie unter [DNS-Server aktualisieren für WorkSpaces](#).

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](#).

Ihren 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-Managementkonsole Zugriff deaktivieren. Weitere Informationen finden Sie unter [Zugriff wird deaktiviert AWS-Managementkonsole](#).
 - Um Amazon zu deaktivieren WorkSpaces, müssen Sie den Service aus dem Verzeichnis in der WorkSpaces Konsole abmelden. Weitere Informationen finden Sie unter [Löschen eines Verzeichnisses](#) im WorkSpaces Amazon-Administratorhandbuch.
 - Um sie zu deaktivieren WorkDocs, müssen Sie die WorkDocs Site in der WorkDocs 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 for Windows File Server zu deaktivieren, müssen Sie das FSx Amazon-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter [Arbeiten mit Active Directory in FSx für Windows File Server](#) im Amazon FSx for Windows File 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 [Arbeiten mit Client VPN](#) im AWS Client VPN Administratorhandbuch.
- Zur Deaktivierung von Amazon Connect müssen Sie die Amazon Connect-Instance löschen. Weitere Informationen finden Sie unter [Löschen Ihrer Amazon Connect Connect-Instance](#) im Amazon Connect Connect-Administratorhandbuch.
- Um Amazon Quick zu deaktivieren, müssen Sie sich von Amazon Quick abmelden. Weitere Informationen finden Sie unter [Schließen Ihres Amazon Quick Kontos](#) in der Amazon-Kurzanleitung.

 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.

Ihr AD-Connector-Verzeichnis sichern

Sie können Funktionen wie Multi-Faktor-Authentifizierung (MFA), clientseitiges Lightweight Directory Access Protocol over Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS) und AWS Private Certificate Authority zur Sicherung Ihres AD Connector verwenden. Zu den Möglichkeiten, wie Sie Ihren AD Connector schützen können, gehören:

- Aktivieren Sie MFA, was die Sicherheit Ihres AD Connector erhöht.
- Aktivieren Sie das clientseitige Lightweight Directory Access Protocol über Secure Sockets Layer (SSL) /Transport Layer Security (TLS) (LDAPS), sodass die Kommunikation über LDAP verschlüsselt wird und die Sicherheit verbessert wird.
- Aktivieren Sie die zertifikatsbasierte Mutual Transport Layer Security (mTLS) -Authentifizierung mit Smartcards, sodass sich Benutzer über Ihr Active Directory und AD Connector bei Amazon Web Services authentifizieren können.
- Aktualisieren Sie die Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos.
- Richten Sie AWS Private CA Connector für AD ein, damit Sie Zertifikate für Ihren AD Connector ausstellen und verwalten können.

Aufgaben zur Sicherung Ihres AD Connector

- [Multi-Faktor-Authentifizierung für AD Connector aktivieren](#)
- [Aktivieren von clientseitigem LDAPS mithilfe von AD Connector](#)
- [Aktivierung der mTLS-Authentifizierung in AD Connector für die Verwendung mit Smartcards](#)
- [Aktualisierung der Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos in AWS-Managementkonsole](#)
- [AWS Private CA Connector für AD einrichten](#)

Multi-Faktor-Authentifizierung für AD Connector aktivieren

Sie können die Multi-Faktor-Authentifizierung für AD Connector aktivieren, wenn Active Directory lokal oder in Amazon EC2 EC2-Instances ausgeführt wird. Weitere Informationen zur Verwendung der Multi-Faktor-Authentifizierung mit finden Sie unter. Directory Service [AD-Connector-Voraussetzungen](#)

 Note

Die Multifaktor-Authentifizierung ist für Simple AD nicht verfügbar. MFA kann jedoch für Ihr AWS verwaltetes Microsoft AD-Verzeichnis aktiviert werden. Weitere Informationen finden Sie unter [Aktivierung der 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-Managementkonsole oder auf Amazon Enterprise-Anwendungen und -Services wie WorkSpaces Amazon Quick oder Amazon Chime. Es bietet keine MFA für Windows-Workloads, die auf EC2-Instances ausgeführt werden, oder für die Anmeldung bei einer EC2-Instance. Directory Service unterstützt keine RADIUS-Authentifizierung.

Challenge/Response

Benutzer müssen ihren MFA-Code bei der Eingabe ihres Benutzernamens und Passworts 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 lokales Netzwerk muss eingehenden Datenverkehr über den standardmäßigen RADIUS-Serverport (UDP:1812) von den Servern zulassen. 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.

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.

Aktivieren von clientseitigem LDAPS mithilfe von AD Connector

Die clientseitige LDAPS-Unterstützung in AD Connector verschlüsselt die Kommunikation zwischen Microsoft Active Directory (AD) und Anwendungen. AWS Beispiele für solche Anwendungen sind WorkSpaces, AWS IAM Identity Center, Quick und Amazon Chime. Diese Verschlüsselung hilft Ihnen, die Identitätsdaten Ihres Unternehmens besser zu schützen und Ihre Sicherheitsanforderungen zu erfüllen.

Sie können auch clientseitiges LDAPS abmelden und deaktivieren.

Themen

- [Voraussetzungen](#)
- [Aktivierung von clientseitigem LDAPS](#)
- [Clientseitiges LDAPS verwalten](#)

Voraussetzungen

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

Voraussetzungen:

- [Serverzertifikate in Active Directory bereitstellen](#)
- [CA-Zertifikat-Anforderungen](#)
- [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

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 AD Connector (ausgehend) und selbstverwaltetem Active Directory (eingehend) zu ermöglichen.

Aktivierung von clientseitigem LDAPS

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 wird der gesamte LDAP-Verkehr zwischen AWS Anwendungen und Ihrem selbstverwalteten Active Directory mit Secure Sockets Layer (SSL) -Kanalverschlüsselung übertragen.

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

Zertifikat wird registriert in Directory Service

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

Methode 1: Um Ihr Zertifikat in Directory Service (AWS-Managementkonsole) 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. 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.

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

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

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

Überprüfen Sie den Registrierungsstatus

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 Directory Service (AWS-Managementkonsole) zu überprüfen

1. Gehen Sie zum Abschnitt Clientseitiges LDAPS auf der Seite Verzeichnisdetails.
2. Überprüfen Sie den aktuellen Status der Zertifikatsregistrierung, 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 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
```

Aktivierung von clientseitigem LDAPS

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

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 Directory Service AWS CLI

- Führen Sie den folgenden Befehl aus.

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

Der LDAPS-Status wird überprüft

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

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

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 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
```

Weitere Informationen zum Anzeigen Ihres clientseitigen LDAPS-Zertifikats, zum Abmelden oder Deaktivieren Ihres LDAPS-Zertifikats finden Sie unter [Clientseitiges LDAPS verwalten](#)

Clientseitiges LDAPS verwalten

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-Managementkonsole Methode oder die Methode verwenden. AWS CLI

Zertifikatsdetails anzeigen

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

Methode 1: Um die Zertifikatsdetails in Directory Service (AWS-Managementkonsole) anzuzeigen

- Wählen Sie im Navigationsbereich der [AWS Directory Service -Konsole](#) Verzeichnisse.
- Klicken Sie auf den Verzeichnis-ID-Link für Ihr Verzeichnis.
- Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
- Im Abschnitt Client-side LDAPS (Clientseitiges LDAPS) werden unter CA certificates (CA-Zertifikate) Informationen zum Zertifikat angezeigt.

Methode 2: So zeigen Sie die Zertifikatsdetails in 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 zuerst LDAPS deaktivieren, bevor Sie das Zertifikat abmelden können.

Methode 1: Um die Registrierung eines Zertifikats in Directory Service () aufzuheben AWS-Managementkonsole

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).

Methode 2: Um die Registrierung eines Zertifikats in () aufzuheben Directory Service AWS 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 das clientseitige LDAPS in () zu deaktivieren Directory Service AWS-Managementkonsole

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).

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

- Führen Sie den folgenden Befehl aus.

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

Aktivierung der mTLS-Authentifizierung in AD Connector für die Verwendung mit Smartcards

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)
- AWS GovCloud (US-Ost)

Sie können die Zertifikate auch abmelden und deaktivieren.

Themen

- [Voraussetzungen](#)
- [Smartcard-Authentifizierung aktivieren](#)
- [Verwaltung der Einstellungen für die Smartcard-Authentifizierung](#)

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 Ihr selbstverwaltetes Active Directory integriert ist. Weitere Informationen zur Einrichtung der Smartcard-Authentifizierung bei Amazon WorkSpaces und Active Directory finden Sie im [Amazon WorkSpaces Administration Guide](#).

Bevor Sie die Smartcard-Authentifizierung für aktivieren WorkSpaces, überprüfen Sie bitte die folgenden Voraussetzungen:

- [CA-Zertifikat-Anforderungen](#)
- [Voraussetzungen für ein Benutzer-Zertifikat](#)
- [Prozess zur Überprüfung des Zertifikatswiderrufs](#)
- [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.

 Note

Verzeichnisse, die nach dem 7. Oktober 2025 erstellt wurden, erfordern, dass OCSP-Server, die für die SmartCard Zertifikatsvalidierung verwendet werden, über die Netzwerkkonfiguration Ihrer VPC routingfähig sind. Wenn Ihr OCSP-Server nicht über die Routing-Tabellen, Sicherheitsgruppen und das Netzwerk Ihrer VPC zugänglich ist, schlägt die SmartCard Authentifizierung bei der ACLs Zertifikatssperrprüfung fehl. Um dieses Problem zu lösen, stellen Sie bitte sicher, dass:

- **Netzwerk-Routing:** Ihre VPC-Routing-Tabellen ermöglichen es, dass Datenverkehr Ihren OCSP-Server aus den Subnetzen erreicht, in denen Ihre AD Connector Connector-Verzeichnisinstanzen bereitgestellt sind.
- **Sicherheitsgruppen:** Die Sicherheitsgruppen, die den Netzwerkschnittstellen Ihres Verzeichnisses zugeordnet sind, ermöglichen ausgehenden Datenverkehr zu Ihrem OCSP-Server an Port 80 (HTTP).
- **Netzwerk ACLs:** Ihr Subnetznetzwerk ACLs ermöglicht bidirektionalen Verkehr to/from mit Ihrem OCSP-Server.
- **Internet-Gateway/NAT:** Wenn Ihr OCSP-Server mit dem Internet verbunden ist, stellen Sie sicher, dass Ihre VPC über eine geeignete Internet Gateway- oder NAT-Gateway-Konfiguration für die Verzeichnissubnetze verfügt. Wenn Ihr Netzwerktyp ist IPv4, müssen Sie NAT und Internet-Gateway mit Ihrer VPC konfiguriert haben.

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.

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.

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.

Schritte

- [Aktivieren der eingeschränkten Kerberos-Delegierung für das AD Connector Connector-Dienstkonto](#)
- [Registrierung des CA-Zertifikats in AD Connector](#)
- [Aktivierung der Smartcard-Authentifizierung für unterstützte AWS Anwendungen und Dienste](#)

Aktivieren der eingeschränkten Kerberos-Delegierung für das AD Connector Connector-Dienstkonto

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 dieser Funktion können Administratoren Vertrauensgrenzen für Anwendungen festlegen und durchsetzen, indem sie den Bereich einschränken, in dem Anwendungsdienste im Namen eines Benutzers agieren können. Weitere Informationen finden Sie unter [Kerberos Constrained Delegation](#).

Note

Kerberos Constrained Delegation (KCD) erfordert, dass der Benutzernamenanteil des AD Connector Connector-Dienstkontos mit dem AMAccount s-Namen desselben Benutzers übereinstimmt. Der AMAccount Name s ist auf 20 Zeichen beschränkt. s AMAccount Name 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 Delegation.
4. Wählen Sie die Optionen Diesem Benutzer nur für die Delegation 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 Delegation 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.

Registrierung des CA-Zertifikats in AD Connector

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-Managementkonsole)

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 Zertifikats Widerrufs](#).

6. Wählen Sie die Option Register certificate (Zertifikat registrieren) aus. Wenn Sie sehen, dass sich der Status des Zertifikats in Registriert ändert, wurde der Registrierungsprozess 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 Zertifikatsdaten auf den Speicherort der Zertifizierungsstellen-Zertifikatsdatei. 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.

Aktivierung der Smartcard-Authentifizierung für unterstützte AWS Anwendungen und Dienste

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-Managementkonsole)

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.

Weitere Informationen zum Anzeigen Ihres Zertifikats, zum Abmelden oder Deaktivieren Ihres Zertifikats finden Sie unter [Verwaltung der Einstellungen für die Smartcard-Authentifizierung](#)

Verwaltung der Einstellungen für die Smartcard-Authentifizierung

Sie können zwei verschiedene Methoden zur Verwaltung der Smartcard-Einstellungen verwenden. Sie können entweder die AWS-Managementkonsole 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 Directory Service (AWS-Managementkonsole) 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 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 Directory Service () aufzuheben AWS-Managementkonsole

- Wählen Sie im Navigationsbereich der [AWS Directory Service -Konsole](#) Verzeichnisse.
- Wählen Sie den Verzeichnis-ID-Link für Ihr AD Connector-Verzeichnis aus.
- Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
- 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.

- 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 Directory Service AWS 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 Directory Service () zu deaktivieren AWS-Managementkonsole

- Wählen Sie im Navigationsbereich der [AWS Directory Service -Konsole](#) Verzeichnisse.
- Wählen Sie den Verzeichnis-ID-Link für Ihr AD Connector-Verzeichnis aus.
- Wählen Sie auf der Seite Directory details (Verzeichnisdetails) die Registerkarte Networking & security (Netzwerk & Sicherheit) aus.
- Wählen Sie im Abschnitt Smartcard-Authentifizierung die Option Deaktivieren aus.
- Wählen Sie im Dialogfeld Smartcard-Authentifizierung deaktivieren die Option Deaktivieren aus.

Methode 2: Um die Smartcard-Authentifizierung in Directory Service (AWS CLI) zu deaktivieren

- Führen Sie den folgenden Befehl aus.

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

Aktualisierung der Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos in AWS-Managementkonsole

Die AD Connector Connector-Anmeldeinformationen, in denen Sie angeben, Directory Service stellen das Dienstkonto dar, das für den Zugriff auf Ihr vorhandenes lokales Verzeichnis verwendet wird. Sie können die Anmeldeinformationen für das Dienstkonto ändern, Directory Service indem Sie die folgenden Schritte ausführen.

 Note

Wenn für das Verzeichnis aktiviert AWS IAM Identity Center ist, Directory Service muss der Dienstprinzipalname (SPN) vom aktuellen Dienstkonto auf das neue Dienstkonto übertragen werden. 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 Connector-Dienstkontos in 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.

AWS Private CA Connector für AD einrichten

Sie können Ihr selbstverwaltetes Active Directory in die AWS Private Certificate Authority Verwendung von AD Connector integrieren, um Zertifikate für Ihre in eine AD-Domäne eingebundenen Benutzer, Gruppen und Maschinen auszustellen und zu verwalten. AWS Private CA Connector for AD bietet eine vollständig verwaltete Lösung AWS Private CA als direkten Ersatz für Ihr selbstverwaltetes Unternehmen, CAs ohne dass Sie lokale Agenten oder Proxyserver bereitstellen, patchen oder aktualisieren müssen.

Sie können diese Integration über die Directory Service Konsole, die AWS Private CA Connector for AD-Konsole oder durch Aufrufen der [CreateTemplate](#)API einrichten. Informationen zur

Verwendung der AWS Private CA Connector für Active Directory-Konsole finden Sie unter [AWS Private CA Connector für Active Directory](#). In den folgenden Abschnitten wird beschrieben, wie Sie diese Integration von der Directory Service Konsole aus einrichten.

Voraussetzungen

Anweisungen zur Einrichtung finden Sie unter [Connector für AD einrichten](#) im AWS Private CA Connector for AD-Benutzerhandbuch.

AWS Private CA Connector für AD einrichten

Um einen privaten CA-Connector für Active Directory zu erstellen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die 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 Anwendungsverwaltung und im Bereich AWS Apps und Dienste die Option AWS Private CA Connector for AD aus.
4. Führen Sie auf der Seite Privates CA-Zertifikat für Active Directory erstellen die Schritte aus, um Ihren privaten CA for Active Directory-Connector zu erstellen.

Weitere Informationen finden Sie unter [Einen Konnektor erstellen](#).

Sehen Sie sich Ihren AWS Private CA Connector für AD an

Um die Details des privaten CA-Connectors anzuzeigen

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Directory Service Konsole unter <https://console.aws.amazon.com/directoryservicev2/>.
2. Wählen Sie auf der Seite Directories (Verzeichnisse) Ihre Verzeichnis-ID aus.
3. Sehen Sie sich auf der Registerkarte Anwendungsverwaltung und im Bereich AWS Apps und Dienste Ihre Private CA-Connectors und die zugehörige private CA an. Die folgenden Felder werden angezeigt:
 - a. AWS Private CA Connector-ID — Die eindeutige Kennung für einen AWS Private CA Connector. Wählen Sie es aus, um die Detailseite anzuzeigen.
 - b. AWS Private CA Betreff — Informationen zum eindeutigen Namen der CA. Wählen Sie es aus, um die Detailseite aufzurufen.

c. Status — Ergebnisse der Statusprüfung für den AWS Private CA Connector und AWS Private CA:

- Aktiv — Beide Prüfungen bestehen
- 1/2 Prüfungen fehlgeschlagen — Eine Prüfung schlägt fehl
- Fehlgeschlagen — Beide Prüfungen schlagen fehl

Einzelheiten zum Status „Fehlgeschlagen“ erhalten Sie, wenn Sie mit der Maus auf den Hyperlink zeigen, um zu sehen, welche Prüfung fehlgeschlagen ist.

d. Registrierungsstatus für DC-Zertifikate — Statusüberprüfung für den Status des Domänencontroller-Zertifikats:

- Aktiviert — Die Zertifikatsregistrierung ist aktiviert
- Deaktiviert — Die Zertifikatsregistrierung ist deaktiviert

e. Erstellungsdatum — Wann der AWS Private CA Connector erstellt wurde.

Weitere Informationen finden Sie unter [Konnektor-Details anzeigen](#).

Überprüfen Sie die Ausstellung von Zertifikaten für AD-Benutzer

Gehen Sie wie folgt vor, um zu bestätigen, AWS Private CA dass Zertifikate für Ihr selbstverwaltetes Active Directory ausgestellt werden:

- Starten Sie Ihre lokalen Domänencontroller neu.
- Zeigen Sie Ihre Zertifikate mit Microsoft Management Console an. Weitere Informationen finden Sie in der [Microsoft-Dokumentation](#).

Ihr AD-Connector-Verzeichnis überwachen

Sie können Ihren AD Connector optimal nutzen, indem Sie mehr über die verschiedenen AD Connector-Status und deren Bedeutung für Ihren AD Connector erfahren. Sie können Amazon Simple Notification Service auch verwenden, um Benachrichtigungen über Ihren AD Connector Connector-Status zu erhalten.

Aufgaben zur Überwachung Ihres AD Connector:

- [Erläuterungen zum Verzeichnisstatus](#)

- [Aktivierung von AD Connector Connector-Verzeichnisstatusbenachrichtigungen mit Amazon SNS](#)

Erläuterungen zum Verzeichnisstatus

Im Folgenden sind die verschiedenen Zustandsangaben für ein Verzeichnis aufgeführt.

Aktiv

Das Verzeichnis funktioniert normal. 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 Verzeichnismvorgängen die volle Leistungskapazität erreicht. Es gibt viele mögliche Gründe dafür, dass sich das Verzeichnis in diesem Zustand befindet. Dazu gehören normale Wartungsaktivitäten wie Patchen oder EC2 Instanzrotation, temporäres Hotspotting durch eine Anwendung auf einem Ihrer Domänencontroller 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 bei normalen Wartungsproblemen diese Probleme 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 [Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots](#).

Inoperable (Funktionsunfähig)

Das Verzeichnis ist nicht funktionsfähig. Alle Verzeichnisendpunkte haben Probleme gemeldet.

Angefragt

Eine Anforderung zum Erstellen Ihres Verzeichnisses steht zurzeit an.

Aktivierung von AD Connector Connector-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 ein Amazon SNS SNS-Thema Directory Service als Herausgeber hinzufügen. Wenn 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?](#).

So aktivieren Sie SNS Messaging für Ihr Verzeichnis

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die [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, für die nur die [DirectoryServiceFullAccess](#) verwaltete Richtlinie gilt, muss Ihr Themename mit „DirectoryMonitoring“ beginnen. Wenn Sie Ihren Themennamen anpassen möchten, benötigen Sie zusätzliche Berechtigungen für SNS.

8. Wählen Sie Erstellen aus.

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-Managementkonsole .Directory Service](#)
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 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 übersehen werden, verknüpfen Sie Ihr Verzeichnis daher mit einem anderen Amazon SNS SNS-Thema Directory Service, bevor Sie ein Thema löschen, von dem Nachrichten empfangen werden.

Zugriff auf AWS Anwendungen und Dienste über AD Connector

Sie können Ihrem AD Connector Zugriff auf AWS Anwendungen und Dienste für Ihr verbundenes Active Directory gewähren. Zu den unterstützten AWS Anwendungen und Diensten gehören:

- Amazon Chime

- Amazon WorkSpaces
- IAM Identity Center
- AWS-Managementkonsole

Es gibt keine Anwendungen von Drittanbietern, die mit AD Connector kompatibel sind.

Aufgaben für den Zugriff auf AWS Anwendungen und Dienste über AD Connector

- [Richtlinie zur Anwendungskompatibilität für AD-Connector](#)
- [Zugriff auf AWS Anwendungen und Dienste über AD Connector ermöglichen](#)

Richtlinie zur Anwendungskompatibilität für AD-Connector

Als Alternative zum AWS Directory Service für Microsoft Active Directory ([AWS Verwaltetes Microsoft AD](#)) ist AD Connector ein Active Directory-Proxy nur für AWS erstellte Anwendungen und Dienste. 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.

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 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 [Möglichkeiten, eine EC2 Amazon-Instance mit Ihrem Active Directory zu verbinden](#).
- AWS-Managementkonsole — Sie können AD Connector verwenden, um AWS-Managementkonsole Benutzer mit ihren Active Directory-Anmeldeinformationen zu authentifizieren, ohne eine SAML-Infrastruktur einrichten zu müssen. Weitere Informationen finden Sie unter [AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft AD-Anmeldeinformationen aktivieren](#).

- Schnell — Weitere Informationen finden Sie unter [Benutzerkonten in Quick Enterprise Edition verwalten](#).
- AWS IAM Identity Center — Ausführliche Anweisungen finden Sie unter [Connect von IAM Identity Center mit einem lokalen Active Directory](#).
- AWS Transfer Family - Eine ausführliche Anleitung finden Sie unter [Arbeiten mit Directory Service für Microsoft Active Directory](#).
- AWS Client VPN — Ausführliche Anweisungen finden Sie unter [Client-Authentifizierung und Autorisierung](#).
- 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 kompatibel. Weitere Informationen finden Sie im Abschnitt AWS Managed Microsoft AD auf der [Directory Service FAQs](#)Seite.

Zugriff auf AWS Anwendungen und Dienste über AD Connector ermöglichen

Benutzer können AD Connector autorisieren, AWS Anwendungen und Diensten wie Amazon WorkSpaces Zugriff auf Ihr Active Directory zu gewähren. Die folgenden AWS Anwendungen und Dienste können für die Verwendung mit AD Connector aktiviert oder deaktiviert werden.

AWS Anwendung/Dienst	Weitere Informationen ...
Amazon Chime	Weitere Informationen finden Sie unter Verbindung mit Active Directory herstellen.

AWS Anwendung/Dienst	Weitere Informationen ...
Amazon Connect	Weitere Informationen finden Sie im Administrationshandbuch für Amazon Connect .
Amazon WorkDocs	Weitere Informationen finden Sie unter Erste Schritte mit Amazon WorkDocs .
Amazon WorkMail	Weitere Informationen finden Sie unter Organisation erstellen .
Amazon WorkSpaces	Sie können direkt von Simple AD, AWS Managed Microsoft AD oder AD Connector 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-Managementkonsole	Weitere Informationen finden Sie unter AWS-Managementkonsole Zugriff mit AWS verwaltet en Microsoft AD-Anmeldeinformationen aktivieren .
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 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 Directory Service. [Autorisierung für AWS Anwendungen und Dienste, die Directory Service](#)

Möglichkeiten, eine EC2 Amazon-Instance mit Ihrem Active Directory zu verbinden

AD Connector ist ein Verzeichnissgateway, mit dem Sie Verzeichnisanfragen an Ihr lokales Microsoft Active Directory umleiten können, ohne Informationen in der Cloud zwischenspeichern. Hier finden Sie weitere Informationen darüber, wie Sie ein Amazon EC2 mit einer Active Directory-Domain verbinden können:

- Sie können eine EC2 Amazon-Instance nahtlos mit Ihrer Active Directory-Domain verbinden, wenn die Instance gestartet wird. Weitere Informationen zum Hinzufügen einer EC2 Windows-Instanz zu einem AWS verwalteten Microsoft AD finden Sie unter [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#).
- Wenn Sie eine EC2 Instanz manuell mit Ihrer Active Directory-Domäne verbinden müssen, müssen Sie die Instanz in der richtigen Sicherheitsgruppe oder im Subnetz starten AWS-Region und die Instanz dann der Active Directory-Domäne hinzufügen.
- 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 Instance mit Ihrem selbstverwalteten Active Directory (On-Premises) verbinden, kommuniziert die Instance direkt mit Ihrem Active Directory und umgeht den AD Connector.

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

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](#)
- [Probleme mit der Verbindung](#)
- [Probleme bei der Authentifizierung](#)
- [Probleme mit der Wartung](#)
- [Ich kann meinen AD Connector nicht löschen](#)
- [Allgemeine Tools zur Untersuchung von AD Connector Connector-Emittenten](#)

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.](#)
- [Ich erhalte die Fehlermeldung „Verbindungsprobleme erkannt“, wenn ich versuche, AD Connector zu erstellen](#)

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 Directory Service Verzeichnisse unterstützen. Wenn Sie beim Erstellen eines Active Directory eine solche Fehlermeldung erhalten, 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 unter [Testen 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 beitrifft, überprüfen Sie das Passwort Ihres AD Connectors. AD Connector muss die Anforderungen an die AWS Passwortkomplexität erfüllen. Weitere Informationen finden Sie unter Dienstkonto unter [AD-Connector-Voraussetzungen](#).

Wenn Ihr AD Connector diese Anforderungen nicht erfüllt, erstellen Sie Ihren AD Connector mit einem Passwort neu, das diesen Anforderungen entspricht.

Ich erhalte die Meldung „Beim Verbinden des Verzeichnisses ist ein interner Dienstfehler aufgetreten. Bitte versuchen Sie den Vorgang erneut.“ Fehler beim Erstellen eines AD Connector

Dieser Fehler tritt normalerweise auf, wenn der AD Connector keinen gültigen Domänencontroller für Ihre selbstverwaltete Active Directory-Domäne erstellen kann und keine Verbindung zu diesem herstellen kann.

 Note

Als [bewährte Methode](#) gilt: Wenn in Ihrem selbstverwalteten Netzwerk Active Directory-Standorte definiert sind, müssen Sie Folgendes sicherstellen:

- Die VPC-Subnetze, in denen sich Ihr AD Connector befindet, sind an einem Active Directory-Standort definiert.
- Es bestehen keine Konflikte zwischen Ihren VPC-Subnetzen und den Subnetzen an Ihren anderen Standorten.

AD Connector verwendet den Active Directory-Standort, dessen Subnetz-IP-Adressbereiche denen in der VPC nahe kommen, die den AD Connector enthalten, um Ihre AD-Domänencontroller zu ermitteln. Wenn Sie einen Standort haben, dessen Subnetze dieselben IP-Adressbereiche wie die in Ihrer VPC haben, erkennt AD Connector die Domänencontroller an diesem Standort. Der Domänencontroller befindet sich möglicherweise nicht in der Nähe der Region, in der sich Ihr AD Connector befindet.

- Inkonsistenzen in DNS-SRV-Einträgen (diese Einträge verwenden die folgende Syntax: `_ldap._tcp.<DnsDomainName>` und `_kerberos._tcp.<DnsDomainName>`), die in der vom Kunden verwalteten Active Directory-Domäne erstellt wurden. Dies kann der Fall sein, wenn AD Connector auf der Grundlage dieser SRV-Einträge keinen gültigen Domänencontroller finden und keine Verbindung zu diesem herstellen konnte.
- Netzwerkprobleme zwischen AD Connector und vom Kunden verwaltetem AD, z. B. Firewallgeräten.

Sie können die [Erfassung von Netzwerkpaketen](#) auf Ihren Domänencontrollern, DNS-Servern und VPC-Flussprotokollen von Verzeichnisnetzwerkschnittstellen verwenden, um dieses Problem zu untersuchen. Wenden Sie sich an, [AWS Support](#) wenn Sie weitere Unterstützung benötigen.

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 lokalen Verzeichnis herstellen: Verbindungsprobleme festgestellt: LDAP nicht verfügbar (TCP-Port 389) für IP: *<IP address>* Kerberos/authentication nicht verfügbar (TCP-Port 88) für IP: *<IP address>*
Bitte stellen Sie sicher, dass die aufgelisteten Ports verfügbar sind, und wiederholen Sie den Vorgang.

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 Anschlüsse. In der folgenden Liste finden Sie einige dieser Anschlüsse. 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 bei 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: FEHLER: Die Zertifikatsüberprüfung ist fehlgeschlagen. Bitte versuchen Sie es erneut, indem Sie Ihren Browser oder Ihre Anwendung neu starten, und stellen Sie sicher, dass Sie das richtige Zertifikat ausgewählt haben. 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 unter [Voraussetzungen](#).

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/spnzum Dienstprinzipalnamen 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:

- Navigieren Sie im Registrierungseditor zum folgenden Hive-Schlüssel

HKEY_LOCAL_MACHINE\SYSTEM\ Services\ Kdc\ CurrentControlSet UseSubjectAltName

- Untersuchen Sie den UseSubjectAltName Wert von:
 - i. Wenn der Wert auf 0 gesetzt ist, ist die Zuordnung von alternativen Antragstellernamen deaktiviert und Sie müssen ein bestimmtes Zertifikat explizit nur einem Benutzer zuordnen. Wenn ein Zertifikat mehreren Benutzern zugeordnet ist und dieser Wert 0 ist, schlägt die Anmeldung mit diesem Zertifikat fehl.
 - ii. Wenn der Wert nicht oder auf 1 gesetzt ist, müssen Sie ein bestimmtes Zertifikat explizit nur einem Benutzer zuordnen oder das Feld Alternativer Name des Antragstellers für die Anmeldung verwenden.

- A. Wenn das Feld Alternativer Name des Antragstellers auf dem Zertifikat vorhanden ist, wird es priorisiert.
- B. Wenn das Feld Alternativer Name des Antragstellers nicht auf dem Zertifikat vorhanden ist und das Zertifikat explizit mehr als einem Benutzer zugeordnet ist, schlägt die Anmeldung mit diesem Zertifikat fehl.

 Note

Wenn der Registrierungsschlüssel auf den lokalen Domänencontrollern festgelegt ist, kann der AD Connector die Benutzer in Active Directory nicht finden, was zu der obigen Fehlermeldung führt.

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 befindlichen WorkSpaces.
- Offline- und Root-CA-Zertifikate enthalten keine OCSP-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 NTAAuth Directory-Speicher 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 NTAAuth Directory-Speicher zu veröffentlichen:

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

Weitere Informationen zum Veröffentlichen von Zertifikaten im NTAAuth Store finden Sie unter [Import des ausstellenden CA-Zertifikats in den Enterprise NTAAuth Store](#) 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 Certificate_name.cer
```

4. Nach dem Befehl sollte ein Popup-Fenster erscheinen. Wählen Sie die OCSP-Option 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 Meldung „Ein Fehler ist aufgetreten“ oder „Ein unerwarteter Fehler“, wenn ich versuche, das AD Connector Connector-Dienstkonto zu aktualisieren

Die folgenden Fehler oder Symptome treten bei der Suche nach Benutzern in AWS Unternehmensanwendungen wie dem [Amazon WorkSpaces Console Launch Wizard](#) auf:

- Ein Fehler ist aufgetreten. Wenn du weiterhin ein Problem hast, kontaktiere das AWS Support Team in den Community-Foren und über den AWS Premium-Support.
- Es ist ein Fehler aufgetreten. Ihr Verzeichnis benötigt eine Aktualisierung der Anmeldeinformationen. Bitte aktualisieren Sie die Anmeldeinformationen für das Verzeichnis.

Wenn Sie versuchen, die Anmeldeinformationen Ihres AD Connector-Dienstkontos in AD Connector zu aktualisieren, erhalten Sie möglicherweise die folgenden Fehlermeldungen:

- Unerwarteter Fehler. Ein unerwarteter Fehler ist aufgetreten.

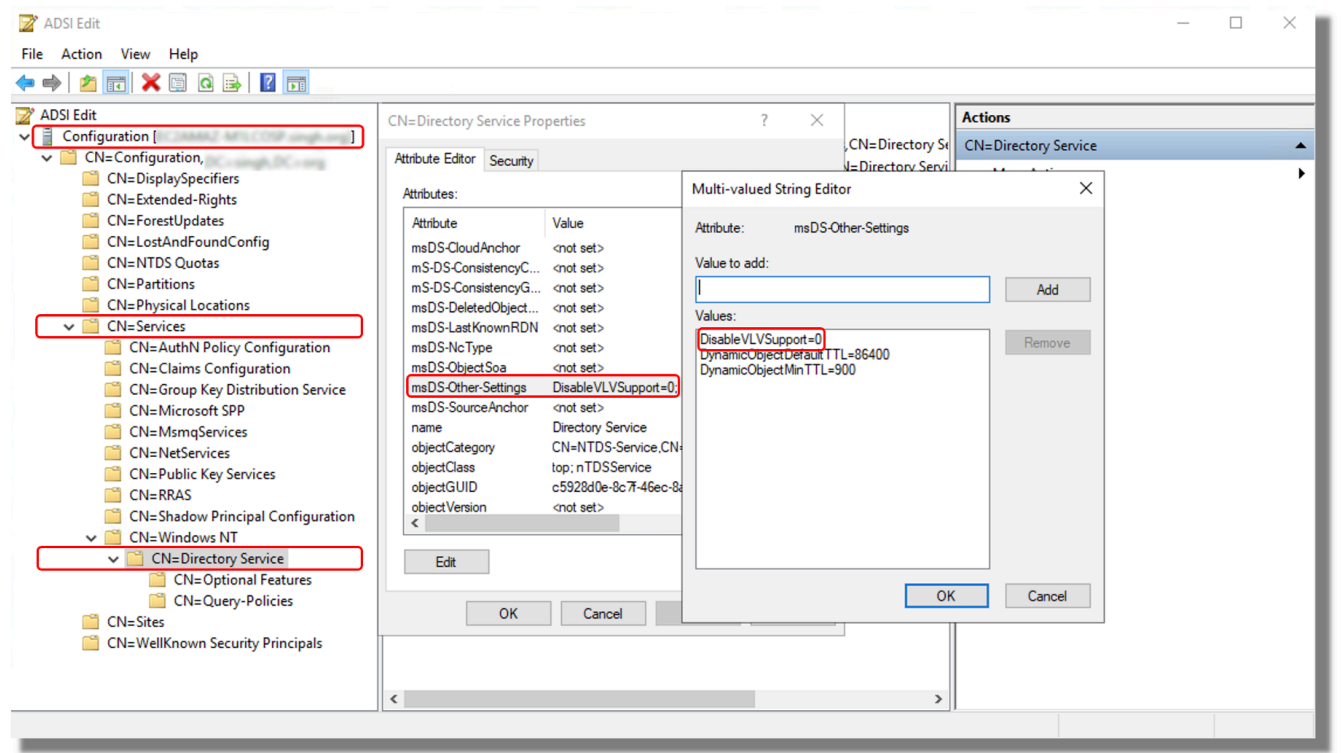
- Es ist ein Fehler aufgetreten. Bei der account/password Dienstkombination ist ein Fehler aufgetreten. Bitte versuchen Sie es erneut.

Das Dienstkonto des AD Connector Connector-Verzeichnisses befindet sich im vom Kunden verwalteten Active Directory. Das Konto wird als Identität verwendet, um Abfragen und Operationen in der vom Kunden verwalteten Active Directory-Domäne über den AD Connector im Namen von AWS Enterprise Applications durchzuführen. AD Connector verwendet Kerberos und LDAP, um diese Operationen auszuführen.

In der folgenden Liste wird erklärt, was diese Fehlermeldungen bedeuten:

- 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. Stellen Sie sicher, dass es keine Probleme mit der Zeitsynchronisierung zwischen den vom Kunden verwalteten Domänencontrollern gibt. 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 in den folgenden Abschnitten:
 - [So funktioniert der Windows Time Service](#)
 - [Maximale Toleranz für die Synchronisation der Computeruhr](#)
 - [WindowsTools und Einstellungen für den Zeitservice](#)
- Ein zwischengeschaltetes Netzwerkgerät mit einer [Netzwerk-MTU-Beschränkung](#), wie z. B. Firewall- oder VPN-Hardwarekonfigurationen, zwischen dem AD Connector und vom Kunden verwalteten Domänencontrollern kann diesen Fehler aufgrund von [Netzwerkfragmentierung](#) verursachen.
 - Um die MTU-Beschränkung zu überprüfen, können Sie einen [Ping-Test](#) zwischen Ihrem vom Kunden verwalteten Domain-Controller und einer Amazon EC2 EC2-Instance durchführen, die in einem Ihrer Verzeichnissubnetze gestartet wird, das über AD Connector verbunden ist. Die Framegröße sollte nicht größer als die Standardgröße von 1500 Byte sein
 - Der Ping-Test hilft Ihnen zu verstehen, ob die Framegröße mehr als 1500 Byte beträgt (auch bekannt als Jumbo-Frames) und ob sie die AD Connector Connector-VPC und das Subnetz erreichen können, ohne dass eine Fragmentierung erforderlich ist. Erkundigen Sie sich bei Ihrem Netzwerkteam weiter und stellen Sie sicher, dass Jumbo-Frames auf den Netzwerkgeräten zwischen den Geräten zulässig sind.

- Dieses Problem kann auftreten, wenn [clientseitiges LDAPS](#) auf AD Connector aktiviert ist und die Zertifikate abgelaufen sind. [Stellen Sie sicher, dass sowohl das serverseitige Zertifikat als auch das CA-Zertifikat gültig sind, nicht abgelaufen sind und die Anforderungen gemäß der Dokumentation erfüllen. LDAPS](#)
- Wenn die [Support für virtuelle Listenansichten](#) in der vom Kunden verwalteten Active Directory-Domäne deaktiviert ist, können AWS Anwendungen keine Benutzer suchen, da AD Connector die VLV-Suche in LDAP-Abfragen verwendet. Die Support virtueller Listenansichten ist deaktiviert, wenn der Wert Disable auf einen Wert ungleich Null gesetzt VLVSupport ist. Stellen Sie mithilfe der folgenden Schritte sicher, dass die [Support für virtuelle Listenansicht \(VLV\)](#) in Active Directory aktiviert ist:
 1. Melden Sie sich mit einem Konto mit Schema-Admin-Anmeldeinformationen als Besitzer der Schemamaster-Rolle beim Domänencontroller an.
 2. Wählen Sie Start und dann Ausführen aus und geben Sie die Eingabetaste ein **Adsiedit.msc**.
 3. Stellen Sie im ADSI-Bearbeitungstool Connect zur Konfigurationspartition her und erweitern Sie den Knoten Konfiguration [DomainController].
 4. Erweitern Sie den Container CN=Configuration, DC=. DomainName
 5. Erweitern Sie das Objekt CN=Services.
 6. Erweitern Sie das CN=Windows NT-Objekt.
 7. Wählen Sie das Objekt cn=Directory Service aus. Wählen Sie Properties (Eigenschaften).
 8. Wählen Sie in der Liste Attribute die Option MSDS-Other-Settings aus. Wählen Sie Bearbeiten aus.
 9. Wählen Sie in der Werteliste eine beliebige Instanz von Disable VLVSupport =x aus, bei der x nicht gleich 0 ist, und wählen Sie Entfernen aus.
 10. Geben **DisableVLVSupport=0** Sie nach dem Entfernen ein. Wählen Sie Hinzufügen aus.
 11. Wählen Sie OK. Sie können das ADSI-Edit-Tool schließen. Die folgende Abbildung zeigt das Dialogfeld „Editor für mehrwertige Zeichenketten“ im ADSI-Bearbeitungsfenster:



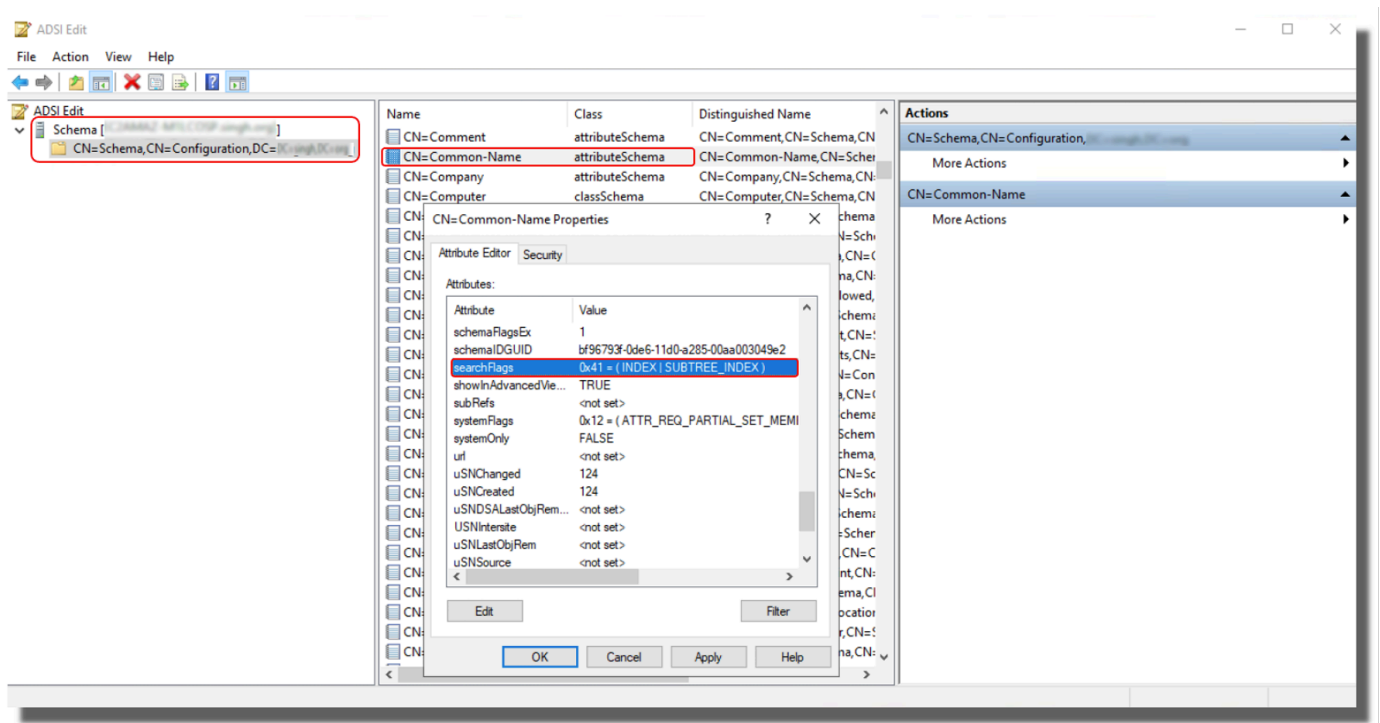
Note

In einer großen Active Directory-Infrastruktur mit mehr als 100.000 Benutzern können Sie möglicherweise nur nach bestimmten Benutzern suchen. Wenn Sie jedoch versuchen, alle Benutzer gleichzeitig aufzulisten (z. B. Alle Benutzer im WorkSpaces Launch Wizard anzeigen), kann dies zu demselben Fehler führen, auch wenn die VLV-Unterstützung aktiviert ist. AD Connector erfordert, dass die Ergebnisse mithilfe des Subtree Index nach dem Attribut „CN“ sortiert werden. Der Subtree Index ist der Indextyp, der die Domänencontroller auf die Ausführung eines LDAP-Suchvorgangs (Virtual List View) vorbereitet, der es AD Connector ermöglicht, eine sortierte Suche durchzuführen. Dieser Index verbessert die VLV-Suche und verhindert die Verwendung der aufgerufenen temporären Datenbanktabelle. [MaxTempTableSize](#) Die Größe dieser Tabelle kann variieren, aber standardmäßig beträgt die maximale Anzahl von Einträgen 10000 (die MaxTempTableSize Einstellung der Standard-Abfragerichtlinie). Das Erhöhen von MaxTempTableSize ist weniger effizient als die Verwendung der Subtree Indexing. Um diese Fehler in großen AD-Umgebungen zu vermeiden, wird empfohlen, Subtree Indexing zu verwenden.

Sie können den Subtree-Index aktivieren, indem Sie das [searchflags-Attribut](#) in der Attributdefinition im Active Directory-Schema mit einem Wert von 65 (0x41) ändern. Gehen Sie dabei ADSEdit wie folgt vor:

1. Melden Sie sich beim Domänencontroller als Inhaber der Schemamaster-Rolle mit einem Konto mit Schemaadministrator-Anmeldeinformationen an.
2. Wählen Sie Start und Ausführen und geben Sie ein **Adsiedit.msc**.
3. Stellen Sie im ADSI Edit Tool eine Verbindung zur Schemapartition her.
4. Erweitern Sie den Container CN=Schema, CN=Configuration, DC=. DomainName
5. Suchen Sie das Attribut "Common-Name", klicken Sie mit der rechten Maustaste und wählen Sie Eigenschaften aus.
6. Suchen Sie das searchFlags-Attribut und ändern Sie seinen Wert in, um die **65 (0x41)** SubTree Indizierung zusammen mit dem normalen Index zu aktivieren.

Die folgende Abbildung zeigt das Eigenschaftendialogfeld cn=Common-Name im ADSI-Bearbeitungsfenster:



7. Wählen Sie OK. Sie können das ADSI-Edit-Tool schließen.
8. Zur Bestätigung sollte Ihnen eine Ereignis-ID 1137 (Quelle: Active Directory_DomainServices) angezeigt werden, die angibt, dass das AD den neuen Index für das angegebene Attribut erfolgreich erstellt hat.

Weitere Informationen finden Sie in der [Microsoft-Dokumentation](#).

Ich erhalte die Fehlermeldung „Authentifizierung nicht möglich“, wenn ich AWS Anwendungen für die Suche nach Benutzern oder Gruppen verwende

Bei der Suche nach Benutzern oder bei der Anmeldung bei AWS Anwendungen wie WorkSpaces oder Quick können Fehler auftreten, auch wenn der AD Connector Connector-Status aktiv war. Wenn das Passwort des AD Connector-Dienstkontos geändert wurde oder abgelaufen ist, kann AD Connector die Active Directory-Domäne nicht mehr abfragen. Wenden Sie sich an Ihren AD-Administrator und überprüfen Sie Folgendes:

- Überprüfen Sie, ob das Passwort für das AD Connector Connector-Dienstkonto nicht abgelaufen ist
- Aktiviert, dass für das AD Connector Connector-Dienstkonto die Option Benutzer muss das Passwort bei der nächsten Anmeldung ändern nicht aktiviert ist.
- Vergewissern Sie sich, dass das AD Connector Connector-Dienstkonto nicht gesperrt ist.
- Wenn Sie sich nicht sicher sind, ob das Passwort abgelaufen ist oder geändert wurde, können Sie das Passwort für das Dienstkonto zurücksetzen und dasselbe Passwort auch in AD Connector [aktualisieren](#).

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:

Meldung: Es ist ein Fehler aufgetreten Ihr Verzeichnis muss aktualisiert werden. Bitte aktualisieren Sie die Anmeldeinformationen für das Verzeichnis. Ein Fehler ist aufgetreten Ihr Verzeichnis muss aktualisiert werden. Bitte aktualisieren Sie die Verzeichnisanmeldedaten wie folgt: Update your AD Connector Service Account Credentials: Ein Fehler ist aufgetreten Ihre Anfrage hat ein Problem. Bitte beachten Sie die folgenden Details. Bei der Kombination aus Dienstkonto und Passwort ist ein Fehler aufgetreten

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](#). Weitere Informationen zu Zeitdienst und Synchronisation finden Sie unten:

- [So 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](#) unter 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 AD Connector daran hindern, Computerobjekte in Ihrem Active Directory zu erstellen.

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 Ihrem Active Directory.
2. Aktualisieren Sie das Passwort für das Dienstkonto in Ihrem AD Connector in Directory Service. Weitere Informationen finden Sie unter [Aktualisierung der Anmeldeinformationen Ihres AD Connector Connector-Dienstkontos in AWS-Managementkonsole](#).

 Important

Wenn Sie das Kennwort nur in aktualisieren, wird die Kennwortänderung Directory Service nicht auf Ihr vorhandenes lokales Active Directory übertragen. 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 unter [Ihren AD Connector löschen](#). Wenn Sie Ihren AD Connector immer noch nicht löschen können, können Sie hier Hilfe anfordern [AWS Support](#).

Allgemeine Tools zur Untersuchung von AD Connector Connector-Emittenten

Die folgenden Tools können zur Behebung verschiedener AD Connector Connector-Probleme im Zusammenhang mit Erstellung, Authentifizierung und Konnektivität verwendet werden:

DirectoryServicePortTest Tool

Das [DirectoryServicePortTest](#) Testtool kann bei der Behebung von Verbindungsproblemen zwischen AD Connector und vom Kunden verwalteten Active Directory- oder DNS-Servern hilfreich sein. Weitere Informationen zur Verwendung des Tools finden Sie unter [Testen Sie Ihren AD Connector](#).

Tool zur Paketerfassung

Sie können das integrierte Windows Paketerfassungsprogramm ([netsh](#)) verwenden, um potenzielle Probleme mit der Netzwerk- oder Active Directory-Kommunikation (LDAP und Kerberos) zu untersuchen und zu beheben. Weitere Informationen finden Sie unter [Eine Netzwerkverfolgung erfassen, ohne etwas zu installieren](#).

VPC Flow-Protokolle

Um besser zu verstehen, welche Anfragen von AD Connector empfangen und gesendet werden, können Sie [VPC-Flussprotokolle](#) für die Verzeichnisnetzwerkschnittstellen konfigurieren. Sie

können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, Directory Service anhand der Beschreibung identifizieren: `AWS created network interface for directory your-directory-id`.

Ein einfacher Anwendungsfall ist die AD Connector Connector-Erstellung mit einer vom Kunden verwalteten Active Directory-Domäne mit einer großen Anzahl von Domänencontrollern. Sie können VPC-Flussprotokolle verwenden und nach dem Kerberos-Port (88) filtern, um herauszufinden, welche Domänencontroller im vom Kunden verwalteten Active Directory zur Authentifizierung kontaktiert werden.

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 EC2 Amazon-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 EC2 Amazon-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 WorkDocs, oder Amazon WorkMail.
- Sie können AWS Ressourcen über den rollenbasierten IAM-Zugriff auf die verwalten. AWS-Managementkonsole
- Tägliche automatische Snapshots ermöglichen die Wiederherstellung. point-in-time

Simple AD unterstützt Folgendes nicht:

- WorkSpaces Amazon-Anwendungen
- Amazon Chime

- Amazon FSx
- 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](#)
- [Bewährte Methoden für Simple AD](#)
- [Ihr Simple-AD-Verzeichnisses verwalten](#)
- [Sichern Sie Ihr Simple AD AD-Verzeichnis](#)
- [Ihr Simple-AD-Verzeichnis überwachen](#)
- [Zugriff auf AWS Anwendungen und Dienste von Ihrem Simple AD](#)
- [Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem Simple AD zu verbinden](#)
- [Benutzer- und Gruppenverwaltung in Simple AD](#)
- [Kontingente für Simple AD](#)
- [Beheben von Fehlern in Simple AD](#)

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, 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

- [Simple-AD-Voraussetzungen](#)
- [Erstellen Sie Ihr Simple AD](#)
- [Was wird mit Ihrem Simple AD erstellt](#)

Simple-AD-Voraussetzungen

Um ein Simple AD Active Directory zu erstellen, benötigen Sie eine Amazon-VPC mit den folgenden Komponenten:

- Die VPC muss über Standard-Hardware-Tenancy verfügen.

Sie können es IPv6 für Ihre VPC verwenden. Weitere Informationen finden Sie unter [IPv6 Support für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

- Mindestens zwei Subnetze in zwei verschiedenen Availability Zones und müssen vom gleichen Netzwerktyp sein. 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, 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.

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.

 Important

Wenn eine der Simple AD-Voraussetzungen nach der Erstellung Ihres Simple AD geändert wird, kann Ihr Simple AD beeinträchtigt werden. Um Ihren Simple AD AD-Impaired-Status zu lösen, müssen Sie sich an uns wenden [AWS Support](#).

Erstellen Sie Ihr Simple AD

Dieses Verfahren führt Sie durch alle notwendigen Schritte, um ein Simple AD zu erstellen. Es soll Ihnen einen schnellen und einfachen Einstieg in Simple AD ermöglichen, ist jedoch nicht für den Einsatz in einer umfangreichen Produktionsumgebung vorgesehen.

Schritte

- [Voraussetzungen](#)
- [Erstellen und Konfigurieren Ihrer Amazon VPC für Ihr Simple AD](#)
- [Erstellen Sie Ihr Simple AD](#)

Voraussetzungen

Bei diesem Verfahren wird Folgendes vorausgesetzt:

- Sie haben eine aktive AWS-Konto.
- Ihr Konto hat das Amazon-Limit 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`
- Sie befinden sich in einer Region, in der Simple AD verfügbar ist. Weitere Informationen finden Sie unter [Verfügbarkeit in der Region für Directory Service](#).

Weitere Informationen finden Sie unter [Simple-AD-Voraussetzungen](#).

Erstellen und Konfigurieren Ihrer Amazon VPC für Ihr Simple AD

Zunächst erstellen und konfigurieren Sie eine Amazon VPC für die Verwendung mit Ihrem Simple AD. Bevor Sie dieses Verfahren beginnen, stellen Sie sicher, dass Sie die [Voraussetzungen](#) erfüllt haben.

Die VPC, die Sie erstellen, wird zwei öffentliche Subnetze haben. Directory Service erfordert zwei Subnetze in Ihrer VPC, und jedes Subnetz muss sich in einer anderen Availability Zone befinden.

Erstellen einer VPC

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 sein. 10.0.0.0/16
 - Lassen Sie die Option „Kein IPv6 CIDR-Block“ ausgewählt.
 - Die Tenancy sollte Standard bleiben.
 - Wählen Sie 2 für die Anzahl der Availability Zones (AZs) aus.
 - 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.

Erstellen Sie Ihr Simple AD

Gehen Sie wie folgt vor, um ein neues Simple AD zu erstellen. Bevor Sie mit diesem Verfahren beginnen, stellen Sie sicher, dass Sie die folgenden Schritte unter [Voraussetzungen](#) und ausgeführt haben [Erstellen und Konfigurieren Ihrer Amazon VPC für Ihr Simple AD](#).

Erstellen Sie ein Simple AD

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. Während des Verzeichniserstellungsprozesses 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.

Important

Achten Sie darauf, dieses Passwort zu speichern. Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen werden. Sie können ein Passwort jedoch über die Directory Service Konsole oder mithilfe der [ResetUserPasswordAPI](#) zurücksetzen.

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.

Weitere Informationen darüber, was mit Ihrem Simple AD erstellt wird, finden Sie unter [Was wird mit Ihrem Simple AD erstellt](#).

Was wird mit Ihrem Simple AD erstellt

Wenn Sie ein Active Directory mit Simple AD erstellen, Directory Service führt es die folgenden Aufgaben in Ihrem Namen 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. Directory Service speichert dieses Passwort nicht und es kann nicht abgerufen werden. Sie können ein Passwort jedoch über die 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 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 Directory Service sicher gespeichert.
- Erstellt automatisch eine Elastic-Network-Schnittstelle (ENI) und ordnet sie jedem Ihrer Domain-Controller zu. Jedes dieser Elemente ist für ENIs die Konnektivität zwischen Ihrer VPC und den Directory Service Domänencontrollern unerlässlich und sollte niemals gelöscht werden. Sie können alle Netzwerkschnittstellen, die für die Verwendung reserviert sind, Directory Service anhand der Beschreibung identifizieren: "Netzwerkschnittstelle für Verzeichnis-ID AWS wurde erstellt". Weitere Informationen finden Sie unter [Elastic Network Interfaces](#) im EC2 Amazon-Benutzerhandbuch. Der Standard-DNS-Server des AWS verwalteten 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.

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

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 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 einfaches 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 Directory Service Optionen finden Sie unter [Welche sollte man auswählen](#).

Stellen Sie sicher, dass Ihre VPCs und Instances korrekt konfiguriert sind

Um eine Verbindung zu Ihren Verzeichnissen herzustellen, sie zu verwalten und zu verwenden, müssen Sie die Verzeichnisse, VPCs denen die Verzeichnisse zugeordnet sind, ordnungsgemäß konfigurieren. Weitere Informationen über die Anforderungen zur VPC-Sicherheit und Netzwerken finden Sie unter [Voraussetzungen für die Erstellung eines AWS verwalteten 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 [Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem AWS Managed Microsoft AD zu verbinden](#) 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 Ihres Verzeichnisses 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

Sie können Sicherheitsgruppen für Ihre Verzeichnisse ändern, aber nur, wenn Sie die Sicherheitsgruppenfilterung vollständig verstehen. Weitere Informationen finden Sie unter [Amazon-EC2-Sicherheitsgruppen für Linux-Instances](#) im Amazon-EC2-Benutzerhandbuch. Unsachgemäße Änderungen können die Kommunikation mit den vorgesehenen Computern und Instanzen stören. AWS empfiehlt, keine zusätzlichen Ports für Ihr Verzeichnis zu öffnen, da dies die Sicherheit verringert. Prüfen Sie das [Modell der AWS geteilten Verantwortung](#), bevor Sie Änderungen vornehmen.

 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 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

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 WorkDocs WorkMail, Amazon oder Quick verwendet werden. 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-Dienst oder den Dynamic DNS-Dienst (DDNS) Ihres AWS verwalteten Microsoft AD, um nach Domänencontrollern zu suchen (DCs). Nehmen Sie keine Hartkodierung an Anwendungen mit der Adresse eines Domain-Controllers vor. Der DC-Suchdienst sorgt für eine Verteilung der Verzeichnislaster und ermöglicht

Ihnen die Nutzung einer horizontalen Skalierung durch das Hinzufügen von Domain-Controllern zu Ihrer Bereitstellung. Wenn Sie Ihre Anwendung an einen festen DC binden und der DC gepatcht oder wiederhergestellt wird, verliert Ihre Anwendung den Zugriff auf den DC, anstatt einen der verbleibenden zu verwenden. DCs 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 Directory Service , mit dem Sie Domänencontroller hinzufügen können, um eine hohe Leistung zu erzielen. Weitere Informationen finden Sie unter [Bereitstellung zusätzlicher Domänencontroller für Ihr AWS verwaltetes Microsoft AD](#).

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.

Ihr Simple-AD-Verzeichnisses verwalten

Sie können das verwenden AWS-Managementkonsole , um Ihr Simple AD zu verwalten und day-to-day administrative Aufgaben zu erledigen. Zu den Möglichkeiten, wie Sie Ihr Simple AD verwalten können, gehören:

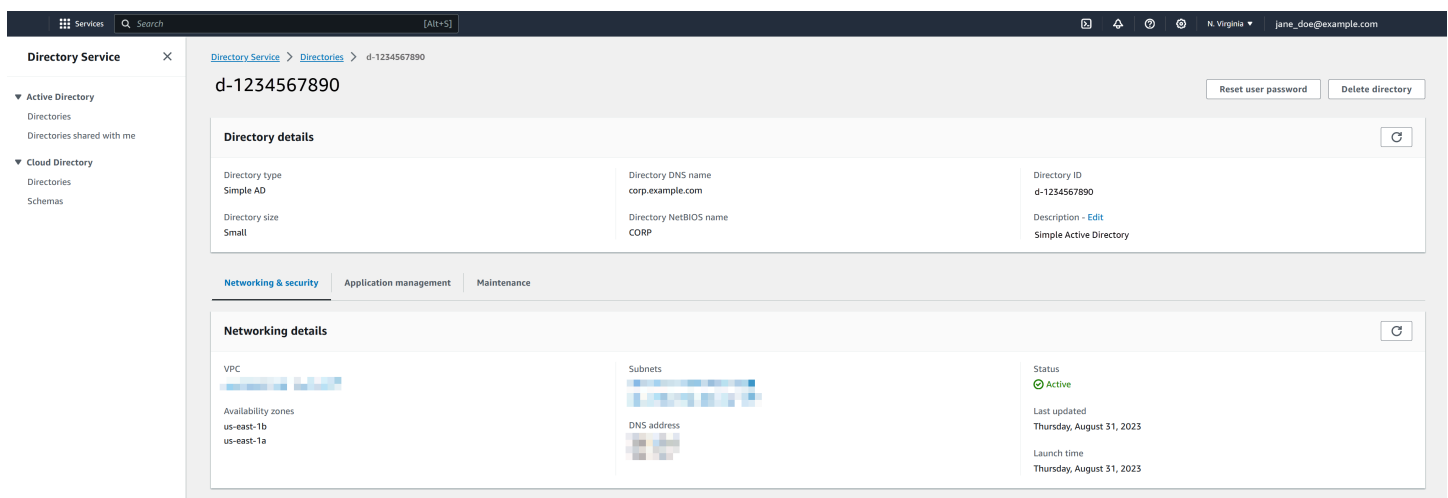
- [Zeigen Sie Details zu Ihrem Simple AD](#) wie den DNS-Namen, die Verzeichnis-ID und den Verzeichnisstatus an.
- [Aktualisieren Sie die DNS-Adresse für Ihr Simple AD](#).
- [Stellen Sie Ihr Simple AD mit Snapshots](#) wieder her. Sie können auch Snapshots erstellen und Snapshots löschen.
- [Löschen Sie Ihr Simple AD](#), wenn es nicht mehr benötigt wird.

Simple AD AD-Verzeichnisinformationen anzeigen

So rufen Sie detaillierte Informationen zu einem Verzeichnis auf

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. Informationen über das Verzeichnis werden auf der Seite Verzeichnisdetails angezeigt.

Weitere Informationen zum Feld Status finden Sie unter [Den Status Ihres Simple AD AD-Verzeichnisses verstehen](#).



Netzwerktyp des Verzeichnisses aktualisieren

Sie können den Netzwerktyp Ihres Directory Service Verzeichnisses von IPv4 auf Dual-Stack (IPv4 und IPv6) ändern. Wenn Sie den Netzwerktyp so aktualisieren, dass er IPv6 IP-Adressen einschließt, steht Ihnen ein größerer Adressraum zur Verfügung als IPv4. IPv4 und IPv6 Kommunikation sind unabhängig voneinander.

Einzelheiten finden Sie unter [Vergleichen IPv4 und IPv6](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.

Important

Dies ist ein unidirektionaler Vorgang, der nicht rückgängig gemacht werden kann. Testen Sie zuerst in einer Umgebung außerhalb der Produktionsumgebung.

Voraussetzungen

Bevor Sie den Netzwerktyp Ihres Verzeichnisses aktualisieren, stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind:

- Ihre VPC muss mit IPv6 CIDR-Bereichen konfiguriert sein. Einzelheiten finden Sie unter [IPv6 Support für Ihre VPC](#) im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch.
- Sie haben Administratorzugriff auf die AWS-Managementkonsole.
- Ihr Verzeichnis muss sich im Status Aktiv befinden.
- Sie verfügen über die entsprechenden IAM-Berechtigungen, um Directory Service Einstellungen zu ändern.

Um den Netzwerktyp des Verzeichnisses zu aktualisieren

Um Ihr Verzeichnis auf Dual-Stack-Netzwerke zu aktualisieren

Note

Wenn Ihr Verzeichnis in mehreren Regionen repliziert wird, führen Sie dieses Update in jeder Region durch.

1. Wählen Sie im Navigationsbereich der [AWS Directory Service -Konsole](#) Directories aus.
2. Wählen Sie das Zielverzeichnis aus.
3. Gehen Sie zur Registerkarte Netzwerk und Sicherheit.
4. Wählen Sie IPv6 Support hinzufügen aus. Diese Option ist nur für Verzeichnisse verfügbar, die IPv4 nur diese Option enthalten.

IPv6 nur Verzeichnisse werden nicht unterstützt.

5. Lesen Sie die Aktualisierungsinformationen und Preisdetails.
6. Wählen Sie Hinzufügen, um das Update zu bestätigen.

Nach dem Start des Updates ändert sich der Verzeichnisstatus während des Aktualisierungsvorgangs in Aktualisierung. Die Aktualisierung dauert in der Regel 15 bis 30 Minuten. Sobald der Vorgang abgeschlossen ist, wird der Verzeichnisstatus wieder auf Aktiv zurückgesetzt.

Konfiguration von DNS-Servern für Simple AD

Sie können DNS für Simple AD je nach Ihrer Netzwerkarchitektur und Ihren Anforderungen auf zwei Arten konfigurieren.

Simple AD als primäres DNS verwenden

Konfigurieren Sie Ihre Client-Computer so, dass sie die Simple AD AD-DNS-Server-IP-Adressen als primäre DNS-Resolver verwenden. 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](#).

Während der Simple AD AD-Erstellung führt der Service einen Erreichbarkeitstest für amazon.com durch, um zu ermitteln, welcher DNS-Resolver verwendet werden soll:

- Kunden-VPC-DNS-Resolver (ETH1) — Wird ausgewählt, wenn amazon.com vom Kunden-VPC-Resolver aus erreichbar ist. Diese Option aktiviert private, gehostete Route-53-Zonen und Resolver-Firewallregeln.
- Amazon Internal Resolver (ETH0) — Wird ausgewählt, wenn amazon.com vom Kunden-VPC DNS Resolver () nicht erreichbar ist. ETH1 Route 53-Integration, private gehostete Zonen und Resolver-Firewallregeln funktionieren mit dieser Option nicht.

Important

Die Auswahl des DNS-Resolvers erfolgt automatisch bei der Simple AD AD-Erstellung und kann danach nicht mehr geändert werden. Wir empfehlen Ihnen, sicherzustellen, dass amazon.com in Ihrer VPC auflösbar ist, bevor Sie Simple AD erstellen, um die Route 53-Integration zu aktivieren.

Verwenden Sie Route 53 als primäres DNS

Sie können Route 53 auch als Ihren primären DNS-Dienst verwenden:

- Konfigurieren Sie Ihre Client-Computer so, dass sie Route 53 Resolver-IP-Adressen als primäre DNS-Resolver verwenden

- Erstellen Sie Route 53-Resolver-Regeln, um nur die FQDN-Abfragen (Fully Qualified Domain Name) Ihrer Domain bedingt an Simple AD weiterzuleiten
- Bei diesem Ansatz wird Route 53 als autoritative DNS-Quelle beibehalten, wobei Simple AD nur domänenspezifische Abfragen verarbeitet.

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 sich außerhalb Ihrer VPC befinden, und Sie privates DNS verwenden möchten, müssen Sie die Konfiguration 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](#).
- [Integrieren Sie Ihre Directory Service' DNS-Auflösung mit](#). Amazon Route 53 Resolver

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.

Simple AD mit Snapshot 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](#)

- [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. Wenn Sie dieses Limit bereits erreicht haben, müssen Sie einen Ihrer vorhandenen manuellen Snapshots löschen, bevor Sie einen weiteren erstellen können.

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 wissen, dass alle DNS-Server DCs und DNS-Server, die dem Verzeichnis zugeordnet sind, offline sind, bis der Wiederherstellungsvorgang 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.

Löschen Sie Ihr Simple AD

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.

Wenn ein AWS verwaltetes Microsoft AD-, Simple AD- oder Hybridverzeichnis 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.

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 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 bereitgestellt wird. Weitere Informationen finden Sie unter [Wählen einer Region](#).
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-Managementkonsole den Zugriff. Weitere Informationen finden Sie unter [Zugriff wird deaktiviert AWS-Managementkonsole](#).
- Um Amazon zu deaktivieren WorkSpaces, müssen Sie den Service aus dem Verzeichnis in der WorkSpaces Konsole abmelden. Weitere Informationen finden Sie unter [Löschen eines Verzeichnisses](#) im WorkSpaces Amazon-Administratorhandbuch.
- Um sie zu deaktivieren WorkDocs, müssen Sie die WorkDocs Site in der WorkDocs 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 for Windows File Server zu deaktivieren, müssen Sie das FSx Amazon-Dateisystem aus der Domain entfernen. Weitere Informationen finden Sie unter [Arbeiten mit Active Directory in FSx für Windows File Server](#) im Amazon FSx for Windows File 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 [Arbeiten mit Client VPN](#) im AWS Client VPN Administratorhandbuch.
- Zur Deaktivierung von Amazon Connect müssen Sie die Amazon Connect-Instance löschen. Weitere Informationen finden Sie unter [Löschen Ihrer Amazon Connect Connect-Instance](#) im Amazon Connect Connect-Administratorhandbuch.
- Um Amazon Quick zu deaktivieren, müssen Sie sich von Amazon Quick abmelden. Weitere Informationen finden Sie unter [Schließen Ihres Amazon Quick Kontos](#) in der Amazon-Kurzanleitung.

 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.

Sichern Sie Ihr Simple AD AD-Verzeichnis

In diesem Abschnitt werden Überlegungen zur Sicherung Ihrer Simple AD AD-Umgebung beschrieben.

Themen

- [So setzen Sie ein Simple AD krbtgt-Kontopasswort zurück](#)

So setzen Sie ein Simple AD krbtgt-Kontopasswort zurück

Das krbtgt-Konto spielt bei den Kerberos-Ticketbörsen eine wichtige Rolle. Das krbtgt-Konto ist ein spezielles Konto, das für die Verschlüsselung von Kerberos-Tickets (TGT) verwendet wird. Es spielt eine entscheidende Rolle für die Sicherheit des Kerberos-Authentifizierungsprotokolls. In Samba AD wird krbtgt als (deaktiviertes) Benutzerkonto dargestellt. Das Passwort für dieses Konto wird bei der Bereitstellung der Domain zufällig generiert. Der Zugriff auf dieses Geheimnis kann dazu führen, dass die gesamte Domäne nicht nachweisbar ist, da neue Kerberos-Tickets ohne Prüfung gedruckt werden können. [Weitere Informationen finden Sie in der Samba-Dokumentation.](#)

Es wird empfohlen, dieses Passwort regelmäßig alle 90 Tage zu ändern. Sie können das Passwort für das krbtgt-Konto von einer Amazon EC2 Windows EC2-Instance zurücksetzen, die mit Ihrem Simple AD verbunden ist.

Note

AWS Simple AD wird von Samba-AD unterstützt. Samba-AD speichert keinen N-1-Hash für das krbtgt-Konto. Wenn das Passwort für das krbtgt-Konto zurückgesetzt wird, muss der Kerberos-Client daher bei seiner nächsten Service Ticket (ST) -Anfrage ein neues Ticket Granting Ticket (TGT) aushandeln. Um mögliche Serviceunterbrechungen zu

minimieren, sollten Sie das Zurücksetzen des Kennworts für das krbtgt-Konto außerhalb der Geschäftszeiten planen. Dieser Ansatz minimiert die Auswirkungen auf den laufenden Betrieb und gewährleistet eine reibungslose Kontinuität der Authentifizierung.

Die folgenden Verfahren zeigen, wie Sie das Passwort für das krbtgt-Konto von einer Amazon EC2 Windows EC2-Instance aus zurücksetzen können.

Voraussetzungen

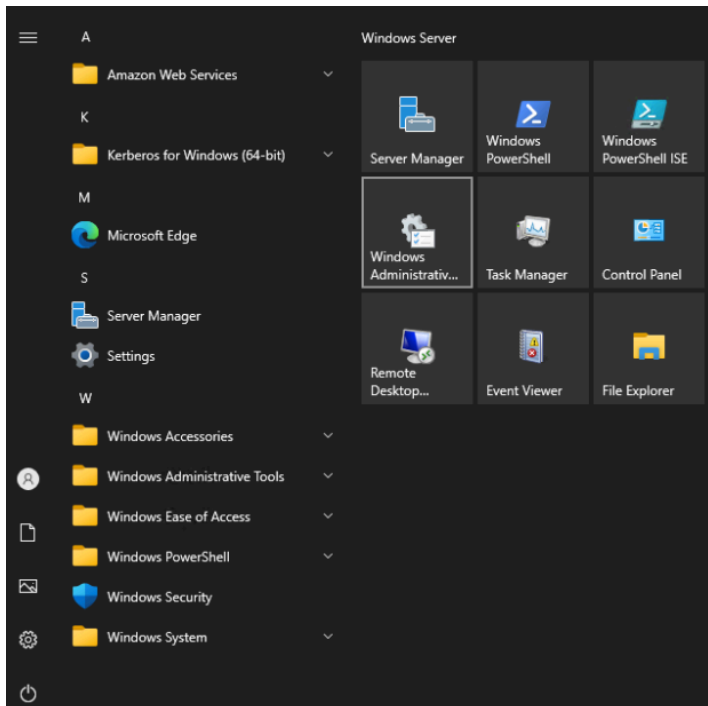
- Bevor Sie mit diesem Verfahren beginnen können, gehen Sie wie folgt vor:
 - Sie haben eine EC2-Instance mit Ihrem Simple AD AD-Verzeichnis domänenverknüpft.
 - Weitere Informationen zum Verbinden einer Windows EC2-Instance mit einem Simple AD finden Sie unter [the section called “Einer Windows-Instance beitreten”](#).
 - Sie haben die Administratoranmeldedaten für das Simple AD AD-Verzeichnis. Für dieses Verfahren melden Sie sich als Simple AD AD-Verzeichnisadministrator an.

Note

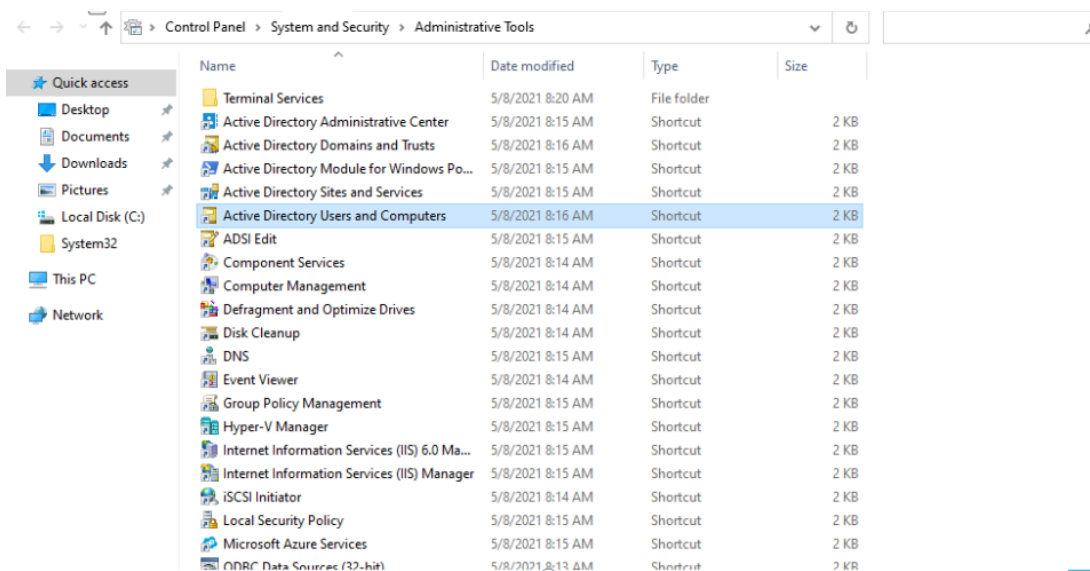
Einige, AWS-Services wie Amazon WorkDocs und Amazon WorkSpaces, erstellen in Ihrem Namen eine Simple AD.

Setzen Sie das Simple AD krbtgt-Kontopasswort zurück

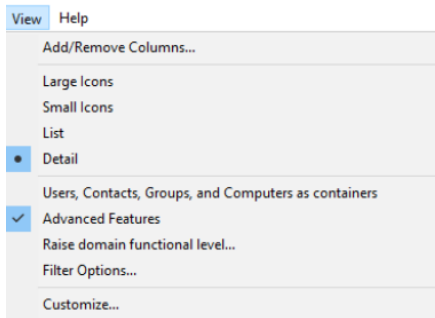
1. Öffnen Sie die Amazon-EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie in der Amazon EC2 EC2-Konsole Instances und dann die Windows Server-Instance aus. Wählen Sie dann Verbinden aus.
3. Wählen Sie auf der Seite Mit Instance verbinden die Option RDP-Client aus.
4. Kopieren Sie im Windows-Sicherheitsdialogfeld Ihre lokalen Administratoranmeldedaten für den Windows Servercomputer, 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 würden [the section called “Erstellen Sie Ihr Simple AD”](#).
5. Nachdem Sie sich am Windows Servercomputer angemeldet haben, öffnen Sie im Startmenü die Option WindowsVerwaltung, indem Sie den Ordner WindowsVerwaltungstools auswählen.



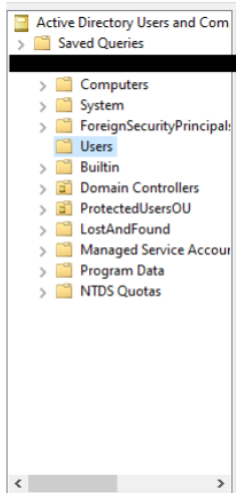
6. Öffnen Sie im Dashboard mit den Windows Verwaltungstools die Option Active Directory-Benutzer und -Computer, indem Sie Active Directory-Benutzer und -Computer auswählen.



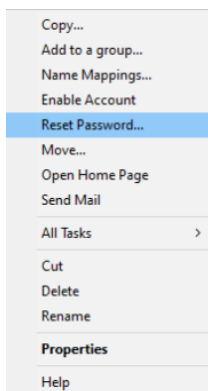
7. Wählen Sie im Fenster „Active Directory-Benutzer und -Computer“ die Option „Ansicht“ und dann „Erweiterte Funktionen aktivieren“ aus.



8. Wählen Sie im Fenster „Active Directory-Benutzer und -Computer“ im linken Bereich die Option Benutzer aus.



9. Suchen Sie den Benutzer mit dem Namen krbtgt, klicken Sie mit der rechten Maustaste darauf und wählen Sie Passwort zurücksetzen.



10. Geben Sie im neuen Fenster das neue Passwort ein, geben Sie es erneut ein und wählen Sie dann OK, um das Passwort für das krbtgt-Konto zurückzusetzen.

Reset Password ? X

New password:

Confirm password:

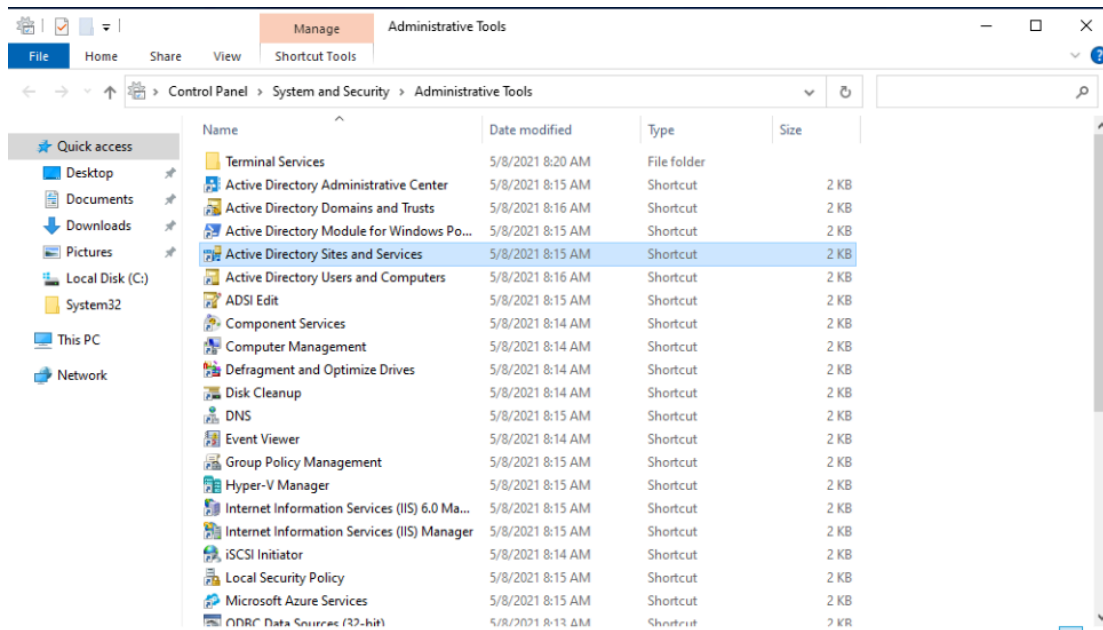
☐ User must change password at next logon
The user must logoff and then logon again for the change to take effect.

Account Lockout Status on this Domain Controller: Unlocked

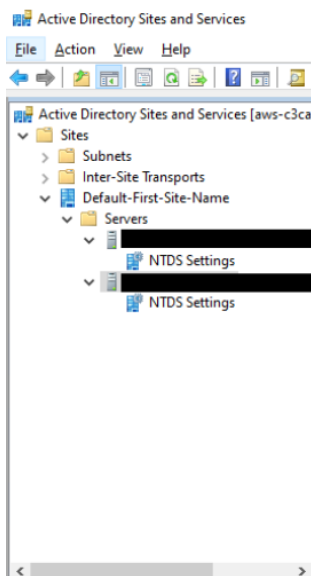
☐ Unlock the user's account

OK Cancel

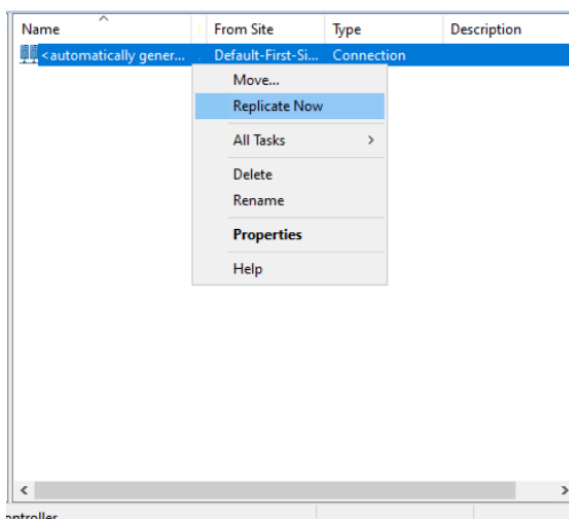
11. Wählen Sie im Dashboard „Windows Verwaltungstools“ die Option Active Directory-Standorte und -Dienste aus.



12. Erweitern Sie im Fenster Active Directory-Standorte und -Dienste die Optionen Site, Default-First-Site-Name und Server.



13. Klicken Sie im Fenster NTDS-Einstellungen mit der rechten Maustaste auf den Server und wählen Sie Jetzt replizieren aus.



14. Wiederholen Sie die Schritte 13 bis 14 für Ihre anderen Server.

Ihr Simple-AD-Verzeichnis überwachen

Sie können das Beste aus Ihrem Simple AD herausholen, indem Sie mehr über die verschiedenen Simple AD-Status und deren Bedeutung für Ihr Simple AD erfahren. Sie können auch AWS Dienste wie Amazon Simple Notification Service verwenden, um Ihr Simple AD zu überwachen. Amazon Simple Notification Service kann Ihnen Benachrichtigungen über den Status Ihres Simple AD AD-Verzeichnisses senden.

Aufgaben zur Überwachung Ihres Simple AD

- [Den Status Ihres Simple AD AD-Verzeichnisses verstehen](#)
- [Aktivieren von Statusbenachrichtigungen für Simple AD AD-Verzeichnisse mit Amazon Simple Notification Service](#)

Den Status Ihres Simple AD AD-Verzeichnisses verstehen

Im Folgenden sind die verschiedenen Zustandsangaben für ein Verzeichnis aufgeführt.

Aktiv

Das Verzeichnis funktioniert normal. 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. Ihr Verzeichnis kann einen beeinträchtigten Status haben, wenn Sie die unter beschriebenen Einstellungen ändern [Simple-AD-Voraussetzungen](#). Weitere Informationen finden Sie unter [Problembehandlung bei AWS verwaltetem Microsoft AD](#), [Fehlerbehebung in AD Connector](#), [Beheben von Fehlern in Simple AD](#). AWS Behebt bei normalen Wartungsproblemen diese Probleme 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 [Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots](#).

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 [Problembehandlung bei Simple AD AD-Verzeichnisstatusmeldungen](#).

Aktivieren von Statusbenachrichtigungen für Simple AD AD-Verzeichnisse mit Amazon Simple Notification Service

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 ein Amazon SNS SNS-Thema Directory Service als Herausgeber hinzufügen. Wenn 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?](#).

So aktivieren Sie SNS Messaging für Ihr Verzeichnis

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die [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, für die nur die [DirectoryServiceFullAccess](#)-verwaltete Richtlinie gilt, muss Ihr Themename mit „DirectoryMonitoring“ beginnen. Wenn Sie Ihren Themennamen anpassen möchten, benötigen Sie zusätzliche Berechtigungen für SNS.

8. Wählen Sie Erstellen aus.

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-Managementkonsole .Directory Service](#)
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 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 Directory Service, bevor Sie ein Thema löschen, von dem Nachrichten empfangen werden.

Zugriff auf AWS Anwendungen und Dienste von Ihrem Simple AD

Sie können Ihren Simple AD AD-Benutzern Zugriff auf AWS Anwendungen und Dienste gewähren. Einige dieser AWS Anwendungen und Dienste umfassen:

- Amazon WorkDocs
- AWS-Managementkonsole
- Amazon WorkSpaces

Sie können Access URLs und Single Sign-On auch mit Ihrem Simple AD verwenden.

Themen

- [Richtlinie zur Anwendungskompatibilität für Simple AD](#)
- [Zugriff auf AWS Anwendungen und Dienste für Ihr Simple AD ermöglichen](#)
- [Aktivieren des Zugriffs auf die AWS-Managementkonsole mit Simple AD AD-Anmeldeinformationen](#)

- [Zugriffs-URL für Simple AD erstellen](#)
- [Aktivieren des einmaligen Anmeldens](#)

Richtlinie zur Anwendungskompatibilität für Simple AD

Simple AD ist eine Samba-Implementierung, die viele der grundlegenden Features von Active Directory bereitstellt. 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 Simple AD durchführen. Obwohl AWS wir mit Kunden zusammenarbeiten, um mögliche Probleme bei der Anwendungsinstallation zu lösen, können wir nicht garantieren, dass eine Anwendung mit Simple AD kompatibel ist oder weiterhin sein wird.

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 Gründung 2010
 - SharePoint 2010 Unternehmen
 - SharePoint 2013 Unternehmen

Kunden können sich dafür entscheiden, den AWS Directory Service für Microsoft Active Directory ([AWS Verwaltetes Microsoft AD](#)) zu verwenden, um ein höheres Maß an Kompatibilität auf der Grundlage von Active Directory zu erzielen.

Zugriff auf AWS Anwendungen und Dienste für Ihr Simple AD ermöglichen

Benutzer können Simple AD autorisieren, AWS Anwendungen und Diensten wie Amazon WorkSpaces Zugriff auf Ihr Active Directory zu gewähren. Die folgenden AWS Anwendungen und Dienste können aktiviert oder deaktiviert werden, damit sie mit Simple AD funktionieren.

AWS Anwendung/Dienst	Weitere Informationen ...
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 direkt von Simple AD, AWS Managed Microsoft AD oder AD Connector aus erstellen WorkSpaces. Starten Sie einfach Advanced Setup bei der Erstellung Ihres Workspace. Weitere Informationen finden Sie im Amazon WorkSpaces Administration Guide.
AWS-Managementkonsole	Weitere Informationen finden Sie unter AWS-Managementkonsole Zugriff mit AWS verwalteten Microsoft 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. Gehen Sie wie folgt vor, um die oben beschriebenen Links zu AWS Anwendungen und Diensten in der 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 Directory Service. [Autorisierung für AWS Anwendungen und Dienste, die Directory Service](#)

Aktivieren des Zugriffs auf die AWS-Managementkonsole mit Simple AD AD-Anmeldeinformationen

Directory Service ermöglicht es Ihnen, Mitgliedern Ihres Verzeichnisses Zugriff auf die zu gewähren AWS-Managementkonsole. Standardmäßig haben Ihre Verzeichnismitglieder keinen Zugriff auf AWS Ressourcen. Sie weisen Ihren Verzeichnismitgliedern IAM-Rollen zu, um ihnen Zugriff auf die verschiedenen AWS Dienste und Ressourcen zu gewähren. 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 [AWS Verwaltete Microsoft AD-Verzeichnisinformationen anzeigen](#). Weitere Informationen zum Erstellen einer Zugriffs-URL finden Sie unter [Zugriffs-URL für AWS Managed Microsoft AD erstellen](#).

Weitere Informationen zum Erstellen von IAM-Rollen und zum Zuweisen dieser Rollen zu den Mitgliedern Ihres Verzeichnisses finden Sie unter [Benutzern und Gruppen von AWS verwaltetem Microsoft AD Zugriff auf AWS Ressourcen mit IAM-Rollen gewähren](#).

Themen

- [Zugriff aktivieren AWS-Managementkonsole](#)
- [Zugriff wird deaktiviert AWS-Managementkonsole](#)
- [Länge der Anmeldesitzung festlegen](#)

Verwandter Blogartikel zum Thema AWS Sicherheit

- [So greifen Sie AWS-Managementkonsole mithilfe von AWS verwaltetem Microsoft AD und Ihren lokalen Anmeldeinformationen auf](#)

Verwandter Artikel AWS re:Post

- [Wie kann ich lokalen Active Directory-Benutzern Zugriff auf die gewähren? AWS-Managementkonsole](#)

Zugriff aktivieren AWS-Managementkonsole

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-Managementkonsole die Option Aktivieren aus. Der Konsolenzugriff ist jetzt für Ihr Verzeichnis aktiviert.

Important

Bevor sich Benutzer mit Ihrer Zugriffs-URL an der Konsole anmelden können, müssen Sie Ihre Benutzer zunächst der IAM-Rolle hinzufügen. Weitere Informationen zum Zuweisen von Benutzern zu IAM-Rollen finden Sie unter [Zuweisen von Benutzern oder Gruppen zu einer vorhandenen IAM-Rolle](#). Nachdem die IAM-Rollen zugewiesen wurden, können die entsprechenden Benutzer über die Zugriffs-URL auf die Konsole zugreifen. Wenn Ihre Verzeichniszugriffs-URL beispielsweise example-corp.awsapps.com lautet, lautet die URL für den Zugriff auf die Konsole. `https://example-corp.awsapps.com/console/`

Zugriff wird deaktiviert AWS-Managementkonsole

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-Managementkonsole 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.

Länge 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 Weiter aus.
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.

Zugriffs-URL für Simple AD erstellen

Eine Zugriffs-URL wird mit AWS Anwendungen und Diensten wie Amazon verwendet WorkDocs, um zu einer Anmeldeseite zu gelangen, 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

Sobald Sie eine Anwendungszugriffs-URL für dieses Verzeichnis erstellt haben, 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` angezeigt.

Aktivieren des einmaligen Anmeldens

AWS Directory Service bietet die Möglichkeit, Ihren Benutzern den Zugriff 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 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 zu aktivieren oder zu deaktivieren mit 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 zu aktivieren. WorkDocs

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 [Zugriffs-URL für AWS Managed Microsoft AD erstellen](#).

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 zu einem späteren Zeitpunkt 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 zugelassenen 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](#)
- [Manuelles Update für Single Sign-On in OS X](#)
- [Gruppenrichtlinieneinstellungen für Single Sign-On](#)

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 [AuthServerAllowlist](#) Richtlinie 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 [AuthServerAllowlist](#)Richtlinie 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 *<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-Baumstruktur zu 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-Baumstruktur zu 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>) zur Liste der zugelassenen 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](https://support.mozilla.org/en-US/questions/939037).

Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem Simple AD zu verbinden

Sie können eine Amazon EC2 EC2-Instance nahtlos mit Ihrer Active Directory-Domain verbinden, wenn die Instance gestartet wird. Weitere Informationen finden Sie unter [Hinzufügen einer Amazon EC2 Windows-Instance zu Ihrem AWS verwalteten Microsoft AD Active Directory](#). [Mit Automation können Sie auch direkt von der Directory Service Konsole aus eine EC2-Instance starten und sie einer Active Directory-Domain hinzufügen](#). [AWS Systems Manager](#)

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

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

- [Hinzufügen einer Amazon EC2 EC2-Windows-Instance zu Ihrem Simple AD Active Directory](#)
- [Fügen Sie Ihrem Simple AD Active Directory eine Amazon EC2 Linux-Instance hinzu](#)
- [Delegieren von Verzeichnisbeitrittsberechtigungen für Simple AD](#)
- [Einen DHCP-Optionssatz für Simple AD erstellen](#)

Hinzufügen einer Amazon EC2 EC2-Windows-Instance zu Ihrem Simple AD Active Directory

Sie können eine Amazon EC2 Windows EC2-Instance starten und mit einem Simple AD verbinden. Alternativ können Sie eine bestehende Windows EC2-Instance manuell mit einem Simple AD verbinden

Seamlessly join an EC2 Windows

Für einen nahtlosen Domänenbeitritt zu einer EC2-Instance müssen Sie die folgenden Schritte ausführen:

Voraussetzungen

- Über eine Simple AD verfügen Weitere Informationen finden Sie unter [Erstellen Sie Ihr Simple AD](#).
- Sie benötigen die folgenden IAM-Berechtigungen, um einer Windows EC2-Instance problemlos beitreten zu können:
 - IAM-Instanzprofil mit den folgenden IAM-Berechtigungen:
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - Die Benutzerdomäne, die EC2 nahtlos mit Simple AD verbindet, benötigt die folgenden IAM-Berechtigungen:
 - Directory Service Berechtigungen:
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Amazon VPC-Berechtigungen:
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"

- "ec2:DescribeNetworkInterfaces"
- "ec2:CreateNetworkInterface"
- "ec2:AttachNetworkInterface"
- EC2-Berechtigungen:
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
- AWS Systems Manager Berechtigungen:
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Wenn Ihr Simple AD erstellt wird, wird eine Sicherheitsgruppe mit Regeln für eingehenden und ausgehenden Datenverkehr erstellt. Weitere Informationen zu diesen Regeln und Ports finden Sie unter [Was wird mit Ihrem Simple AD erstellt](#). Für einen nahtlosen Domänenbeitritt zu einer Windows EC2-Instance sollte Ihre VPC, in der Sie Ihre Instance starten, dieselben Ports zulassen, die in den eingehenden und ausgehenden Regeln Ihrer Simple AD-Sicherheitsgruppe zulässig sind.

- Abhängig von Ihren Netzwerksicherheits- und Firewall-Einstellungen müssen Sie möglicherweise zusätzlichen ausgehenden Datenverkehr zulassen. Dieser Datenverkehr würde über HTTPS (Port 443) zu den folgenden Endpunkten erfolgen:

Endpoint	Rolle
ec2messages. <i>region</i> .amazonaws.com	Erstellt und löscht Sitzungskanäle mit dem Session Manager-Dienst. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .

Endpoint	Rolle
ssm. <i>region</i> .amazonaws.com	Endpoint für AWS Systems Manager Session Manager. Weitere Informationen finden Sie unter AWS Systems Manager - Endpunkte und -Kontingente .
ssmmessages. <i>region</i> .amazonaws.com	Erstellt und löscht Sitzungskanäle mit dem Session Manager-Dienst. Weitere Informationen finden Sie unter AWS Systems Manager -Endpunkte und -Kontingente .
ds. <i>region</i> .amazonaws.com	Endpoint für Directory Service. Weitere Informationen finden Sie unter Verfügbarkeit in der Region für Directory Service .

- Wir empfehlen, einen DNS-Server zu verwenden, der Ihren Simple AD AD-Domainnamen auflöst. Zu diesem Zweck können Sie einen DHCP-Optionssatz erstellen. Weitere Informationen finden Sie unter [Einen DHCP-Optionssatz für Simple AD erstellen](#).
 - Wenn Sie sich dafür entscheiden, keinen DHCP-Optionssatz zu erstellen, sind Ihre DNS-Server statisch und werden von Ihrem Simple AD entsprechend konfiguriert.
1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole 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 heruntergeladen. 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:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

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-Instance-Profil ein IAM-Instance-Profil aus, dem die AWS verwalteten Richtlinien Amazon SSMManged InstanceCore und Amazon SSMDirectory ServiceAccess zugeordnet 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 unter Berechtigungen hinzufügen in der Liste der Richtlinien die Amazon SSMManged InstanceCore - und SSMDirectoryServiceAccessAmazon-Richtlinien aus. Geben Sie im Suchfeld **SSM** ein, um die Liste zu filtern. Wählen Sie Weiter aus.

 Note

Amazon SSMDirectory ServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einem Active Directory, das von verwaltet wird Directory Service. Amazon SSMManged InstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des AWS Systems Manager Dienstes erforderlich sind. 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.

Manually join an EC2 Windows

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. [Hinzufügen einer Amazon EC2 EC2-Windows-Instance zu Ihrem Simple AD Active Directory](#)

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.

The screenshot shows the AWS Directory Service console. On the left, the 'Directory Service' sidebar is visible with 'Directories' highlighted. The main content area shows the details for directory 'd-1234567890'. The 'Directory details' section includes:

Property	Value
Directory type	Microsoft AD
Edition	Standard
Operating system version	Windows Server 2019
Directory DNS name	corp.example.com
Directory NetBIOS name	corp
Directory administration EC2 instance(s)	-

Below this, the 'Networking details' section is shown, which includes a VPC and its subnets. The 'DNS address' for the subnets is listed as 192.0.2.1 and 198.51.100.1.

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 das IPv4 TCP/-Eigenschaftendialogfeld auf der Instanz.
 - 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, 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.

Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

Advanced...

OK Cancel

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

i 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 [Delegieren von Verzeichnisbeitrittsberechtigungen für Simple 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 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 der Active-Directory-Verwaltungstools für Simple AD](#).

Fügen Sie Ihrem Simple AD Active Directory eine Amazon EC2 Linux-Instance hinzu

Sie können eine Amazon EC2 EC2-Linux-Instance starten und Ihrem Simple AD hinzufügen in. AWS-Managementkonsole Sie können die EC2-Linux-Instance auch manuell mit Ihrem Simple AD verbinden.

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

Distributionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 und 8 unterstützen die Funktion zum nahtlosen Domänenbeitritt nicht.

Möglichkeiten zum Domänenbeitritt zu einer EC2-Linux-Instance:

- [Fügen Sie eine Amazon EC2 EC2-Linux-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu](#)
- [Manuelles Hinzufügen einer Amazon EC2 EC2-Linux-Instance zu Ihrem Simple AD Active Directory](#)

Fügen Sie eine Amazon EC2 EC2-Linux-Instance nahtlos zu Ihrem Simple AD Active Directory hinzu

Durch dieses Verfahren wird eine Amazon EC2 EC2-Linux-Instance nahtlos mit Ihrem Simple AD Active Directory 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

Distributionen vor Ubuntu 14 und Red Hat Enterprise Linux 7 und 8 unterstützen die Funktion zum nahtlosen Domänenbeitritt 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. Weitere Informationen finden Sie unter [Create an AWS Secrets Manager Secret](#).

Note

Für Secrets Manager fallen Gebühren an. Weitere Informationen finden Sie unter [Preise](#) im AWS Secrets Manager Benutzerhandbuch.

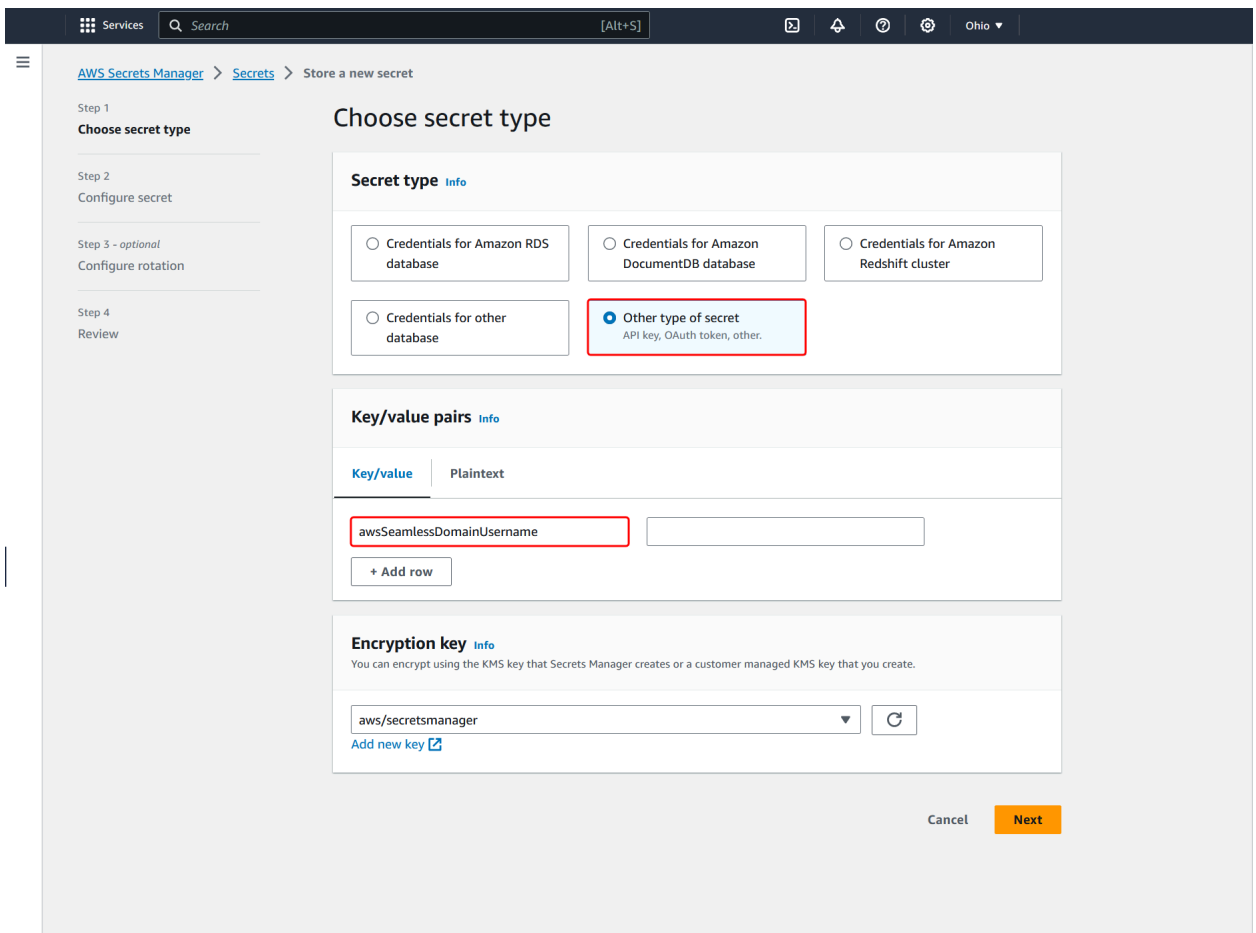
So erstellen Sie Secrets und speichern die Kontoinformationen des Domainservices

1. Melden Sie sich bei der an AWS-Managementkonsole 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.



The screenshot shows the AWS Secrets Manager console with the 'Store a new secret' wizard. The 'Choose secret type' step is active. The 'Secret type' section has four options: 'Credentials for Amazon RDS database', 'Credentials for Amazon DocumentDB database', 'Credentials for Amazon Redshift cluster', and 'Other type of secret' (selected). The 'Key/value pairs' section has a table with one row: 'awsSeamlessDomainUsername' in the 'Key/value' column and an empty 'Plaintext' column. The 'Encryption key' section shows 'aws/secretsmanager' selected. The 'Next' button is highlighted in orange.

- 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.
 - 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 **d-xxxxxxxx** ersetzen Sie ihn durch Ihre Verzeichnis-ID:

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

Dies wird verwendet, um Secrets in der Anwendung abzurufen.

 Note

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

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

Secret name must contain only alphanumeric characters and the characters /_+:@-

Description - optional

Maximum 250 characters.

Tags - optional
No tags associated with the secret.

Resource permissions - optional [Info](#)
Add or edit a resource policy to access secrets across AWS accounts.

Replicate secret - optional
Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

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.

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 EC2 DomainJoin Linux-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-Managementkonsole als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Öffnen Sie dann die IAM-Konsole unter <https://console.aws.amazon.com/iam/>
2. Wählen Sie im Navigationsbereich Access Management die Option Policies 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:xxxxxxxx:secret:aws/directory-
services/d-xxxxxxxx/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-xxxxxxxx-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 EC2 DomainJoin Linux-Rolle

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

Um die EC2 DomainJoin Linux-Rolle zu erstellen

1. Melden Sie sich AWS-Managementkonsole als Benutzer an, der berechtigt ist, IAM-Richtlinien zu erstellen. Öffnen Sie dann 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.

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected. The 'Service or use case' dropdown is set to 'EC2'. The 'Choose a use case for the specified service' section shows 'EC2' as the selected use case, with a description: 'Allows EC2 instances to call AWS services on your behalf.'

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

Amazon SSMDirectory ServiceAccess bietet die Berechtigungen zum Hinzufügen von Instances zu einem Active Directory, das von verwaltet wird Directory Service. Amazon SSMManged InstanceCore stellt die Mindestberechtigungen bereit, die für die Nutzung des AWS Systems Manager Dienstes erforderlich sind. 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

Um Ihrer Linux-Instance nahtlos beizutreten

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die Amazon EC2 EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Wählen Sie aus der Regionsauswahl 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 Linux EC2-Instance verwenden möchten.

5. (Optional) Wählen Sie Zusätzliche Tags hinzufügen, um ein oder mehrere Tag-Schlüssel-Wert-Paare hinzuzufügen, um den Zugriff für diese EC2-Instance zu organisieren, zu verfolgen oder zu kontrollieren.
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 einer Active Directory-Domäne hinzugefügt wird. Das Plugin ändert den Hostnamen für die Linux-Instanzen in das Format EC2 AMAZ-**XXXXXXX**. Weitere Informationen `aws:domainJoin` dazu finden Sie in der [Plugin-Referenz zum AWS Systems Manager Befehlsdokument](#) im AWS Systems Manager Benutzerhandbuch.

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 heruntergeladen. 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:

 An error was detected in your existing SSM document. You can [delete the existing SSM document here](#) and we'll create a new one with correct properties on instance launch. 

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: Linux-Rolle erstellen. EC2 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-Instanz so, dass sie die DNS-Server-IP-Adressen der 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* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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 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.

- Überprüfen Sie, ob Ihre CentOS 7-Instance auf dem aktuellen Stand ist.

```
sudo yum -y update
```

- 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
```

- 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* Domäne, 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 Verzeichnisbeitrittsberechtigungen für AWS Managed Microsoft AD](#).

example.com

Der vollständig berechtigte DNS-Name Ihres Verzeichnisses.

```
...  
* Successfully enrolled machine in realm
```

- 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 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
```

Der AMAccounts-Name für ein Konto in der *example.com* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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 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

Der AMAccounts-Name für ein Konto in der *example.com* Domäne, 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 Verzeichnisbeitrittsberechtigungen 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/krb5.conf` auf `False`. `etc/krb5.conf` Beispiel:

```
[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. Beispiel:

```
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 lautet der Gruppenname. *admins*

ou

Dies ist die Organisationseinheit, in der sich die oben genannte Gruppe befindet. In diesem Beispiel ist die Organisationseinheit *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/sss/sss.conf` hinzufügen.

Öffnen Sie die Datei `/etc/sss/sss.conf` in einem Text-Editor.

```
sudo vi /etc/sss/sss.conf
```

Danach sieht `sss.conf` wie folgt aus:

```
[sss]
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. Diese Methoden sind:

1. Zentralisiert
2. Verteilt

Note

Für die zentrale Zuordnung von Benutzeridentitäten in Active Directory ist ein Portable Operating System Interface oder POSIX erforderlich.

Zentralisierte Zuordnung von Benutzeridentitäten

Active Directory oder ein anderer LDAP-Dienst (Lightweight Directory Access Protocol) stellt den Linux-Benutzern UID und GID zur Verfügung. In Active Directory werden diese Bezeichner in den Benutzerattributen gespeichert, wenn die POSIX-Erweiterung konfiguriert ist:

- 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 aus Active Directory zu konfigurieren, 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 Active Directory eine UID, UID-Nummer und GID-Nummer hinzugefügt haben.

Zuordnung verteilter Benutzeridentitäten

Wenn Active Directory nicht über die POSIX-Erweiterung verfügt 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.

Häufige Probleme

Wenn Sie dies festlegen `ldap_id_mapping = False`, schlägt das Starten des SSSD-Dienstes manchmal fehl. Der Grund für diesen Fehler liegt darin, dass Änderungen UIDs nicht unterstützt werden. Wir empfehlen Ihnen, den SSSD-Cache zu löschen, wenn Sie von ID-Zuordnung zu POSIX-Attributen oder von POSIX-Attributen zu ID-Zuordnung wechseln. Weitere Informationen zur ID-Zuordnung und den `ldap_id_mapping`-Parametern finden Sie in der Manpage `sssd-ldap (8)` in der Linux-Befehlszeile.

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%		

Delegieren von Verzeichnisbeitrittsberechtigungen für Simple AD

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. Klicken Sie anschließend auf Weiter.

Delegation of Control Wizard ✕

Active Directory Object Type
Indicate the scope of the task you want to delegate.

Delegate control of:

☐ This folder, existing objects in this folder, and creation of new objects in this folder

☒ Only the following objects in the folder:

- ☐ Site Settings objects
- ☐ Sites Container objects
- ☐ Subnet objects
- ☐ Subnets Container objects
- ☐ Trusted Domain objects
- ☒ User objects

☒ Create selected objects in this folder

☒ Delete selected objects in this folder

< Back Next > Cancel Help

10. Wählen Sie Read und Write und dann Next.

Delegation of Control Wizard ✕

Permissions
Select the permissions you want to delegate.

Show these permissions:

☒ General

☒ Property-specific

☐ Creation/deletion of specific child objects

Permissions:

- ☐ Full Control
- ☒ Read
- ☐ Write
- ☐ Create All Child Objects
- ☐ Delete All Child Objects
- ☐ Read All Properties

< Back Next > Cancel Help

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 Directory Service Verzeichnis herzustellen.

Einen DHCP-Optionssatz für Simple AD erstellen

AWS empfiehlt, dass Sie einen DHCP-Optionssatz für Ihr 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-Namensserver

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 des neuen Satzes von DHCP-Optionen (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 Ihr aus. VPCs
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](#)

Benutzer- und Gruppenverwaltung in Simple AD

„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 Directory Service Verzeichnis zu erstellen, müssen Sie eine beliebige Instanz (entweder lokal oder EC2) verwenden, die zu Ihrem Directory Service Verzeichnis hinzugefügt wurde, und als Benutzer angemeldet sein, der über die Rechte zum Erstellen von Benutzern und Gruppen verfügt. Sie müssen außerdem die Active Directory-Tools auf Ihrer EC2 Instanz installieren, damit Sie Ihre Benutzer und Gruppen mit dem Snap-In „Active Directory-Benutzer und -Computer“ hinzufügen können. Weitere Informationen zum Einrichten einer EC2 Instanz und zur Installation der erforderlichen Tools finden Sie unter [Möglichkeiten, eine Amazon EC2 EC2-Instance mit Ihrem Simple AD zu verbinden](#).

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 der Active-Directory-Verwaltungstools für Simple AD](#)
- [Einen Simple AD AD-Benutzer erstellen](#)
- [Löschen eines Simple AD AD-Benutzers](#)
- [Ein Simple AD AD-Benutzerkennwort zurücksetzen](#)
- [Eine Simple AD AD-Gruppe erstellen](#)

- [Einen Simple AD AD-Benutzer zu einer Gruppe hinzufügen](#)

Installieren der 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](#).
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: **AmazonSSMManagedInstanceCore** und **AmazonSSMDirectoryServiceAccess**. Weitere Informationen finden Sie unter [Hinzufügen einer Amazon EC2 EC2-Windows-Instance zu Ihrem Simple AD Active Directory](#).
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 haben [Erstellen Sie Ihr Simple AD](#), enthält Ihr Administrator-Benutzername Ihren NetBIOS-Namen, **corp\administrator**.

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 würden Erstellen Sie Ihr Simple 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, sind das Active Directory-Modul für PowerShell, die AD DS-Tools und die AD LDS-Snap-Ins und Befehlszeilentools ausgewählt. Scrollen Sie nach unten und wählen Sie DNS Server Tools und dann Weiter.

Select features

DESTINATION SERVER

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select one or more features to install on the selected server.

Features

- ☐ Remote Differential Compression
- ☒ Remote Server Administration Tools
 - ☐ Feature Administration Tools
 - ☒ Role Administration Tools
 - ☒ AD DS and AD LDS Tools
 - ☒ Active Directory module for Windows PowerShell
 - ☒ AD DS Tools
 - ☒ AD LDS Snap-Ins and Command-Line Tools
 - ☐ Hyper-V Management Tools
 - ☐ Remote Desktop Services Tools
 - ☐ Windows Server Update Services Tools
 - ☐ Active Directory Certificate Services Tools
 - ☐ Active Directory Rights Management Services Tools
 - ☐ DHCP Server Tools
 - ☒ DNS Server Tools
 - ☐ Fax Server Tools
 - ☐ File Services Tools
 - ☐ Network Controller Management Tools
 - ☐ Network Policy and Access Services Tools

Description

Remote Server Administration Tools includes snap-ins and command-line tools for remotely managing roles and features.

< Previous

Next >

Install

Cancel

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.

Einen Simple AD AD-Benutzer erstellen

Gehen Sie wie folgt vor, um einen Benutzer mit einer EC2 Amazon-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.

So erstellen Sie einen Benutzer

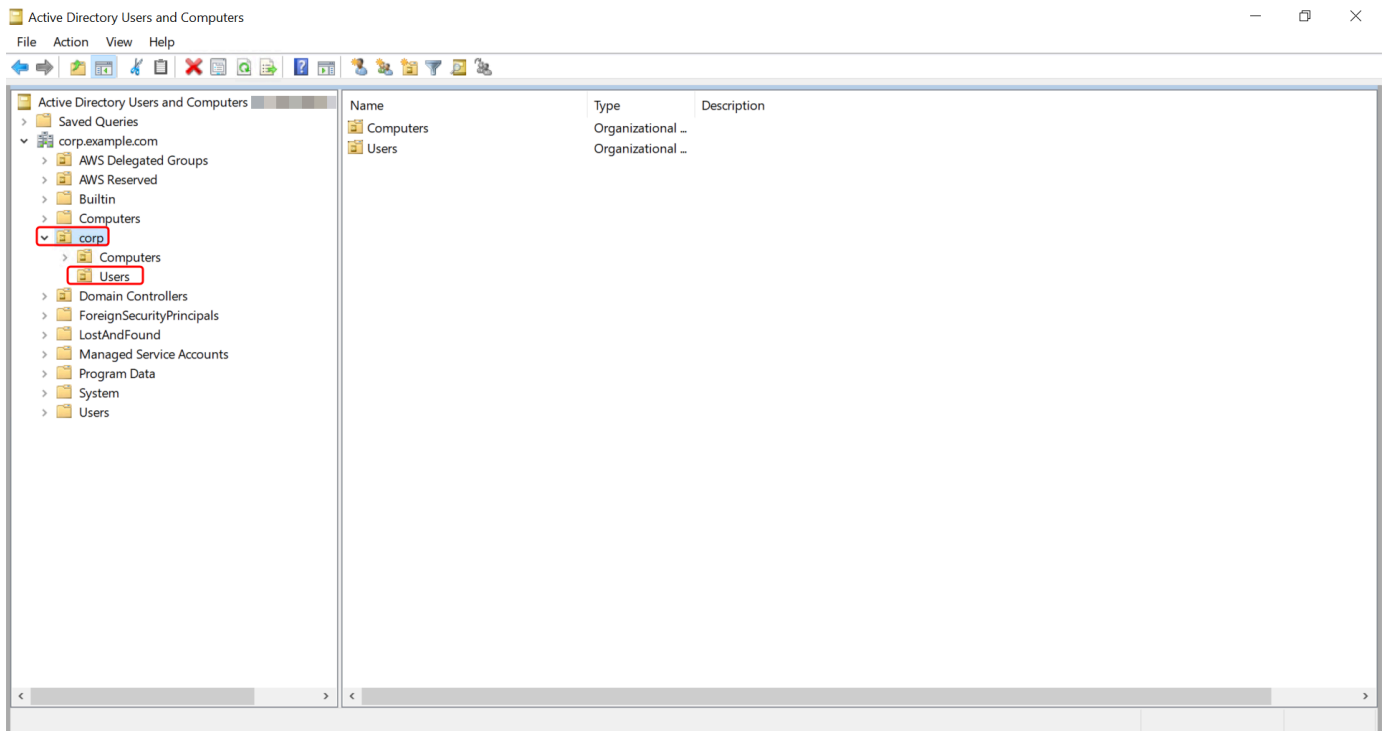
1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool „Active Directory-Benutzer und -Computer“ im Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

 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 unter [Was wird mit Ihrem AWS Managed Microsoft AD 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.

Löschen eines Simple AD AD-Benutzers

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.

So löschen Sie einen Benutzer

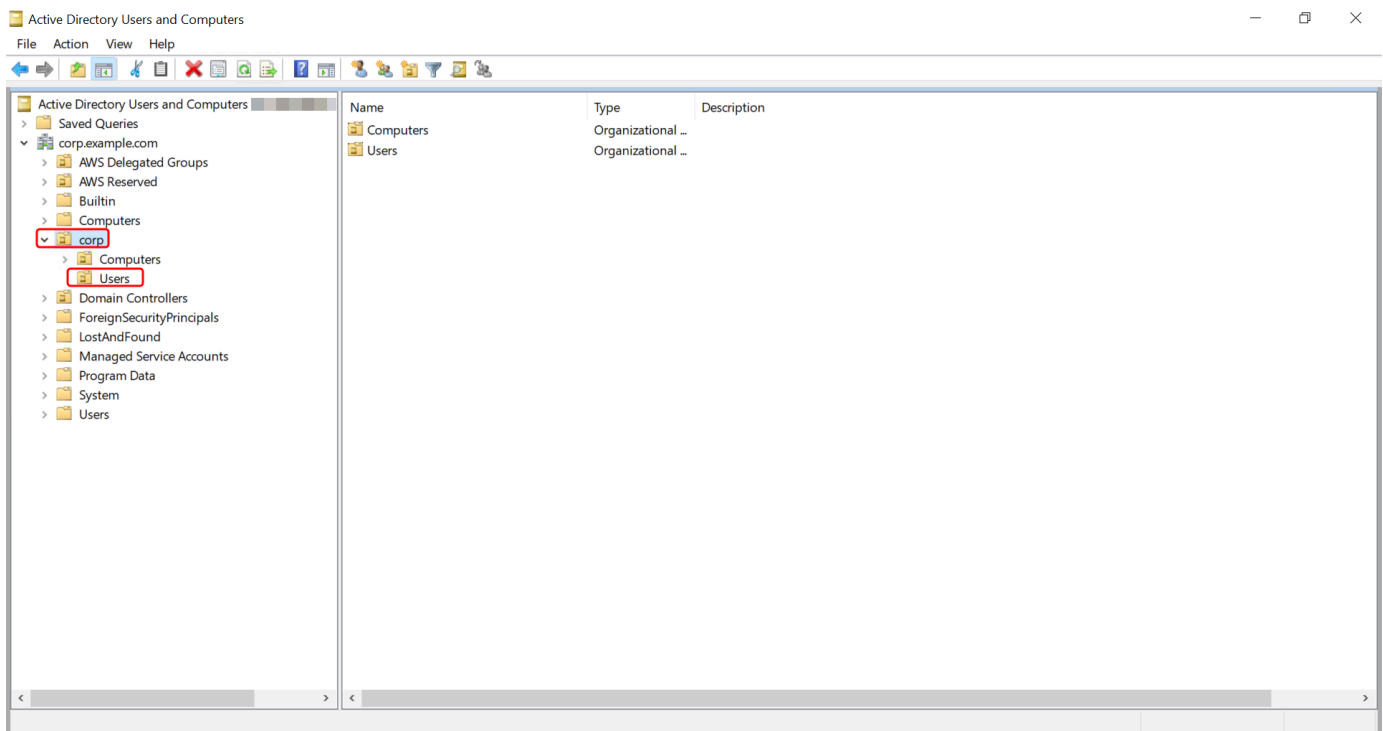
1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool „Active Directory-Benutzer und -Computer“ im Windows-Startmenü. Im Ordner Windows-Verwaltungstools befindet sich eine Verknüpfung zu diesem Tool.

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.

Ein Simple AD AD-Benutzerkennwort zurücksetzen

Benutzer müssen sich an die im Active Directory definierten Kennwortrichtlinien halten. 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, 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 Directory Service Ressourcen](#).

Sie können das Passwort für jeden Benutzer in Ihrem Active Directory zurücksetzen, 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 [Erstellen Sie Ihr Simple AD](#) befolgen würden, wäre Ihr NetBIOS-Name CORP und die Benutzerkennwörter, die Sie zurücksetzen könnten, wären Mitglieder von Corp/Users OU.
- 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 unter [Was wird mit Ihrem Simple AD erstellt](#).
- 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-Managementkonsole
- AWS CLI

AWS-Managementkonsole

1. Wählen Sie im Navigationsbereich der [Directory Service Konsole](#) unter Active Directory die Option Verzeichnisse aus, und wählen Sie dann in der Liste das Active Directory 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 Kennwort geändert werden muss.
4. Geben Sie ein Passwort unter Neues Passwort und Passwort bestätigen ein und wählen Sie dann Passwort zurücksetzen.

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 Kennwort **P@ssw0rd** durch Ihre Active Directory-Verzeichnis-ID und die gewünschten Anmeldeinformationen. Weitere Informationen finden Sie [reset-user-password](#) in der AWS CLI Befehlsreferenz.

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

Eine Simple AD AD-Gruppe erstellen

Gehen Sie wie folgt vor, um eine Sicherheitsgruppe mit einer EC2 Amazon-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.

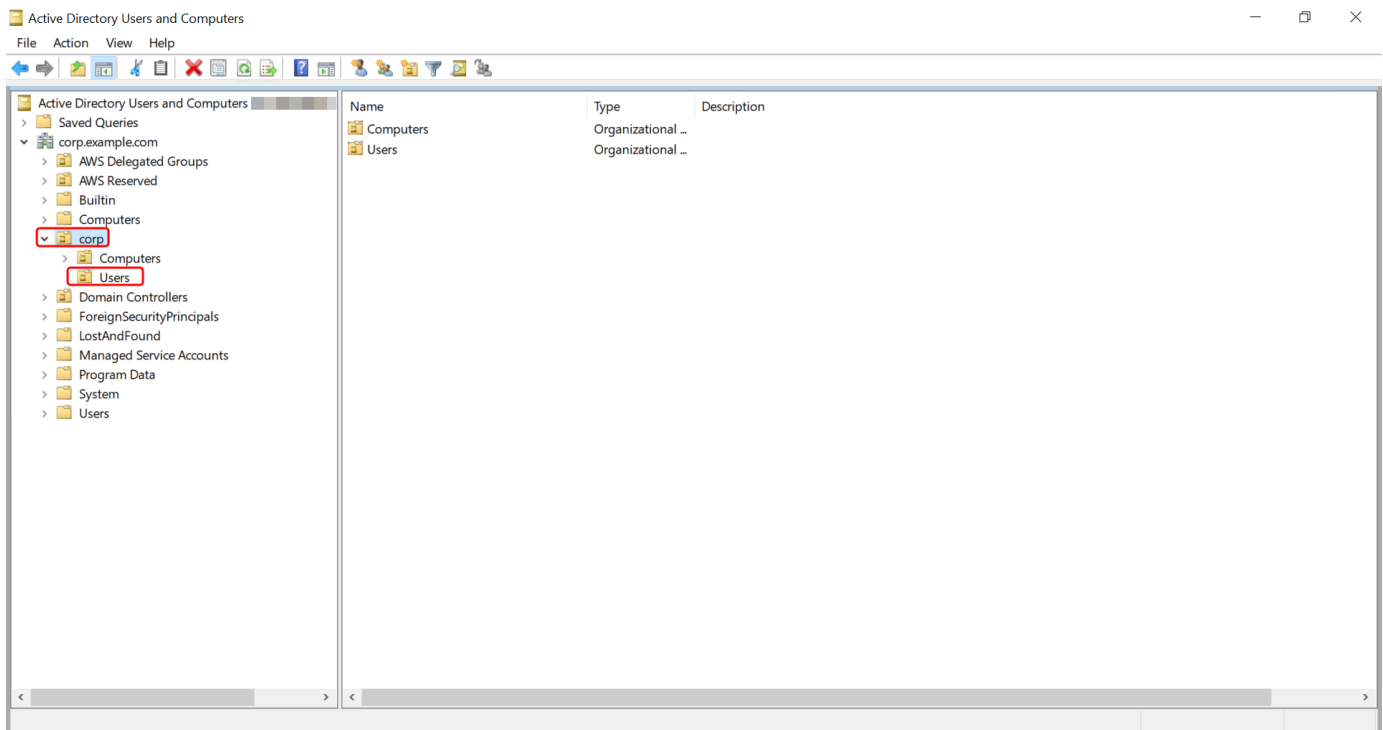
- Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

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
```

- 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 unter [Was wird mit Ihrem AWS Managed Microsoft AD erstellt](#).



- Klicken Sie im MenüAction auf New und dann auf Group, um den Assistenten für neue Gruppen aufzurufen.
- 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 Instanz hinzuzufügen, die mit Ihrem Simple AD AD-Verzeichnis verknüpft ist.

So fügen Sie einer Gruppe einen Benutzer hinzu

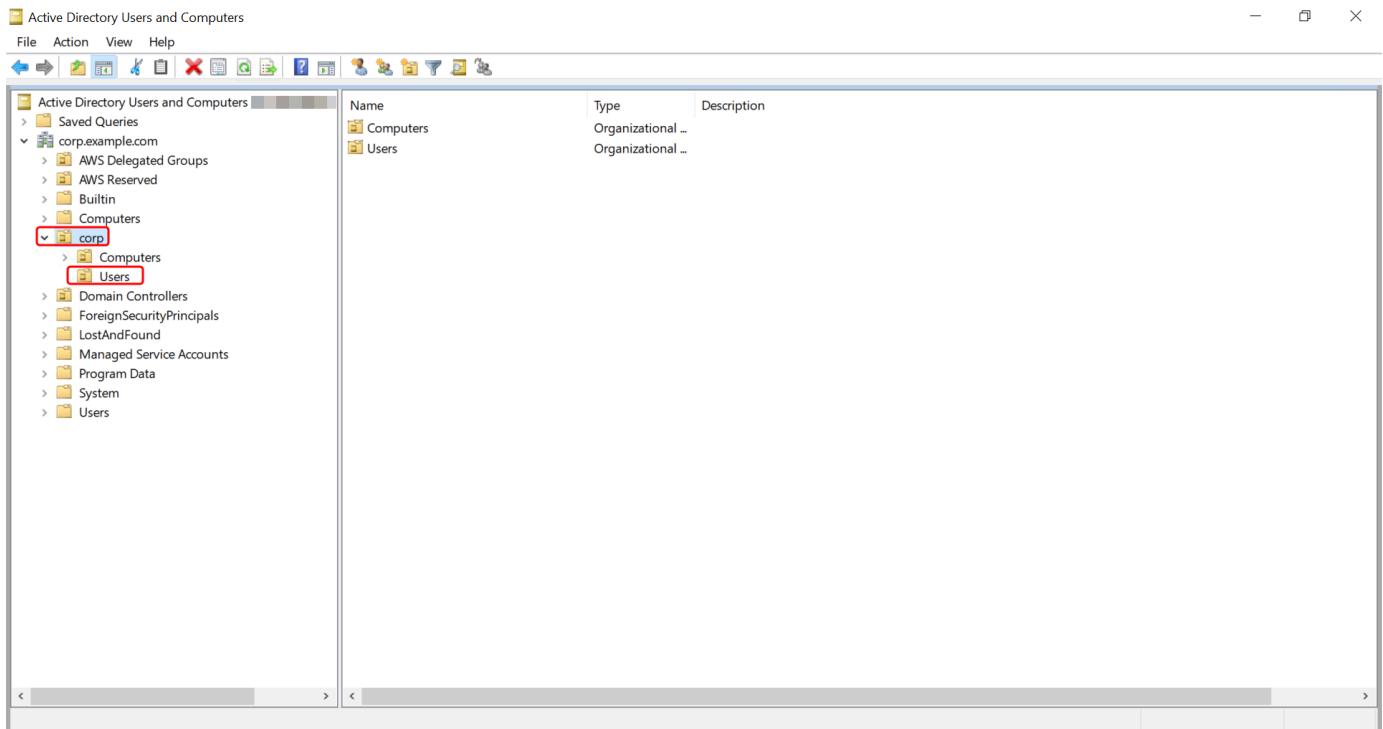
1. Verbinden Sie sich mit der Instance, auf der die Active Directory Administration Tools installiert wurden.
2. Öffnen Sie das Tool "Active Directory-Benutzer und -Computer". Im Ordner Administrative Tools befindet sich eine Verknüpfung zu diesem Tool.

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.

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-Funktionen sollten Sie stattdessen den AWS Directory Service für 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 Ihrem AWS elastic network interface (ENI) keine öffentliche IP-Adresse zuordnen.

Beheben von Fehlern in Simple AD

Im Folgenden können Sie einige häufig auftretende Probleme beheben, die bei der Erstellung oder Verwendung von Simple AD Active Directory auftreten können.

Themen

- [Wiederherstellen des Passworts](#)
- [Ich erhalte die Fehlermeldung „KDC kann die angeforderte Option nicht erfüllen“, wenn ich einen Benutzer zu Simple AD hinzufüge](#)
- [Ich kann den DNS-Namen oder die IP-Adresse einer meiner Domain zugeordneten Instance nicht aktualisieren \(dynamische DNS-Aktualisierung\).](#)
- [Ich kann mich nicht mit einem SQL Server-Konto bei SQL Server anmelden](#)
- [Mein Simple AD steckt im Status „Angefordert“ fest](#)
- [Ich erhalte die Fehlermeldung „AZ constrained“, wenn ich ein Simple AD erstelle](#)
- [Einige meiner Benutzer können sich nicht mit meinem Simple AD authentifizieren](#)
- [Weitere Ressourcen](#)
- [Problembehandlung bei Simple AD AD-Verzeichnisstatusmeldungen](#)

Wiederherstellen des Passworts

Wenn ein Benutzer ein Passwort vergisst oder Probleme hat, sich in Ihrem Simple AD AD-Verzeichnis anzumelden, können Sie sein Passwort entweder mit der AWS-Managementkonsole, PowerShell oder dem AWS CLI zurücksetzen.

Weitere Informationen finden Sie unter [Ein Simple AD AD-Benutzerkennwort zurücksetzen](#).

Ich erhalte die Fehlermeldung „KDC kann die angeforderte Option nicht erfüllen“, wenn ich einen Benutzer zu Simple AD hinzufüge

Dies kann auftreten, wenn der Samba-CLI-Client die `net` Befehle nicht korrekt an alle Domain-Controller sendet. Wenn Sie diese Fehlermeldung sehen, wenn Sie den `net ads` Befehl zum Hinzufügen eines Benutzers zu Ihrem Simple AD AD-Verzeichnis verwenden, verwenden Sie das `-S` Argument und geben Sie die IP-Adresse eines Ihrer Domänencontroller 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 der 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 nicht mit einem SQL Server-Konto bei SQL Server anmelden

Möglicherweise wird eine Fehlermeldung angezeigt, wenn Sie versuchen, SQL Server Management Studio (SSMS) mit einem SQL Server-Konto zu verwenden, um sich bei SQL Server anzumelden, der auf einer Windows 2012 R2 Amazon EC2 EC2-Instance ausgeführt wird. Das Problem tritt auf, wenn SSMS als Domänenbenutzer ausgeführt wird, und kann zu dem Fehler führen `Login failed for user`, selbst wenn gültige Anmeldeinformationen angegeben werden. Dies ist ein bekanntes Problem und wir AWS arbeiten aktiv daran, es zu lösen.

Um das Problem zu umgehen, können Sie sich bei SQL Server mit Windows Authentifizierung statt mit SQL-Authentifizierung anmelden. Oder Sie starten SSMS als lokalen anstatt als Simple AD-Domain-Benutzer.

Mein Simple AD steckt im Status „Angefordert“ fest

Wenn Sie über ein Simple AD verfügen, das sich seit mehr als fünf Minuten im Requested Status befindet, versuchen Sie, das Verzeichnis zu löschen und neu zu erstellen. Wenn dieses Problem weiterhin besteht, wenden Sie sich an das [AWS Support -Zentrum](#).

Ich erhalte die Fehlermeldung „AZ constrained“, wenn ich ein Simple AD erstelle

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 Verzeichnisse unterstützen. Directory Service 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 nicht mit meinem Simple AD 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](#) bei Simple AD TechNet.

Weitere Ressourcen

Die folgenden Ressourcen können Ihnen bei der Problembehebung bei der Arbeit mit AWS helfen.

- [AWS Knowledge Center](#) — Hier finden Sie weitere Ressourcen FAQs und Links zu diesen, 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

- [Problembehandlung bei Simple AD AD-Verzeichnisstatusmeldungen](#)

Problembehandlung bei Simple AD AD-Verzeichnisstatusmeldungen

Wenn ein Simple AD beeinträchtigt oder nicht funktionsfähig ist, enthält die Verzeichnisstatusmeldung zusätzliche Informationen. Die Statusmeldung wird in der Directory Service Konsole angezeigt oder von der API an das [DirectoryDescription.StageReason](#) Mitglied zurückgegeben. [DescribeDirectories](#) Weitere Informationen über den Verzeichnisstatus finden Sie unter [Den Status Ihres AWS verwalteten Microsoft AD-Verzeichnisses verstehen](#).

Die folgenden Meldungen sind Statusmeldungen für ein Simple-AD-Verzeichnis:

Themen

- [Die Elastic-Network-Schnittstelle des Verzeichnisdienstes ist nicht verbunden](#)
- [Probleme wurden von der Instance erkannt](#)
- [Der kritische Directory Service reservierte Benutzer fehlt im Verzeichnis](#)
- [Der kritische Directory Service reservierte Benutzer muss der Gruppe Domain-Admins angehören](#)
- [Der kritische Directory Service reservierte Benutzer ist deaktiviert](#)
- [Der Haupt-Domain-Controller hat nicht alle FSMO-Rollen](#)
- [Domain-Controller Replikationsfehler](#)

Die Elastic-Network-Schnittstelle des Verzeichnisdienstes ist nicht verbunden

Description

Das Critical elastic network interface (ENI), das in Ihrem Namen bei der Verzeichniserstellung erstellt wurde, um die Netzwerkkonnektivität mit Ihrer VPC herzustellen, ist nicht an die Directory-Instance angehängt. AWS Anwendungen, die von diesem Verzeichnis unterstützt werden, funktionieren nicht. 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 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

Description

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. Wenn das Problem weiterhin besteht, wenden Sie sich an uns, Support um weitere Unterstützung zu erhalten.

Der kritische Directory Service reservierte Benutzer fehlt im Verzeichnis

Description

Wenn ein Simple AD erstellt wird, wird im Verzeichnis ein Dienstkonto mit dem Namen Directory Service erstellt `AWSAdminD-xxxxxxxxxx`. Dieser Fehler wird empfangen, wenn dieses Service-Konto nicht gefunden wird. Ohne dieses Konto kann 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 kritische Directory Service reservierte Benutzer muss der Gruppe Domain-Admins angehören

Description

Wenn ein Simple AD erstellt wird, wird im Verzeichnis ein Dienstkonto mit dem Namen Directory Service erstellt `AWSAdminD-xxxxxxxxxx`. Dieser Fehler wird empfangen, wenn dieses Service-Konto kein Mitglied der Domain Admins-Gruppe ist. Die Mitgliedschaft in dieser Gruppe ist erforderlich, um ihr Directory Service die Rechte zu gewähren, die sie für Wartungs- und Wiederherstellungsvorgänge benötigt, z. B. die Übertragung von FSMO-Rollen, den Beitritt zu neuen Verzeichniscontrollern und die Wiederherstellung aus Snapshots.

Fehlerbehebung

Verwenden Sie das Tool Active Directory-Benutzer und -Computer, um das Service-Konto der Domain Admins-Gruppe wieder hinzuzufügen.

Der kritische Directory Service reservierte Benutzer ist deaktiviert

Description

Wenn ein Simple AD erstellt wird, wird im Verzeichnis ein Dienstkonto mit dem Namen Directory Service erstellt `AWSAdminD-xxxxxxxxxx`. Dieser Fehler wird empfangen, wenn dieses Service-Konto deaktiviert ist. Dieses Konto muss aktiviert sein, damit Wartungs- und Wiederherstellungsvorgänge im Verzeichnis ausgeführt werden Directory Service können.

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

Description

Nicht alle FSMO-Rollen sind im Besitz des Simple-AD-Verzeichnis-Controllers. 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 zum Verschieben der FSMO-Rollen finden Sie <https://docs.microsoft.com/troubleshoot/unter windows- server/identity/transfer--or-seize-fsmo-roles>. In AD Falls das Problem dadurch nicht behoben wird, wenden Sie sich bitte an uns, um weitere Support Unterstützung zu erhalten.

Domain-Controller Replikationsfehler

Description

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.
- Das Netzwerk ACLs ist 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 [Voraussetzungen für die Erstellung eines AWS verwalteten 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 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 Directory Service. In den folgenden Themen erfahren Sie, wie Sie die Konfiguration vornehmen 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 Directory Service Ressourcen unterstützen.

Sicherheitsthemen

Die folgenden Sicherheitsthemen finden Sie in diesem Abschnitt:

- [Identitäts- und Zugriffsmanagement für Directory Service](#)
- [Anmeldung und Überwachung 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

- [AWS Verwaltetes Microsoft AD-Administratorkonto und Gruppenberechtigungen](#)
- [Gruppenverwaltete Service-Konten](#)
- [Aufbau einer Vertrauensbeziehung zwischen Ihrem AWS verwalteten Microsoft AD und selbstverwaltetem AD](#)
- [Eingeschränkte Kerberos-Delegierung](#)
- [Benutzern und Gruppen von AWS verwalteten Microsoft AD Zugriff auf AWS Ressourcen mit IAM-Rollen gewähren](#)
- [Autorisierung für AWS Anwendungen und Dienste, die Directory Service](#)

Ihr Verzeichnis sichern

- [Schützen Sie Ihr AWS verwaltetes Microsoft AD](#)
- [Ihr AD-Connector-Verzeichnis sichern](#)

Protokollierung und Überwachung

- [Überwachen Sie Ihr AWS verwaltetes Microsoft AD](#)
- [Ihr AD-Connector-Verzeichnis überwachen](#)

Ausfallsicherheit

- [Patching und Wartung für AWS Managed Microsoft AD](#)

Identitäts- und Zugriffsmanagement für Directory Service

Für den Zugriff auf 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 Directory Service Verzeichnis. In den folgenden Abschnitten erfahren Sie, wie Sie [AWS Identity and Access Management \(IAM\)](#) verwenden und 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. Directory Service Sie müssen beispielsweise über Berechtigungen zum Erstellen eines Directory Service Verzeichnisses oder zum Erstellen eines Verzeichnissnapshots verfügen.

In den folgenden Abschnitten wird beschrieben, wie Sie Berechtigungen für verwalten Directory Service. Wir empfehlen Ihnen, zunächst die Übersicht zu lesen.

- [Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre Directory Service Ressourcen](#)
- [Verwendung identitätsbasierter Richtlinien \(IAM-Richtlinien\) für Directory Service](#)
- [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#)

Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre Directory Service Ressourcen

Jede AWS Ressource gehört einem AWS Konto. Daher werden die Berechtigungen zum Erstellen oder Zugreifen auf die Ressourcen durch Berechtigungsrichtlinien geregelt. Ein Kontoadministrator, bei dem es sich um einen Benutzer mit Administratorrechten handelt, kann Ressourcen jedoch Berechtigungen zuweisen. Sie haben auch die Möglichkeit, IAM-Identitäten wie Benutzern, Gruppen und Rollen Berechtigungsrichtlinien zuzuweisen, und einige Dienste unterstützen AWS Lambda auch das Anhängen von Berechtigungsrichtlinien an Ressourcen.

Note

Informationen zur Rolle des Kontoadministrators finden Sie unter [Bewährte Methoden für IAM](#) im IAM-Benutzerhandbuch.

Themen

- [Directory Service Ressourcen und Abläufe](#)
- [Grundlegendes zum Eigentum an Ressourcen](#)
- [Verwaltung des Zugriffs auf -Ressourcen](#)
- [Angaben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale](#)
- [Angaben von Bedingungen in einer Richtlinie](#)

Directory Service Ressourcen und Abläufe

Directory Service ist die primäre Ressource ein Verzeichnis. Da Verzeichnis-Snapshot-Ressourcen Directory Service unterstützt werden, können Sie Snapshots nur im Kontext eines vorhandenen Verzeichnisses erstellen. Dieser Snapshot wird als Unterressource bezeichnet.

Diesen Ressourcen sind eindeutige Amazon-Ressourcennamen (ARNs) zugeordnet, wie in der folgenden Tabelle dargestellt.

Ressourcentyp	ARN-Format
Verzeichnis	<code>arn:aws:ds: <i>region</i>:<i>account-id</i> :directory/ <i>external-directory-id</i></code>
Schnappschuss	<code>arn:aws:ds: <i>region</i>:<i>account-id</i> :snapshot/ <i>external-snapshot-id</i></code>

Directory Service umfasst zwei Dienst-Namespaces, die auf der Art der von Ihnen ausgeführten Operationen basieren.

- Der ds Dienst-Namespace bietet eine Reihe von Vorgängen für die Arbeit mit den entsprechenden Ressourcen. Eine Liste der verfügbaren Operationen finden Sie unter [Verzeichnisservice-Aktionen](#).
- Der ds-data Dienst-Namespace stellt eine Reihe von Operationen für Active Directory-Objekte bereit. Eine Liste der verfügbaren Operationen finden Sie unter [Directory Service Data API Reference](#).

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 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 Directory Service Ressourcen gewähren, kann der Benutzer auch 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 Directory Service Ressourcen erstellen, kann jeder, der die Rolle übernehmen kann, Directory Service Ressourcen erstellen. Ihr AWS Konto, zu dem die Rolle gehört, besitzt die Directory Service Ressourcen.

Verwaltung 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 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. 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 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 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 Directory Service Ressourcen zulässig sind, die dem Konto gehören.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen zur Verwendung identitätsbasierter Richtlinien mit Directory Service finden Sie unter [Verwendung identitätsbasierter Richtlinien \(IAM-Richtlinien\) für 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. Directory Service unterstützt keine ressourcenbasierten Richtlinien.

Angaben der Richtlinienelemente: Aktionen, Effekte, Ressourcen und Prinzipale

Für jede Directory Service Ressource definiert der Dienst eine Reihe von API-Operationen. Weitere Informationen finden Sie unter [Directory Service Ressourcen und Abläufe](#). Eine Liste der verfügbaren API-Operationen finden Sie unter [Verzeichnisservice-Aktionen](#).

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 Directory Service Ressourcen verwenden Sie in IAM-Richtlinien immer das Platzhalterzeichen (*). Weitere Informationen finden Sie unter [Directory Service Ressourcen und Abläufe](#).
- **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 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). 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 Directory Service API-Aktionen und den Ressourcen, für die sie gelten, finden Sie unter [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 Richtlinienyntax finden Sie im Thema [Bedingung](#) im IAM Benutzerhandbuch.

Bedingungen werden mithilfe vordefinierter Bedingungsschlüssel formuliert. Für 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.

AWS verwaltete Richtlinien für AWS Directory Service

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [vom Kunden verwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

In den folgenden Abschnitten werden die AWS verwalteten Richtlinien beschrieben, die spezifisch für sind Directory Service. Sie können diese Richtlinien Benutzern in Ihrem Konto zuordnen.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinie: AWSDirectoryServiceFullAccess

Sie können die AWSDirectoryServiceFullAccess-Richtlinie an Ihre IAM-Identitäten anfügen. Die vollständigen Berechtigungen für diese Richtlinie finden Sie [AWSDirectoryServiceFullAccess](#) in der Referenz zu AWS verwalteten Richtlinien.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Prinzipal vollen Zugriff auf alle Directory Service Aktionen gewähren. Prinzipale mit diesen Berechtigungen können Verzeichnisse erstellen, konfigurieren und verwalten, darunter Simple AD, AD Connector und Managed Microsoft AD. Sie können auch die gemeinsame Nutzung von Verzeichnissen, Vertrauensbeziehungen und Überwachungskonfigurationen verwalten. Diese Richtlinie beinhaltet Berechtigungen zur Verwaltung der zugrunde liegenden Netzwerkinfrastruktur, die für Verzeichnisdienste erforderlich ist.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **ds**— Ermöglicht Prinzipalen vollen Zugriff auf alle Directory Service Aktionen.
- **ec2**— Ermöglicht Prinzipalen die Verwaltung von Netzwerkschnittstellen und Sicherheitsgruppen und die Beschreibung von VPC-Ressourcen, die für Verzeichnisoperationen erforderlich sind.
- **sns**— Ermöglicht Prinzipalen das Erstellen und Verwalten von SNS-Themen für die Verzeichnisüberwachung, insbesondere Themen, deren Namen mit "" beginnen.
DirectoryMonitoring
- **iam**— Ermöglicht Prinzipalen, IAM-Rollen für Verzeichnisdienstoperationen aufzulisten.
- **organizations**— Ermöglicht Prinzipalen die Verwaltung der AWS Unternehmensintegration und des enable/disable Dienstzugriffs für Verzeichnisdienste.

AWS verwaltete Richtlinie: AWSDirectoryServiceReadOnlyAccess

Sie können die `AWSDirectoryServiceReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Die vollständigen Berechtigungen für diese Richtlinie finden Sie [AWSDirectoryServiceReadOnlyAccess](#) in der Referenz zu AWS verwalteten Richtlinien.

Diese Richtlinie gewährt nur Leseberechtigungen, mit denen Benutzer Informationen einsehen können. Directory Service Prinzipale, denen diese Richtlinie zugewiesen ist, können keine Aktualisierungen an Verzeichnissen oder deren Konfigurationen vornehmen. Prinzipale mit diesen Berechtigungen können beispielsweise Verzeichnisdetails, Vertrauensstellungen und Überwachungskonfigurationen einsehen, aber keine neuen Verzeichnisse erstellen oder bestehende ändern. Sie können auch verwandte EC2-Netzwerkressourcen und SNS-Themen im Zusammenhang mit Verzeichnissen einsehen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `ds`— Ermöglicht Benutzern, schreibgeschützte Aktionen auszuführen, bei denen Verzeichnisinformationen zurückgegeben werden. Dazu gehören API-Operationen, die mit `Check`, `Describe`, `GetList`, oder `beginnen`. `Verify`
- `ec2`— Ermöglicht Benutzern die Beschreibung von Netzwerkschnittstellen, Subnetzen und VPCs zugehörigen Verzeichnisdiensten.
- `sns`— Ermöglicht Benutzern das Auflisten und Abrufen von Informationen zu SNS-Themen und Abonnements, die für die Verzeichnisüberwachung verwendet werden.
- `organizations`— Ermöglicht Benutzern, AWS Organizations Konten und Dienstzugriffskonfigurationen im Zusammenhang mit Verzeichnisdiensten zu beschreiben.

AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess

Sie können die `AWSDirectoryServiceDataFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Die vollständigen Berechtigungen für diese Richtlinie finden Sie [AWSDirectoryServiceDataFullAccess](#) in der Referenz zu AWS verwalteten Richtlinien.

Diese Richtlinie gewährt Administratorberechtigungen, die einem Prinzipal vollen Zugriff auf Verzeichnisdienstdatenoperationen gewähren. Prinzipale mit diesen Berechtigungen können Active Directory-Benutzer und -Gruppen in verwalteten Verzeichnissen erstellen, aktualisieren und löschen. Sie können Gruppenmitgliedschaften verwalten, Benutzer aktivieren oder deaktivieren und

umfassende Benutzer- und Gruppenverwaltungsvorgänge durchführen. Diese Richtlinie richtet sich an Administratoren, die Active Directory-Objekte programmgesteuert verwalten müssen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `ds`— Ermöglicht Prinzipalen den Zugriff auf Verzeichnisdaten über die Directory Service Data API.
- `ds-data`— Ermöglicht Prinzipalen vollen Zugriff auf alle Operationen mit Verzeichnisdienstdaten, einschließlich des Erstellens, Aktualisierens und Löschens von Benutzern und Gruppen, der Verwaltung von Gruppenmitgliedschaften und der Suche nach Verzeichnisobjekten.

AWS verwaltete Richtlinie: `AWSDirectoryServiceDataReadOnlyAccess`

Sie können die `AWSDirectoryServiceDataReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Die vollständigen Berechtigungen für diese Richtlinie finden Sie [AWSDirectoryServiceDataReadOnlyAccess](#) in der Referenz zu AWS verwalteten Richtlinien.

Diese Richtlinie gewährt nur Leseberechtigungen, mit denen Benutzer Active Directory-Objekte in verwalteten Verzeichnissen anzeigen und durchsuchen können. Prinzipale, denen diese Richtlinie zugewiesen ist, können keine Aktualisierungen an Benutzern, Gruppen oder Gruppenmitgliedschaften vornehmen. Prinzipale mit diesen Berechtigungen können beispielsweise nach Benutzern und Gruppen suchen, Benutzer- und Gruppendetails anzeigen und Gruppenmitgliedschaften auflisten, aber keine Verzeichnisobjekte erstellen, ändern oder löschen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- `ds`— Ermöglicht Prinzipalen den Zugriff auf Verzeichnisdaten über die Directory Service Data API.
- `ds-data`— Ermöglicht Benutzern, schreibgeschützte Aktionen auszuführen, bei denen Verzeichnisobjektinformationen zurückgegeben werden. Dazu gehören API-Operationen, die mit `DescribeList`, oder beginnen. `Search`

`AWSDirectoryServiceServiceRolePolicy`

Sie können die `AWSDirectoryServiceServiceRolePolicy` Richtlinie nicht an Ihre IAM-Identitäten anhängen. Diese Richtlinie ist einer dienstbezogenen Rolle zugeordnet, die es dem AWS Directory Service ermöglicht, Aktionen in Ihrem Namen auszuführen. Informationen zu den

Berechtigungen für diese Richtlinie finden Sie unter [AWSDirectoryServiceServiceRolePolicy](#) in der Referenz zu von AWS verwalteten Richtlinien.

Diese Richtlinie gewährt Berechtigungen, mit denen Directory Service selbstverwaltete Domänencontroller in hybriden Active Directory-Umgebungen überwacht und bewertet werden können. Der Dienst verwendet diese Berechtigungen, um automatische Integritätsbewertungen durchzuführen, PowerShell Skripts für Kompatibilitätstests auszuführen und Netzwerkkonfigurationsinformationen zu sammeln, um die ordnungsgemäße Hybridkonnektivität und automatische Wiederherstellungsfunktionen sicherzustellen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen:

- **ssm**— Ermöglicht dem Dienst, PowerShell Befehle an lokale Domänencontroller zu senden und die Ergebnisse der Befehlsausführung zu Überwachungs- und Bewertungszwecken abzurufen.
- **ec2**— Ermöglicht dem Dienst, Netzwerkressourcen wie Subnetze VPCs, Sicherheitsgruppen und Netzwerkschnittstellen zu beschreiben, um hybride Konnektivitätskonfigurationen zu validieren.

IAM und Directory Service Aktualisierungen verwalteter Richtlinien AWS

Sehen Sie sich Details zu Aktualisierungen von IAM und AWS verwalteten Richtlinien an, seit der Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf den Seiten IAM und Directory Service Dokumentenverlauf, um automatische Benachrichtigungen über Änderungen an dieser Seite zu erhalten.

Änderungen	Beschreibung	Date
AWSDirectoryServiceServiceRolePolicy – Neue Richtlinie	Directory Service hat eine neue Richtlinie hinzugefügt, die es ermöglicht AWS , die selbstverwalteten Domain-Controller eines Kunden zu überwachen.	30. Juli 2025
AWS verwaltete Richtlinien: AWSDirectoryService	Directory Service hat eine neue Richtlinie hinzugefügt, die einem Benutzer oder	17. September 2024

Änderungen	Beschreibung	Date
eDataReadOnlyAccess – Neue Richtlinie	einer Gruppe Zugriff auf das Anzeigen und Suchen von AD-Benutzern, -Mitgliedern und -Gruppen gewährt.	
AWS verwaltete Richtlinie: AWSDirectoryServiceDataFullAccess – Neue Richtlinie	Directory Service hat eine neue Richtlinie hinzugefügt, die einem Benutzer oder einer Gruppe den Zugriff auf die integrierte Objektverwaltung mit Verzeichnisdienstdaten ermöglicht, um AD-Benutzer, -Mitglieder und -Gruppen zu erstellen, zu verwalten und anzuzeigen.	17. September 2024
Directory Service hat begonnen, Änderungen zu verfolgen	Directory Service hat begonnen, Änderungen für die AWS verwalteten Richtlinien zu verfolgen.	17. September 2024

Verwendung identitätsbasierter Richtlinien (IAM-Richtlinien) für Directory Service

In diesem Thema finden Sie Beispiele für identitätsbasierte Richtlinien, in denen ein Kontoadministrator den IAM-Identitäten (Benutzern, Gruppen und Rollen) Berechtigungsrichtlinien zuweisen kann. Diese Beispiele veranschaulichen IAM-Richtlinien in Directory Service. Sie sollten Ihre eigenen Richtlinien ändern und erstellen, um sie an Ihre Bedürfnisse und Ihre Umgebung anzupassen.

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 Directory Service Ressourcen verwalten können. Weitere Informationen finden Sie

unter [Überblick über die Verwaltung von Zugriffsberechtigungen für Ihre Directory Service Ressourcen](#).

Dieses Thema besteht aus folgenden Abschnitten:

- [Für die Verwendung der Directory Service Konsole sind Berechtigungen erforderlich](#)
- [AWS verwaltete \(vordefinierte\) Richtlinien für Directory Service](#)
- [Beispiele für vom Kunden verwaltete Richtlinien](#)
- [Verwenden von Tags mit IAM-Richtlinien](#)

Dies ist ein Beispiel für eine Berechtigungsrichtlinie.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDsEc2IamGetRole",
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeSubnets",
        "iam:GetRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
```

```

        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
    },
    {
        "Sid": "AllowPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::111122223333:role/Your-Role-Name",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "cloudwatch.amazonaws.com"
            }
        }
    }
}
]
}

```

Die drei Aussagen in der Richtlinie gewähren Berechtigungen wie folgt:

- Die erste Anweisung erteilt die Erlaubnis, ein Directory Service Verzeichnis zu erstellen. Da Berechtigungen auf Ressourcenebene Directory Service nicht unterstützt werden, gibt die Richtlinie ein Platzhalterzeichen (*) als Resource Wert an.
- Die zweite Anweisung gewährt Zugriffsberechtigungen für IAM-Aktionen, sodass IAM-Rollen in Ihrem Namen gelesen und erstellt werden 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 eine bestimmte Gruppe von Ressourcen in Amazon EC2, die erforderlich sind, um die zugehörigen Verzeichnisse erstellen, konfigurieren und löschen Directory Service zu können. Ersetzen Sie die Rolle ARN durch Ihre Rolle. Weitere Informationen finden Sie unter [Amazon EC2 EC2-Aktionen](#).

In der Richtlinie wird kein Principal Element angezeigt, da Sie in einer identitätsbasierten Richtlinie nicht den Prinzipal angeben, der die Genehmigung erhält. Wenn Sie einem Benutzer die

Richtlinie zuweisen, ist der Benutzer implizit der Prinzipal. Wird die Berechtigungsrichtlinie einer IAM-Rolle zugewiesen, erhält der in der Vertrauensrichtlinie der Rolle angegebene Prinzipal die Berechtigungen.

Eine Tabelle mit allen Directory Service API-Aktionen und den Ressourcen, für die sie gelten, finden Sie unter. [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#)

Für die Verwendung der Directory Service Konsole sind Berechtigungen erforderlich

Damit ein Benutzer mit der 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 beschrieben [AWS verwaltete \(vordefinierte\) Richtlinien für 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 Directory Service

AWS adressiert viele gängige Anwendungsfälle durch die Bereitstellung vordefinierter oder verwalteter IAM-Richtlinien, die von erstellt und verwaltet AWS werden. Verwaltete Richtlinien gewähren die erforderlichen Berechtigungen für allgemeine Anwendungsfälle, sodass Sie leichter entscheiden können, welche Berechtigungen Sie benötigen. Weitere Informationen finden Sie unter [AWS verwaltete Richtlinien für AWS Directory Service](#).

Beispiele für vom Kunden verwaltete Richtlinien

In diesem Abschnitt finden Sie Beispiele für Benutzerrichtlinien, die Berechtigungen für verschiedene Directory Service Aktionen gewähren.

Note

Alle Beispiele verwenden die Region USA West (Oregon) (us-west-2) und enthalten ein fiktives Konto. IDs

Beispiele

- [Beispiel 1: Erlauben Sie einem Benutzer, eine Beschreibe-Aktion für eine beliebige Ressource auszuführen Directory Service](#)

- [Beispiel 2: Einem Benutzer das Erstellen eines Verzeichnisses erlauben](#)

Beispiel 1: Erlauben Sie einem Benutzer, eine Beschreibe-Aktion für eine beliebige Ressource auszuführen Directory Service

Die folgende Berechtigungsrichtlinie gewährt einem Benutzer die Berechtigung, alle Aktionen auszuführen, die Describe in einem AWS verwalteten Microsoft AD mit der Verzeichnis-ID d-1234567890 in beginnen AWS-Konto 111122223333. Diese Aktionen zeigen Informationen zu einer Directory Service -Ressource, z. B. einem Verzeichnis oder Snapshot. Stellen Sie sicher, dass Sie die AWS-Region Kontonummer auf die Region, die Sie verwenden möchten, und auf Ihre Kontonummer ändern.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "arn:aws:ds:us-west-2:111122223333:directory/d-1234567890"
    }
  ]
}
```

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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```

        "Action": [
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateNetworkInterface",
            "ec2:CreateSecurityGroup",
            "ec2>DeleteNetworkInterface",
            "ec2>DeleteSecurityGroup",
            "ec2:DescribeNetworkInterfaces",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:CreateTags"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ds:CreateDirectory",
            "ds:DescribeDirectories"
        ],
        "Resource": "arn:aws:ds:*:111122223333:*"
    }
]
}

```

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. 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 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.

Die folgende Tag-Richtlinie ermöglicht die Erstellung eines Directory Service Verzeichnisses, sofern die folgenden Tags verwendet werden:

- Umgebung: Produktion
- Besitzer: Infrastructure Team
- Kostenstelle: 1234

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateDirectory"
      ],
      "Resource": "*",
    }
  ]
}
```

```
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/Environment": "Production",
                "aws:RequestTag/Owner": "Infrastructure-Team",
                "aws:RequestTag/CostCenter": "12345"
            }
        }
    ]
}
```

Die folgende Tag-Richtlinie ermöglicht das Aktualisieren und Löschen von Directory Service Verzeichnissen, sofern die folgenden Tags verwendet werden:

- Projekt: Atlas
- Abteilung: Ingenieurwesen
- Umgebung: Inszenierung

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ds:DeleteDirectory",
        "ds:UpdateDirectory"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Project": "Atlas",
          "aws:ResourceTag/Department": "Engineering",
          "aws:ResourceTag/Environment": "Staging"
        }
      }
    }
  ]
}
```

```
}
```

Die folgende Tag-Richtlinie verweigert das Tagging von Ressourcen Directory Service , wenn die Ressource eines der folgenden Tags hat:

- Produktion
- Sicherheit
- Vertraulich

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ds:AddTagsToResource"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": ["Production", "Security", "Confidential"]
        }
      }
    }
  ]
}
```

Weitere Informationen zu ARNs finden Sie unter [Amazon Resource Names \(ARNs\) und AWS Service Namespaces](#).

Die folgende Liste von 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](#)

- [RemovePRoutes](#)
- [RemoveTagsFromResource](#)
- [ResetUserPassword](#)
- [RestoreFromSnapshot](#)
- [ShareDirectory](#)
- [StartSchemaExtension](#)
- [UnshareDirectory](#)
- [UpdateConditionalForwarder](#)
- [UpdateNumberOfDomainControllers](#)
- [UpdateRadius](#)
- [UpdateTrust](#)
- [VerifyTrust](#)

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 [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#)-Tabelle als Referenz verwenden. Jeder API-Eintrag in der enthält Folgendes:

- Der Name jeder API-Operation
- Die entsprechende Aktion oder Aktionen jeder API-Operation, für die Sie Berechtigungen zur Durchführung 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 möglicherweise die Verwendung von nichtöffentlichen Directory Service API-Operationen wie `ds:AuthorizeApplication`, `ds:CheckAlias`, `ds:CreateIdentityPoolDirectory`, `ds:GetAuthorizedApplicationDetails`, `ds:UpdateAuthorizedApplication`, und `ds:UnauthorizeApplication` in ihren Richtlinien.

Einige Directory Service APIs können nur über den AWS-Managementkonsole aufgerufen werden. Sie sind nicht öffentlich 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:DisableRoleAccess`, `ds:EnableRoleAccess`, und `ds:UpdateDirectory`.

Sie können AWS globale Bedingungsschlüssel in Ihren Richtlinien Directory Service und Directory Service Data verwenden, um Bedingungen auszudrücken. Eine vollständige Liste der AWS Schlüssel finden Sie unter [Verfügbare globale Bedingungsschlüssel](#) im IAM-Benutzerhandbuch.

Directory Service API und erforderliche Berechtigungen für Aktionen

AWS Directory Service Data API und erforderliche Berechtigungen für Aktionen

Note

Um eine Aktion anzugeben, verwenden Sie das `ds-data:` Präfix, gefolgt vom Namen der API-Operation (z. B. `ds-data:AddGroupMember`).

API-Operationen Directory Service Verzeichnisdienst daten	Erforderliche Berechtigungen (API-Akti onen)	Ressourcen
AddGroupMember	<code>ds-data:AddGroupMember</code>	*
CreateGroup	<code>ds-data:CreateGroup</code>	*
CreateUser	<code>ds-data:CreateUser</code>	*
DeleteGroup	<code>ds-data>DeleteGroup</code>	*
DeleteUser	<code>ds-data>DeleteUser</code>	*
DescribeGroup	<code>ds-data:DescribeGroup</code>	*
DescribeUser	<code>ds-data:DescribeUser</code>	*
DisableUser	<code>ds-data:DisableUser</code>	*

API-Operationen Directory Service Verzeichnisdienstdaten	Erforderliche Berechtigungen (API-Aktionen)	Ressourcen
ListGroup	ds-data:ListGroup	*
ListGroupMembers	ds-data:ListGroupMembers	*
ListGroupForMember	ds-data:ListGroupForMember	*
ListUsers	ds-data:ListUsers	*
RemoveGroupMember	ds-data:RemoveGroupMember	*
SearchGroups	ds-data:DescribeGroup ds-data:SearchGroups	*
SearchUsers	ds-data:DescribeUser ds-data:SearchUsers	*
UpdateGroup	ds-data:UpdateGroup	*
UpdateUser	ds-data:UpdateUser	*

Verwandte Themen

- [Zugriffskontrolle](#)

Bedingungsschlüssel Directory Service Verzeichnisdienstdaten

Verwenden Sie die Bedingungsschlüssel für [Verzeichnisdienstdaten](#), um spezifische Anweisungen für Benutzer und den Zugriff auf Gruppenebene hinzuzufügen. Auf diese Weise können Benutzer entscheiden, welche Principals Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen können.

Mit dem Condition-Element oder dem Condition-Block können Sie Bedingungen angeben, unter denen eine Anweisung gültig ist. Das Bedingungelement ist optional. Sie können bedingte Ausdrücke erstellen, die Bedingungsoperatoren wie gleich (=) oder kleiner als (<) verwenden, um die Bedingung in der Richtlinie den Werten in der Anforderung zuzuordnen.

Wenn Sie mehrere Condition-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzigen Condition-Element angeben, werden diese mithilfe einer logischen AND-Operation AWS ausgewertet. Wenn Sie mehrere Werte für einen einzelnen Bedingungs Schlüssel angeben, AWS wertet die Bedingung mithilfe einer logischen OR-Operation aus. Alle Bedingungen müssen erfüllt sein, bevor die Berechtigungen für die Anweisung erteilt werden. Sie können bei der Angabe von Bedingungen auch Platzhaltervariablen verwenden. Beispielsweise können Sie einem IAM-Benutzer nur dann Zugriff auf eine Ressource gewähren, wenn diese mit seinem Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [Bedingung mit mehreren Schlüsseln oder Werten](#) im IAM-Benutzerhandbuch.

Eine Liste der Aktionen, die diese Bedingungs Schlüssel unterstützen, finden Sie unter [Durch AWS Verzeichnisdienstdaten definierte Aktionen](#) in der Service Authorization Reference.

 Note

Informationen zu tagbasierten Berechtigungen auf Ressourcenebene finden Sie unter [Verwenden von Tags mit IAM-Richtlinien](#)

ds-data: Name SAMAccount

Funktioniert mit [String-Operatoren](#).

Verwenden Sie diesen Schlüssel, um einer IAM-Rolle ausdrücklich das Ausführen von Aktionen für bestimmte Benutzer und Gruppen zuzulassen oder zu verweigern.

 Important

Wenn Sie SAMAccountName oder verwendenMemberName, empfehlen wir die Angabe ds-data:Identifizier alsSAMAccountName. Dadurch wird verhindert, dass future Kennungen, die von AWS Directory Service Data unterstützt werdenSID, z. B. bestehende Berechtigungen verletzen.

Die folgende Richtlinie verhindert, dass der IAM-Prinzipal den Benutzer joe oder die Gruppe beschreibt. joegroup

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyDescribe",
      "Effect": "Deny",
      "Action": "ds-data:Describe*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe",
            "joegroup"
          ],
          "ds-data:identifier": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

Note

Bei dieser Bedingung wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie müssen Operatoren [StringEqualsIgnoreCase](#) oder [StringNotEqualsIgnoreCase](#) Bedingungsoperatoren verwenden, um Zeichenkettenwerte unabhängig von der Groß- und Kleinschreibung zu vergleichen.

DS-Data: Bezeichner

[Funktioniert mit String-Operatoren.](#)

Verwenden Sie diesen Schlüssel, um zu definieren, welcher Bezeichner in den IAM-Richtlinienberechtigungen verwendet werden soll. Derzeit wird nur `SAMAccountName` unterstützt.

Die folgende Richtlinie ermöglicht es dem IAM-Prinzipal, den Benutzer zu aktualisieren. joe

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateJoe",
      "Effect": "Allow",
      "Action": "ds-data:UpdateUser",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "joe"
          ],
          "ds-data:identifier": [
            "SAMAccountName"
          ]
        }
      }
    }
  ]
}
```

DS-Daten: MemberName

Funktioniert mit [String-Operatoren](#).

Verwenden Sie diesen Schlüssel, um die Elemente zu definieren, an denen Operationen ausgeführt werden können.

Important

Wenn Sie `MemberName` oder `verwendenSAMAccountName` verwenden, empfehlen wir die Angabe `ds-data:Identifier` als `SAMAccountName`. Dadurch wird verhindert, dass future Kennungen,

die von Directory Service Data unterstützt werden SID, z. B. bestehende Berechtigungen verletzen.

Die folgende Richtlinie ermöglicht es dem IAM-Prinzipal, für jedes Mitglied joe in AddGroupMember einer beliebigen Gruppe Aufgaben auszuführen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AddJoe",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "joe"
        }
      }
    }
  ]
}
```

Note

Bei diesem Bedingungsschlüssel wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie müssen Operatoren [StringEqualsIgnoreCase](#) oder [StringNotEqualsIgnoreCase](#) Bedingungsoperatoren verwenden, um Zeichenkettenwerte zu vergleichen, unabhängig von der Groß- und Kleinschreibung.

DS-Daten: MemberRealm

Funktioniert mit [String-Operatoren](#).

Verwenden Sie diesen Schlüssel, um zu überprüfen, ob der `ds-data:MemberRealm` Wert in der Richtlinie mit dem Mitgliedsbereich in der Anfrage übereinstimmt.

 Note

Bei diesem Bedingungsschlüssel wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie müssen Operatoren [StringEqualsIgnoreCase](#) oder [StringNotEqualsIgnoreCase](#) Bedingungsoperatoren verwenden, um Zeichenkettenwerte zu vergleichen, unabhängig von der Groß- und Kleinschreibung.

Die folgende Richtlinie ermöglicht es dem IAM-Principal, bob im Realm `ONE.TRU1.AMAZON.COM` nach Mitgliedern zu `AddGroupMember` suchen.

 Note

Im folgenden Beispiel wird nur der `ds-data:MemberName` Kontextschlüssel verwendet.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "addbob",
      "Effect": "Allow",
      "Action": "ds-data:AddGroupMember",
      "Resource": "arn:aws:ds:us-east-1:111122223333:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": "bob",
          "ds-data:MemberRealm": "one.tru1.amazon.com"
        }
      }
    }
  ]
}
```

DS-Data: Realm

Funktioniert mit String-Operatoren.

Verwenden Sie diesen Schlüssel, um zu überprüfen, ob der `ds-data:Realm` Wert in der Richtlinie dem Bereich entspricht, den ein IAM-Prinzipal für Anfragen an Verzeichnisdienst-APIs verwenden kann.

Note

Bei diesem Bedingungsschlüssel wird nicht zwischen Groß- und Kleinschreibung unterschieden. Sie müssen Operatoren [StringEqualsIgnoreCase](#) oder [StringNotEqualsIgnoreCase](#) Bedingungsoperatoren verwenden, um Zeichenkettenwerte unabhängig von der Groß- und Kleinschreibung zu vergleichen.

Die folgende Richtlinie verhindert, dass der IAM-Principal den Realm `ListUsers` aufruft.
`one.tru1.amazon.com`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyTrustedList",
      "Effect": "Deny",
      "Action": "ds-data:ListUsers",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:Realm": [
            "one.tru1.amazon.com"
          ]
        }
      }
    }
  ]
}
```

Autorisierung für AWS Anwendungen und Dienste, die Directory Service

In diesem Thema wird die Autorisierung von AWS Anwendungen und Diensten beschrieben, die AWS Verzeichnisdienstdaten verwenden AWS Directory Service .

Autorisieren einer AWS Anwendung in einem Active Directory

Directory Service gewährt ausgewählten Anwendungen spezifische Berechtigungen für die nahtlose Integration in Ihr Active Directory, wenn Sie eine AWS Anwendung autorisieren. AWS Anwendungen wird nur der Zugriff gewährt, der für ihre spezifischen Anwendungsfälle erforderlich ist. Im Folgenden finden Sie eine Reihe interner Berechtigungen, die Anwendungen und Anwendungsadministratoren nach der Autorisierung gewährt werden:

Note

Die `ds:AuthorizationApplication` Berechtigung ist erforderlich, um eine neue AWS Anwendung für ein 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

Organisationseinheit, 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 Directory Service API-Berechtigungen finden Sie unter [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 unter [Zugriff auf AWS Anwendungen und Dienste von Ihrem AWS Managed Microsoft AD](#). Weitere Informationen zum Aktivieren von AWS Anwendungen und Diensten für Simple AD finden Sie unter [Zugriff auf AWS Anwendungen und Dienste von Ihrem Simple AD](#). Informationen zum Aktivieren von AWS Anwendungen und Diensten für AD Connector finden Sie unter [Zugriff auf AWS Anwendungen und Dienste über AD Connector](#).

Deauthorisierung einer AWS Anwendung in einem Active Directory

Die `ds:UnauthorizedApplication` Berechtigung ist erforderlich, um einer AWS Anwendung die Berechtigungen für den Zugriff auf ein Active Directory zu entziehen. Folgen Sie dem von der Anwendung bereitgestellten Verfahren, um sie zu deaktivieren.

AWS Anwendungsautorisierung mit Directory Service Data

Für AWS verwaltete Microsoft AD-Verzeichnisse bietet die Directory Service Data (ds-data) -API programmgesteuerten Zugriff auf Benutzer- und Gruppenverwaltungsaufgaben. Das Autorisierungsmodell von AWS Anwendungen ist von den Zugriffskontrollen für Verzeichnisdienstdaten getrennt, was bedeutet, dass Zugriffsrichtlinien für Verzeichnisdienstdatenaktionen die Autorisierung von AWS Anwendungen nicht beeinflussen. Die Verweigerung des Zugriffs auf ein Verzeichnis in DS-Data beeinträchtigt weder die AWS Anwendungsintegration noch die Anwendungsfälle von Anwendungen. AWS

Beachten Sie beim Schreiben von Zugriffsrichtlinien für AWS verwaltete Microsoft AD-Verzeichnisse, die AWS Anwendungen autorisieren, dass Benutzer- und Gruppenfunktionen möglicherweise verfügbar sind, wenn Sie entweder eine autorisierte AWS Anwendung oder eine Directory Service Data API aufrufen. Amazon WorkDocs, Amazon WorkMail, Amazon WorkSpaces, Amazon Quick und Amazon Chime bieten alle Benutzer- und Gruppenverwaltungsaktionen in ihren APIs. Steuern Sie den Zugriff auf diese AWS Anwendungsfunktionen mithilfe von IAM-Richtlinien.

Beispiele

Die folgenden Auszüge zeigen die falschen und korrekten Methoden, um DeleteUser Funktionen zu verweigern, wenn AWS Anwendungen wie Amazon WorkDocs und Amazon für das WorkMail Verzeichnis autorisiert sind.

Falsch

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser"
    ],
    "Resource": "*"
  }]
}
```

Korrekt

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser",
      "workmail:DeleteUser",
      "workdocs:DeleteUser"
    ],
    "Resource": "*"
  }]
}
```

Verwenden von serviceverknüpften Rollen für Directory Service

AWS Directory Service verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, mit der direkt verknüpft ist. Directory Service mit Diensten verknüpfte Rollen sind vordefiniert Directory Service und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine dienstbezogene Rolle Directory Service erleichtert die Einrichtung, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Directory Service definiert die Berechtigungen ihrer dienstbezogenen Rollen und Directory Service kann, sofern nicht anders definiert, nur ihre Rollen übernehmen. Die definierten Berechtigungen enthält die Vertrauens- und Berechtigungsrichtlinie, die keinen anderen IAM-Entitäten zugewiesen werden kann.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem die zugehörigen Ressourcen gelöscht wurden. Dadurch wird verhindert, dass Sie den Zugriff auf Ihre Directory Service Ressourcen verlieren, da Sie die Zugriffsberechtigungen für die Ressourcen nicht versehentlich entfernen können.

Weitere Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter [AWS -Services, die mit IAM funktionieren](#).

Themen

- [Mit dem Dienst verknüpfte Rollenberechtigungen für Directory Service](#)
- [Erstellung einer dienstbezogenen Rolle für Directory Service](#)
- [Bearbeiten einer serviceverknüpften Rolle für Directory Service](#)
- [Löschen einer dienstbezogenen Rolle für Directory Service](#)
- [Unterstützte Regionen für serviceverknüpfte Rollen Directory Service](#)

Mit dem Dienst verknüpfte Rollenberechtigungen für Directory Service

Directory Service verwendet die dienstgebundene Rolle mit dem Namen `AWSServiceRoleForDirectoryService`— Ermöglicht AWS die Überwachung der vom Kunden selbst verwalteten Domänencontroller.

Die serviceverknüpfte Rolle `AWSServiceRoleForDirectoryService` vertraut darauf, dass die folgenden Services die Rolle annehmen:

- `ds.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie `AWSDirectoryServiceServiceRolePolicy` ermöglicht es Directory Service, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen. Die vollständigen Richtlinienberechtigungen finden Sie [AWSDirectoryServiceServiceRolePolicy](#) in der Referenz für AWS verwaltete Richtlinien.

- `ec2`— Ermöglicht dem Dienst, Netzwerkressourcen wie Subnetze VPCs, Sicherheitsgruppen und Netzwerkschnittstellen zu beschreiben, um hybride Konnektivitätskonfigurationen zu validieren:
 - `ec2:DescribeAvailabilityZones`
 - `ec2:DescribeDhcpOptions`
 - `ec2:DescribeNetworkInterfaces`
 - `ec2:DescribeRouteTables`
 - `ec2:DescribeSecurityGroups`
 - `ec2:DescribeSubnets`
 - `ec2:DescribeVpcs`
- `ssm`— Ermöglicht dem Dienst, PowerShell Guilabels zu Überwachungs- und Bewertungszwecken an lokale Domänencontroller zu senden und zu überwachen:
 - `ssm:Sendguilabel`
 - `ssm:Listguilabels`
 - `ssm:GetguilabelInvocation`
 - `ssm:DescribeInstanceInformation`
 - `ssm:GetConnectionStatus`

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Erstellung einer dienstbezogenen Rolle für Directory Service

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie AWS die Überwachung der selbstverwalteten Domänencontroller des Kunden in der AWS-Managementkonsole, der oder der AWS API AWS CLI zulassen, Directory Service wird die serviceverknüpfte Rolle für Sie erstellt. Weitere Informationen zu dieser Änderung finden Sie unter [Richtlinienaktualisierungen](#).

 Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Außerdem gilt: Wenn Sie den Directory Service Dienst vor dem 1. Januar 2017 genutzt haben, als er begann, dienstbezogene Rollen zu unterstützen, haben Sie die `AWSServiceRoleForDirectoryService` dann in Ihrem Konto Directory Service erstellt. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem AWS-Konto erschienen](#).

Bearbeiten einer serviceverknüpften Rolle für Directory Service

Directory Service erlaubt es Ihnen nicht, die `AWSServiceRoleForDirectoryService` dienstbezogene Rolle zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer dienstbezogenen Rolle für Directory Service

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

 Note

Wenn der Directory Service Dienst die Rolle zu dem Zeitpunkt verwendet, zu dem Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um Directory Service Ressourcen zu löschen, die verwendet werden von `AWSServiceRoleForDirectoryService`

- Informationen zum Löschen Ihres Verzeichnisses finden Sie unter [Löschen Ihres AWS verwalteten Microsoft AD](#).

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die `AWSServiceRoleForDirectoryServiceserviceverknüpfte` Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Rollen Directory Service

Directory Service unterstützt nicht die Verwendung von dienstbezogenen Rollen in allen Regionen, in denen der Dienst verfügbar ist. Directory Service Verwendet die `AWSServiceRoleForDirectoryServiceRolle` jedoch nur dort, AWS-Regionen wo Sie sich für Hybridverzeichnisse anmelden können.

Unterstützung für Regionen mit Opt-in-Option für Hybridverzeichnisse

Name der Region	Regions-ID	Opt-in-Unterstützung
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Europa (Stockholm)	eu-north-1	Ja
Naher Osten (Bahrain)	me-south-1	Ja
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Europa (Paris)	eu-west-3	Ja
Asien-Pazifik (Jakarta)	ap-southeast-3	Ja
Afrika (Kapstadt)	af-south-1	Ja
Europa (Irland)	eu-west-1	Ja
Naher Osten (VAE)	me-central-1	Ja
Europa (Frankfurt)	eu-central-1	Ja

Name der Region	Regions-ID	Opt-in-Unterstützung
Südamerika (São Paulo)	sa-east-1	Ja
Asien-Pazifik (Hongkong)	ap-east-1	Ja
Asien-Pazifik (Hyderabad)	ap-south-2	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Europa (London)	eu-west-2	Ja
Asien-Pazifik (Melbourne)	ap-southeast-4	Ja
Europa (Milan)	eu-south-1	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Kanada (Zentral)	ca-central-1	Ja
Europa (Spain)	eu-south-2	Ja
Europa (Zürich)	eu-central-2	Ja

Anmeldung und Überwachung 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 [Aktivierung der Amazon](#)

[CloudWatch Logs-Protokollweiterleitung für AWS Managed Microsoft AD](#). Darüber hinaus können Sie CloudWatch Metrics verwenden, um die Leistung von Domain-Controllern zu überwachen. Weitere Informationen finden Sie unter [Feststellen, wann Domänencontroller mit CloudWatch Metriken hinzugefügt werden sollen](#).

- AWS CloudTrail
 - Sie können es CloudTrail mit allen Directory Service Verzeichnistypen verwenden. Weitere Informationen finden Sie unter [Protokollieren von AWS Directory Service API-Aufrufen mit AWS CloudTrail](#).
 - Sie können AWS es CloudTrail mit Managed Microsoft AD in der Directory Service Data API verwenden. Weitere Informationen finden Sie unter [Protokollieren von API-Aufrufen für AWS Verzeichnisdienstdaten mit AWS CloudTrail](#).

Protokollieren von AWS Directory Service API-Aufrufen mit AWS CloudTrail

Die AWS Managed Microsoft AD API ist in einen Service integriert AWS CloudTrail, der API-Aufrufe von oder im Namen von AWS Managed Microsoft AD in Ihrem erfasst AWS-Konto und die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket übermittelt. CloudTrail erfasst API-Aufrufe von der AWS Managed Microsoft AD-Konsole und von Codeaufrufen an das AWS Managed Microsoft AD APIs. Anhand der von gesammelten Informationen können Sie feststellen CloudTrail, welche Anfrage an AWS Managed Microsoft AD gestellt wurde, von welcher Quell-IP-Adresse die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde usw. Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

AWS Verwaltete Microsoft AD-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn eine Aktivität in AWS Managed Microsoft AD auftritt, wird diese Aktivität zusammen mit anderen CloudTrail AWS Dienstereignissen im Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für AWS Managed Microsoft AD, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste

konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Wenn die CloudTrail Protokollierung in Ihrem aktiviert ist AWS-Konto, werden alle API-Aufrufe an AWS verwaltete Microsoft AD-Aktionen in Protokolldateien nachverfolgt. AWS Verwaltete Microsoft AD-Datensätze werden zusammen mit anderen AWS Dienstdatensätzen in eine Protokolldatei geschrieben. CloudTrail bestimmt anhand eines Zeitraums und der Dateigröße, wann eine neue Datei erstellt und in diese geschrieben werden soll. Alle Aufrufe der Directory Service API- oder CLI-Aufrufe werden von protokolliert CloudTrail.

Jeder Protokolleintrag enthält Informationen über den Ersteller der Anforderung. Anhand der Benutzeridentitätsinformationen im Protokoll können Sie feststellen, ob die Anfrage mit Root- oder IAM-Benutzeranmeldedaten, mit temporären Sicherheitsanmeldedaten für eine Rolle oder einen Verbundbenutzer oder von einem anderen AWS Dienst gestellt wurde. Weitere Informationen finden Sie im Feld `userIdentity` in der [CloudTrail -Ereignisreferenz](#).

Sie können Ihre Protokolldateien beliebig lange im Bucket speichern. Sie können aber auch Amazon S3-Lebenszyklusregeln aufstellen, anhand derer die Protokolldateien automatisch archiviert oder gelöscht werden. Standardmäßig werden die Protokolldateien mit serverseitiger Amazon S3-Verschlüsselung (SSE) verschlüsselt.

Sie können festlegen, dass Amazon SNS SNS-Benachrichtigungen CloudTrail veröffentlicht werden, wenn neue Protokolldateien zugestellt werden, wenn Sie bei der Übermittlung der Protokolldateien schnell reagieren möchten. Weitere Informationen finden Sie unter [Konfigurieren von Amazon SNS-Benachrichtigungen](#).

Sie können auch AWS verwaltete Microsoft AD-Protokolldateien aus mehreren AWS Regionen AWS-Konten in einem einzigen Amazon S3 S3-Bucket zusammenfassen. Weitere Informationen finden Sie unter [Aggregieren von CloudTrail Protokolldateien zu einem einzigen Amazon S3 S3-Bucket](#).

Grundlegendes zu AWS verwalteten Microsoft AD-Protokolldateieinträgen

CloudTrail Protokolldateien können einen oder mehrere Protokolleinträge enthalten, wobei jeder Eintrag aus mehreren Ereignissen im JSON-Format besteht. Ein Protokolleintrag stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, etwaige Parameter und das Datum und die Uhrzeit der Aktion. Es kann nicht garantiert werden, dass sich die Protokolleinträge in einer bestimmten Reihenfolge befinden. Das heißt, es handelt sich nicht um einen geordneten Stack-Trace der öffentlichen API-Aufrufe.

Sensible Informationen, z. B. Kennwörter, Authentifizierungstoken, Dateikommentare und Dateiinhalt sind in den Protokolleinträgen geschwärzt.

Das folgende Beispiel zeigt ein Beispiel für einen CloudTrail Protokolleintrag für AWS Managed Microsoft AD:

```
{
  "Records" : [
    {
      "eventVersion" : "1.02",
      "userIdentity" :
      {
        "type" : "IAMUser",
        "principalId" : "<user_id>",
        "arn" : "<user_arn>",
        "accountId" : "<account_id>",
        "accessKeyId" : "<access_key_id>",
        "userName" : "<username>"
      },
      "eventTime" : "<event_time>",
      "eventSource" : "ds.amazonaws.com",
      "eventName" : "CreateDirectory",
      "awsRegion" : "<region>",
      "sourceIPAddress" : "<IP_address>",
      "userAgent" : "<user_agent>",
      "requestParameters" :
      {
        "name" : "<name>",
        "shortName" : "<short_name>",
        "vpcSettings" :
        {
          "vpcId" : "<vpc_id>",
          "subnetIds" : [
```

```

        "<subnet_id_1>",
        "<subnet_id_2>"
    ]
},
"type" : "<size>",
"setAsDefault" : <option>,
"password" : "****OMITTED****"
},
"responseElements" :
{
    "requestId" : "<request_id>",
    "directoryId" : "<directory_id>"
},
"requestID" : "<request_id>",
"eventID" : "<event_id>",
"eventType" : "AwsApiCall",
"recipientAccountId" : "<account_id>"
}
]
}

```

Protokollieren von API-Aufrufen für AWS Verzeichnisdienstdaten mit AWS CloudTrail

AWS Directory Service Data lässt sich in einen Dienst integrieren AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführten Aktionen in Directory Service Data bereitstellt. CloudTrail erfasst alle API-Aufrufe für Verzeichnisdienstdaten als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Directory Service Data-Konsole und Codeaufrufen von Directory Service Data-API-Vorgängen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Verzeichnisdienstdaten. Anhand der von gesammelten Informationen können Sie die Anfrage CloudTrail, die an Directory Service Data gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Informationen zu Verzeichnisdienstdaten in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn unterstützte Ereignisaktivitäten (Verwaltungsereignisse) in den Verzeichnisdienstdaten auftreten, wird diese

Aktivität zusammen mit anderen AWS Dienstereignissen im Ereignisverlauf in einem CloudTrail Ereignis aufgezeichnet. Sie können die Verwaltungsereignisse der letzten 90 Tage in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#). Die Anzeige des Eventverlaufs ist kostenlos.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS-Konto, einschließlich Ereignissen für Verzeichnisdienstdaten, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail unterstützte Dienste und Integrationen](#)
- [Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle Directory Service Data-Aktionen werden von der [Directory Service Data API-Referenz](#) protokolliert CloudTrail und sind in dieser Dokumentation dokumentiert. Beispielsweise generieren Aufrufe von `DescribeUser` und `SearchGroups` Aktionen Einträge in den CloudTrail Protokolldateien. `AddGroupMember`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter [CloudTrail -Element userIdentity](#).

Grundlegendes zu Einträgen in Verzeichnisdienst-Datenprotokolldateien

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die [CreateUser](#)Aktion demonstriert.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-30T18:22:38Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2023-05-30T19:17:03Z",
  "eventSource": "ds.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "ap-northeast-2",
  "sourceIPAddress": "10.24.34.0",
  "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
  "requestParameters": {
    "directoryId": "d-1234567890",
    "sAMAccountName": "johnsmith",
```

```
"clientToken": "example_token"
"emailAddress": "HIDDEN_DUE_TO_SECURITY_REASONS",
"givenName": "HIDDEN_DUE_TO_SECURITY_REASONS",
"surname": "HIDDEN_DUE_TO_SECURITY_REASONS",
"otherAttributes": {
  "physicalDeliveryOfficeName": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "telephoneNumber": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "streetAddress": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "displayName": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "homePhone": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "postalCode": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "description": {
    "s": "HIDDEN_DUE_TO_SECURITY_REASONS"
  }
},
"clientToken": "createUserToken4"
},
"responseElements": {
  "directoryId": "d-1234567890",
  "sID": "S-1-5-21-1234567890-123456789-123456789-1234",
  "sAMAccountName": "johnsmith"
},
"additionalEventData": {
  "SID": "S-1-5-21-1234567890-123456789-123456789-1234"
},
"requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
"eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
"readOnly": false,
"resources": [
  {
    "accountId": "111222333444",
    "type": "AWS::DirectoryService::MicrosoftAD",
```

```

        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
    }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444",
"eventCategory": "Management",
"tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
}
},

```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die [ListUsers](#)Aktion demonstriert.

Aktionen, die kein Objekt erstellen oder ändern, geben eine Null-Antwort zurück.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
        "accountId": "111222333444",
        "accessKeyId": "021345abcdef6789",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "1234567890abcdef0",
                "arn": "arn:aws:iam::111222333444:role/AdAdmin",
                "accountId": "111222333444",
                "userName": "AdAdmin"
            },
            "attributes": {
                "creationDate": "2023-05-30T18:22:38Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-05-30T18:22:52Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "ListUsers",
    "awsRegion": "ap-northeast-2",

```

```

    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.list-users",
    "requestParameters": {
        "directoryId": "d-1234567890",
        "maxResults": 1
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1244",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111222333444",
            "type": "AWS::DirectoryService::MicrosoftAD",
            "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
}

```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die [ListGroups](#)Aktion demonstriert.

Note

Das NextToken Element wurde aus allen Protokolleinträgen entfernt.

```

{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "1234567890abcdef0:admin-role",
        "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",

```



```
"accountId": "111222333444",
"accessKeyId": "021345abcdef6789",
"sessionContext": {
  "sessionIssuer": {
    "type": "Role",
    "principalId": "1234567890abcdef0",
    "arn": "arn:aws:iam::111222333444:role/AdAdmin",
    "accountId": "111222333444",
    "userName": "AdAdmin"
  },
  "attributes": {
    "creationDate": "2023-05-30T18:22:38Z",
    "mfaAuthenticated": "false"
  }
},
"eventTime": "2023-05-30T18:29:15Z",
"eventSource": "ds.amazonaws.com",
"eventName": "ListGroup",
"awsRegion": "ap-northeast-2",
"sourceIPAddress": "10.24.34.0",
"userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.list-groups",
"requestParameters": {
  "directoryId": "d-1234567890",
  "nextToken": "REDACTED",
  "maxResults": 1
},
"responseElements": null,
"requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
"eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
"readOnly": true,
"resources": [
  {
    "accountId": "111222333444",
    "type": "AWS::DirectoryService::MicrosoftAD",
    "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
  }
],
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444",
"eventCategory": "Management",
"tlsDetails": {
```

```
    "tlsVersion": "TLSv1.3",  
    "cipherSuite": "TLS_AES_128_GCM_SHA256",  
    "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"  
  }  
}
```

Logeinträge für Ausnahmefehler

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für den Fehler „Zugriff verweigert“. Hilfe zu diesem Fehler finden Sie unter [Problembehandlung bei Fehlermeldungen mit Zugriffsverweigerung](#) im IAM-Benutzerhandbuch.

Note

Im Protokoll „Zugriff verweigert“ werden keine Anforderungsparameter angezeigt.

```
{  
  "eventVersion": "1.08",  
  "userIdentity": {  
    "type": "AssumedRole",  
    "principalId": "1234567890abcdef0:admin-role",  
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",  
    "accountId": "111222333444",  
    "accessKeyId": "021345abcdef6789",  
    "sessionContext": {  
      "sessionIssuer": {  
        "type": "Role",  
        "principalId": "1234567890abcdef0",  
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",  
        "accountId": "111222333444",  
        "userName": "AdAdmin"  
      },  
      "attributes": {  
        "creationDate": "2023-05-31T23:25:49Z",  
        "mfaAuthenticated": "false"  
      }  
    }  
  },  
  "eventTime": "2023-05-31T23:38:18Z",  
  "eventSource": "ds.amazonaws.com",  
  "eventName": "CreateUser",  
}
```

```

    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.create-user",
    "errorCode": "AccessDenied",
    "errorMessage": "User: arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-
role is not authorized to perform: ds-data:CreateUser on resource: arn:aws:ds:ap-
northeast-2:111222333444:directory/d-1234567890 because no identity-based policy allows
the ds-data:CreateUser action",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": false,
    "resources": [
      {
        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111222333444",
    "eventCategory": "Management",
    "tlsDetails": {
      "tlsVersion": "TLSv1.3",
      "cipherSuite": "TLS_AES_128_GCM_SHA256",
      "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
    }
  }
}

```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag für den Fehler „Ressource nicht gefunden“.

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "1234567890abcdef0:admin-role",
    "arn": "arn:aws:sts::111222333444:assumed-role/AdAdmin/admin-role",
    "accountId": "111222333444",
    "accessKeyId": "021345abcdef6789",

```

```
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::111222333444:role/AdAdmin",
        "accountId": "111222333444",
        "userName": "AdAdmin"
      },
      "attributes": {
        "creationDate": "2023-05-30T20:41:50Z",
        "mfaAuthenticated": "false"
      }
    },
    "eventTime": "2023-05-30T21:10:16Z",
    "eventSource": "ds.amazonaws.com",
    "eventName": "DescribeUser",
    "awsRegion": "ap-northeast-2",
    "sourceIPAddress": "10.24.34.0",
    "userAgent": "aws-cli/2.9.20 Python/3.11.1 Darwin/21.6.0 source/x86_64 prompt/off
command/ds-data.describe-user",
    "errorCode": "ResourceNotFoundException",
    "errorMessage": "User not found in directory d-1234567890.",
    "requestParameters": {
      "directoryId": "d-1234567890",
      "sAMAccountName": "nonExistingUser",
      "otherAttributes": [
        "co",
        "givenName",
        "sn",
        "telephoneNumber"
      ]
    },
    "responseElements": null,
    "requestID": "4567ab89-c12d-3333-2222-1e0012f34a7c",
    "eventID": "1234567b-f0a0-12ab-3c45-d678900d1255",
    "readOnly": true,
    "resources": [
      {
        "accountId": "111222333444",
        "type": "AWS::DirectoryService::MicrosoftAD",
        "ARN": "arn:aws:ds:ap-northeast-2:111222333444:directory/d-1234567890"
      }
    ],
```

```
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111222333444"
"eventCategory": "Management",
"tlsDetails": {
  "tlsVersion": "TLSv1.3",
  "cipherSuite": "TLS_AES_128_GCM_SHA256",
  "clientProvidedHostHeader": "ds-data.ap-northeast-2.amazonaws.com"
}
}
```

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. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

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 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 [Wiederherstellung Ihres AWS verwalteten Microsoft AD mit Snapshots](#).

Sicherheit der Infrastruktur in AWS Directory Service

Als verwalteter Dienst AWS Directory Service ist er durch AWS globale Netzwerksicherheit geschützt. Informationen zu AWS Sicherheitsdiensten und zum AWS Schutz der Infrastruktur finden Sie unter [AWS Cloud-Sicherheit](#). Informationen zum Entwerfen Ihrer AWS Umgebung unter Verwendung der bewährten Methoden für die Infrastruktursicherheit finden Sie unter [Infrastructure Protection](#) in Security Pillar AWS Well-Architected Framework.

Sie verwenden AWS veröffentlichte API-Aufrufe für den Zugriff Directory Service über das Netzwerk. Kunden müssen Folgendes unterstützen:

- Transport Layer Security (TLS). Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Verschlüsselungs-Suiten mit Perfect Forward Secrecy (PFS) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Die meisten modernen Systeme wie Java 7 und höher unterstützen diese Modi.

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 privilegiere 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 Directory Service für Microsoft Active Directory der Ressource einen anderen

Dienst gewähren. 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 einer 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. Beispiel, `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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:us-east-1:111122223333:log-group:/aws/directoryservice/Log_Group_Name:*"
    ]
  }
}
```

```

    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ds:us-east-1:111122223333:directory/Directory_Name"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}

```

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. Beispiel, `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.

JSON

```

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

```



```

        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "SNS:AddPermission",
        "SNS:RemovePermission",
        "SNS:DeleteTopic",
        "SNS:Subscribe",
        "SNS:ListSubscriptionsByTopic",
        "SNS:Publish"
    ],
    "Resource": [
        "arn:aws:sns:us-east-1:111122223333:SNS_TOPIC_NAME"
    ],
    "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ds:us-east-1:111122223333:directory/EXTERNAL_DIRECTORY_ID"
        },
        "StringEquals": {
            "aws:SourceAccount": "111122223333"
        }
    }
}

```

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 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.

JSON

```

{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Principal": {
            "Service": "ds.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole"
        ]
    }
}

```

```
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ds:us-
east-1:111122223333:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "111122223333"
      }
    }
  }
}
```

Directory Service API und Schnittstelle Amazon VPC-Endpunkte mit AWS PrivateLink

Sie können AWS PrivateLink verwenden, um eine private Verbindung zwischen Ihrer VPC Directory Service und den Verzeichnisdienst-APIs herzustellen. Auf diese Weise können Sie auf Verzeichnisdienst-APIs zugreifen, die sich in Ihrer VPC befinden, und zwar ohne die Verwendung eines Internet-Gateways, eines NAT-Geräts, einer VPN-Verbindung oder einer Direct Connect-Verbindung. Instanzen in Ihrer Amazon VPC benötigen keine öffentlichen IP-Adressen für den Zugriff auf Directory Service Verzeichnisdienst-APIs.

Um eine private Verbindung herzustellen, erstellen Sie eine Amazon VPC-Schnittstelle, die mit Strom AWS PrivateLink versorgt wird. Wir erstellen eine Endpunkt-Netzwerkschnittstelle in jedem Subnetz, das Sie für den Schnittstellen-Endpunkt aktivieren. Dabei handelt es sich um vom Anforderer verwaltete Netzwerkschnittstellen, die als Einstiegspunkt für den Datenverkehr dienen, der für AWS Verzeichnisdienst-APIs AWS Directory Service bestimmt ist.

Weitere Informationen finden Sie AWS PrivateLink im Handbuch unter [Access AWS-Services through AWS PrivateLink](#).

Überlegungen zu Directory Service Verzeichnisdienst-APIs

Mit Directory Service und Directory Service Data können Sie API-Aktionen über Schnittstellenendpunkte aufrufen. Informationen zu den Voraussetzungen, die Sie berücksichtigen müssen, bevor Sie einen Schnittstellenendpunkt erstellen, finden Sie im AWS PrivateLink Handbuch unter [Zugriff und AWS-Service Verwendung eines Amazon VPC-Endpunkts mit einer Schnittstelle](#).

Directory Service und Verfügbarkeit von Verzeichnisdienst-Daten

Directory Service und Directory Service Data unterstützt Schnittstellenendpunkte überall AWS-Regionen dort, wo sie verfügbar sind. Informationen zur Unterstützung Directory Service und zu AWS-Regionen den Verzeichnisdienst-Daten finden Sie unter [Verfügbarkeit nach Regionen für Directory Service](#).

Erstellen Sie eine Schnittstelle, einen Amazon VPC-Endpunkt für Directory Service und Directory Service Data

Sie können APIs mithilfe der Amazon VPC-Konsole oder der AWS Command Line Interface (AWS CLI) einen Schnittstellenendpunkt für Directory Service und Directory Service Data erstellen.

Beispiel: Directory Service

Erstellen Sie einen Schnittstellenendpunkt für die Directory Service APIs Verwendung des folgenden Servicenamens:

```
com.amazonaws.region.ds
```

Beispiel: Verzeichnisdienst-Daten

Erstellen Sie einen Schnittstellenendpunkt für Directory Service Data APIs mit dem folgenden Dienstenamen:

```
com.amazonaws.region.ds-data
```

Weitere Informationen zum Erstellen eines Schnittstellenendpunkts finden Sie unter [Zugreifen und AWS-Service Verwenden eines Amazon VPC-Schnittstellenendpunkts](#) im AWS PrivateLink Handbuch.

Erstellen Sie eine Amazon VPC-Endpunkttrichtlinie für Ihre Schnittstelle — Amazon VPC-Endpunkt

Eine Endpunkttrichtlinie ist eine IAM-Ressourcenrichtlinie, die Sie an einen Schnittstellenendpunkt anhängen.

 Note

Wenn Sie Ihrem Schnittstellenendpunkt keine Endpunktrichtlinie zuordnen, AWS PrivateLink fügt er Ihrem Schnittstellenendpunkt in Ihrem Namen eine Standard-Endpunktrichtlinie hinzu. Weitere Informationen finden Sie unter [AWS PrivateLink -Konzepte](#).

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Principals (AWS-Konten, IAM-Benutzer und IAM-Rollen), die Aktionen ausführen können
- Aktionen, die ausgeführt werden können
- Die Ressourcen, auf denen die Aktionen ausgeführt werden können

Weitere Informationen finden Sie unter [Steuern des Zugriffs auf Services mit Endpunktrichtlinien](#) im AWS PrivateLink -Leitfaden.

Sie können den Zugriff APIs von Ihrer Amazon VPC aus steuern, indem Sie eine benutzerdefinierte Endpunktrichtlinie an Ihren Schnittstellen-Endpunkt anhängen.

Beispiel: Amazon VPC-Endpunktrichtlinie für Directory Service API-Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellen-Endpunkt anhängen, gewährt sie allen Principals auf allen Ressourcen Zugriff auf die aufgelisteten Directory Service Aktionen.

Ersetzen Sie *action-1*, *action-2*, und *action-3* durch die erforderlichen Berechtigungen für die Directory Service APIs , die Sie in Ihre Richtlinie aufnehmen möchten. Eine vollständige Liste finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds:action-1",
        "ds:action-2",
        "ds:action-3"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": "*"    
  }  
]  
}
```

Beispiel: Amazon VPC-Endpunktrichtlinie für Directory Service Data API-Aktionen

Im Folgenden finden Sie ein Beispiel für eine benutzerdefinierte Endpunktrichtlinie. Wenn Sie diese Richtlinie an Ihren Schnittstellenendpunkt anhängen, gewährt sie allen Prinzipalen auf allen Ressourcen Zugriff auf die aufgelisteten Verzeichnisdienstdatenaktionen.

Ersetzen Sie *action-1*, *action-2*, und *action-3* durch die erforderlichen Berechtigungen für die Verzeichnisdienstdaten APIs, die Sie in Ihre Richtlinie aufnehmen möchten. Eine vollständige Liste finden Sie unter [Directory Service API-Berechtigungen: Referenz zu Aktionen, Ressourcen und Bedingungen](#).

```
{  
  "Statement": [  
    {  
      "Principal": "*",  
      "Effect": "Allow",  
      "Action": [  
        "ds-data:action-1",  
        "ds-data:action-2",  
        "ds-data:action-3"  
      ],  
      "Resource": "*"    
    }  
  ]  
}
```

Service Level Agreement für Directory Service

Directory Service ist ein hochverfügbarer Service, der auf einer AWS verwalteten Infrastruktur aufbaut. Er wird durch eine Service Level (SLA) -Vereinbarung unterstützt, die unsere Richtlinien zur Serviceverfügbarkeit festlegt.

- Die SLA gilt für AWS Managed Microsoft AD, AD Connector und Simple AD.
- In der SLA werden Servicegutschriften und SLA-Ausschlüsse behandelt und Begriffe wie „Covered Directory“, „Prozentsatz der monatlichen Verfügbarkeit“ und „Anfragen“ definiert.
- Weitere Informationen finden Sie unter [Service Level Agreement für Directory Service](#).

Verfügbarkeit in der Region für Directory Service

Die folgende Tabelle enthält eine Liste mit regionsspezifischen Endpunkten, die von dem Verzeichnistyp unterstützt werden.

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Verwaltetes Microsoft AD (Standard und Enterprise Edition)	AWS Verwaltetes Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
USA Ost (Nord-Virginia)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Ja
USA Ost (Ohio)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
USA West (Nordkalifornien)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
USA West (Oregon)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Ja

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Managed Microsoft AD (Standard Edition)	AWS Managed Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
Afrika (Kapstadt)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asien-Pazifik (Hongkong)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asien-Pazifik (Taipeh)	ap-east-2	ds.ap-east-2.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein
Asien-Pazifik (Hyderabad)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asien-Pazifik (Jakarta)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Managed Microsoft AD (Standard Edition)	AWS Managed Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
Asien-Pazifik (Malaysia)	ap-southeast-5	ds.ap-southeast-5.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein
Asien-Pazifik (Melbourne)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asien-Pazifik (Thailand)	ap-southeast-7	ds.ap-southeast-7.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein
Asien-Pazifik (Neuseeland)	ap-southeast-6	ds.ap-southeast-6.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Managed Microsoft AD (Standard Edition)	AWS Managed Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
Asien-Pazifik (Mumbai)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asia Pacific (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asien-Pazifik (Seoul)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Asien-Pazifik (Singapur)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Ja
Asien-Pazifik (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Ja

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Managed Microsoft AD (Standard Edition)	AWS Managed Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
Asien-Pazifik (Tokio)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Ja
Kanada (Zentral)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Kanada West (Calgary)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein
China (Beijing)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 Ja	 Nein	 Ja	 Nein
China (Ningxia)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	 Ja	 Nein	 Ja	 Nein
Europa (Frankfurt)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Europa (Irland)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Ja

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Managed Microsoft AD (Standard Edition)	AWS Managed Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
Europa (London)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Europa (Milan)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Europa (Paris)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Europa (Spain)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Europa (Stockholm)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Europa (Zürich)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Israel (Tel Aviv)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein

Name der Region	Region	Endpunkt	Protokoll (Protokoll)	AWS Verwaltes Microsoft AD (Standard und Enterprise Edition)	AWS Verwaltes Microsoft AD (Hybrid Edition)	AD Connect	Simple AD
Mexiko (Zentral)	mx-central-1	ds.mx-central-1.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein
Naher Osten (Bahrain)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Naher Osten (VAE)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
Südamerika (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 Ja	 Ja	 Ja	 Nein
AWS GovCloud (USA West)	us-gov-west-1	ds.us-gov-west-1.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein
AWS GovCloud (US-Ost)	us-gov-east-1	ds.us-gov-east-1.amazonaws.com	HTTPS	 Ja	 Nein	 Ja	 Nein

Informationen zur Nutzung Directory Service in den Regionen AWS GovCloud (USA West) und AWS GovCloud (USA Ost) finden Sie im Benutzerhandbuch unter [Service-Endpunkte](#). AWS GovCloud (US)

Informationen zur Verwendung Directory Service in den Regionen Peking und Ningxia finden Sie unter [Endpoints und ARNs für Amazon Web Services in China](#) unter Erste Schritte AWS in China.

Informationen zu den FIPS-Endpunkten, die von Directory Service Data unterstützt werden, finden Sie im [Referenzhandbuch unter Endpunkte und Kontingente für Verzeichnisdienstdaten](#). Allgemeine AWS-Referenz

Unterstützt AWS-Regionen für Verzeichnisdienstdaten

Die folgende Tabelle enthält eine Liste der regionsspezifischen Endpunkte, die Directory Service Data nach Verzeichnistyp unterstützt.

Name der Region	Region	Endpunkt	Protocol (Protokoll)	AWS Verwaltes Microsoft AD	AD Connect	Simple AD
USA Ost (Ohio)	us-east-2	ds-data.us-east-2.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
USA Ost (Nord-Virginia)	us-east-1	ds-data.us-east-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
USA West (Nordkalifornien)	us-west-1	ds-data.us-west-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein

Name der Region	Region	Endpoint	Protocol (Protokoll)	AWS Verwaltes Microsoft AD	AD Connect	Simple AD
USA West (Oregon)	us-west-2	ds-data.us-west-2.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Asien-Pazifik (Hongkong)	ap-east-1	ds-data.ap-east-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Asien-Pazifik (Mumbai)	ap-south-1	ds-data.ap-south-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Asia Pacific (Osaka)	ap-northeast-3	ds-data.ap-northeast-3.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Asien-Pazifik (Seoul)	ap-northeast-2	ds-data.ap-northeast-2.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Asien-Pazifik (Singapur)	ap-southeast-1	ds-data.ap-southeast-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Asien-Pazifik (Sydney)	ap-southeast-2	ds-data.ap-southeast-2.amazonaws.com	HTTPS	 Ja	 Nein	 Nein

Name der Region	Region	Endpoint	Protocol (Protokoll)	AWS Verwaltes Microsoft AD	AD Connect	Simple AD
Asien-Pazifik (Tokio)	ap-northeast-1	ds-data.ap-northeast-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Kanada (Zentral)	ca-central-1	ds-data.ca-central-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Europa (Frankfurt)	eu-central-1	ds-data.eu-central-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Europa (Irland)	eu-west-1	ds-data.eu-west-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Europa (London)	eu-west-2	ds-data.eu-west-2.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Europa (Paris)	eu-west-3	ds-data.eu-west-3.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Europa (Stockholm)	eu-north-1	ds-data.eu-north-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein
Südamerika (São Paulo)	sa-east-1	ds-data.sa-east-1.amazonaws.com	HTTPS	 Ja	 Nein	 Nein

Informationen zu den FIPS-Endpunkten, die von Directory Service Data unterstützt werden, finden Sie im [Referenzhandbuch unter Endpunkte und Kontingente für Verzeichnisdienstdaten](#). Allgemeine AWS-Referenz

Browserkompatibilität für AWS Directory Service

AWS Anwendungen und Dienste wie Amazon WorkSpaces WorkMail, Amazon Connect, Amazon Chime usw. benötigen gültige Anmeldedaten von einem kompatiblen Browser WorkDocs, bevor Sie darauf zugreifen können. AWS IAM Identity Center 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 bestätigt haben, dass Sie eine unterstützte Version Ihres Browsers verwenden, empfehlen wir Ihnen, auch den folgenden Abschnitt zu lesen, um sicherzustellen, dass Ihr Browser für die Verwendung der Transport Layer Security (TLS) -Einstellung konfiguriert wurde, die für erforderlich ist AWS.

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. Im Internet Explorer finden Sie beispielsweise unter Inteneteigenschaften, auf der Registerkarte Erweitert und dann im Abschnitt Sicherheit verschiedene TLS-Optionen. Spezifische Anweisungen finden Sie auf der Hilfeseite Ihres Browserherstellers.

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen seit der letzten Veröffentlichung des Administratorhandbuchs für AWS Directory Service beschrieben.

Änderung	Beschreibung	Datum
Unterstützung für Dual-Stack-Netzwerktypen	AWS Directory Service unterstützt jetzt die Aktualisierung des Verzeichnis-Netzwerktyps von IPv4 auf Dual-Stack (IPv4 und IPv6). Diese Funktion bietet einen größeren Adressraum und ermöglicht IPv6 Konnektivität für Ihre Verzeichnisse. Sie können auch Ihre AD Connector Connector-Verzeichnisse und Simple AD AD-Verzeichnisse mit Dual-Stack-Unterstützung aktualisieren.	30. September 2025
Neue AWS dienstverknüpfte Rolle	Directory Service fügt eine neue AWS dienstbezogene Rolle <code>AWSServiceRoleForDirectoryService</code> und eine AWS verwaltete Richtlinie <code>AWSDirectoryServiceServiceRolePolicy</code> hinzu. Die Richtlinie ermöglicht AWS die Überwachung von vom Kunden verwalteten Domänencontrollern.	30. Juli 2025
AWS Verwaltetes Microsoft AD (Hybrid Edition)	AWS Managed Microsoft AD (Hybrid Edition) verbindet Ihr selbstverwaltetes Active	30. Juli 2025

Directory mit dem AWS Directory Service für Microsoft Active Directory und schafft so eine integrierte Identitätsumgebung, die sowohl Ihre Infrastruktur als auch die AWS Cloud

[Das Thema Protokollierung und Überwachung wurde aktualisiert — neue Abschnitte](#)

Es wurden Abschnitte zum AWS Directory Service Thema AWS Verzeichnisdienstdaten im Thema Protokollierung und Überwachung hinzugefügt.

18. September 2024

[Neue API und Attribute für Verzeichnisdienstdaten](#)

AWS Directory Service Data bietet eine integrierte Objektverwaltung. Sie können jetzt Objekte mit einer [Liste unterstützter AD-Attribute suchen und](#) aktualisieren.

18. September 2024

[AWS verwaltete Richtlinien — neue Richtlinien](#)

AWS Directory Service Data fügt neue AWS verwaltete Richtlinien hinzu: AWSDirectoryServiceDataFullAccess undAWSDirectoryServiceDataReadOnlyAccess. Die Richtlinien gewähren Zugriff auf die Objektverwaltung von Directory Service Data.

18. September 2024

[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-Managementkonsole, 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	Inhalt zum Hinzufügen weiterer Domain-Controller 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 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. 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
Trennung der Anleitungen	Teilen Sie das 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.