



管理ガイド

AWS Directory Service



Version 1.0

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Directory Service: 管理ガイド

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

とは AWS Directory Service	1
AWS Directory Service オプション	1
オプションの選択	5
Amazon EC2 の操作	6
AWS Managed Microsoft AD	7
入門	9
AWS Managed Microsoft AD の前提条件	10
AWS IAM Identity Center 前提条件	10
Multi-Factor Authentication の前提条件	11
AWS Managed Microsoft AD の作成	12
AWS Managed Microsoft AD で作成されるもの	14
管理者アカウントとグループのアクセス許可	25
主要なコンセプトとベストプラクティス	28
主要なコンセプト	29
ベストプラクティス	33
ユースケース	43
ユースケース 1: Active Directory 認証情報を使用して AWS アプリケーションとサービスにサインインする	44
ユースケース 2: Amazon EC2 インスタンスを管理する	49
ユースケース 3: Active Directory 対応のワークロードにディレクトリサービスを提供する ...	49
ユースケース 4: Office 365 およびその他のクラウドアプリケーション AWS IAM Identity Center へ	49
ユースケース 5: オンプレミスを Active Directory に拡張する AWS クラウド	50
ユースケース 6: ディレクトリを共有して、AWS アカウント間で Amazon EC2 インスタンスをドメインにシームレスに結合する	50
ディレクトリを維持する	51
ディレクトリ情報の表示	52
スナップショットを使用したディレクトリの復元	54
追加ドメインコントローラのデプロイ	60
AWS Managed Microsoft AD のアップグレード	64
代替 UPN サフィックスを追加する	66
ディレクトリのサイト名の変更	67
AWS Managed Microsoft AD の削除	68
ディレクトリをセキュリティで保護する	69

パスワードポリシーについて	70
多要素認証の有効化	76
Secure LDAP (LDAPS) の有効化	80
ディレクトリのコンプライアンスを管理する	94
ネットワークセキュリティの強化	96
ディレクトリセキュリティ設定の編集	109
AWS Private CA Connector for AD のセットアップ	120
ディレクトリをモニタリングする	124
ディレクトリのステータスを把握する	125
Amazon SNS でディレクトリステータスの通知の有効化	126
ディレクトリログについて	129
Amazon CloudWatch ログ転送の有効化	132
CloudWatch を使用してディレクトリをモニタリングする	136
Amazon CloudWatch ログ転送の無効化	140
Microsoft イベントビューアーによる DNS サーバーの監視	140
AWS アプリケーションとサービスへのアクセス	141
アプリケーションの互換性	142
AWS アプリケーションとサービスへのアクセス	144
へのアクセスの有効化 AWS Management Console	147
アクセス URL の作成	151
シングルサインオンの有効化	152
AWS リソースへのアクセスの許可	161
新しいロールの作成	162
既存のロールの信頼関係の編集	163
ユーザーまたはグループの既存のロールへの割り当て	164
ロールに割り当てられたユーザーとグループの表示	166
ユーザーまたはグループからのロールの削除	167
AWS 管理ポリシーの使用	168
マルチリージョンレプリケーションの設定	169
仕組み	170
利点	172
グローバル機能とリージョン機能	173
プライマリリージョンと追加のリージョン	174
レプリケートされたリージョンの追加	175
レプリケートされたリージョンの削除	178
ディレクトリの共有	178

主要なコンセプト	178
考慮事項	180
チュートリアル: AWS Managed Microsoft AD ディレクトリを共有する	181
ディレクトリの共有解除	193
Active Directory ユーザーの AWS Managed Microsoft AD への移行	194
既存の Active Directory インフラストラクチャに接続する	194
信頼関係の作成	194
IP ルートを追加する	201
チュートリアル: AWS Managed Microsoft AD と自己管理型 Active Directory ドメイン間で 信頼関係を作成する	202
チュートリアル: AWS Managed Microsoft AD ドメイン間に信頼関係を作成する	214
ディレクトリスキーマを拡張する	221
AWS Managed Microsoft AD スキーマを拡張するタイミング	221
チュートリアル: AWS Managed Microsoft AD スキーマの拡張	221
ディレクトリをインスタンスに結合する方法	229
ディレクトリ管理インスタンスを起動する	229
Windows インスタンスへの結合	233
Linux インスタンスとの結合	241
Mac インスタンスへの結合	296
ディレクトリ結合権限を委任する	298
DHCP オプションセットの作成または変更	301
ユーザーとグループの管理	303
AWS Management Console	303
AWS CLI	304
AWS Tools for PowerShell	305
オンプレミスまたは Amazon EC2 インスタンス	305
コンソール、CLI、または を使用してユーザーとグループを管理する PowerShell	306
Amazon EC2 インスタンスを使用してユーザーとグループを管理する	350
Directory Service Data	361
レプリケーションと整合性	362
AWS Directory Service Data 属性	363
グループタイプとグループスコープ	368
Microsoft Entra Connect Sync に接続する	370
前提条件	370
Active Directory のドメインユーザーを作成する	370
Entra Connect Sync のダウンロード	371

スクリプト PowerShell を実行	371
Entra Connect Sync をインストールする	373
AWS Managed Microsoft AD テストラボのチュートリアル	376
チュートリアル: 基本的な AWS Managed Microsoft AD テストラボをセットアップする	377
チュートリアル: AWS Managed Microsoft AD から EC2 へのセルフマネージド AD インス トールへの信頼を作成する	396
クォータ	408
トラブルシューティング	410
AWS Managed Microsoft AD の問題	410
Netlogon とセキュリティでセキュリティで保護されたチャネルでの通信に関する問題	410
ユーザーのパスワードをリセットしようとする、 「応答ステータス: 400 リクエストの失 敗」 エラーが表示されます。	411
パスワードの復旧	411
追加リソース	411
Amazon EC2 Linux インスタンスドメインの結合エラー	412
利用可能なストレージスペースの低下	415
スキーマ拡張のエラー	419
信頼作成ステータスの理由	422
AD Connector	427
入門	428
AD Connector の前提条件	428
AD Connector を作成する	444
AD Connector で作成されるもの	446
ベストプラクティス	447
セットアップ: 前提条件	447
アプリケーションをプログラミングする	449
ディレクトリを使用する	450
ディレクトリを維持する	450
ディレクトリ情報の表示	451
AD Connector の DNS アドレスを更新する	451
AD Connector を削除する	452
ディレクトリをセキュリティで保護する	453
多要素認証の有効化	454
クライアント側の LDAPS の有効化	456
IAM 認証を有効化する	463
AD Connector サービスアカウントの認証情報を更新する	472

AWS Private CA Connector for AD をセットアップする	473
ディレクトリをモニタリングする	475
ディレクトリのステータスを把握する	475
Amazon SNS でディレクトリステータスの通知を有効にする	477
AWS アプリケーションとサービスへのアクセス	479
アプリケーションの互換性	479
AD Connector から AWS アプリケーションとサービスへのアクセスを有効にする	481
Amazon EC2 インスタンスを Active Directory に結合する方法	483
クォータ	483
トラブルシューティング	484
作成に関する問題	484
接続の問題	486
認証問題	488
メンテナンスの問題	497
AD Connector を削除できない	498
AD Connector 発行者を調査するための一般的なツール	498
Simple AD	500
入門	501
Simple AD の前提条件	502
Simple AD を作成する	503
Simple AD で作成されるもの	507
ベストプラクティス	508
セットアップ: 前提条件	508
セットアップ: ディレクトリを作成する	510
アプリケーションをプログラミングする	511
ディレクトリを維持する	512
ディレクトリ情報の表示	512
DNS サーバーの設定	513
スナップショットでディレクトリの復元	513
Simple AD を削除する	516
ディレクトリをセキュリティで保護する	518
krbtgt アカウントのパスワードをリセットする	518
ディレクトリをモニタリングする	523
ディレクトリのステータスを把握する	523
Amazon Simple Notification Service によるディレクトリステータス通知の有効化	525
AWS アプリケーションとサービスへのアクセス	527

アプリケーションの互換性	528
AWS アプリケーションとサービスへのアクセス	529
AWS Management Consoleへのアクセスの有効化	530
アクセス URL の作成	533
シングルサインオンの有効化	534
ディレクトリへのインスタンスの結合	543
Windows インスタンスへの結合	544
Linux インスタンスを結合	552
ディレクトリ結合権限の委任	578
DHCP オプションセットを作成する	580
ユーザーとグループの管理	582
AD 管理ツールのインストール	583
ユーザーの作成	585
ユーザーの削除	587
ユーザーパスワードのリセット	588
グループの作成	590
ユーザーをグループに追加する	591
クォータ	593
トラブルシューティング	593
パスワードの復旧	594
Simple AD にユーザーを追加したとき、「KDC can't fulfill requested option」というエラー が表示される	594
ドメインに結合したインスタンスの、DNS 名または IP アドレスの更新 (DNS の動的更新) ができない	594
SQL Server のアカウントを使用して SQL Server にログインできない	594
Simple AD が「リクエスト済み」状態で止まっている	595
Simple AD を作成すると、「AZ constrained」エラーが表示される	595
一部のユーザーが Simple AD で認証できない	595
追加リソース	411
ディレクトリステータスメッセージのトラブルシューティング	596
セキュリティ	600
Identity and Access Management	601
認証	602
アクセスコントロール	602
アクセス管理の概要	602
AWS の 管理ポリシー AWS Directory Service	607

アイデンティティベースのポリシー (IAM ポリシー) の使用	609
AWS Directory Service API アクセス許可リファレンス	619
Directory Service Data の条件キー	621
を使用した AWS アプリケーションとサービスの認可 AWS Directory Service	628
Active Directory での AWS アプリケーションの認可	628
AWS Directory Service Data を使用したアプリケーション認可	629
ログ記録とモニタリング	631
AWS Directory Service ログ	631
AWS Directory Service データログ	634
コンプライアンス検証	644
耐障害性	645
インフラストラクチャセキュリティ	645
サービス間の混乱した代理の防止	646
AWS PrivateLink	650
考慮事項	650
可用性	650
Amazon VPC エンドポイントを作成する	651
エンドポイントポリシーを作成する	651
サービスレベルアグリーメント	654
利用可能なリージョン	655
Directory Service Data AWS リージョン でサポート	662
ブラウザの互換性	666
TLS とは何ですか?	666
IAM Identity Center でどの TLS バージョンがサポートされているか	666
サポートされている TLS バージョンをブラウザで有効にする方法	667
ドキュメント履歴	668
.....	dclxxii

とは AWS Directory Service

AWS Directory Service には、他の AWS サービスで Microsoft Active Directory (AD) を使用する複数の方法が用意されています。ディレクトリには、ユーザー、グループ、デバイスに関する情報が保存され、管理者はそれらを使用して情報とリソースへのアクセスを管理します。は、クラウド内の既存の Microsoft AD または Lightweight Directory Access Protocol (LDAP) 対応アプリケーションを使用するお客様に、複数のディレクトリの選択肢 AWS Directory Service を提供します。また、ユーザー、グループ、デバイス、アクセスを管理するディレクトリーが必要な開発者に、その選択肢を提供します。

AWS Directory Service オプション

AWS Directory Service には、選択できる複数のディレクトリタイプが含まれています。詳細については、次のいずれかのタブを選択してください。

AWS Directory Service for Microsoft Active Directory

AWS Managed Microsoft AD と呼ばれる AWS Directory Service for Microsoft Active Directory は、クラウド AWS でによって管理される実際の Microsoft Windows Server Active Directory (AD) AWS を使用します。これにより、さまざまな Active Directory 対応アプリケーションを AWS クラウドに移行できます。AWS マネージド Microsoft AD は Microsoft SharePoint、Microsoft SQL Server Always On 可用性グループ、および多くの .NET アプリケーションで動作します。また、「[Amazon WorkSpaces](#)」、「[Amazon WorkDocs](#)」、「[Amazon QuickSight](#)」、「[Amazon Chime](#)」、「[Amazon Connect](#)」、「[Amazon Relational Database Service for Microsoft SQL Server](#)」(Amazon RDS for SQL Server、Amazon RDS for Oracle、および Amazon RDS for PostgreSQL) などの AWS 管理アプリケーションおよびサービスもサポートしています。

AWS Managed Microsoft AD は、ディレクトリのコンプライアンスを有効にするときに、[米国の医療保険の相互運用性と説明責任に関する法律](#) (HIPAA) または [Payment Card Industry Data Security Standard](#) (PCI DSS) に準拠する、AWS クラウド内のアプリケーションに対して承認されています。https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_compliance.html

互換性のあるすべてのアプリケーションは、AWS Managed Microsoft AD に保存されたユーザー認証情報を使用して動作します。または、信頼された「[既存の AD インフラストラクチャに接続](#)

して」、オンプレミスや EC2 Windows で実行される Active Directory からの認証情報を使用することもできます。[EC2 インスタンスを AWS Managed Microsoft AD に参加](#)させると、ユーザーはオンプレミスネットワークのワークロードにアクセスする場合と同じ Windows シングルサインオン (SSO) エクスペリエンスで AWS クラウドの Windows ワークロードにアクセスできます。

AWS Managed Microsoft AD は、Active Directory 認証情報を使用したフェデレーティッドユースケースもサポートしています。Managed AWS Microsoft AD を使用すると、にサインインできます [AWS Management Console](#)。では [AWS IAM Identity Center](#)、AWS SDK および CLI で使用するための短期的な認証情報を取得し、事前設定された SAML 統合を使用して多くのクラウドアプリケーションにサインインすることもできます。Microsoft Entra Connect (以前はと呼ばれていました Azure Active Directory Connect) と、オプションで Active Directory Federation Service (AD FS) を追加することで、AWS Managed Microsoft AD に保存されている認証情報を使用して Microsoft Office 365 や他のクラウドアプリケーションにサインインできます。

このサービスには、[スキーマの拡張](#)や[パスワードポリシーの管理](#)、Secure Socket Layer (SSL)/Transport Layer Security (TLS) 経由の[安全な LDAP 通信の有効化](#)といった主要な機能が含まれています。[AWS Managed Microsoft AD の多要素認証 \(MFA\) を有効](#)にして、ユーザーがインターネットから AWS アプリケーションにアクセスするときにセキュリティレイヤーを追加することもできます。Active Directory は LDAP ディレクトリであるため、Linux Secure Shell (SSH) 認証や他の LDAP 対応アプリケーションにも、AWS Managed Microsoft AD を使用できます。

AWS は、サービスの一部としてモニタリング、日次スナップショット、リカバリを提供します。Managed [Microsoft AD にユーザーとグループを追加し、AWS](#) Managed Microsoft AD AWS ドメインに参加している Windows コンピュータで実行されている使い慣れた Active Directory ツールを使用してグループポリシーを管理します。また、[ドメインコントローラーを追加でデプロイ](#)してディレクトリをスケールし、より多くのドメインコントローラー間でリクエストを分散させることで、アプリケーションのパフォーマンスを向上させることもできます。

AWS Managed Microsoft AD は、Standard と Enterprise の 2 つのエディションで利用できます。

- Standard Edition: AWS Managed Microsoft AD (Standard Edition) は、従業員数が 5,000 名までの、中小企業向けのプライマリディレクトリとして最適化されています。ユーザー、グループ、コンピュータなど、最大 30,000* のディレクトリオブジェクトをサポートするために十分なストレージ容量を提供します。
- Enterprise Edition: AWS Managed Microsoft AD (Enterprise Edition) は、最大 500,000* のディレクトリオブジェクトをサポートする、エンタープライズ組織向けに設計されています。

* 上限数は概数です。ディレクトリでサポートできるディレクトリオブジェクトの数は、オブジェクトのサイズ、アプリケーションの動作やパフォーマンスニーズに応じて増減する場合があります。

どのようなときに使うか

AWS Managed Microsoft AD は、Amazon Relational Database Service for など、AWS アプリケーションやWindowsワークロードをサポートするために実際のActive Directory機能が必要な場合に最適ですMicrosoft SQL Server。また、クラウドActive Directoryで Office 365 をサポートするスタンドアロン AWS が必要な場合や、Linux アプリケーションをサポートする LDAP ディレクトリが必要な場合にも最適です。詳細については、「[AWS Managed Microsoft AD](#)」を参照してください。

AD Connector

AD Connector は、Amazon WorkSpaces、Amazon QuickSight、Windows Serverインスタンス用の [Amazon EC2](#) などの互換性のある AWS アプリケーションを既存のオンプレミス Microsoft に簡単に接続できるプロキシサービスですActive Directory。AD Connector によって、Active Directory に簡単に[1つのサービスアカウントを追加](#)できます。AD Connector を使用すると、ディレクトリを同期化する必要がなくなり、フェデレーションインフラストラクチャをホストするコストや複雑さからも解放されます。

Amazon QuickSight などの AWS アプリケーションにユーザーを追加すると、AD Connector は既存の を読み取りActive Directory、選択するユーザーとグループのリストを作成します。ユーザーが AWS アプリケーションにログインすると、AD Connector はサインインリクエストをオンプレミスのActive Directoryドメインコントローラーに転送して認証を行います。AD Connector は、[Amazon WorkSpaces](#)、[Amazon WorkDocs](#)、Amazon [Amazon QuickSight Chime](#)、[Amazon Connect](#)、[Amazon WorkMail](#) など、多くの AWS アプリケーションやサービスと連携します。「[シームレスなドメイン結合](#)」により、AD Connector 経由で、オンプレミスの Active Directory ドメインに「[EC2 Windows インスタンスを結合させる](#)」こともできます。AD Connector では、ユーザーは既存のActive Directory認証情報でログインして にアクセスし AWS Management Console 、 AWS リソースを管理できます。AD Connector は RDS SQL Server との互換性はありません。

AD Connector を使用して、既存の RADIUS ベースの MFA インフラストラクチャに接続することで、AWS アプリケーションユーザーの[多要素認証 \(MFA\) を有効にする](#)こともできます。これにより、ユーザーが AWS アプリケーションにアクセスするときに、別のセキュリティレイヤーが追加されます。

AD Connector を使用すると、Active Directory を、引き続き現在と同じ方法で管理できます。例えば、新しいユーザーとグループの追加、パスワードの更新は、すべてのオンプレミス Active Directory で標準の Active Directory 管理ツールを使用して行います。これにより、ユーザーがオンプレミスまたは AWS クラウドのリソースにアクセスしているかどうかにかかわらず、パスワードの有効期限、パスワード履歴、アカウントロックアウトなどのセキュリティポリシーを一貫して適用できます。

どのようなときに使うか

AD Connector は、互換性のある AWS サービスで既存のオンプレミスディレクトリを使用する場合に最適です。詳細については、「[AD Connector](#)」を参照してください。

Simple AD

Simple AD は、Samba 4 にサポートされた AWS Directory Service からの、Microsoft Active Directory との互換性があるディレクトリです。Simple AD は、ユーザーアカウント、グループメンバーシップ、Linux ドメインまたは Windows ベースの EC2 インスタンスの結合、Kerberos ベースの SSO、グループポリシーなどの基本的な Active Directory 機能をサポートしています。は、サービスの一部としてモニタリング、毎日のスナップショット、リカバリ AWS を提供します。

Simple AD はクラウド内のスタンドアロンなディレクトリです。ユーザー ID の作成や管理、アプリケーションへのアクセスの管理を行います。基本的な Active Directory の機能が必要な、多くの使い慣れた Active Directory 対応のアプリケーションやツールを使用できます。Simple AD は、[Amazon WorkSpaces](#)、[Amazon WorkDocs](#)、[Amazon QuickSight](#)、[Amazon WorkMail](#) の各 AWS アプリケーションと互換性があります。Simple AD ユーザーアカウントと AWS Management Console を使用してサインインし、AWS リソースを管理することもできます。

Simple AD は、Multi-Factor Authentication (MFA)、信頼関係、DNS 動的更新、スキーマ拡張、LDAPS を介した通信、PowerShell AD コマンドレット、または FSMO ロールの転送は、サポートしていません。Simple AD は RDS SQL Server との互換性はありません。実際の の機能を必要とするお客様 Microsoft Active Directory、または RDS SQL Server でディレクトリを使用することを想定しているお客様は、代わりに AWS Managed Microsoft AD を使用する必要があります。Simple AD を使用するときは、必要なアプリケーションが Samba 4 と完全な互換性があることを、事前に確認してください。詳細については、<https://www.samba.org> を参照してください。

どのようなときに使うか

Simple AD をクラウドのスタンドアロンディレクトリとして使用して、基本Active Directory機能、互換性のある AWS アプリケーションを必要とするWindowsワークロードをサポートしたり、LDAP サービスを必要とする Linux ワークロードをサポートしたりできます。詳細については、「[Simple AD](#)」を参照してください。

リージョンごとにサポートされているディレクトリタイプのリストについては、「[のリージョンの可用性 AWS Directory Service](#)」を参照してください。

オプションの選択

ニーズに最適な機能とスケーラビリティを提供するディレクトリサービスを選択できます。次の表は、組織に最適な AWS Directory Service ディレクトリオプションを決定するのに役立ちます。

目的	推奨 AWS Directory Service オプション
クラウドでのアプリケーションで、Active Directory または LDAP が必要	Active Directory 対応のワークロード、または Amazon WorkSpaces や Amazon QuickSight などの AWS アプリケーションおよびサービスをサポートする AWS クラウド内の実際の Microsoft Active Directory が必要、または、Linux アプリケーション向けの LDAP サポートが必要な場合、[AWS Directory Service for Microsoft Active Directory] (Standard Edition または Enterprise Edition) を使用してください。 オンプレミスユーザーがActive Directory認証情報を使用して AWS アプリケーションやサービスにログインすることのみを許可する場合は、AD Connector を使用します。AD Connector を使用して Amazon EC2 インスタンスを既存の Active Directory ドメインに結合することもできます。 Samba 4 互換アプリケーションをサポートする、基本的な Active Directory 互換性を持つ低スケール、低コストのディレクトリが必要な場合、または LDAP 対応アプリケーションに LDAP との互換性を対応する必要がある場合は、[Simple AD] を使用します。

目的	推奨 AWS Directory Service オプション
SaaS アプリケーションを開発する	高スケーラの SaaS アプリケーションを開発する場合、サブスクライバーを管理および認証するために、ソーシャルメディア ID に対応しているスケーラブルなディレクトリが必要なときは、Amazon Cognito を使用します。

AWS Directory Service ディレクトリオプションの詳細については、[「ソリューションの選択方法 Active DirectoryAWS」](#)を参照してください。

Amazon EC2 の操作

AWS Directory Serviceを使用するときは、Amazon EC2 の基本を理解することが重要です。最初に次のトピックを読むことをお勧めします。

- 「Amazon VPC ユーザーガイド」の「[Amazon EC2 とは](#)」。
- 「Amazon EC2 ユーザーガイド」の「[Amazon EC2 インスタンスの起動](#)」
- 「Amazon EC2 ユーザーガイド」の「[EC2 インスタンスの Amazon EC2 セキュリティグループ](#)」
- 「Amazon VPC ユーザーガイド」の「[Amazon VPC とは?](#)」。
- 「Amazon VPC ユーザーガイド」の「[AWS Virtual Private Networkを使用して VPC をリモートネットワークに接続する](#)」。

AWS Managed Microsoft AD

AWS Directory Service では Microsoft Active Directory、(AD) をマネージドサービスとして実行できます。Microsoft Active Directory 用 AWS ディレクトリサービスは Managed AWS Microsoft AD と呼ばれ、Windows Server 2019 を利用しています。このディレクトリタイプを選択して起動すると、仮想プライベートクラウド (Amazon VPC) に接続されたドメインコントローラーの可用性が高いペアとして作成されます。各ドメインコントローラーは、お客様が選択するリージョンの異なるアベイラビリティゾーンで実行されます。ホストのモニタリングと復旧、データレプリケーション、スナップショット、およびソフトウェアの更新は自動的に設定および管理されます。

AWS Managed Microsoft AD を使用すると、Microsoft SharePoint やカスタム .NET および SQL Server ベースのアプリケーションなど、ディレクトリ対応のワークロードを AWS クラウドで実行できます。AWS クラウド内の AWS Managed Microsoft AD と既存のオンプレミス Microsoft との間の信頼関係を設定して Active Directory、を使用して、ユーザーとグループにいずれかのドメインのリソースへのアクセスを許可することもできます AWS IAM Identity Center。

AWS Directory Service を使用すると、AWS クラウドでディレクトリを簡単にセットアップして実行したり、リソースを AWS 既存のオンプレミス Microsoft に接続したりできます Active Directory。ディレクトリを作成すると、次のようなさまざまなタスクに使用できます。

- ユーザーとグループを管理する
- アプリケーションとサービスでシングルサインオンを可能にする
- グループポリシーを作成し適用する
- クラウドベースの Linux および Microsoft Windows ワークロードのデプロイと管理を簡単にする
- AWS Managed Microsoft AD を使用して、既存の RADIUS ベースの MFA インフラストラクチャと統合することで多要素認証を有効にし、ユーザーが AWS アプリケーションにアクセスするときに追加のセキュリティレイヤーを提供できます。
- Amazon EC2 Linux および Windows インスタンスに安全に接続する

Note

AWS は Windows サーバーインスタンスのライセンスを管理します。必要なのは、使用するインスタンスの料金だけです。アクセスは料金に含まれているため、追加の Windows Server クライアントアクセスライセンス (CAL) を購入する必要はありません。各インスタンスには、管理者用の 2 つのリモート接続が付属しています。3 つ以上の接続が必要な場合、

または管理者以外の目的でこれらの接続が必要な場合は、AWSで使用するために Remote Desktop Services CAL を追加する必要があることがあります。

このセクションのトピックを読んで、AWS Managed Microsoft AD ディレクトリの作成、AWS Managed Microsoft AD とオンプレミスディレクトリ間の信頼関係の作成、AWS Managed Microsoft AD スキーマの拡張を開始します。

トピック

- [AWS Managed Microsoft AD の開始方法](#)
- [AWS Managed Microsoft AD の主要なコンセプトとベストプラクティス](#)
- [AWS Managed Microsoft AD のユースケース](#)
- [AWS Managed Microsoft AD を維持する](#)
- [AWS Managed Microsoft AD を保護する](#)
- [AWS Managed Microsoft AD のモニタリング](#)
- [AWS Managed Microsoft AD から AWS アプリケーションとサービスへのアクセス](#)
- [AWS Managed Microsoft AD ユーザーとグループに IAM ロールを持つリソースへのアクセス権 AWS を付与する](#)
- [AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#)
- [AWS Managed Microsoft AD を共有する](#)
- [Active Directory ユーザーの AWS Managed Microsoft AD への移行](#)
- [AWS Managed Microsoft AD を既存の Active Directory インフラストラクチャに接続する](#)
- [AWS Managed Microsoft AD スキーマを拡張する](#)
- [Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法](#)
- [AWS Managed Microsoft AD でのユーザーとグループの管理](#)
- [AWS Directory Service データ](#)
- [AWS Managed Microsoft AD を に接続する Microsoft Entra Connect Sync](#)
- [AWS Managed Microsoft AD テストラボのチュートリアル](#)
- [AWS Managed Microsoft AD のクォータ](#)
- [AWS Managed Microsoft AD のトラブルシューティング](#)

関連する AWS セキュリティブログ記事

- [AWS Managed Microsoft AD ディレクトリの管理をオンプレミスActive Directoryユーザーに委任する方法](#)
- [AWS Directory Service for AWS Managed Microsoft AD を使用して、セキュリティ基準を満たすためにさらに強力なパスワードポリシーを設定する方法](#)
- [ドメインコントローラーを追加して AWS Directory Service 、 for AWS Managed Microsoft AD の冗長性とパフォーマンスを向上させる方法](#)
- [AWS Managed Microsoft AD にリモートデスクトップライセンスマネージャーをデプロイして Microsoft リモートデスクトップの使用を有効にする方法](#)
- [AWS Managed Microsoft AD とオンプレミス認証情報 AWS Management Console を使用して にアクセスする方法](#)
- [AWS Managed Microsoft AD とオンプレミス認証情報を使用して AWS サービスの多要素認証を有効にする方法](#)
- [オンプレミスを使用して AWS サービスに簡単にログインする方法 Active Directory](#)

AWS Managed Microsoft AD の開始方法

AWS Managed Microsoft AD AWS クラウド は、 Microsoft Active Directoryでフルマネージド型 を作成し、WindowsServer 2019 を搭載し、2012 R2 フォレストおよびドメインの機能レベルで動作します。AWS Managed Microsoft AD でディレクトリを作成すると、 は 2 つのドメインコントローラー AWS Directory Service を作成し、ユーザーに代わって DNS サービスを追加します。ドメインコントローラーは、1 つの Amazon VPC の異なるサブネットに作成されます。この冗長性により、障害が発生してもディレクトリに確実にアクセスできます。さらに追加のドメインコントローラーが必要になれば、後で追加できます。詳細については、「[AWS Managed Microsoft AD に追加するドメインコントローラーのデプロイ](#)」を参照してください。

AWS Managed Microsoft AD のデモと概要については、次のYouTube動画を参照してください。

[AWS Managed Microsoft AD のデモと概要](#)

トピック

- [AWS Managed Microsoft AD を作成するための前提条件](#)
- [AWS IAM Identity Center 前提条件](#)
- [Multi-Factor Authentication の前提条件](#)
- [AWS Managed Microsoft AD の作成](#)
- [AWS Managed Microsoft AD で作成されるもの](#)

- [AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#)

AWS Managed Microsoft AD を作成するための前提条件

AWS Managed Microsoft AD を作成するにはActive Directory、以下を含む Amazon VPC が必要です。

- 少なくとも 2 つのサブネット。各サブネットはそれぞれ異なるアベイラビリティーゾーンにある必要があります。
- VPC にはデフォルトのハードウェアテナンシーが必要です。
- 198.18.0.0/15 アドレス空間のアドレスを使用して VPC に AWS Managed Microsoft AD を作成することはできません。

AWS Managed Microsoft AD ドメインを既存のオンプレミスActive Directoryドメインと統合する必要がある場合は、オンプレミスドメインのフォレストとドメインの機能レベルを Windows Server 2003 以上に設定する必要があります。

AWS Directory Service は 2 つの VPC 構造を使用します。ディレクトリを構成する EC2 インスタンスは、AWS アカウント外で実行され、によって管理されます AWS。これらには、2 つのネットワークアダプタ (ETH0 および ETH1) があります。ETH0 は管理アダプタで、アカウント外部に存在します。ETH1 はアカウント内で作成されます。

ディレクトリの ETH0 ネットワークの管理 IP 範囲は 198.18.0.0/15 です。

AWS 環境と AWS Managed Microsoft AD を作成する方法のチュートリアルについては、「」を参照してください[AWS Managed Microsoft AD テストラボのチュートリアル](#)。

AWS IAM Identity Center 前提条件

AWS Managed Microsoft AD で IAM Identity Center を使用する予定がある場合は、以下が満たされていることを確認する必要があります。

- AWS Managed Microsoft AD ディレクトリは AWS 、組織の管理アカウントで設定されます。
- IAM Identity Center のインスタンスは、AWS Managed Microsoft AD ディレクトリがセットアップされているのと同じリージョンにあります。

詳細については、AWS IAM Identity Center ユーザーガイドの「[IAM Identity Center prerequisites](#)」を参照してください。

Multi-Factor-Authentication の前提条件

AWS Managed Microsoft AD ディレクトリで多要素認証をサポートするには、次の方法でオンプレミスまたはクラウドベースの [Remote Authentication Dial-In User Service \(RADIUS\)](#) サーバーを設定して、の AWS Managed Microsoft AD ディレクトリからのリクエストを受け入れる必要があります AWS。

1. RADIUS サーバーで、両方の AWS Managed Microsoft AD ドメインコントローラー (DCs) を表す 2 つの RADIUS クライアントを作成します AWS。次の一般的なパラメータ (RADIUS サーバーが異なる場合があります) を使用して両方のクライアントを設定する必要があります。
 - アドレス (DNS または IP): これは AWS Managed Microsoft AD DCs。どちらの DNS アドレスも、MFA を使用する予定の AWS Managed Microsoft AD ディレクトリの詳細ページの AWS Directory Service Console にあります。表示される DNS アドレスは、で使用される両方の AWS Managed Microsoft AD DCs の IP アドレスを表します AWS。

Note

RADIUS サーバーが DNS アドレスをサポートしている場合は、RADIUS クライアント設定を 1 つだけ作成する必要があります。それ以外の場合は、AWS Managed Microsoft AD DC ごとに 1 つの RADIUS クライアント設定を作成する必要があります。

- ポート番号: RADIUS サーバーが RADIUS クライアント接続を受け付けるポート番号を設定します。標準の RADIUS ポートは 1812 です。
 - 共有シークレット: RADIUS サーバーの RADIUS クライアントとの接続に使用される共有シークレットを入力または生成します。
 - プロトコル: AWS Managed Microsoft AD DCs と RADIUS サーバーの間で認証プロトコルを設定する必要がある場合があります。サポートされているプロトコルは、PAP、CHAP MS-CHAPv1、および MS-CHAPv2 です。非常に強力な 3 つのオプションのセキュリティを用意している MS-CHAPv2 を推奨します。
 - アプリケーション名: これは一部の RADIUS サーバーでは必須ではなく、通常はメッセージまたはレポートでアプリケーションを識別します。
2. RADIUS クライアント (AWS マネージド Microsoft AD DCsDNS アドレス、ステップ 1 を参照) から RADIUS サーバーポートへのインバウンドトラフィックを許可するように既存のネットワークを設定します。
 3. AWS Managed Microsoft AD ドメインの Amazon EC2 セキュリティグループに、前に定義した RADIUS サーバーの DNS アドレスとポート番号からのインバウンドトラフィックを許可するルー

ルを追加します。詳細については、「EC2 ユーザーガイド」の「[セキュリティグループへのルールの追加](#)」を参照してください。

MFA で AWS Managed Microsoft AD を使用方法の詳細については、「」を参照してください [AWS Managed Microsoft AD の多要素認証の有効化](#)。

AWS Managed Microsoft AD の作成

新しい AWS Managed Microsoft AD を作成するには Active Directory、次の手順を実行します。この手順を開始する前に、「[AWS Managed Microsoft AD を作成するための前提条件](#)」で定義されている前提条件を満たしていることを確認します。

AWS Managed Microsoft AD を作成するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ)、[Set up directory] (ディレクトリの設定) の順に選択します。
2. [Select directory type] (ディレクトリタイプの選択) ページで [AWS Managed Microsoft AD] を選択してから、[Next] (次へ) をクリックします。
3. [Enter directory information] (ディレクトリ情報の入力) ページに、以下の情報を指定します。

エディション

AWS Managed Microsoft AD の Standard Edition または Enterprise Edition から選択します。エディションの詳細については、「[AWS Directory Service for Microsoft Active Directory](#)」を参照してください。

[Directory DNS name] (ディレクトリの DNS 名)

ディレクトリの完全修飾名 (例: corp.example.com)。

Note

DNS に Amazon Route 53 を使用する予定の場合、AWS Managed Microsoft AD のドメイン名は Route 53 ドメイン名とは異なる必要があります。Route 53 と AWS Managed Microsoft AD が同じドメイン名を共有している場合、DNS 解決の問題が発生する可能性があります。

[Directory NetBIOS name] (ディレクトリの NetBIOS 名)

ディレクトリの短縮名 (例: CORP)。

[Directory description] (ディレクトリの説明)

必要に応じて、ディレクトリの説明。この説明は、AWS Managed Microsoft AD の作成後に変更できます。

管理者パスワード

ディレクトリ管理者のパスワードです。ディレクトリの作成プロセスでは、ユーザー名 Admin とこのパスワードを使用して管理者アカウントが作成されます。AWS Managed Microsoft AD の作成後に管理者パスワードを変更できます。

パスワードには、「admin」という単語を含めることはできません。

ディレクトリ管理者のパスワードは大文字と小文字が区別され、8 文字以上 64 文字以下の長さにする必要があります。また、次の 4 つのカテゴリうち 3 つから少なくとも 1 文字を含める必要があります。

- 小文字 (a～z)
- 大文字 A～Z
- 数字 (0～9)
- アルファベットと数字以外の文字 (~!@#\$%^&*_-+=`|\(){}[];'"<>.,?/)

[Confirm password] (パスワードを確認)

管理者のパスワードをもう一度入力します。

(オプション) ユーザーとグループの管理

から AWS Managed Microsoft AD のユーザーとグループの管理を有効にするには AWS Management Console、でユーザーとグループの管理を選択します AWS Management Console。ユーザーおよびグループ管理の使用方法的詳細については、「[the section called “コンソール、CLI、またはを使用してユーザーとグループを管理する PowerShell”](#)」を参照してください。

4. [Choose VPC and subnets] (VPC とサブネットの選択) ページで、次の情報を指定して [Next] (次へ) をクリックします。

[VPC]

ディレクトリ用の VPC。

[Subnets] (サブネット)

ドメインコントローラーのサブネットを選択します。2 つのサブネットは、異なるアベイラビリティゾーンに存在している必要があります。

5. [Review & create] (確認と作成) ページでディレクトリ情報を確認し、必要に応じて変更を加えます。情報が正しい場合は、[Create directory] (ディレクトリの作成) を選択します。ディレクトリの作成所要時間は 20～40 分です。作成が完了すると、[Status] (ステータス) 値が [Active] (アクティブ) に変わります。

AWS Managed Microsoft AD で作成される内容の詳細については、以下を参照してください。

- [AWS Managed Microsoft AD で作成されるもの](#)
- [AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#)

AWS Managed Microsoft AD で作成されるもの

AWS Managed Microsoft AD Active Directoryで を作成すると、 はユーザーに代わって次のタスク AWS Directory Service を実行します。

- Elastic Network Interface (ENI) を自動作成し、各ドメインコントローラーと関連付けます。これらの各 ENIs は VPC と AWS Directory Service ドメインコントローラー間の接続に不可欠であり、削除しないでください。で使用するために予約されているすべてのネットワークインターフェイスは、「ディレクトリ directory-id 用にAWS 作成されたネットワークインターフェイス」という説明 AWS Directory Service で識別できます。詳細については、「Amazon EC2 ユーザーガイド」の「[Elastic Network Interface](#)」を参照してください。AWS Managed Microsoft AD のデフォルトの DNS サーバーActive Directoryは、Classless Inter-Domain Routing (CIDR)+2 の VPC DNS サーバーです。詳細については、「Amazon VPC ユーザーガイド」の「[Amazon DNS サーバー](#)」を参照してください。

Note

ドメインコントローラーは、デフォルトでリージョン内の 2 つのアベイラビリティゾーンにまたがってデプロイされ、Amazon VPCloud (VPC) に接続されます。バックアップは

1 日に 1 回自動的に実行され、Amazon EBS (EBS) ボリュームは保管中のデータを保護するために暗号化されます。障害が発生したドメインコントローラーは、同じ IP アドレスを使用して同じアベイラビリティゾーン内で自動的に置き換えられ、最新のバックアップを使用して完全な災害対策を実行できます。

- 耐障害性と高可用性を確保するために、2 つのドメインコントローラーを使用して VPC 内に Active Directory をプロビジョニングします。ディレクトリが正常に作成されて [Active](#) になった後で、回復性とパフォーマンスを高めるためにドメインコントローラーを追加でプロビジョニングできます。詳細については、「[AWS Managed Microsoft AD に追加するドメインコントローラーのデプロイ](#)」を参照してください。

Note

AWS では、AWS Managed Microsoft AD ドメインコントローラーにモニタリングエージェントをインストールすることはできません。

- ドメインコントローラーに出入りするトラフィックのネットワークルールを確立する[AWS セキュリティグループ](#) `sg-1234567890abcdef0` を作成します。デフォルトのアウトバウンドルールは、すべての IPv4 アドレスへのすべてのトラフィックを許可します。デフォルトのインバウンドルールでは、AWS Managed Microsoft AD の VPC ホスティングに関連付けられたプライマリ IPv4 CIDR ブロック Active Directory からに必要なポート経由のトラフィックのみが許可されます。セキュリティを強化するため、作成された ENI には Elastic IP がアタッチされず、これらの ENI に Elastic IP をアタッチするためのアクセス許可はユーザーに付与されません。したがって、デフォルトで AWS Managed Microsoft AD と通信できるインバウンドトラフィックはローカル VPC のみです。セキュリティグループのルールを変更して、VPN 経由で到達可能な他のピア接続された VPCs や CIDRs など、追加のトラフィックソースを許可できます。これらのルールを変更すると、ドメインコントローラーと通信できなくなる可能性があるため、変更する場合は細心の注意を払ってください。詳細については、「[AWS Managed Microsoft AD のベストプラクティス](#)」および「[AWS Managed Microsoft AD ネットワークセキュリティ設定の強化](#)」を参照してください。

[プレフィックスリスト](#)を使用して、セキュリティグループルール内の CIDR ブロックを管理できます。プレフィックスリストを使用すると、セキュリティグループとルートテーブルの管理と設定が容易になります。複数の CIDR ブロックを同じポートとプロトコルに統合して、ネットワークトラフィックをスケーリングできます。

- Windows 環境では、クライアントは[サーバーメッセージブロック \(SMB\)](#) またはポート 445 を介して通信することがよくあります。このプロトコルは、ファイルとプリンターの共有や一般的なネットワーク通信など、さまざまなアクションを容易にします。AWS Managed Microsoft AD

ドメインコントローラーの管理インターフェイスへのクライアントトラフィックがポート 445 に表示されます。

このトラフィックは、SMB クライアントが DNS (ポート 53) と NetBIOS (ポート 138) の名前解決に依存して AWS Managed Microsoft AD ドメインリソースを見つけるときに発生します。これらのクライアントは、ドメインリソースを見つけるときに、ドメインコントローラーで可能なインターフェイスに転送されます。この動作は想定されており、多くの場合、複数のネットワークアダプターを持つ環境で発生し、[SMB マルチチャネル](#)を使用すると、クライアントはパフォーマンスと冗長性を向上させるために異なるインターフェイス間で接続を確立できます。

デフォルトでは、次の AWS セキュリティグループルールが作成されます。

インバウンドルール

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
ICMP	該当なし	AWS Managed Microsoft AD VPC IPv4 CIDR	Ping	LDAP キープアライブ、DFS
TCP と UDP	53	AWS Managed Microsoft AD VPC IPv4 CIDR	DNS	ユーザーとコンピュータの認証、名前解決、信頼
TCP と UDP	88	AWS Managed Microsoft AD VPC IPv4 CIDR	Kerberos	ユーザーとコンピュータの認証、フォレストレベルの信頼
TCP と UDP	389	AWS Managed Microsoft AD VPC IPv4 CIDR	LDAP	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directoryの使用
TCP と UDP	445	AWS Managed Microsoft AD VPC IPv4 CIDR	SMB / CIFS	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP と UDP	464	AWS Managed Microsoft AD VPC IPv4 CIDR	Kerberos パスワードの変更 / 設定	レプリケーション、ユーザーとコンピュータの認証、信頼
TCP	135	AWS Managed Microsoft AD VPC IPv4 CIDR	レプリケーション	RPC、EPM
TCP	636	AWS Managed Microsoft AD VPC IPv4 CIDR	LDAP SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	1024-65535	AWS Managed Microsoft AD VPC IPv4 CIDR	RPC	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	3268 - 3269	AWS Managed Microsoft AD VPC IPv4 CIDR	LDAP GC および LDAP GC SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directoryの使用
UDP	123	AWS Managed Microsoft AD VPC IPv4 CIDR	Windows タイム	Windows タイム、信頼
UDP	138	AWS Managed Microsoft AD VPC IPv4 CIDR	DFSN と NetLogon	DFS、グループポリシー
すべて	すべて	AWS がドメインコントローラー用に作成したセキュリティグループ (<i>sg-1234567890abcde f0</i>)	すべてのトラフィック	

アウトバウンドルール

プロトコル	ポート範囲	送信先	トラフィックの種類	Active Directoryの使用
すべて	すべて	0.0.0.0/0	すべてのトラフィック	

- Active Directory で使用されるポートおよびプロトコルの詳細については、Microsoft ドキュメント内の「[サービス概要および Windows のネットワークポート要件](#)」を参照してください。
- 「Admin」というユーザー名と指定されたパスワードを使用して、ディレクトリ管理者アカウントを作成します。このアカウントは にあります Users OU (例: Corp > Users)。このアカウントを使用して、 のディレクトリを管理します AWS クラウド。詳細については、「[AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#)」を参照してください。

⚠ Important

このパスワードは必ず保存してください。このパスワードは保存 AWS Directory Service されず、取得できません。ただし、パスワードは AWS Directory Service コンソールからリセットすることも、[ResetUserPassword](#) API を使用してリセットすることもできます。

- ドメインのルートに次の 3 つの組織単位 (OU) を作成します。

OU 名	説明
AWS Delegated Groups	AWS 特定のアクセス許可をユーザーに委任するために使用できるすべてのグループを保存します。
AWS Reserved	すべての AWS 管理固有のアカウントを保存します。
<yourdomainname>	この OU の名前は、ディレクトリの作成時に入力した NetBIOS 名に基づきます。NetBIOS 名を指定しなかった場合、デフォルトで、Directory DNS 名の最初の部分が使用されます (例えば、corp.example.com の場合、NetBIOS 名は corp となります)。この OU は、によって所有 AWS され、AWS 関連するすべてのディレクトリオブジェクトが含まれており、フルコントロールが付与されます。デフォルトでは、この OU の下に 2 つの子 OU (Computers および Users) が存在します。例: • Corp • Computers • Users

- に次のグループを作成します AWS Delegated Groups OU。

グループ名	説明
AWS Delegated Account Operators	このセキュリティグループのメンバーには、パスワードのリセットなどの限定されたアカウント管理機能が付与されています。
AWS Delegated Active Directory Based Activation Administrators	このセキュリティグループのメンバーは、Active Directory ポリウムライセンスアクティベーションオブジェクトを作成できます。これにより、エンタープライズはドメインへの接続を介してコンピュータをアクティベートできます。
AWS Delegated Add Workstations To Domain Users	このセキュリティグループのメンバーは、10台のコンピュータをドメインに参加させることができます。
AWS Delegated Administrators	このセキュリティグループのメンバーは、AWS Managed Microsoft AD を管理し、OU 内のすべてのオブジェクトを完全に制御し、に含まれるグループを管理できますAWS Delegated Groups OU。
AWS Delegated Allowed to Authenticate Objects	このセキュリティグループのメンバーには、のコンピュータリソースに対して認証する機能が提供されます AWS Reserved OU (選択的認証が有効な Trusts を持つオンプレミスオブジェクトにのみ必要です)。
AWS Delegated Allowed to Authenticate to Domain Controllers	このセキュリティグループのメンバーには、のコンピュータリソースに対して認証する機能が提供されます Domain Controllers OU (選択的認証が有効な Trusts を持つオンプレミスオブジェクトにのみ必要です)。

グループ名	説明
AWS Delegated Deleted Object Lifetime Administrators	このセキュリティグループのメンバーは、削除されたmsDS-DeletedObjectLifetimeオブジェクトを AD ごみ箱から復旧できる期間を定義する オブジェクトを変更できます。
AWS Delegated Distributed File System Administrators	このセキュリティグループのメンバーは、FRS、DFS-R、DFS の名前空間を追加および削除できます。
AWS Delegated Domain Name System Administrators	このセキュリティグループのメンバーは、Active Directory に統合された DNS を管理できます。
AWS Delegated Dynamic Host Configuration Protocol Administrators	このセキュリティグループのメンバーは、エンタープライズ内の Windows DHCP サーバーを承認できます。
AWS Delegated Enterprise Certificate Authority Administrators	このセキュリティグループのメンバーは、Microsoft Enterprise Certificate Authority インフラストラクチャをデプロイおよび管理できます。
AWS Delegated Fine Grained Password Policy Administrators	このセキュリティグループのメンバーは、作成済みの詳細なパスワードポリシーを変更できます。
AWS Delegated FSx Administrators	このセキュリティグループのメンバーは、Amazon FSx リソースを管理できます。
AWS Delegated Group Policy Administrators	このセキュリティグループのメンバーは、グループポリシー管理タスク (作成、編集、削除、リンク) を実行できます。
AWS Delegated Kerberos Delegation Administrators	このセキュリティグループのメンバーは、コンピュータおよびユーザーアカウントオブジェクトに対する委任を有効にすることができます

グループ名	説明
AWS Delegated Managed Service Account Administrators	このセキュリティグループのメンバーは、マネージド型サービスアカウントを作成および削除できます。
AWS Delegated MS-NPRC Non-Compliant Devices	このセキュリティグループのメンバーは、ドメインコントローラーとの安全なチャネル通信を行う必要はありません。このグループはコンピュータアカウント用です。
AWS Delegated Remote Access Service Administrators	このセキュリティグループのメンバーは、RAS および IAS サーバークラスに対して RAS サーバークラスを追加および削除できます。
AWS Delegated Replicate Directory Changes Administrators	このセキュリティグループのメンバーは、Active Directory のプロファイル情報を SharePoint Server と同期できます。
AWS Delegated Server Administrators	このセキュリティグループのメンバーは、すべてのドメイン参加済みコンピュータのローカル管理者グループに含まれます。
AWS Delegated Sites and Services Administrators	このセキュリティグループのメンバーは、Active Directory のサイトとサービスで Default-First-Site-Name オブジェクトの名前を変更できます。
AWS Delegated System Management Administrators	このセキュリティグループのメンバーは、システムマネジメントコンテナ内のオブジェクトを作成および管理できます。
AWS Delegated Terminal Server Licensing Administrators	このセキュリティグループのメンバーは、ターミナルサーバークラスライセンスサーバークラスに属するターミナルサーバークラスライセンスサーバークラスを追加および削除できます。

グループ名	説明
AWS Delegated User Principal Name Suffix Administrators	このセキュリティグループのメンバーは、ユーザープリンシパル名のサフィックスを追加および削除できます。

 Note

これらの に を追加できますAWS Delegated Groups。

- 次のグループポリシーオブジェクト (GPO) を作成して適用します。

 Note

これらの GPO を削除、変更、またはリンク解除するアクセス許可がありません。これは AWS、使用のために予約されているため、設計上です。必要に応じて、制御している OU にそれらをリンクできます。

グループポリシー名	適用対象	説明
Default Domain Policy	ドメイン	ドメインパスワードと Kerberos ポリシーが含まれます。
ServerAdmins	ドメインコントローラー以外のすべてのコンピュータアカウント	のメンバー'AWS Delegated Server Administrators'としてを追加しますBUILTIN\Administrators Group。
AWS Reserved Policy\User	AWS Reserved user accounts	のすべてのユーザーアカウントに推奨されるセキュリティ設定を設定しますAWS Reserved OU。
AWS Managed Active Directory Policy	すべてのドメインコントローラー	すべてのドメインコントローラーに対して推奨されるセ

グループポリシー名	適用対象	説明
		セキュリティ設定を設定します。
TimePolicyNT5DS	PDCe 以外のすべてのドメインコントローラー	Windows タイム (NT5DS) を使用するように、PDCe 以外のすべてのドメインコントローラーのタイムポリシーを設定します。
TimePolicyPDC	PDCe ドメインコントローラー	ネットワークタイムプロトコル (NTP) を使用するように PDCe ドメインコントローラーのタイムポリシーを設定します。
Default Domain Controllers Policy	使用されていない	ドメインの作成時にプロビジョニングされた AWS マネージド Active Directory ポリシーが代わりに使用されます。

各 GPO の設定を確認する場合は、[グループポリシー管理コンソール \(GPMC\)](#) を有効にしてドメイン結合した Windows インスタンスから設定を表示できます。

- AWS Managed Microsoft AD 管理default local accounts用に以下を作成します。

 Important

管理者パスワードを必ず保存してください。このパスワードは保存 AWS Directory Service されず、取得できません。ただし、[パスワードは AWS Directory Service コンソールからリセット](#)することも、[ResetUserPassword](#) API を使用してリセットすることもできます。

Admin

Admin は、AWS Managed Microsoft AD が最初に directory administrator account 作成されたときに作成されるです。AWS Managed Microsoft AD を作成するときに、このアカウントのパスワードを指定します。このアカウントは にあります Users OU (例: Corp > Users)。このアカウントを使用して、AWS内の Active Directory を管理します。詳細については、「[AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#)」を参照してください。

AWS_111111111111

で始まり、アンダースコアが AWS 付き、 にあるアカウント名AWS Reserved OUは、サービスマネージドアカウントです。このサービスマネージドアカウントは、 とやり取り AWS するために によって使用されますActive Directory。これらのアカウントは、AWS Directory Service Data が有効になっているとき、および で新しい AWS アプリケーションが承認されるたびに作成されますActive Directory。これらのアカウントには、AWS のサービスのみがアクセスできます。

krbtgt account

krbtgt account は、AWS Managed Microsoft AD で使用される Kerberos チケット交換で重要な役割を果たします。krbtgt account は、Kerberos チケット付与チケット (TGT) 暗号化に使用される特別なアカウントであり、Kerberos 認証プロトコルのセキュリティに重要な役割を果たします。詳細については、[Microsoft のドキュメント](#)を参照してください。

AWS は AWS Managed Microsoft AD のkrbtgt accountパスワードを 90 日に 2 回自動的にローテーションします。90 日ごとに 2 回の連続ローテーションの間には 24 時間の待機期間があります。

管理者アカウントおよび Active Directory によって作成された他のアカウントの詳細については、「[Microsoft ドキュメント](#)」を参照してください。

AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可

AWS Directory Service for Microsoft Active Directory ディレクトリを作成すると、 は組織単位 (OU) AWS を作成して、AWS 関連するすべてのグループとアカウントを保存します。この OU の詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。これには管理者

アカウントも含まれます。管理者アカウントには、OU に対して次の一般的な管理アクティビティを実行するためのアクセス許可があります。

- ユーザー、グループ、コンピュータを追加、更新、または削除する。詳細については、「[AWS Managed Microsoft AD でのユーザーとグループの管理](#)」を参照してください。
- ファイルやプリントサーバーなどのドメインにリソースを追加して、追加したリソースへのアクセス許可を OU のユーザーとグループに割り当てる。
- 追加の OU やコンテナを作成する。
- 追加の OU とコンテナの権限を委任する。詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。
- グループポリシーを作成し、リンクする。
- 削除されたオブジェクトを Active Directory のごみ箱から元に戻す。
- Active Directory Web Service で Active Directory と DNS PowerShell モジュールを実行する。
- グループ管理サービスアカウントを作成して設定する。詳細については、「[グループ管理サービスアカウント](#)」を参照してください。
- Kerberos の制約付き委任を設定する。詳細については、「[Kerberos の制約付き委任](#)」を参照してください。

管理者アカウントには、ドメイン全体に関係する次のアクティビティを実行する権限もあります。

- DNS 設定 (レコード、ゾーン、フォワーダーの追加、削除、更新) を管理する
- DNS イベントログを参照する
- セキュリティイベントログを参照する

ここにリストされているアクションのみが、管理者アカウントに許可されます。また、管理者アカウントには、親 OU 上など、特定の OU 以外のディレクトリ関連のアクションに対するアクセス許可はありません。

考慮事項

- AWS ドメイン管理者は、でホストされているすべてのドメインへの完全な管理アクセス権を持ちます AWS。が AWS システムに保存しているディレクトリ情報を含むコンテンツ AWS を処理する方法の詳細については、との契約 AWS と [AWS データ保護に関するよくある質問](#) を参照してください。

- このアカウントを削除したり、名前を変更したりしないでください。アカウントが不要になった場合は、長いパスワード (64 個以上のランダムな文字) を設定して、アカウントを無効にすることをお勧めします。

Note

AWS は、ドメイン管理者とエンタープライズ管理者の特権ユーザーとグループを排他的に制御します。これにより、AWS は ディレクトリの運用管理を実行できます。

エンタープライズおよびドメイン管理者の特権のあるアカウント

AWS は、組み込みの管理者パスワードを 90 日ごとにランダムなパスワードに自動的にローテーションします。人間が使用するために組み込み管理者パスワードがリクエストされるたびに、AWS チケットが作成され、AWS Directory Service チームに記録されます。アカウントの認証情報は暗号化され、安全なチャネルで処理されます。また、管理者アカウントの認証情報は、AWS Directory Service 管理チームによってのみリクエストできます。

ディレクトリの運用管理を実行するために、AWS はエンタープライズ管理者およびドメイン管理者権限を持つアカウントを排他的に制御します。これには、Active Directory 管理者アカウントの排他的制御が含まれます。は、パスワードボルトを使用してパスワード管理を自動化することで、このアカウント AWS を保護します。管理者パスワードの自動ローテーション中に、は一時的なユーザーアカウント AWS を作成し、ドメイン管理者権限を付与します。この一時アカウントは、管理者アカウントでパスワードのローテーションが失敗した場合のバックアップとして使用されます。が管理者パスワードを AWS 正常に更新すると、は一時管理者アカウント AWS を削除します。

通常、ディレクトリは自動化によって完全に AWS 動作します。自動化プロセスで運用上の問題を解決できない場合は、サポートエンジニアがドメインコントローラー (DC) にサインインして診断を実行 AWS する必要があります。このようなまれに、はアクセスを許可するリクエスト/通知システム AWS を実装します。このプロセスでは、AWS オートメーションによって、ドメイン管理者のアクセス許可を持つ時間制限付きのユーザーアカウントがディレクトリに作成されます。は、ユーザーアカウントをディレクトリで作業するように割り当てられたエンジニアに AWS 関連付けます。は、この関連付けをログシステムに AWS 記録し、使用する認証情報をエンジニアに提供します。エンジニアによるアクションはすべて、Windows のイベントログに記録されます。割り当てられた時間が経過すると、ユーザーアカウントはオートメーションによって削除されます。

管理者アカウントアクションをモニタリングするには、ディレクトリのログ転送機能を使用します。この機能では、モニタリングソリューションを実装できる CloudWatch システムに AD セキュリティ

イベントを転送することができます。詳細については、「[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#)」を参照してください。

誰かが DC にインタラクティブにログオンすると、セキュリティイベント ID 4624、4672、および 4648 はすべてログに記録されます。ドメインに参加している Windows コンピュータから Event Viewer Microsoft マネジメントコンソール (MMC) を使用して、各 DC の Windows セキュリティイベントログを表示できます。また、[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#) を行って、すべてのセキュリティイベントログをアカウントの CloudWatch Logs に送信することもできます。

AWS リザーブド OU 内で作成および削除されたユーザーが表示されることがあります。AWS は、この OU 内のすべてのオブジェクト、およびアクセスおよび管理のためのアクセス許可を委任していないその他の OU またはコンテナの管理とセキュリティを担当します。その OU 内の作成と削除が表示される場合があります。これは、が自動化 AWS Directory Service を使用してドメイン管理者パスワードを定期的に更新するためです。パスワードがローテーションされると、ローテーションが失敗した場合にバックアップが作成されます。ローテーションが成功すると、バックアップアカウントは自動的に削除されます。また、トラブルシューティングの目的で DCs にインタラクティブアクセスが必要なまれなケースでは、AWS Directory Service エンジニアが使用する一時的なユーザーアカウントが作成されます。エンジニアが作業を完了すると、一時的なユーザーアカウントは削除されます。ディレクトリに対してインタラクティブ認証情報がリクエストされるたびに、AWS Directory Service 管理チームに通知されることに注意してください。

AWS Managed Microsoft AD の主要なコンセプトとベストプラクティス

Managed AWS Microsoft AD を最大限に活用するには、主要な概念とベストプラクティスを理解する必要があります。主要な概念は、AWS Managed Microsoft AD の仕組みを理解するのに役立ちます。主要な概念には、Active Directoryスキーマ、パッチ適用スケジュール、グループマネージドサービスアカウントの詳細が含まれます。Active Directoryスキーマには、AWS 属性、クラス、オブジェクトなどの要素が含まれており、AWS Managed Microsoft AD ドメインコントローラーにユーザーに代わってMicrosoft更新を適用 AWS します。また、マネージドサービスアカウント (gMSAs) のグループ化と AWS Managed Microsoft AD での使用についても詳しく説明します。

Managed Microsoft AD AWS の問題を回避するには、ベストプラクティスを考慮します。ベストプラクティスには、次のようなものがあります:

- AWS Managed Microsoft AD をセットアップするときは、ニーズに合わせてセキュリティグループを設定し、管理者アカウント ID とパスワードを覚えておき、条件付きフォワーダー設定を有効にします。
- AWS Managed Microsoft AD を使用する場合は、ディレクトリの作成時に AWS 作成された組織単位を変更したり、Amazon CloudWatch や Amazon SNS などのツールを使用してパフォーマンスをモニタリングしたり、SMB 2.x クライアントを使用したりしないでください。
- AWS Managed Microsoft AD と連携するようにアプリケーションをプログラミングする場合は、WindowsDC ロケータサービスを使用し、本番環境にロールアウトする前にテストの変更をロードし、効率的な LDAP クエリを使用してドメインコントローラーの CPU サイクルが大幅に発生しないようにします。

トピック

- [AWS Managed Microsoft AD の主要な概念](#)
- [AWS Managed Microsoft AD のベストプラクティス](#)

AWS Managed Microsoft AD の主要な概念

以下の主要な概念に精通していれば、AWS Managed Microsoft AD をさらに活用できます。

トピック

- [Active Directory スキーマ](#)
- [AWS Managed Microsoft AD のパッチ適用とメンテナンス](#)
- [グループ管理サービスアカウント](#)
- [Kerberos の制約付き委任](#)

Active Directory スキーマ

スキーマとは、分散ディレクトリの一部をなしている属性とクラスの定義のことであり、データベースにおけるフィールドとテーブルに類似しています。スキーマには、データベースに追加または含めることができるデータの型や形式を決定する、一連のルールが含まれています。User クラスは、データベースに保存される クラス の一例です。ユーザークラス属性の例には、ユーザーの名、姓、電話番号などが含まれます。

スキーマの要素

属性、クラス、オブジェクトは、スキーマのオブジェクト定義を作成するために使用される基本要素です。Managed AWS Microsoft AD スキーマを拡張するプロセスを開始する前に知っておくべきスキーマ要素の詳細を以下に示します。

属性

各スキーマ属性は、データベース内のフィールドと類似しており、それ自体の特性を定義するためのプロパティをいくつか含んでいます。例えば、LDAPDisplayName は属性を読み書きするために LDAP クライアントで使用されるプロパティです。LDAPDisplayName プロパティは、すべての属性とクラスにおいて一意である必要があります。属性の特性に関する詳細な一覧については、MSDN ウェブサイトの「[Characteristics of Attributes](#)」(属性の特性)を参照してください。新しい属性の作成方法に関する詳細なガイダンスについては、MSDN ウェブサイトの「[Defining a New Attribute](#)」(新しい属性の定義)を参照してください。

クラス

クラスは、データベースにおけるテーブルに相当するもので、複数のプロパティを定義することができます。例えば、objectClassCategory は、クラスのカテゴリを定義します。クラスの詳細なリストについては、MSDN ウェブサイトの「[Characteristics of Object Classes](#)」(オブジェクトクラスの特性)を参照してください。新しいクラスの作成方法に関する詳細については、MSDN ウェブサイトの「[Defining a New Class](#)」(新しいクラスの定義)を参照してください。

オブジェクト識別子 (OID)

各クラスおよび属性には、オブジェクトの全体で一意である OID を含める必要があります。ソフトウェアベンダーは、独自の OID を取得して、一意性を確保する必要があります。一意性を確保することで、複数のアプリケーションにおいて同一の属性が異なる目的で使用された場合の競合が回避されます。一意性を確保するには、ISO Name Registration Authority (ISO 名前登録機関) からルート OID を取得します。あるいは、Microsoft から基本 OID を取得することも可能です。OID および OID の取得方法に関する詳細については、MSDN ウェブサイトの「[Object Identifiers](#)」(オブジェクト識別子)を参照してください。

スキーマとリンクした属性

一部の属性は、2 つのクラス間で、前後の双方向でリンクされています。この最も適切な例としてはグループがあります。グループを調べると、そのグループのメンバーを確認でき、ユーザーを見た場合は、それが所属するグループを確認できます。ユーザーをグループに追加すると、Active Directory によってグループに対する前方リンクが作成されます。次に Active

Directory は、グループからユーザーへの後方リンクを追加します。リンクされる属性が作成される際には、一意のリンク ID も生成される必要があります。詳細については、MSDN ウェブサイトの「[Linked Attributes](#)」(リンク属性) を参照してください。

関連トピック

- [AWS Managed Microsoft AD スキーマを拡張するタイミング](#)
- [チュートリアル: AWS Managed Microsoft AD スキーマの拡張](#)

AWS Managed Microsoft AD のパッチ適用とメンテナンス

AWS Directory Service for Microsoft Active Directory は、DS for AWS Managed Microsoft AD AWS とも呼ばれ、実際には Microsoft Active Directory Domain Services (AD DS) であり、マネージドサービスとして提供されます。システムはドメインコントローラー (DCs) に Microsoft Windows Server 2019 を使用し、サービス管理の目的でソフトウェアを DCs AWS に追加します。は DC AWS を更新 (パッチ適用) して新機能を追加し、Microsoft Windows Server ソフトウェアを最新の状態に保ちます。DCs パッチ適用プロセス中も、ディレクトリは引き続き使用可能な状態を維持します。

可用性の確保

デフォルトでは、各ディレクトリは 2 つの DC で構成され、それぞれが異なるアベイラビリティーゾーンにインストールされています。お客様の選択により、DC を追加して可用性をさらに高めることができます。高可用性と耐障害性を必要とする重要な環境では、追加の DCs をデプロイすることをお勧めします。これにより、アクティブなパッチ適用 AWS 中の AWS DCs が使用できなくなります。1 つ以上の DCs が一時的に停止している場合、は、ディレクトリに少なくとも 2 つの運用 DC があるまでパッチ適用を AWS 延期します。DCs これにより、パッチ処理中であっても、ユーザーには運用可能な他の DC を提供することができます。通常、パッチには DC ごとに 30〜45 分を要しますが、この時間は変動する可能性があります。パッチを含む何らかの理由で 1 つ以上の DC が利用できない場合に、アプリケーションが動作中の DC にアクセスできるようにするには、静的な DC アドレスではなく Windows DC ロケーターサービスを使用するように、そのアプリケーションを設定します。

パッチ適用のスケジュールを理解する

DCs で Microsoft Windows Server ソフトウェアを最新の状態に保つために、は Microsoft の更新 AWS を使用します。Microsoft が毎月のロールアップパッチを Windows Server で使用できるように AWS するため、は、3 暦週間以内にロールアップをテストしてすべてのカスタマー DCs に適用するために最善を尽くします。さらに、は、DCs への適用性と緊急性に基づいて、Microsoft が毎月

のロールアップ外でリリースする更新 AWS を確認します。Microsoft によりクリティカルまたは重要と評価され、DC に関連性のあるセキュリティパッチについて、AWS は、5 日間以内にそのパッチをテストしデプロイするための最大限の努力を払います。

グループ管理サービスアカウント

Microsoft は、グループ管理サービスアカウント (gMSA) と呼ばれる (サービス用の) アカウントを、管理者が管理するための新たな手法を Windows Server 2012 に導入しました。gMSA を使用することで、サービス管理者はサービスインスタンス間のパスワードを手動で同期させる必要がなくなります。代わりに、管理者は Active Directory 内に単一の gMSA を作成し、この gMSA を複数のサービスインスタンスで使用するよう設定します。

AWS Managed Microsoft AD のユーザーが gMSA を作成できるようにするには、AWS 委任 Managed Service アカウント管理者セキュリティグループのメンバーとしてアカウントを追加する必要があります。管理者アカウントは、デフォルトでこのグループのメンバーになっています。gMSA の詳細については、Microsoft TechNet ウェブサイトの「[Group Managed Service Accounts Overview](#)」(グループ管理サービスアカウントの概要) を参照してください。

関連する AWS セキュリティブログの投稿

- [AWS Managed Microsoft AD が Active Directory 統合 .NET アプリケーションのデプロイを簡素化し、セキュリティを向上させる方法](#)

Kerberos の制約付き委任

Kerberos の制約付き委任は、Windows Server の機能の 1 つです。この機能を使用すると、サービス管理者は、アプリケーションサービスがユーザーに代わって動作できる範囲を制限することで、アプリケーションの信頼境界を指定して適用できます。これは、バックエンドサービスに委任できるフロントエンドサービスアカウントを指定する際の役に立ちます。Kerberos の制約付き委任は、任意あるいはすべてのサービスに、gMSA が Active Directory ユーザーに代わり接続することを防止し、承認されていない開発者による不正使用の可能性を排除します。

たとえば、user jsmith が HR アプリケーションにログインするとします。SQL Server で jsmith のデータベースアクセス許可を適用します。ただし、デフォルトで SQL Server は、jsmith が設定したアクセス許可ではなく、hr-app-service のアクセス許可を適用するサービスアカウントの認証情報を使用してデータベース接続を開きます。HR 給与アプリケーションが jsmith の認証情報を使用して SQL Server データベースにアクセスできるようにする必要があります。そのためには、AWS 内にある AWS Managed Microsoft AD ディレクトリの hr-app-service サービスアカウントに対し

て Kerberos の制約付き委任を有効にします。jsmith がログオンすると、このユーザー がネットワークの他のサービスへのアクセスを試みた場合に Windows が自動的に使用する Kerberos チケットが、Active Directory から提供されます。Kerberos の委任により、hr-app-service アカウントは jsmith の Kerberos チケットを再利用してデータベースにアクセスできます。つまり、jsmith に固有のアクセス許可を適用してデータベース接続を開くことが可能です。

AWS Managed Microsoft AD のユーザーに Kerberos 制約付き委任の設定を許可するアクセス許可を付与するには、委任 AWS Kerberos 委任管理者セキュリティグループのメンバーとしてアカウントを追加する必要があります。管理者アカウントは、デフォルトでこのグループのメンバーになっています。Kerberos の制約付き委任の詳細については、Microsoft TechNet ウェブサイトの「[Kerberos Constrained Delegation Overview](#)」(Kerberos の制約付き委任の概要) を参照してください。

[リソースベースの制約付き委任](#)が、Windows Server 2012 に導入されました。これを使用することで、バックエンドサービス管理者は、サービスのために制約付き委任を設定できます。

AWS Managed Microsoft AD のベストプラクティス

問題を回避し、AWS Managed Microsoft AD を最大限に活用するために考慮すべき提案とガイドラインをいくつか紹介します。

トピック

- [AWS Managed Microsoft AD 設定のベストプラクティス](#)
- [AWS Managed Microsoft AD ディレクトリを使用する際のベストプラクティス](#)
- [AWS Managed Microsoft AD 用にアプリケーションをプログラミングする際のベストプラクティス](#)

AWS Managed Microsoft AD 設定のベストプラクティス

AWS Managed Microsoft AD を設定する際の推奨事項とガイドラインをいくつか示します。

トピック

- [前提条件](#)
- [AWS Managed Microsoft AD の作成](#)

前提条件

ディレクトリを作成する前に、これらのガイドラインを考慮してください。

ディレクトリタイプが正しいことを確認する

AWS Directory Service には、他の AWS のサービス Microsoft Active Directory で使用する複数の方法があります。予算に合わせたコストで必要な機能を備えた、ディレクトリサービスを次のように選択できます。

- AWS Directory Service for Microsoft Active Directory は、AWS クラウド上で Microsoft Active Directory ホストされる機能豊富なマネージド型です。AWS マネージド Microsoft AD は、5,000 人を超えるユーザーがあり、ホストディレクトリとオンプレミスディレクトリの間に AWS 信頼関係を設定する必要がある場合に最適です。
- AD Connector は、既存のオンプレミスをに接続するだけです Active Directory AWS。AD Connector は、AWS のサービスで既存のオンプレミスのディレクトリを使用する場合に最適な選択です。
- Simple AD は、基本的な Active Directory 互換性を持つ低スケール、低コストのディレクトリです。5,000 人以下のユーザー、Samba 4 互換アプリケーション、LDAP 対応アプリケーションの LDAP 互換性をサポートします。

AWS Directory Service オプションの詳細については、「」を参照してください [オプションの選択](#)。

VPC とインスタンスが正しく設定されていることを確認する

ディレクトリに接続して、管理および使用するためには、ディレクトリが関連付けられている VPC を適切に設定する必要があります。VPC セキュリティおよびネットワーク要件の詳細については、「[AWS Managed Microsoft AD を作成するための前提条件](#)」、「[AD Connector の前提条件](#)」、「[Simple AD の前提条件](#)」のいずれかを参照してください。

ドメインにインスタンスを追加する場合は、「[Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法](#)」に説明されているように、インスタンスへの接続およびリモートアクセスがあることを確認します。

制限を理解する

特定のディレクトリタイプのさまざまな制限について説明します。ディレクトリに保存できるオブジェクトの数については、使用可能なストレージとオブジェクトの集約サイズのみ制限があります。選択したディレクトリに関する詳細については、「[AWS Managed Microsoft AD のクォータ](#)」、「[AD Connector クォータ](#)」、「[Simple AD のクォータ](#)」のいずれかを参照してください。

ディレクトリ AWS のセキュリティグループの設定と使用を理解する

AWS は [セキュリティグループ](#) を作成し、ディレクトリのドメインコントローラーの [Elastic Network Interface](#) にアタッチします。このセキュリティグループは、ドメインコントローラーへの不要なトラフィックをブロックし、Active Directory 通信に必要なトラフィックを許可します。は Active Directory、通信に必要なポートのみを開くようにセキュリティグループ AWS を設定します。デフォルト設定では、セキュリティグループは AWS Managed Microsoft AD VPC IPv4 CIDR アドレスからのこれらのポートへのトラフィックを受け入れます。は、ピア接続またはサイズ変更された VPC 内からアクセスできるドメインコントローラーのインターフェイスにセキュリティグループを AWS アタッチします。 [VPCs](#) これらのインターフェイスにインターネットからアクセスすることはできません (ルーティングテーブルを変更しても、VPC へのネットワーク接続を変更しても、 [NAT ゲートウェイサービス](#) を設定してもアクセスできません)。そのため、VPC へのネットワークパスを持つインスタンスとコンピュータのみがディレクトリにアクセスできます。これにより、特定のアドレス範囲を設定する必要がないため、セットアップが簡素化されます。代わりに、信頼できるインスタンスやコンピュータからのトラフィックのみを許可するルートやセキュリティグループを VPC 内に設定します。

ディレクトリのセキュリティグループを変更する

ディレクトリのセキュリティグループのセキュリティを強化する場合は、セキュリティグループが受け付けるトラフィックの送信元 IP アドレスのリストを絞り込みます。例えば、受け付けるアドレスを VPC IPv4 CIDR の範囲から単一のサブネットやコンピュータに限られた CIDR 範囲に変更できます。同様に、ドメインコントローラーが通信できる送信先アドレスを制限することもできます。このような変更を行うのは、セキュリティグループのフィルタリング機能を完全に理解している場合に限りです。詳細については、「Amazon EC2 ユーザーガイド」の「[Amazon EC2 security groups for Linux instances](#)」(Linux インスタンス用の Amazon EC2 セキュリティグループ) を参照してください。不適切な変更を行うと、目的のコンピュータやインスタンスとの通信が失われる可能性があります。では、ディレクトリのセキュリティが低下するため、ドメインコントローラーへの追加のポートを開かないように AWS することをお勧めします。「[AWS 責任共有モデル](#)」をよくお読みください。

Warning

ディレクトリで使用するセキュリティグループを、ユーザーが作成した他の EC2 インスタンスと関連付けることは技術的には可能です。ただし、AWS は、マネージドディレクトリの機能上またはセキュリティ上のニーズに対応するために、通知なしにセキュリティグループを変更する理由がある AWS 場合があります。このような変更は、ユーザーがディレクトリのセキュリティグループを関連付けるインスタンスに影響します。さらに、ディレクトリ

のセキュリティグループを EC2 インスタンスに関連付けると、EC2 インスタンスのセキュリティリスクが発生する可能性があります。ディレクトリセキュリティグループは、AWS Managed Microsoft AD VPC IPv4 CIDR アドレスからの必要な Active Directory ポートでのトラフィックを受け入れます。このセキュリティグループを関連付ける EC2 インスタンスにインターネットにアタッチされたパブリック IP アドレスがあると、開いているポートでインターネット上の任意のコンピュータが EC2 インスタンスと通信できます。

AWS Managed Microsoft AD の作成

AWS Managed Microsoft AD を作成する際に考慮すべき提案をいくつか紹介します。

トピック

- [管理者 ID とパスワードを記憶する](#)
- [DHCP オプションセットの作成](#)
- [条件付きフォワーダー設定を有効にします](#)
- [追加ドメインコントローラーのデプロイ](#)
- [AWS アプリケーションのユーザーネームの制限を理解する](#)

管理者 ID とパスワードを記憶する

ディレクトリを設定するときに、管理者アカウントのパスワードを指定します。そのアカウント ID は AWS Managed Microsoft AD の管理者です。このアカウント用に作成したパスワードを忘れないでください。そうでないと、ディレクトリにオブジェクトを追加できません。

DHCP オプションセットの作成

AWS Directory Service ディレクトリの DHCP オプションセットを作成し、ディレクトリがある VPC に DHCP オプションセットを割り当てることをお勧めします。このようにすると、その VPC 内のすべてのインスタンスは指定されたドメインを参照することができ、DNS サーバーはドメイン名を解決できます。

DHCP オプションセットの詳細については、「[AWS Managed Microsoft AD の DHCP オプションセットの作成または変更](#)」を参照してください。

条件付きフォワーダー設定を有効にします

次の条件付きフォワーダーの設定は、この条件付きフォワーダーを Active Directory に格納し、次のようにレプリケートするというオプションを有効にする必要があります。これらの設定を有効にす

ると、インフラストラクチャー障害または過負荷障害によりノードを交換したときに、条件付きフォワーダーの設定が持続的に稼働できると保証します。

条件付きフォワーダーは、前の設定が有効になっている 1 つのドメインコントローラーで作成される必要があります。これにより、他のドメインコントローラーへのレプリケーションが可能になります。

追加ドメインコントローラーのデプロイ

デフォルトでは、は別々のアベイラビリティゾーンに存在する 2 つのドメインコントローラー AWS を作成します。これにより、ソフトウェアのパッチ適用など、1 つのドメインコントローラーが到達不能または利用不可になる可能性があるイベント中の耐障害性が得られます。耐障害性をさらに高め、ドメインコントローラーまたはアベイラビリティゾーンへのアクセスに影響する長期的なイベントの発生時にパフォーマンスが確実にスケールアウトされるように、[追加のドメインコントローラーをデプロイする](#)ことをお勧めします。

詳細については、「[Windows DC ロケーターサービスを使用する](#)」を参照してください。

AWS アプリケーションのユーザーネームの制限を理解する

AWS Directory Service では、ユーザー名の構築に使用できるほとんどの文字形式がサポートされています。ただし、WorkSpaces、WorkDocs、Amazon WorkMail、QuickSight などの AWS アプリケーションへのサインインに使用されるユーザー名には文字制限が適用されます。これらの制限により、以下の文字は使用できません。

- スペース
- マルチバイト文字
- `!"#$%&'()*+,-./:;<=>?@[]^`{|}~`

Note

@ 記号は、UPN サフィックスが後に続く場合に限り、使用できます。

AWS Managed Microsoft AD ディレクトリを使用する際のベストプラクティス

AWS Managed Microsoft AD を使用する際に留意すべき推奨事項をいくつか紹介します。

トピック

- [事前定義されたユーザー、グループ、組織単位を変更しない](#)
- [自動的にドメインを結合する](#)
- [信頼を正しく設定する](#)
- [ドメインコントローラーのパフォーマンスを追跡する](#)
- [スキーマ拡張を慎重に計画する](#)
- [ロードバランサーについて](#)
- [インスタンスのバックアップを作成する](#)
- [SNS メッセージングを設定する](#)
- [ディレクトリサービス設定の適用](#)
- [ディレクトリを削除する前に Amazon エンタープライズアプリケーションを削除する](#)
- [SYSVOL 共有および NETLOGON 共有へのアクセス時に SMB 2.x クライアントを使用する](#)

事前定義されたユーザー、グループ、組織単位を変更しない

AWS Directory Service を使用してディレクトリを起動すると、はディレクトリのすべてのオブジェクトを含む組織単位 (OU) AWS を作成します。この OU はドメインルートにあります。OU にはディレクトリを作成する際に入力した NetBIOS 名があります。ドメインルートは によって所有および管理されます AWS。いくつかのグループと管理ユーザーも作成されます。

これらの事前定義されたオブジェクトを移動、削除、または他の方法で変更しないでください。これにより、自分と の両方がディレクトリにアクセスできなくなる可能性があります AWS。詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。

自動的にドメインを結合する

AWS Directory Service ドメインの一部となる Windows インスタンスを起動する場合、後でインスタンスを手動で追加するのではなく、インスタンス作成プロセスの一部としてドメインに参加する方が簡単です。自動的にドメインを結合するには、新しいインスタンスを起動するときに、単にドメイン結合ディレクトリの適切なディレクトリを選択します。詳細については、「[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)」を参照してください。

信頼を正しく設定する

AWS Managed Microsoft AD ディレクトリと別のディレクトリの間信頼関係を設定するときは、次のガイドラインに注意してください。

- 信頼のタイプは両側 (フォレストまたは外部) で一致する必要があります。
- 一方向の信頼 (信頼するドメインでの送信、信頼されたドメインでの受信) を使用する場合は、信頼の方向が正しく設定されていることを確認します。
- 完全修飾ドメイン名 (FQDN) と NetBIOS 名のどちらも、フォレスト / ドメイン間で一意であることが必要です。

信頼関係の設定の手順の詳細については、「[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)」を参照してください。

ドメインコントローラーのパフォーマンスを追跡する

スケーリングの決定を最適化し、ディレクトリの耐障害性とパフォーマンスを向上させるために、CloudWatch メトリクスを使用することをお勧めします。詳細については、「[CloudWatch を使用した AWS Managed Microsoft AD ドメインコントローラーのパフォーマンスのモニタリング](#)」を参照してください。

CloudWatch コンソールを使用してドメインコントローラーメトリクスを設定する方法については、セキュリティブログの「[使用率メトリクスに基づいて AWS Managed Microsoft AD スケーリングを自動化する方法](#)」を参照してください。AWS

スキーマ拡張を慎重に計画する

重要かつ頻繁なクエリ用にディレクトリへのインデックス付けを行う場合、そのためのスキーマ拡張は慎重に適用します。ディレクトリに過剰にインデックス付けしないように注意します。インデックスがディレクトリ領域を消費するとともに、インデックス付けされた値の急な変更により、パフォーマンスの問題が発生する可能性があるためです。インデックスを追加するには、Lightweight Directory Access Protocol (LDAP) Directory Interchange Format (LDIF) ファイルを作成し、スキーマ変更を拡張する必要があります。詳細については、「[AWS Managed Microsoft AD スキーマを拡張する](#)」を参照してください。

ロードバランサーについて

AWS Managed Microsoft AD エンドポイントの前にロードバランサーを使用しないでください。Active Directory Microsoftは、外部ロードバランシングなしで最も応答性の高い運用 DC を検出するドメインコントローラー (DC) 検出アルゴリズムで使用するよう設計 (AD) されています。外部 network load balancer によるアクティブな DC の検出は正確でない場合があり、アクティブになる予定であっても使用できない DC にアプリケーションが割り当てられることがあります。詳細については、Microsoft TechNet の「[Load balancers and Active Directory](#)」(ロードバランサーと

Active Directory) を参照してください。このページでは、外部ロードバランサーを実装するのではなく、Active Directory を正しく使用するようにアプリケーションを修正することを推奨しています。

インスタンスのバックアップを作成する

インスタンスを既存の AWS Directory Service ドメインに手動で追加する場合は、まずバックアップを作成するか、そのインスタンスのスナップショットを作成します。これは Linux インスタンスを結合する場合には、特に重要です。インスタンスを追加するための手順には、正しく実行しないと、インスタンスに到達できなくなったり、インスタンスが使用できなくなったりするものがあります。詳細については、「[スナップショットを使用した AWS Managed Microsoft AD の復元](#)」を参照してください。

SNS メッセージングを設定する

Amazon Simple Notification Service (Amazon SNS) を使用すると、ディレクトリのステータスが変更された時に E メールまたはテキストメッセージ (SMS) を受け取ることができます。ディレクトリのステータスが Active から Impaired または Inoperable に変わると、通知が送信されます。ディレクトリが Active ステータスに戻ったときも通知を受け取ります。

また、Amazon SNS コンソールからそのトピックを削除する前に AWS Directory Service、メッセージを受信する Amazon SNS トピックがある場合は、ディレクトリを別の SNS トピックに関連付ける必要があります。そうしないと、重要なディレクトリステータスメッセージを失う可能性があります。Amazon SNS を設定する方法については、「[Amazon Simple Notification Service による AWS Managed Microsoft AD ディレクトリのステータス通知の有効化](#)」を参照してください。

ディレクトリサービス設定の適用

AWS Managed Microsoft AD を使用すると、コンプライアンスとセキュリティ要件を満たすようにセキュリティ設定を調整できます。AWS Managed Microsoft AD は、新しいリージョンや追加のドメインコントローラーを追加する場合を含め、ディレクトリ内のすべてのドメインコントローラーに設定をデプロイして維持します。これらのセキュリティ設定は、新規および既存のすべてのディレクトリに対して構成し、適用できます。これは、「[ディレクトリセキュリティ設定の編集](#)」の手順または [UpdateSettings API](#) に従って、コンソールで行うことができます。

詳細については、「[AWS Managed Microsoft AD ディレクトリのセキュリティ設定の編集](#)」を参照してください。

ディレクトリを削除する前に Amazon エンタープライズアプリケーションを削除する

WorkSpaces、Amazon WorkSpaces Application Manager、WorkDocs、Amazon WorkMail、Amazon Relational Database Service (Amazon RDS) などの 1 つ以上の Amazon

Enterprise アプリケーションに関連付けられているディレクトリを削除する前に AWS Management Console、まず各アプリケーションを削除する必要があります。これらのアプリケーションを削除する方法の詳細については、「[AWS Managed Microsoft AD の削除](#)」を参照してください。

SYSVOL 共有および NETLOGON 共有へのアクセス時に SMB 2.x クライアントを使用する

クライアントコンピュータは、サーバーメッセージブロック (SMB) を使用して、グループポリシー、ログインスクリプト、その他のファイル用の AWS Managed Microsoft AD ドメインコントローラーの SYSVOL および NETLOGON 共有にアクセスします。AWS Managed Microsoft AD は、SMB バージョン 2.0 (SMBv2) 以降のみをサポートしています。

SMBv2 バージョン以降のプロトコルには、クライアントのパフォーマンスを向上させ、ドメインコントローラーとクライアントのセキュリティを強化する多数の機能が追加されています。この変更は、SMBv1 の無効化に関する [United States Computer Emergency Readiness Team](#) (米コンピュータ緊急事態対策チーム) と [Microsoft](#) の勧告に従うものです。

Important

現在 SMBv1 クライアントを使用してドメインコントローラーの SYSVOL 共有および NETLOGON 共有にアクセスしている場合は、これらのクライアントを更新して SMBv2 以降を使用する必要があります。ディレクトリは正常に動作しますが、SMBv1 クライアントは AWS Managed Microsoft AD ドメインコントローラーの SYSVOL および NETLOGON 共有に接続できず、グループポリシーも処理できません。

SMBv1 クライアントは、現在使用している他のすべての SMBv1 互換ファイルサーバーに対しては動作します。ただし、すべての SMB サーバーとクライアントを SMBv2 以降に更新 AWS することをお勧めします。システムの SMBv1 を無効にして新しい SMB バージョンに更新する方法の詳細については、「[Microsoft TechNet](#)」および「[Microsoft ドキュメント](#)」を参照してください。

SMBv1 リモート接続の追跡

AWS Managed Microsoft AD ドメインコントローラーにリモート接続している Microsoft-Windows-SMBServer/Audit Windows イベントログを確認できます。このログのすべてのイベントは SMBv1 接続を示します。これらのログの 1 つに表示される情報の例を次に示します。

SMB1 アクセス

クライアントアドレス: ####.####.####.####

ガイダンス:

このイベントは、クライアントが SMB1 を使用してサーバーにアクセスしようとしたことを示します。SMB1 アクセスの監査を停止するには、PowerShell cmdlet の Set-SmbServerConfiguration を使用します。

AWS Managed Microsoft AD 用にアプリケーションをプログラミングする際のベストプラクティス

AWS Managed Microsoft AD と連携するようにアプリケーションをプログラムする前に、次の点を考慮してください。

トピック

- [Windows DC ロケーターサービスを使用する](#)
- [本番稼働用環境にロールアウトする前の負荷テスト](#)
- [効率的な LDAP クエリを使用する](#)

Windows DC ロケーターサービスを使用する

アプリケーションを開発するときは、WindowsDC ロケーターサービスを使用するか、AWS Managed Microsoft AD の動的 DNS (DDNS) サービスを使用してドメインコントローラー (DCs)。アプリケーションを DC のアドレスでハードコーディングしないでください。DC Locator Service では、ディレクトリの負荷を分散できるだけでなく、デプロイにドメインコントローラーを追加することにより水平スケーリングを活用できます。アプリケーションを固定 DC にバインドした場合、その DC がパッチ適用または復旧を行うと、アプリケーションは残りのいずれかの DC を使用することなく、DC へのアクセスを失います。さらに、DC をハードコーディングすると、1 つの DC にホットスポットが発生する可能性があります。極端な場合、ホットスポットが原因で DC が応答しなくなる可能性があります。このような場合、AWS ディレクトリの自動化によってディレクトリに障害があるとフラグが立てられ、応答しない DC を置き換える復旧プロセスがトリガーされる可能性があります。

本番稼働用環境にロールアウトする前の負荷テスト

本番稼働用環境のワークロードを表すオブジェクトとリクエストを使用してラボテストを行い、ディレクトリがアプリケーションの負荷に合わせてスケーリングされることを確認します。追加のキャパシティーが必要な場合は、DC 間でリクエストを分散しながら追加の DC でテストします。詳細については、「[AWS Managed Microsoft AD に追加するドメインコントローラーのデプロイ](#)」を参照してください。

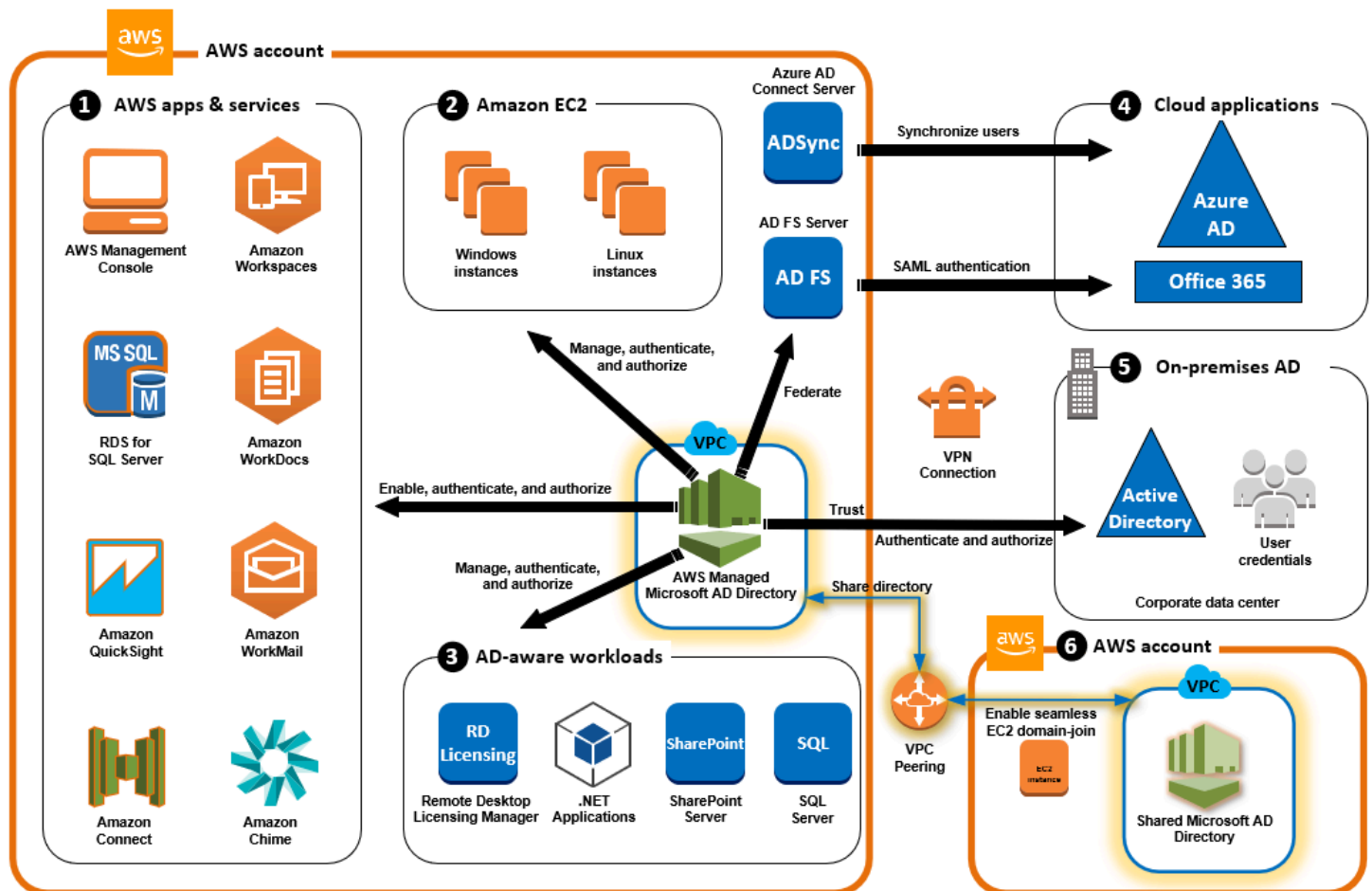
効率的な LDAP クエリを使用する

何万個ものオブジェクトにまたがるドメインコントローラーへの広範な LDAP クエリにより、1 つの DC で大量の CPU サイクルが消費されて、ホットスポットが発生することがあります。これは、クエリ中に同じ DC を共有するアプリケーションに影響を与える可能性があります。

AWS Managed Microsoft AD のユースケース

AWS Managed Microsoft AD を使用すると、1 つのディレクトリを複数のユースケースで共有できます。例えば、.NET アプリケーション、「[Windows 認証](#)」が有効になっている「[Amazon RDS for SQL Server](#)」、メッセージングおよびビデオ会議用の「[Amazon Chime](#)」のアクセスを認証および承認するディレクトリを共有できます。

次の図は、AWS Managed Microsoft AD ディレクトリのユースケースの一部を示しています。これには、ユーザーに外部クラウドアプリケーションへのアクセスを許可し、オンプレミスの Active Directory ユーザーが AWS クラウド内のリソースを管理してアクセスできるようにする機能が含まれます。



AWS Managed Microsoft AD は、次のいずれかのビジネスユースケースに使用します。

トピック

- [ユースケース 1: Active Directory 認証情報を使用して AWS アプリケーションとサービスにサインインする](#)
- [ユースケース 2: Amazon EC2 インスタンスを管理する](#)
- [ユースケース 3: Active Directory 対応のワークロードにディレクトリサービスを提供する](#)
- [ユースケース 4: Office 365 およびその他のクラウドアプリケーション AWS IAM Identity Center へ](#)
- [ユースケース 5: オンプレミス Active Directory に拡張する AWS クラウド](#)
- [ユースケース 6: ディレクトリを共有して、AWS アカウント間で Amazon EC2 インスタンスをドメインにシームレスに結合する](#)

ユースケース 1: Active Directory 認証情報を使用して AWS アプリケーションとサービスにサインインする

Managed AWS Microsoft AD ディレクトリを使用するには[AWS Client VPN](#)、[AWS Management Console](#)、[AWS IAM Identity Center](#)[Amazon Chime](#)、[Amazon Connect](#)、[Amazon FSx](#)、[QuickSight](#)、[Amazon RDS for SQL Server](#)、[WorkDocs](#)、[Amazon WorkMail](#)、[WorkSpaces](#) などの複数の AWS アプリケーションとサービスを有効にすることができます。ディレクトリで AWS アプリケーションまたはサービスを有効にすると、ユーザーは Active Directory 認証情報を使用してアプリケーションまたはサービスにアクセスできます。

たとえば、ユーザーが[Active Directory 認証情報 AWS Management Console を使用してにサインイン](#)できるようにします。そのためには、ディレクトリ内のアプリケーションとして AWS Management Console を有効にしてから、Active Directory ユーザーとグループを IAM ロールに割り当てます。ユーザーがサインインすると AWS Management Console、AWS リソースを管理する IAM ロールを引き受けます。これにより、SAML インフラストラクチャを個別に設定および管理することなく、ユーザーに AWS Management Console へのアクセスを簡単に許可できます。

エンドユーザーエクスペリエンスをさらに強化するために、WorkDocs の[シングルサインオン](#)機能を有効にできます。これにより、ユーザーは認証情報を個別に入力することなく、ディレクトリに結合されたコンピュータから WorkDocs にアクセスできます。

ディレクトリまたはオンプレミス Active Directory 内のユーザーアカウントへのアクセスを許可することで、既存の認証情報とアクセス許可 AWS CLI を使用して AWS Management Console にサイン

インしたり、既存のユーザーアカウントに直接 IAM ロールを割り当てて AWS リソースを管理したりできます。

FSx for Windows File Server と AWS Managed Microsoft AD の統合

FSx for Windows File Server を AWS Managed Microsoft AD と統合すると、フルマネージド型のネイティブ Microsoft Windows ベースの Server Message Block (SMB) プロトコルファイルシステムが提供され、Windows ベースのアプリケーションとクライアント (共有ファイルストレージを利用) を簡単に移動できます AWS。FSx for Windows File Server は、自己管理型の Microsoft Active Directory と統合できますが、ここではそのシナリオについては説明しません。

Amazon FSx の一般的なユースケースとリソース

このセクションでは、AWS Managed Microsoft AD のユースケースとの一般的な FSx for Windows File Server 統合に関するリソースのリファレンスを提供します。このセクションの各ユースケースは、基本的な AWS Managed Microsoft AD および FSx for Windows File Server の設定から始まります。これらの設定を作成する方法の詳細については、次を参照してください。

- [AWS Managed Microsoft AD の開始方法](#)
- [Amazon FSx の開始](#)

Windows コンテナの永続的ストレージとしての FSx for Windows File Server

[Amazon Elastic Container Service \(ECS\)](#) では、Amazon ECS 向けに最適化された Windows AMI で起動されるコンテナインスタンス上の Windows コンテナがサポートされています。Windows コンテナインスタンスでは、独自のバージョンの Amazon ECS コンテナエージェントを使用します。Amazon ECS 向けに最適化された Windows Server AMI では、Amazon ECS コンテナエージェントはホスト上のサービスとして実行されます。

Amazon ECS では、グループ管理サービスアカウント (gMSA) と呼ばれる特殊なサービスアカウントを使用して、Windows コンテナの Active Directory 認証をサポートしています。Windows コンテナはドメインに結合できないため、gMSA で実行するように Windows コンテナを設定する必要があります。

関連項目

- [FSx for Windows File Server を Windows コンテナの永続的ストレージとして使用する](#)
- [グループ管理サービスアカウント](#)

Amazon AppStream 2.0 のサポート

[Amazon AppStream 2.0](#) は、フルマネージドのアプリケーションストリーミングサービスです。このアプリケーションでは、データを保存し、そのデータにアクセスするためのさまざまなソリューションが提供されます。Amazon AppStream 2.0 で Amazon FSx を使用すると、Amazon FSx を使用したパーソナルな永続的ストレージドライブが提供されます。また、共通のファイルにアクセスするための共有フォルダを利用できるように設定できます。

関連項目

- [チュートリアル 4: Amazon AppStream 2.0 で Amazon FSx を使用する](#)
- [Amazon AppStream 2.0 で Amazon FSx を使用する](#)
- [AppStream 2.0 での Active Directory の使用](#)

Microsoft SQL Server のサポート

FSx for Windows File Server は、Microsoft SQL Server 2012 (2012 バージョン 11.x 以降)、新しいシステムデータベース (Master、Model、MSDB、TempDB など)、および Database Engine のユーザーデータベースにおけるストレージオプションとして使用できます。

関連項目

- [SMB ファイル共有ストレージを使用して SQL Server をインストールする](#)
- [FSx for Windows File Server を使用して Microsoft SQL Server の高可用性デプロイを簡素化する](#)
- [グループ管理サービスアカウント](#)

ホームフォルダおよびローミングユーザープロファイルのサポート

FSx for Windows File Server は、Active Directory のユーザーホームフォルダーや「マイドキュメント」からのデータを中央の場所に保存するために使用できます。Roaming User Profiles のデータの保存に FSx for Windows File Server を使用することもできます。

関連項目

- [Amazon FSx を使用して Windows のホームディレクトリを簡素化する](#)
- [ローミングユーザープロファイルをデプロイする](#)
- [FSx for Windows File Server を WorkSpaces で使用する](#)

ネットワークファイル共有のサポート

FSx for Windows File Server 上のネットワークファイル共有により、管理されたスケーラブルなファイル共有ソリューションが提供されます。ユースケースの 1 つとして、手動またはグループポリシーを使用して作成できるマッピングされたクライアントドライブがあります。

関連項目

- [チュートリアル 6: シャードを使用してパフォーマンスをスケールアウトする](#)
- [ドライブマッピング](#)
- [FSx for Windows File Server を WorkSpaces で使用する](#)

グループポリシーソフトウェアのインストールのサポート

[SYSVOL] フォルダのサイズとパフォーマンスには制限があるため、ベストプラクティスとして、ソフトウェアのインストールファイルなどのデータをそのフォルダに保存しないようにしてください。この問題を解決するために、グループポリシーを使用してインストールされたすべてのソフトウェアファイルを保存するよう FSx for Windows File Server を設定できます。

関連項目

- [グループポリシーを使用してソフトウェアをリモートインストールする](#)

Windows Server Backup ターゲットのサポート

UNC ファイル共有を使用して、FSx for Windows File Server を Windows Server Backup のターゲットドライブとして設定できます。この場合、アタッチされている EBS ボリュームではなく、FSx for Windows File Server への UNC パスを指定します。

関連項目

- [サーバーのシステム状態の復旧を実行する](#)

Amazon FSx は AWS Managed Microsoft AD Directory Sharing もサポートしています。詳細については、以下を参照してください。

- [AWS Managed Microsoft AD を共有する](#)
- [別の VPC またはアカウントで AWS Managed Microsoft AD で Amazon FSx を使用する](#)

Amazon RDS と AWS Managed Microsoft AD の統合

Amazon RDS では、Microsoft Active Directory での Kerberos を使用したデータベースユーザーの外部認証がサポートされています。Kerberos は、チケットと対称キー暗号化を使用したネットワーク認証プロトコルです。このプロトコルでは、ネットワーク経由でパスワードを送信する必要はありません。Amazon RDS での Kerberos および Active Directory のサポートにより、データベースユーザーの一元化認証およびシングルサインオンという利点が得られ、ユーザーの認証情報を Active Directory に保存できます。

このユースケースを開始するには、まず基本的な AWS Managed Microsoft AD と Amazon RDS の設定を行う必要があります。

- [AWS Managed Microsoft AD の開始方法](#)
- [Amazon RDS の開始](#)

以下で参照するすべてのユースケースは、基本 Managed Microsoft AD と Amazon RDS で始まり、Amazon RDS AWS と AWS Managed Microsoft AD を統合する方法について説明します。

- [Amazon RDS for SQL Server DB インスタンスでの Windows 認証の使用](#)
- [MySQL での Kerberos 認証の使用](#)
- [Amazon RDS for Oracle での Kerberos 認証の使用](#)
- [Amazon RDS for PostgreSQL での Kerberos 認証の使用](#)

Amazon RDS は AWS Managed Microsoft AD Directory Sharing もサポートしています。詳細については、以下を参照してください。

- [AWS Managed Microsoft AD を共有する](#)
- 「[Joining your Amazon RDS DB instances across accounts to a single shared domain](#)」(アカウントをまたがった Amazon RDS DB インスタンスを単一の共有ドメインに結合する)

Amazon RDS for SQL Server の Active Directory への結合の詳細については「[Amazon RDS for SQL Server のセルフマネージド型 Active Directory への参加](#)」を参照してください。

グループ管理サービスアカウントで Amazon RDS for SQL Server を使用する .NET アプリケーション

Amazon RDS for SQL Server は、基本的な .NET アプリケーションおよびグループ管理サービスアカウント (gMSA) と統合できます。詳細については、[AWS 「Managed Microsoft AD が Active Directory 統合 .NET アプリケーションのデプロイを簡素化し、セキュリティを向上させる方法」を参照してください。](#)

ユースケース 2: Amazon EC2 インスタンスを管理する

使い慣れた Active Directory 管理ツールを使用して、Active Directory グループポリシーオブジェクト (GPOs) を適用し、インスタンスを Managed Microsoft AD ドメインに結合することで Amazon EC2 for Windows または Linux インスタンスを一元管理できます。 [AWS](#)

さらに、ユーザーは自身の Active Directory の認証情報でインスタンスにサインインできます。これにより、個々のインスタンスの認証情報を使用したり、プライベートキー (PEM) ファイルを配布する必要がなくなります。その結果、使い慣れた Active Directory のユーザー管理ツールを使用して、ユーザーに対してアクセスをすばやく許可または取り消すことができます。

ユースケース 3: Active Directory 対応のワークロードにディレクトリサービスを提供する

AWS Managed Microsoft AD は、[Remote Desktop Licensing Manager](#)、[Microsoft SharePoint](#)、[Microsoft SQL Server Always On](#) などの従来の Active Directory 対応ワークロードを AWS クラウドで Microsoft Active Directory 実行できる実際の です。AWS Managed Microsoft AD は、[グループ Managed Service Accounts \(gMSAs\) と Kerberos 制約付き委任 \(KCD\) を使用することで、Active Directory 統合 .NET アプリケーションのセキュリティを簡素化および改善](#)するのに役立ちます。

ユースケース 4: Office 365 およびその他のクラウドアプリケーション AWS IAM Identity Center へ

AWS Managed Microsoft AD を使用して、クラウドアプリケーション用の AWS IAM Identity Center サービスを提供できます。Microsoft Entra Connect (旧称 Azure Active Directory Connect) を使用してユーザーを Microsoft Entra (旧称 [Azure Active Directory Azure AD]) に同期し、Active Directory フェデレーションサービス (AD FS) を使用して、ユーザーが Active Directory 認証情報を使用して「[Microsoft Office 365](#)」やその他の SAML 2.0 クラウドアプリケーションにアクセスできるようにします。

[AWS Managed Microsoft AD を IAM Identity Center と統合すると](#)、AWS Managed Microsoft AD や オンプレミスの信頼されたドメインに SAML 機能が追加されます。統合すると、ユーザーは IAM Identity Center を SAML をサポートするサービスで使用できます。これには、SAML インフラストラクチャを設定することなく、Office 365、Concur、Salesforce などの AWS Management Console サードパーティーのクラウドアプリケーションが含まれます。オンプレミスユーザーに IAM Identity Center の使用を許可するプロセスのデモンストレーションについては、次の YouTube 動画を視聴してください。

 Note

AWS Single Sign-On の名前が IAM Identity Center に変更されました。

ユースケース 5: オンプレミスを Active Directoryに拡張する AWS クラウド

インフラストラクチャがすでにありActive Directory、Active Directory対応ワークロードを に移行するときに使用する場合は AWS クラウド、AWS マネージド Microsoft AD が役立ちます。[Active Directory 信頼](#)を使用して Managed AWS Microsoft AD を既存の に接続できますActive Directory。つまり、ユーザーは、ユーザー、グループ、またはパスワードを同期しなくても、オンプレミスActive Directory認証情報を使用して Active Directory対応アプリケーションと AWS アプリケーションにアクセスできます。

たとえば、ユーザーは既存のActive Directoryユーザー名とパスワードを使用して AWS Management Console と Amazon WorkSpaces にサインインできます。また、SharePoint などの Active Directory 対応アプリケーションを AWS Managed Microsoft AD と共に使用する場合、ログイン済みの Windows ユーザーは再度認証情報を入力することなくこれらのアプリケーションにアクセスできます。

オンプレミスActive Directoryドメインを に移行 AWS して、[Active Directory移行ツールキット \(ADMT\)](#) とパスワードエクスポートサービス (PES) Active Directoryを使用してインフラストラクチャの運用上の負担を軽減することもできます。

ユースケース 6: ディレクトリを共有して、AWS アカウント間で Amazon EC2 インスタンスをドメインにシームレスに結合する

複数の AWS アカウント間でディレクトリを共有すると、各アカウントと各 VPC のディレクトリを操作することなく、[Amazon EC2](#) などの AWS サービスを簡単に管理できます。この操作では、

AWS リージョン内の任意の AWS アカウントおよび [Amazon VPC](#) からディレクトリを使用できます。この機能により、複数のアカウントと VPC 間で単一のディレクトリを使用して、ディレクトリ対応のワークロードを優れたコスト効果で簡単に管理できます。例えば、単一の AWS Managed Microsoft AD ディレクトリを使用して、EC2 インスタンスにデプロイした [Windows ワークロード](#) を複数のアカウントと VPC 間で簡単に管理できるようになりました。

AWS Managed Microsoft AD ディレクトリを別の AWS アカウントと共有する場合、Amazon EC2 コンソールまたは [AWS Systems Manager](#) を使用して、アカウントと AWS リージョン内の任意の Amazon VPC からインスタンスをシームレスに結合できます。各アカウントや VPC でディレクトリをデプロイしたり、手動でドメインにインスタンスを結合する必要がなくなるため、EC2 インスタンスにディレクトリ対応のワークロードを迅速にデプロイできます。詳細については、「[AWS Managed Microsoft AD を共有する](#)」を参照してください。

AWS Managed Microsoft AD を維持する

を使用して AWS Managed Microsoft AD AWS Management Console を維持し、day-to-day管理タスクを完了できます。ディレクトリを維持する方法は次のとおりです：

- [AWS Managed Microsoft AD ディレクトリの詳細を表示](#)して、AWS Managed Microsoft AD ディレクトリのタイプ、ディレクトリ ID、ディレクトリのステータス、Amazon VPC、サブネット、アベイラビリティゾーンなどのネットワークの詳細を確認します。
- [AWS Managed Microsoft AD をスナップショットで復元します](#)。スナップショットの作成と削除もできます。
- AWS Managed Microsoft AD のパフォーマンスと可用性を向上させるために、[追加のドメインコントローラーをデプロイ](#)します。
- [AWS Managed Microsoft AD を Standard Edition から、より多くのディレクトリオブジェクトをサポートする Enterprise Edition にアップグレードします](#)。
- 「[代替ユーザープリンシパル名 \(UPN\) を追加](#)」して、ユーザーログインエクスペリエンスを向上させます。
- [AWS Managed Microsoft AD サイト名](#)を変更して、オンプレミスディレクトリ内の既存の Active Directory ユーザーを検索および認証する AWS Managed Microsoft AD の機能を向上させます。
- 不要になった [AWS Managed Microsoft AD を削除します](#)。

AWS Managed Microsoft AD ディレクトリ情報の表示

を使用して AWS Management Console 、次のような AWS Managed Microsoft AD ディレクトリの詳細を表示できます。

- [ディレクトリタイプ]
- ディレクトリ ID
- ディレクトリステータス
- AWS Managed Microsoft AD のネットワークの詳細は次のとおりです。
 - Amazon VPC
 - サブネット
 - アベイラビリティーゾーン
 - [DNS アドレス]

AWS Managed Microsoft AD に関する次の情報を確認できます。

- 共有と共有タブで、AWS Managed Microsoft AD を他の と共有 AWS アカウント し、ドメインコントローラーのネットワークの詳細を確認できます。
- アプリケーション管理タブで、AWS Managed Microsoft AD のアプリケーションアクセス URL を有効にし、AWS Managed Microsoft AD の AWS アプリケーションとサービスを有効にできます。
- メンテナンスタブで、Amazon Simple Notification Service を有効にして AWS Managed Microsoft AD のステータスの通知を受信し、AWS Managed Microsoft AD のスナップショットを確認できます。
- [Status] (ステータス) フィールドの詳細については、「[AWS Managed Microsoft AD ディレクトリのステータスについて](#)」を参照してください。

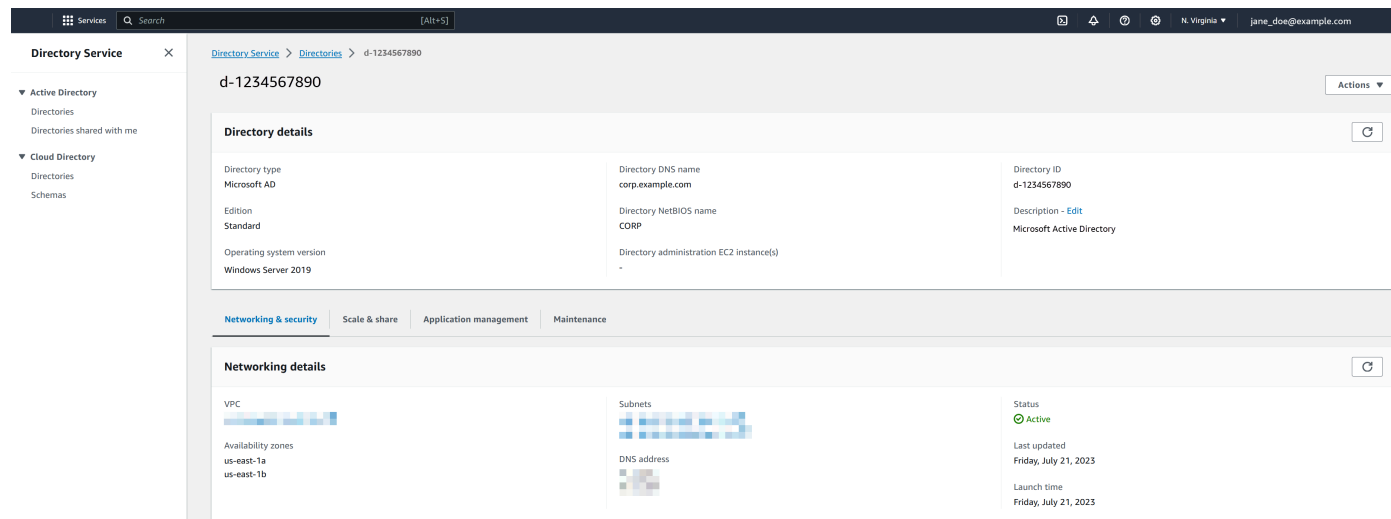
AWS Managed Microsoft AD ディレクトリ情報は AWS Management Console、 、 AWS CLI、またはを使用して表示できますPowerShell。

AWS Management Console

で詳細なディレクトリ情報を表示するには AWS Management Console

1. 「[AWS Directory Service コンソール](#)」のナビゲーションペインで、[Active Directory] の下の [ディレクトリ] を選択します。

2. ディレクトリのディレクトリ ID リンクを選択します。ディレクトリに関する情報は、[Directory details] (ディレクトリの詳細) ページに表示されます。



AWS CLI

を使用して詳細なディレクトリ情報を表示するには AWS CLI

- を開きます AWS CLI。AWS Managed Microsoft AD ディレクトリ情報を表示するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

詳細については、「[describe-directories](#)」を参照してください。

PowerShell

を使用して詳細なディレクトリ情報を表示するには PowerShell

- PowerShell を開きます。AWS Managed Microsoft AD ディレクトリ情報を表示するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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


詳細については、「[Get-DSDirectory](#)」を参照してください。

スナップショットを使用した AWS Managed Microsoft AD の復元

AWS Directory Service は、毎日の自動スナップショットと、AWS Managed Microsoft AD のデータの手動スナップショットを作成する機能を提供しますActive Directory。このスナップショットは、Active Directory の特定時点の復元に使用できます。AWS Managed Microsoft AD ごとに 5 つの手動スナップショットに制限されていますActive Directory。既にこの制限に達している場合は、新しく作成する前に既存の手動スナップショットのいずれかを削除する必要があります。AD Connector ディレクトリのスナップショットを作成することはできません。

Note

スナップショットは AWS Managed Microsoft AD のグローバル機能です。[AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#) を使用している場合、[プライマリリージョン](#) で次の手順を実行する必要があります。変更した内容は、レプリケートされたすべてのリージョンで自動的に適用されます。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

トピック

- [ディレクトリのスナップショットの作成](#)
- [スナップショットからのディレクトリの復元](#)
- [スナップショットの削除](#)

ディレクトリのスナップショットの作成

ディレクトリのスナップショットを使用することで、それが作成された時点の状態に、対象のディレクトリを復元することができます。ディレクトリのスナップショットを手動で作成するには、以下の手順を実行します。

Note

各ディレクトリに作成できる手動スナップショット数は、5 つまでに制限されています。既にこの制限に達している場合は、新しく作成する前に既存の手動スナップショットのいずれかを削除する必要があります。

、AWS Management Console、または を使用して AWS Managed Microsoft AD の手動スナップショットを作成するには AWS CLI、次の手順に従いますPowerShell。

AWS Management Console

で手動スナップショットを作成するには AWS Management Console

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Maintenance] (メンテナンス) タブを開きます。
4. [Snapshots] (スナップショット) セクションで、[Actions] (アクション)、[Create snapshot] (スナップショットの作成) の順に選択します。
5. [Create directory snapshot] (ディレクトリスナップショットの作成) ダイアログボックスで、必要に応じてスナップショットの名前を入力します。準備が整ったら、[Create] (作成) を選択します。

AWS CLI

を使用して手動スナップショットを作成するには AWS CLI

- を開きます AWS CLI。AWS Managed Microsoft AD のスナップショットを作成するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

詳細については、「[create-snapshot](#)」を参照してください。

PowerShell

を使用して手動スナップショットを作成するには PowerShell

- PowerShell を開きます。AWS Managed Microsoft AD のスナップショットを作成するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

詳細については、「[New-DSSnapshot](#)」を参照してください。

ディレクトリのサイズによっては、スナップショットの作成に数分かかる場合があります。スナップショットの準備が整うと、[Status] (ステータス) の値が「Completed」に変わります。

スナップショットからのディレクトリの復元

スナップショットからディレクトリを復元することは、ディレクトリを過去の状態に戻すことを意味します。ディレクトリスナップショットは、元となったディレクトリごとに固有です。スナップショットは、元のディレクトリにのみ復元できます。また、手動スナップショットでサポートされる最大保持期間は 180 日です。詳細については、Microsoft のウェブサイトにある「[Active Directory のシステム状態バックアップの有効保存期間](#)」を参照してください。

Warning

スナップショットを復元しようとする場合は、事前に [AWS サポート センター](#) までお問合せいただくことをお勧めします。スナップショットを復元する必要性を回避できる場合があります。スナップショットから復元した結果、現時点でのデータが失われる場合があります。この復元処理が完了するまで、ディレクトリに関連付けられているすべての DC および DNS サーバーがオフラインになることを、十分に理解しておいてください。

、または を使用してスナップショットからディレクトリを復元するには AWS Management Console AWS CLI、次の手順に従います PowerShell。

AWS Management Console

のスナップショットからディレクトリを復元するには AWS Management Console

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Maintenance] (メンテナンス) タブを開きます。
4. [Snapshots] (スナップショット) セクションでリストからスナップショットを選択し、[Actions] (アクション)、[Restore snapshot] (スナップショットの復元) の順に選択します。
5. [Restore directory snapshot] (ディレクトリスナップショットの復元) ダイアログボックスで情報を確認した後、[Restore] (復元) をクリックします。

AWS CLI

を使用してスナップショットからディレクトリを復元するには AWS CLI

1. を開きます AWS CLI。AWS Managed Microsoft AD のスナップショットを一覧表示するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

2. Managed AWS Microsoft AD をスナップショットから復元するには、[restore-from-snapshot](#) コマンドを使用できます。snapshot-id パラメータを AWS Managed Microsoft AD の復元に使用するスナップショット ID に置き換えてください。

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

PowerShell

を使用してスナップショットからディレクトリを復元するには PowerShell

1. PowerShell を開きます。AWS Managed Microsoft AD のスナップショットを一覧表示するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

2. Managed AWS Microsoft AD をスナップショットから復元するには、[Restore-DSFromSnapshot](#) コマンドを使用できます。snapshot-id パラメータを AWS Managed Microsoft AD の復元に使用するスナップショット ID に置き換えてください。

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

AWS Managed Microsoft AD ディレクトリの場合、ディレクトリが復元されるまでに 2~3 時間かかることがあります。正常に復元されると、ディレクトリの [Status] (ステータス) の値が Active に変わります。スナップショット作成後にディレクトリに対して行われた変更は、すべて上書きされます。

スナップショットの削除

、AWS Management Console、または を使用して AWS Managed Microsoft AD のスナップショットを削除するには AWS CLI、次の手順に従いますPowerShell。

AWS Management Console

でスナップショットを削除するには AWS Management Console

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Maintenance] (メンテナンス) タブを開きます。
4. [Snapshots] (スナップショット) セクションで、[Actions] (アクション)、[Delete snapshot] (スナップショットの削除) の順に選択します。

5. スナップショットを削除することを確認した上で、[Delete] (削除) をクリックします。

AWS CLI

を使用してスナップショットを削除するには AWS CLI

1. を開きます AWS CLI。AWS Managed Microsoft AD のスナップショットを一覧表示するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

2. AWS Managed Microsoft AD のスナップショットを削除するには、[delete-snapshot](#) コマンドを使用できます。snapshot-id パラメータを削除したいスナップショットのスナップショット ID に置き換えてください。

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

PowerShell

を使用してスナップショットを削除するには PowerShell

1. PowerShell を開きます。AWS Managed Microsoft AD のスナップショットを一覧表示するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

2. Managed AWS Microsoft AD をスナップショットから復元するには、[Remove-DSSnapshot](#) コマンドを使用できます。snapshot-id パラメータを削除したいスナップショットのスナップショット ID に置き換えてください。

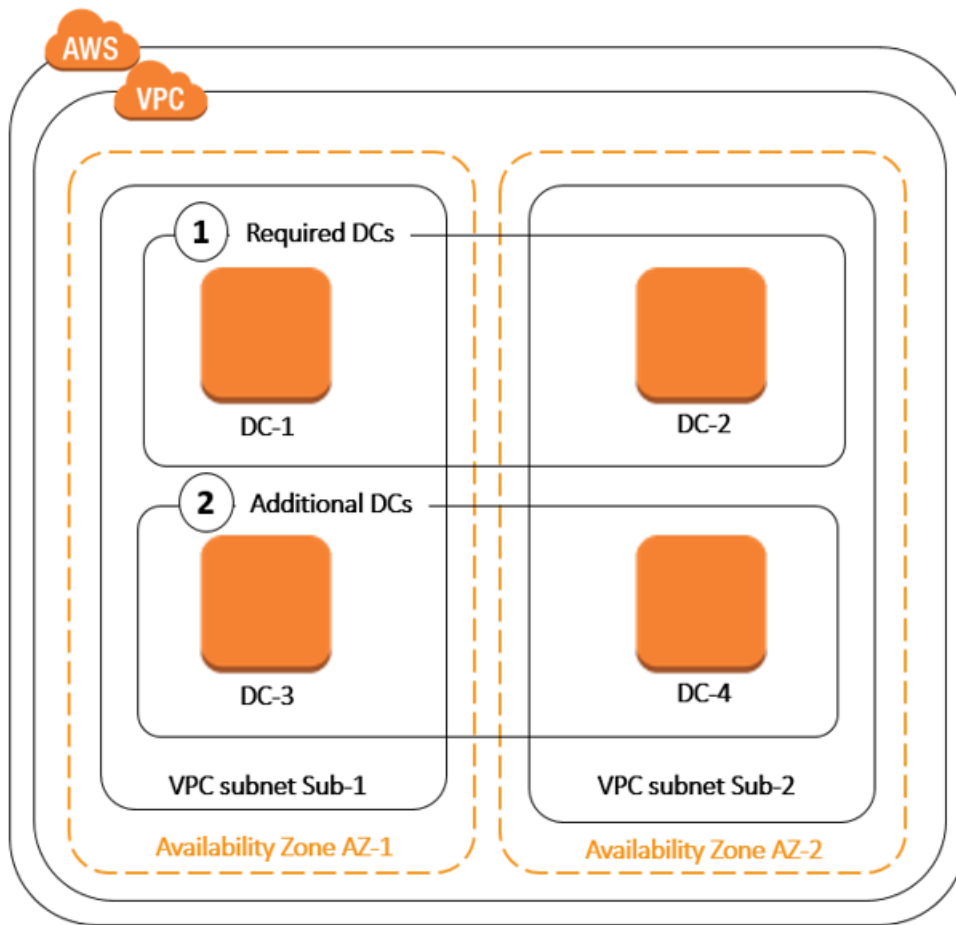
```
Remove-DSSnapshot -SnapshotId s-1234567890
```

AWS Managed Microsoft AD に追加するドメインコントローラーのデプロイ

AWS Managed Microsoft AD に追加のドメインコントローラーをデプロイすると、冗長性が向上し、耐障害性と可用性が向上します。また、Active Directory リクエストのサポート数が増え、ディレクトリのパフォーマンスが向上します。例えば、AWS Managed Microsoft AD を使用して、Amazon EC2 および Amazon RDS for SQL Server インスタンスの大規模なフリートにデプロイされている複数の .NET アプリケーションをサポートできるようになりました。

ディレクトリを初めて作成すると、AWS Managed Microsoft AD は複数のアベイラビリティーゾーンに 2 つのドメインコントローラーをデプロイします。これは高可用性の目的で必要です。後で、必要なドメインコントローラーの総数を指定するだけで、AWS Directory Service コンソールを介して追加のドメインコントローラーを簡単にデプロイできます。AWS マネージド Microsoft AD は、ディレクトリが実行されているアベイラビリティーゾーンと Amazon VPC サブネットに追加のドメインコントローラーを分散します。

例えば、次の図で DC-1 と DC-2 はディレクトリで最初に作成された 2 つのドメインコントローラーを示しています。AWS Directory Service コンソールでは、これらのデフォルトのドメインコントローラーを必須と呼びます。AWS マネージド Microsoft AD は、ディレクトリの作成プロセス中に、これらの各ドメインコントローラーを別々のアベイラビリティーゾーンに意図的に配置します。後で、さらに 2 つのドメインコントローラーを追加し、ログインのピーク時の認証負荷を分散することもできます。DC-3 と DC-4 は新しいドメインコントローラーです。これらは、コンソールで [Additional] (追加) と表示されます。以前と同様に、AWS マネージド Microsoft AD は、ドメインの高可用性を確保するために、新しいドメインコントローラーを別のアベイラビリティーゾーンに自動的に配置します。



このプロセスにより、ディレクトリデータのレプリケーション、毎日の自動スナップショット、または追加のドメインコントローラーのモニタリングを手動で設定する必要がなくなります。独自の Active Directory インフラストラクチャをデプロイして維持する必要がないため、ミッションクリティカルな Active Directory 統合のワークロードを AWS クラウド に移行して実行することも容易になります。

Managed AWS Microsoft AD に追加のドメインコントローラーをデプロイまたは削除するには、次のいずれかのツールを使用できます。

- [update-number-of-domain-controllers](#) AWS CLI コマンド
- [UpdateNumberOfDomainControllers](#) API
- [AWS Management Consoleで追加のドメインコントローラーを追加または削除する](#)

Note

追加のドメインコントローラーは、AWS Managed Microsoft AD のリージョン機能です。
「[マルチリージョンレプリケーション](#)」を使用している場合、次の手順を各リージョンで個別に適用する必要があります。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

AWS Management Consoleで追加のドメインコントローラーを追加または削除する

を使用して AWS Management Console 、 AWS Managed Microsoft AD に追加のドメインコントローラーを追加または削除できます。

前提条件

AWS Managed Microsoft AD に追加のドメインコントローラーを追加または削除する前に、ドメインコントローラーの要件に関する詳細を次に示します。

- 追加のドメインコントローラーをデプロイした後で、ドメインコントローラーの数を 2 まで減らすことができます。これは、耐障害性と高可用性を確保するために必要な最小値です。
- 削除したドメインコントローラーは、追加のドメインコントローラーのリストから削除されます。プライマリドメインコントローラーとセカンダリドメインコントローラーは必須で、削除できません。
- LDAPS を有効にするように AWS Managed Microsoft AD を設定している場合、追加したドメインコントローラーでも LDAPS が自動的に有効になります。詳細については、「[Secure LDAP \(LDAPS\) の有効化](#)」を参照してください。

手順

、または を使用して AWS Managed Microsoft AD に追加のドメインコントローラーをデプロイまたは削除するには AWS Management Console AWS CLI、次の手順に従いますPowerShell。

AWS Management Console

を使用して追加のドメインコントローラーを追加または削除するには AWS Management Console

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。

2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ドメインコントローラーを追加または削除するリージョンを選択し、[Scale & share] (スケーリングと共有) タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Scale & share] (スケーリングと共有) タブを選択します。
4. [Domain controllers] (ドメインコントローラー) セクションで、[Edit] (編集) を選択します。
5. ディレクトリに対して追加または削除するドメインコントローラーの数を指定し、[Modify] (変更) をクリックします。
6. AWS Managed Microsoft AD がデプロイプロセスを完了すると、すべてのドメインコントローラーにアクティブステータスが表示され、割り当てられたアベイラビリティーゾーンと Amazon VPC サブネットの両方が表示されます。新しいドメインコントローラーは、ディレクトリがデプロイ済みのアベイラビリティーゾーンとサブネットに均等に分散されます。

AWS CLI

を使用して追加のドメインコントローラーを追加または削除するには AWS CLI

1. を開きます AWS CLI。ドメインコントローラーの現在の数を確認するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

2. ドメインコントローラーを追加または削除するには、[update-number-of-domain-controllers](#) コマンドを使用できます。たとえば、次のコマンドを使用してドメインコントローラーの総数を 4 に設定することができます。Directory ID を AWS Managed Microsoft AD Directory ID に置き換え、desired-number パラメータをデプロイするドメインコントローラーの数に置き換えます。

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

PowerShell

を使用して追加のドメインコントローラーを追加または削除するには PowerShell

1. PowerShell を開きます。ドメインコントローラーの現在の数を確認するには、次のコマンドを実行し、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

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

2. ドメインコントローラーを追加または削除するには、[Set-DSDomainControllerCount](#) コマンドを使用できます。たとえば、次のコマンドを使用してドメインコントローラーの総数を 4 に設定することができます。Directory ID を AWS Managed Microsoft AD Directory ID に置き換え、DesiredNumber パラメータをデプロイするドメインコントローラーの数に置き換えます。

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

関連する AWS セキュリティブログ記事

- [ドメインコントローラーを追加して、AWS Managed Microsoft AD AWS Directory Service の冗長性とパフォーマンスを向上させる方法](#)

AWS Managed Microsoft AD のアップグレード

Standard Edition AWS Managed Microsoft AD を Enterprise Edition にアップグレードできます。以下に、Standard Edition と Enterprise Edition の違いの概要を示します。

- Standard Edition: AWS Managed Microsoft AD (Standard Edition) は、従業員数が 5,000 名までの、中小企業向けのプライマリディレクトリとして最適化されています。ユーザー、グループ、コンピュータなど、最大 30,000* のディレクトリオブジェクトをサポートするために十分なストレージ容量を提供します。
- Enterprise Edition: AWS Managed Microsoft AD (Enterprise Edition) は、最大 500,000* のディレクトリオブジェクトをサポートする、エンタープライズ組織向けに設計されています。

* 上限数は概数です。ディレクトリでサポートできるディレクトリオブジェクトの数は、オブジェクトのサイズ、アプリケーションの動作やパフォーマンスニーズに応じて増減する場合があります。

Standard Edition AWS Managed Microsoft AD Active Directoryを Enterprise Edition にアップグレードするには、に連絡する必要があります サポート。詳細については、「AWS サポート ユーザーガイド」の「[サポートケースの作成およびケース管理](#)」を参照してください。

 Note

マルチリージョンレプリケーションは、以下のリージョンの AWS Managed Microsoft AD Enterprise Edition でのみ使用できます。

- 米国東部(オハイオ)
- 米国東部 (バージニア北部)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アジアパシフィック (ムンバイ)
- アジアパシフィック (大阪)
- アジアパシフィック (ソウル)
- アジアパシフィック (シンガポール)
- アジアパシフィック (シドニー)
- アジアパシフィック (タイ)
- アジアパシフィック (東京)
- カナダ (中部)
- 中国 (北京)
- 中国 (寧夏)
- メキシコ (中部)
- 欧州 (フランクフルト)
- 欧州 (アイルランド)
- 欧州 (ロンドン)
- 欧州 (パリ)
- 欧州 (ストックホルム)
- 南米 (サンパウロ)
- AWS GovCloud (米国西部)
- AWS GovCloud (米国東部)

AWS Managed Microsoft AD をアップグレードするときに注意すべき制限がいくつかあります。具体的には次の 2 つです。

- アップグレードには追加料金が発生します。詳細については、「[AWS Directory Service 料金表](#)」を参照してください。
- Active Directory がアップグレードされると、以前のエディションに戻すことはできません。
- 以前のスナップショットは、アップグレード後の Active Directory の復元には使用できません。
- アップグレードは、合意されたスケジュールされた日時で行われます サポート。アップグレードは、太平洋標準時の月曜日から金曜日の午前 9 時から午後 5 時までに行われます。
- アップグレードプロセスには 4～5 時間かかります。
- アップグレードプロセス中、AWS Managed Microsoft AD のドメインコントローラーは一度に 1 つずつアップグレードされます。これにより、パフォーマンスに悪影響を与え、メンテナンスウィンドウ中にダウンタイムが発生する可能性があります。
- アップグレードプロセスでは、各ドメインコントローラーインスタンスのホスト名が変更されますが、IP アドレスは変更しません。
- LDAPS (SSL 経由の Lightweight Directory Access Protocol) を使用している場合、ドメインコントローラーには新しい証明書が必要です。

AWS Managed Microsoft AD への代替 UPN サフィックスの追加

AWS Managed Microsoft AD ディレクトリに代替ユーザープリンシパル名 Active Directory (UPN) サフィックスを追加することで、(AD) ログイン名の管理を簡素化し、ユーザーログインエクスペリエンスを向上させることができます。そのためには、Admin アカウント、または AWS Delegated User Principal Name Suffix Administrators グループのメンバーであるアカウントでログインする必要があります。このグループの詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。

代替の UPN サフィックスを追加するには

1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2/>) を開きます。
2. AWS Managed Microsoft AD ディレクトリに参加している Amazon EC2 インスタンスを見つけます。対象のインスタンスを選択し、[Connect] (接続) をクリックします。
3. サーバーマネージャー のウィンドウで、[Tools] (ツール) をクリックします。次に、[Active Directory Domains and Trusts] (Active Directory のドメインと信頼) を選択します。

4. 左側のペインで、[Active Directory Domains and Trusts] (Active Directory のドメインと信頼) を右クリックし、[Properties] (プロパティ) を選択します。
5. [UPN Suffixes] (UPN サフィックス) タブで、代わりの UPN サフィックス (**sales.example.com** など) を入力します。[Add] (追加)、[Apply] (適用) の順に選択します。
6. 代わりの UPN サフィックスをさらに追加する必要がある場合は、必要な UPN サフィックスを得られるまでステップ 5 を繰り返します。

AWS Managed Microsoft AD ディレクトリのサイト名の変更

AWS Managed Microsoft AD ディレクトリのデフォルトサイト名を変更して、既存の Microsoft Active Directory (AD) サイト名と一致させることができます。これにより、AWS Managed Microsoft AD はオンプレミスディレクトリ内の既存の AD ユーザーをすばやく検索して認証できます。その結果、ユーザーは AWS Managed Microsoft AD ディレクトリに結合した [Amazon EC2](#) や [Amazon RDS for SQL Server](#) インスタンスなどの AWS リソースにログインしやすくなります。

そのためには、[管理者] アカウントまたは [AWS が委任したサイトとサービスの管理者] グループのメンバーであるアカウントでログインする必要があります。このグループの詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。

サイト名の変更において、信頼に関連したその他の利点については、Microsoft ウェブサイトの「[Domain Locator Across a Forest Trust](#)」(フォレストトラスト全体のドメインロケーター) を参照してください。

AWS Managed Microsoft AD サイト名を変更するには

1. Amazon EC2 コンソールの <https://console.aws.amazon.com/ec2/> を開いてください。
2. AWS Managed Microsoft AD ディレクトリに参加している Amazon EC2 インスタンスを見つけます。対象のインスタンスを選択し、[Connect] (接続) をクリックします。
3. サーバーマネージャー のウィンドウで、[Tools] (ツール) をクリックします。次に、[Active Directory Sites and Services] (Active Directory サイトとサービス) をクリックします。
4. 左側のペインで、[Sites] フォルダを展開し、サイト名 (デフォルトは「Default-Site-Name」) を右クリックした上で、[Rename] (名前変更) を選択します。
5. 新しいサイト名を入力し、[Enter] (確定) をクリックします。

AWS Managed Microsoft AD の削除

AWS Managed Microsoft AD または Simple AD を削除すると、すべてのディレクトリデータとスナップショットが削除され、復元できなくなります。ディレクトリが削除されても、ディレクトリに結合されているインスタンスはすべてそのまま残ります。ただし、ディレクトリの認証情報を使用して、これらのインスタンスにログインすることはできません。これらのインスタンスにログインするには、インスタンス専用のユーザーアカウントを使用します。

AD Connector を削除してもオンプレミスのディレクトリはそのまま残ります。ディレクトリに結合されているインスタンスもすべてそのまま残り、オンプレミスのディレクトリに結合された状態のまま変わりません。引き続き、ディレクトリの認証情報を使用して、このインスタンスにログインできます。

ディレクトリを削除するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。Active Directory がデプロイ AWS リージョン されている いることを確認します。詳細については、「[リージョンの選択](#)」を参照してください。
2. 削除するディレクトリに対して AWS アプリケーションが有効になっていないことを確認します。有効な AWS アプリケーションでは、AWS Managed Microsoft AD または Simple AD を削除することはできません。
 - a. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
 - b. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。AWS アプリケーションとサービスセクションには、ディレクトリで有効になっている AWS アプリケーションが表示されます。
 - AWS Management Console アクセスを無効にします。詳細については、「[AWS Management Console アクセスの無効化](#)」を参照してください。
 - Amazon WorkSpaces を無効にするには、WorkSpaces コンソールでディレクトリからサービスを登録解除する必要があります。詳細については、Amazon WorkSpaces 管理ガイドの「[ディレクトリの削除](#)」を参照してください。
 - WorkDocs を無効にするには、WorkDocs コンソールで WorkDocs サイトを削除する必要があります。詳細については、「Amazon WorkDocs Administration Guide」(Amazon WorkDocs 管理ガイド) の「[Delete a site](#)」(サイトを削除する) を参照してください。
 - Amazon WorkMail を無効にするには、Amazon WorkMail コンソールで Amazon WorkMail 組織を削除する必要があります。詳細については、「Amazon WorkMail

Administrator Guide」(Amazon WorkMail 管理者ガイド)の「[Remove an organization](#)」(組織を削除する)を参照してください。

- Amazon FSx for Windows File Server を無効にするには、ドメインから Amazon FSx ファイルシステムを削除する必要があります。詳細については、「Amazon FSx for Windows File Server User Guide」の「[Working with Active Directory in FSx for Windows File Server](#)」を参照してください。
- Amazon Relational Database Service を無効にするには、ドメインから Amazon RDS インスタンスを削除する必要があります。詳細については、「[Amazon RDS ユーザーガイド](#)」の「ドメインの DB インスタンスの管理」を参照してください。
- AWS Client VPN サービスを無効にするには、クライアント VPN エンドポイントから ディレクトリサービスを削除する必要があります。詳細については、「AWS Client VPN 管理者ガイド」の「[Work with Client VPN](#)」を参照してください。
- Amazon Connect を無効にするには、Amazon Connect インスタンスを削除する必要があります。詳細については、「Amazon Connect 管理者ガイド」の「[Delete your Amazon Connect instance](#)」を参照してください。
- Amazon QuickSight を無効にするには、Amazon QuickSight のサブスクリプションを解除する必要があります。詳細については、Amazon QuickSight ユーザーガイドの[Amazon QuickSight 「アカウントの閉鎖」](#)を参照してください。

 Note

を使用して AWS IAM Identity Center、以前に削除予定の AWS Managed Microsoft AD ディレクトリに接続したことがある場合は、削除する前に ID ソースを変更する必要があります。詳細については、「IAM Identity Center ユーザーガイド」の「[ID ソースを変更する](#)」を参照してください。

3. ナビゲーションペインで [Directories] (ディレクトリ) を選択します。
4. 削除するディレクトリのみを選択し、[Delete] (削除) をクリックします。ディレクトリが削除されるまでに数分かかります。ディレクトリを削除すると、ディレクトリリストからも削除されます。

AWS Managed Microsoft AD を保護する

パスワードポリシー、多要素認証 (MFA) などの機能、および設定を使用して AWS Managed Microsoft AD を保護できます。ディレクトリを保護する方法は次のとおりです:

- [Managed Microsoft AD ユーザーに適用できるように、 のパスワードポリシーがどのようにActive Directory機能するかを理解します。](#) AWS AWS Managed Microsoft AD パスワードポリシーを管理できるユーザーを委任することもできます。
- AWS Managed Microsoft AD のセキュリティを強化する [MFA を有効にします。](#)
- 「[>Secure Socket Layer \(SSL\)/Transport Layer Security \(TLS\) \(LDAPS\) を介した Lightweight Directory Access Protocol を有効にする](#)」と、LDAP を介した通信が暗号化され、セキュリティが向上します。
- [AWS Managed Microsoft AD のコンプライアンスを、Federal Risk and Authorization Management Program \(FedRAMP\) や Payment Card Industry \(PCI\) Data Security Standard \(DSS\) などの標準に従って管理します。](#) FedRAMP
- 環境のニーズに合わせて AWS セキュリティグループを変更することで、[AWS Managed Microsoft AD ネットワークセキュリティ設定> を強化](#)します。
- ニーズに合わせて、証明書ベース認証、セキュアチャネル暗号、プロトコルなどの [AWS Managed Microsoft AD ディレクトリのセキュリティ設定を編集](#)します。
- [AWS Private Certificate Authority Connector for AD を設定](#)して、AWS Managed Microsoft AD の証明書を発行および管理できるようにします AWS Private CA。

AWS Managed Microsoft AD パスワードポリシーについて

AWS Managed Microsoft AD では、Managed Microsoft AD ドメインで管理するユーザーのグループに対して、異なるパスワードポリシーとアカウントロックアウトポリシー ([きめ細かなパスワードポリシー](#)とも呼ばれます) AWS を定義して割り当てることができます。AWS Managed Microsoft AD ディレクトリを作成すると、デフォルトのドメインポリシーが作成され、に適用されますActive Directory。このポリシーには、以下の設定が含まれます。

ポリシー	設定
適用されるパスワード履歴	24 個のパスワードを記憶
パスワードの最長有効期間	42 日間 *
パスワードの最短有効期間	1 日
パスワードの最小長	7 文字
パスワードに一定の複雑さを要求	有効

ポリシー	設定
可逆的暗号化を使用したパスワードの保存	無効

Note

* パスワードにおける 42 日間の最大有効期間は、管理者パスワードにも適用されます。

例えば、機密レベルが低い情報にのみアクセスする従業員には、厳格度の低いポリシー設定を割り当てることができます。機密情報に定期的にアクセスする上級管理者には、より厳格な設定を適用します。

以下のリソースでは、Microsoft Active Directory きめ細かなパスワードポリシーとセキュリティポリシーに関する詳細情報を提供します。

- [セキュリティポリシー設定を構成する](#)
- [パスワードの複雑さに関する要件](#)
- [パスワードの複雑さに関するセキュリティ上の考慮事項](#)

AWS は、AWS Managed Microsoft AD で設定してグループに割り当てることができる詳細なパスワードポリシーのセットを提供します。ポリシーを構成するには、標準の Microsoft ポリシーツール、例えば「[Active Directory 管理センター](#)」を使用できます。Microsoft ポリシーツールの使用を開始するには、[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#) を参照してください。

パスワードポリシーの適用方法

きめ細かなパスワードポリシーの適用方法は、パスワードがリセットされたか変更されたかによって異なります。ドメインユーザーも自分のパスワードを変更できます。必要なアクセス許可を持つ Active Directory 管理者またはユーザーは、[ユーザーのパスワードをリセット](#) できます。詳細については、以下の図表を参照してください。

ポリシー	パスワードのリセット	パスワードの変更
適用されるパスワード履歴	 いいえ	 はい
パスワードの最長有効期間	 はい	 はい
パスワードの最短有効期間	 いいえ	 はい
パスワードの最小長	 はい	 はい
パスワードに一定の複雑さを要求	 はい	 はい

これらの違いにはセキュリティ上の影響があります。例えば、ユーザーのパスワードがリセットされるたびに、パスワードの実施履歴とパスワードの最小有効期間ポリシーは実施されません。詳細については、「[パスワード履歴を強制適用](#)」と「[パスワードの最小有効期間](#)」ポリシーと関わるセキュリティ上の考慮事項に関する Microsoft ドキュメントを参照してください。

サポートされているポリシー設定

AWS Managed Microsoft AD には、編集不可能な優先順位値を持つ 5 つのきめ細かなポリシーが含まれています。このポリシーでは複数のプロパティの設定が可能で、パスワードの強度を指定したり、ログインが失敗した場合のアカウントロックアウトのアクションを適用したりできます。ポリ

シーは、ゼロ個以上の Active Directory グループに割り当てることができます。エンドユーザーが複数のグループのメンバーであり、複数のパスワードポリシーが適用されている場合には、Active Directory が優先順位値の最も小さいポリシーを適用します。

AWS 事前定義されたパスワードポリシー

次の表に、AWS Managed Microsoft AD ディレクトリに含まれる 5 つのポリシーと、割り当てられた優先順位の値を示します。詳細については、「[優先順位](#)」を参照してください。

ポリシー名	優先順位
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
CustomerPSO-05	50

パスワードポリシーのプロパティ

パスワードポリシーにおいて以下のプロパティを編集することで、ビジネスからのニーズに応じたコンプライアンス標準に準拠させられます。

- ポリシー名
- [適用されるパスワード履歴](#)
- [パスワードの最小長](#)
- [パスワードの最短有効期間](#)
- [パスワードの最長有効期間](#)
- [可逆的暗号化を使用したパスワードの保存](#)
- [パスワードに一定の複雑さを要求](#)

これらのポリシーの優先順位値は、変更することはできません。これらの設定がパスワードの適用に及ぼす影響の詳細については、Microsoft TechNet ウェブサイトの「[AD DS: Fine-grained password policies](#)」(AD DS: きめ細かなパスワードポリシー) を参照してください。これらのポリシーの一般的

な情報については、[Microsoft TechNet](#) ウェブサイトの「Password policy」(パスワードポリシー) を参照してください。

アカウントロックアウトのポリシー

パスワードポリシーでは以下のプロパティを変更することもでき、Active Directory がログインの失敗後にアカウントをロックアウトするかどうかと、その方法を指定できます。

- ログオン試行の失敗の許容回数
- アカウントをロックアウトする期間
- 失敗したログオン試行の特定期間後のリセット

これらのポリシーの一般的な情報については、Microsoft TechNet ウェブサイトの「[Account lockout policy](#)」(アカウントロックアウトのポリシー) を参照してください。

優先順位

優先順位値が低いポリシーほど、その優先順位が高くなります。ユーザーは、パスワードポリシーを Active Directory セキュリティグループに割り当てます。パスワードポリシーは各セキュリティグループに通常 1 つ適用するものですが、単一のユーザーに複数のポリシーを適用することはできます。例えば、jsmith は HR グループのメンバーであり、さらに MANAGERS グループのメンバーでもあるとします。CustomerPSO-05 (優先順位値は 50) を HR グループに割り当て、CustomerPSO-04 (優先順位値は 40) を MANAGERS に割り当てると、優先順位は CustomerPSO-04 の方が高いため、Active Directory ではこのポリシーを jsmith に適用します。

ユーザーまたはグループに複数のポリシーを割り当てた場合、Active Directory は適用するポリシーを、次のように決定します。

1. ユーザーオブジェクトに直接割り当てたポリシーが適用されます。
2. ユーザーオブジェクトに直接割り当てられたポリシーがない場合には、グループのメンバーに参加することでユーザーが受け取ったすべてのポリシーの中で、優先順位値が最も小さいポリシーが適用されます。

詳細については、Microsoft TechNet ウェブサイトの「[AD DS: Fine-grained password policies](#)」(AD DS: きめ細かなパスワードポリシー) を参照してください。

トピック

- [AWS Managed Microsoft AD ユーザーにパスワードポリシーを割り当てる](#)

- [AWS Managed Microsoft AD パスワードポリシーを管理できるユーザーを委任する](#)

関連する AWS セキュリティブログ記事

- [AWS Directory Service for AWS Managed Microsoft AD を使用して、セキュリティ基準を満たすためにさらに強力なパスワードポリシーを設定する方法](#)

AWS Managed Microsoft AD ユーザーにパスワードポリシーを割り当てる

[AWS が委任したきめ細かいパスワードポリシーの管理者] セキュリティグループのメンバーであるユーザーアカウントは、次の手順に従ってユーザーとセキュリティグループにポリシーを割り当てることができます。

パスワードポリシーをユーザーに割り当てるには

1. Managed Microsoft AD ドメインに結合したマネージド EC2 インスタンスから [Active Directory 管理センター \(ADAC\)](#) を起動します。AWS
2. [Tree View] (ツリービュー) に切り替え、System\Password Settings Container に移動します。
3. 編集対象の、きめ細かなポリシーをダブルクリックします。[Add] (追加) をクリックして、ポリシーのプロパティを編集し、ユーザーまたはセキュリティグループをそのポリシーに追加します。AWS Managed Microsoft AD にデフォルトで用意された、きめ細かなポリシーの詳細については、「[AWS 事前定義されたパスワードポリシー](#)」を参照してください。
4. パスワードポリシーが適用されていることを確認するには、次の PowerShell コマンドを実行します。

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

Note

結果が不正確になる可能性があるため、net user コマンドは使用しないでください。

AWS Managed Microsoft AD ディレクトリで 5 つのパスワードポリシーのいずれかを設定しない場合、Active Directory はデフォルトのドメイングループポリシーを使用します。Password Settings Container (パスワード設定コンテナ) の詳細な使用方法については、こちらの [Microsoft ブログ記事](#) を参照してください。

AWS Managed Microsoft AD パスワードポリシーを管理できるユーザーを委任する

AWS Managed Microsoft AD で作成した特定のユーザーアカウントにパスワードポリシーを管理するアクセス許可を委任するには、そのアカウントをAWS 委任されたきめ細かなパスワードポリシー管理者のセキュリティグループに追加します。このグループのメンバーに参加したアカウントには、[上記](#)で示したパスワードポリシーのすべてを、編集および設定する権限が与えられます。

パスワードポリシーの管理権限を委任するには

1. Managed Microsoft AD ドメインに結合したマネージド EC2 インスタンスから [Active Directory 管理センター \(ADAC\)](#) を起動します。AWS
2. [ツリービュー] に切り替え、[AWS の委任グループ] OU に移動します。この OU の詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。
3. [AWS が委任したきめ細かいパスワードポリシーの管理者] ユーザーグループを検索します。使用しているドメインからこのグループに、任意のユーザーまたはグループを追加します。

AWS Managed Microsoft AD の多要素認証の有効化

AWS Managed Microsoft AD ディレクトリの多要素認証 (MFA) を有効にして、ユーザーがサポートされている Amazon Enterprise アプリケーションにアクセスするための AD 認証情報を指定するときにセキュリティを強化できます。MFA が有効化されている場合、ユーザーは、通常と同じくユーザーネームとパスワード (第 1 要素) を入力した後、仮想 MFA ソリューションまたはハードウェア MFA ソリューションから取得する認証コード (第 2 要素) も入力する必要があります。これらの要素によって、有効なユーザー認証情報に加えて MFA コードをユーザーが提供しない限り、Amazon エンタープライズアプリケーションへのアクセスが許可されないというセキュリティが追加されます。

MFA を有効にするには、MFA ソリューションとして [Remote Authentication Dial-In User Service \(RADIUS\)](#) サーバーを使用するか、オンプレミスインフラストラクチャに RADIUS サーバー用の MFA プラグインを実装しておく必要があります。MFA ソリューションでは、ワンタイムパスコード (OTP) を実装する必要があります。ユーザーは、ハードウェアデバイスから、または携帯電話などのデバイスで実行されるソフトウェアから、このコードを取得します、

RADIUS は、業界標準のクライアント/サーバープロトコルであり、ユーザーをネットワークサービスに接続するための認証、認可、アカウント管理の機能を提供します。AWS Managed Microsoft AD には、MFA ソリューションを実装した RADIUS サーバーに接続する RADIUS クライアントが含まれています。この RADIUS サーバーが、ユーザーネームと OTP コードを検証します。RADIUS サーバーがユーザーを正常に検証すると、AWS マネージド Microsoft AD は Active Directory に対し

てユーザーを認証します。Active Directory に対する認証に成功したユーザーは、AWS アプリケーションにアクセスできるようになります。AWS Managed Microsoft AD RADIUS クライアントと RADIUS サーバー間の通信では、ポート 1812 を介した通信を有効にする AWS セキュリティグループを設定する必要があります。

Managed AWS Microsoft AD ディレクトリの多要素認証を有効にするには、次の手順を実行します。RADIUS サーバーと AWS Directory Service および MFA を連携させるための設定方法については、「[Multi-Factor-Authentication の前提条件](#)」を参照してください。

考慮事項

AWS Managed Microsoft AD の多要素認証に関する考慮事項を次に示します:

- Multi-Factor-Authentication は、Simple AD では使用できません。ただし、AD Connector ディレクトリでは、MFA を有効にすることができます。詳細については、「[AD Connector の多要素認証を有効にする](#)」を参照してください。
- MFA は AWS Managed Microsoft AD のリージョン機能です。[マルチリージョンレプリケーション](#)を使用している場合は、AWS Managed Microsoft AD のプライマリリージョンでのみ MFA を使用できます。
- Managed AWS Microsoft AD を外部通信に使用する場合は、これらの通信用に AWS ネットワーク外のネットワークアドレス変換 (NAT) インターネットゲートウェイまたはインターネットゲートウェイを設定することをお勧めします。
 - AWS Managed Microsoft AD と AWS ネットワークでホストされている RADIUS サーバー間の外部通信をサポートする場合は、お問い合わせください[サポート](#)。
- WorkSpaces、WorkDocs、Amazon WorkMail、Amazon QuickSight、およびへのアクセスを含むすべての Amazon Enterprise IT アプリケーション AWS IAM Identity Center AWS Management Console は、MFA で AWS Managed Microsoft AD および AD Connector を使用する場合にサポートされます。MFA を使用するこれらの AWS アプリケーションは、マルチリージョンではサポートされていません。

詳細については、[AWS 「Managed Microsoft AD とオンプレミス認証情報を使用して AWS サービスの多要素認証を有効にする方法」](#)を参照してください。

- Amazon Enterprise アプリケーションへの基本的なユーザーアクセス、AWS シングルサインオン、AWS Management Console の使用を設定する方法については AWS Directory Service、「」および「」を参照してください[AWS Managed Microsoft AD から AWS アプリケーションとサービスへのアクセスAWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化](#)。

- Managed Microsoft AD で Amazon WorkSpaces ユーザーの MFA を有効にする方法、AWS Managed Microsoft AD とオンプレミス認証情報を使用してサービスの多要素認証を有効にする方法については、次の AWS セキュリティブログ記事を参照してください。 [AWSAWS](#)

AWS Managed Microsoft AD の Multi-Factor Authentication を有効にする

次の手順では、AWS Managed Microsoft AD の多要素認証を有効にする方法を示します。

1. RADIUS MFA サーバーと AWS Managed Microsoft AD ディレクトリの IP アドレスを特定します。
2. Virtual Private Cloud (VPC) セキュリティグループを編集して、AWS Managed Microsoft AD IP エンドポイントと RADIUS MFA サーバー間のポート 1812 経由の通信を有効にします。
3. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
4. AWS Managed Microsoft AD ディレクトリのディレクトリ ID リンクを選択します。
5. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、MFA を有効にするリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
6. [Multi-factor authentication] セクションで、[Actions] (アクション)、[Enable] (有効化) の順に選択します。
7. [Enable multi-factor authentication (MFA)] (Multi-Factor Authentication (MFA) の有効化) ページで、次の値を指定します。

[Display label] (表示ラベル)

ラベル名を指定します。

[RADIUS server DNS name or IP addresses] (RADIUS サーバーの DNS 名または IP アドレス)

RADIUS サーバーエンドポイントの IP アドレス、または、RADIUS サーバーロードバランサーの IP アドレス。カンマで区切って、複数の IP アドレスを入力できます (例えば、192.0.0.0,192.0.0.12)。

 Note

RADIUS MFA は、WorkSpaces AWS Management Console、Amazon QuickSight、Amazon Chime などの Amazon Enterprise アプリケーションおよびサービスへのアクセスを認証する場合にのみ適用されます。WorkSpaces Amazon Enterprise のアプリケーションとサービスは、マルチリージョンレプリケーションが AWS Managed Microsoft AD 用に設定されている場合、プライマリリージョンでのみサポートされます。EC2 インスタンスで実行されている Windows ワークロード、または EC2 インスタンスにサインインするための MFA は提供されません。AWS Directory Service は RADIUS チャレンジレスポンス認証をサポートしていません。ユーザーは、ユーザー名とパスワードを入力するときに MFA コードが必要になります。または、ユーザーのプッシュ通知や認証ワンタイムパスワード (OTP) などの MFA out-of-band を実行するソリューションを使用する必要があります。帯域外 MFA ソリューションでは、ソリューションに合わせて RADIUS タイムアウト値を適切に設定する必要があります。帯域外 MFA ソリューションを使用している場合、ユーザーはサインインページで MFA コードの入力を求められます。この場合、ユーザーはパスワードフィールドと MFA フィールドの両方に、自分のパスワードを入力します。

[Port] (ポート)

RADIUS サーバーが通信のために使用しているポート。オンプレミスネットワークでは、AWS Directory Service サーバーからのデフォルトの RADIUS サーバーポート (UDP:1812) 経由のインバウンドトラフィックを許可する必要があります。

[Shared secret code] (共有シークレットコード)

RADIUS エンドポイントの作成時に指定された共有シークレットコード。

[Confirm shared secret code] (共有シークレットコードの確認)

RADIUS エンドポイントの共有シークレットコードを確認します。

[Protocol] (プロトコル)

RADIUS エンドポイントの作成時に指定されたプロトコルを選択します。

[Server timeout (in seconds)] (サーバータイムアウト (秒単位))

RADIUS サーバーのレスポンスを待つ時間 (秒)。これは 1～50 の範囲の値にする必要があります。

 Note

RADIUS サーバのタイムアウトは、20 秒以下に設定することが推奨されます。20 秒を超えるタイムアウトを使用すると、システムは別の RADIUS サーバで再試行できなくなり、タイムアウトで失敗する可能性があります。

[Max RADIUS request retries] (RADIUS リクエストの最大再試行数)

RADIUS サーバーとの通信を試みる回数。これは 0～10 の範囲の値にする必要があります。

Multi-Factor Authentication は、[RADIUS Status] (RADIUS 状態) が [Enabled] (有効) に変わると使用できます。

8. [Enable] (有効化) を選択します。

Secure LDAP (LDAPS) の有効化

LDAP (Lightweight Directory Access Protocol) は、Active Directory に対するデータの読み書きに使用される標準の通信プロトコルです。一部のアプリケーションでは、LDAP を使用して Active Directory のユーザーやグループの追加、削除、または検索を行ったり、そのユーザーを認証するための認証情報を転送したりします。すべての LDAP 通信には、クライアント (アプリケーションなど) とサーバー (Active Directory など) が含まれています。

デフォルトでは、LDAP を介した通信は暗号化されません。そのため、悪意のあるユーザーがネットワークモニタリング用のソフトウェアを使用して、送信されるデータパケットを傍受する可能性があります。この傍受を防止するために、通常、多くの企業のセキュリティポリシーでは、すべての LDAP 通信を暗号化することを組織に義務付けています。

この形式のデータ漏えいを軽減するために、AWS マネージド Microsoft AD には、LDAPS と呼ばれる Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 経由で LDAP を有効にするオプションがあります。LDAPS を使用するユーザーは、ネットワーク全体のセキュリティを向上させる

ことができます。LDAP 対応アプリケーションと AWS Managed Microsoft AD 間のすべての通信を暗号化することで、コンプライアンス要件を満たすこともできます。

AWS Managed Microsoft AD は、以下のデプロイシナリオで LDAPS をサポートします。

- サーバー側 LDAPS は、商用または自社製の (LDAP クライアントとして動作する) LDAP 対応アプリケーションと、(LDAP サーバーとして動作する) AWS Managed Microsoft AD との間で、LDAP 通信を暗号化します。詳細については、「[AWS Managed Microsoft AD を使用したサーバー側の LDAPS の有効化](#)」を参照してください。
- クライアント側の LDAPS: WorkSpaces などの (LDAP クライアントとして動作する) AWS アプリケーションと、自己管理型 (オンプレミス) Active Directory (LDAP サーバーとして動作する) の間の LDAP 通信を暗号化します。詳細については、「[AWS Managed Microsoft AD を使用したクライアント側の LDAPS の有効化](#)」を参照してください。

の実装のセキュリティ保護に関するベストプラクティスの詳細については Certificate Services、Microsoft Active Directory「[Microsoft ドキュメント](#)」を参照してください。

トピック

- [AWS Managed Microsoft AD を使用したサーバー側の LDAPS の有効化](#)
- [AWS Managed Microsoft AD を使用したクライアント側の LDAPS の有効化](#)

AWS Managed Microsoft AD を使用したサーバー側の LDAPS の有効化

サーバー側の Lightweight Directory Access Protocol Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) は、商用または自社開発の LDAP 対応アプリケーションと AWS Managed Microsoft AD ディレクトリ間の LDAP 通信を暗号化します。これにより、Secure Sockets Layer (SSL) 暗号化プロトコルを使用してネットワーク全体のセキュリティを強化し、コンプライアンス要件を満たすことができます。

サーバー側の LDAPS を有効化する

サーバー側の LDAPS と認証機関 (CA) サーバーをセットアップおよび設定する方法の詳細については、AWS セキュリティブログの[AWS「Managed Microsoft AD Directory のサーバー側の LDAPS を有効にする方法」](#)を参照してください。

ほとんどの設定は、AWS Managed Microsoft AD ドメインコントローラーの管理に使用されている Amazon EC2 インスタンスから行う必要があります。次の手順では、AWS クラウドでドメインの LDAPS を有効にする方法について説明します。

オートメーションを使用して PKI インフラストラクチャを設定する場合は、[Microsoft Public Key Infrastructure on AWS QuickStart ガイド](#)を使用できます。具体的には、[Deploy Microsoft PKI into an existing VPC on AWS](#) で、テンプレートをロードする方法について、ガイドの指示に従います。テンプレートをロードした場合には、[Active Directory Domain Services Type] (Active Directory ドメインのサービスタイプ) のオプション設定時に、必ず **AWSManaged** を選択します。QuickStart ガイドを使用している場合は、直接 [ステップ 3: 証明書テンプレートを作成する](#) に移動できます。

トピック

- [ステップ 1: LDAPS を有効化する権限を委任する](#)
- [ステップ 2: 認証機関を設定する](#)
- [ステップ 3: 証明書テンプレートを作成する](#)
- [ステップ 4: セキュリティグループのルールを追加する](#)

ステップ 1: LDAPS を有効化する権限を委任する

サーバー側の LDAPS を有効にするには、AWS Managed Microsoft AD ディレクトリの管理者または AWS 委任されたエンタープライズ認証機関管理者グループのメンバーである必要があります。または、デフォルトの管理ユーザー (管理者アカウント) であれば、この権限を保持しています。必要に応じて、LDAPS を設定するために、管理者アカウント以外のユーザーを使用することができます。この場合、そのユーザーを AWS Managed Microsoft AD ディレクトリの管理者または AWS 委任されたエンタープライズ認証機関管理者グループに追加します。

ステップ 2: 認証機関を設定する

サーバー側の LDAPS を有効にする前に、証明書を作成する必要があります。この証明書は、AWS Managed Microsoft AD ドメインに参加している Microsoft エンタープライズ CA サーバーによって発行される必要があります。作成された証明書は、対象ドメインの各ドメインコントローラーにインストールします。この証明書により、ドメインコントローラーの LDAP サービスは LDAP クライアントからの SSL 接続をリッスンし、自動的に承認できます。

Note

AWS Managed Microsoft AD を使用したサーバー側の LDAPS は、スタンドアロン CA によって発行された証明書をサポートしていません。また、サードパーティーの認証機関により発行された証明書もサポートしていません。

ドメインの CA の設定または接続には、ビジネスのニーズに応じて以下のオプションを使い分けることができます。

- 下位 Microsoft Enterprise CA を作成する – (推奨) このオプションを使用すると、下位 Microsoft Enterprise CA サーバーを AWS クラウドにデプロイできます。サーバーは、Amazon EC2 を使用することで、既存のルート Microsoft CA との連携が可能です。下位 Microsoft エンタープライズ CA を設定する方法の詳細については、「マネージド Microsoft AD ディレクトリのサーバー側の LDAPS を有効にする方法」の「ステップ 4: AWS Microsoft エンタープライズ CA を Microsoft AD ディレクトリに追加する」を参照してください。 [AWS](#)
- ルート Microsoft エンタープライズ CA を作成する – このオプションを使用すると、Amazon EC2 を使用して AWS クラウドにルート Microsoft エンタープライズ CA を作成し、それを AWS Managed Microsoft AD ドメインに結合できます。このルート CA からは、ドメインコントローラーに対し証明書を発行できます。新しいルート CA の設定の詳細については、「Managed Microsoft AD Directory のサーバー側の LDAPS を有効にする方法」の「ステップ 3: オフライン CA をインストールして設定する」を参照してください。 [AWS](#)

EC2 インスタンスをドメインに結合する方法の詳細については、「[Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法](#)」を参照してください。

ステップ 3: 証明書テンプレートを作成する

エンタープライズ CA の設定後は、Kerberos 認証証明書テンプレートを設定することが可能になります。

証明書テンプレートを作成するには

1. Microsoft Windows サーバーマネージャー を起動します。[Tools > Certification Authority] (ツール > 認証機関) をクリックします。
2. [Certificate Authority] (認証機関) ウィンドウで、左サイドペインにある [Certificate Authority] (認証機関) ツリーを展開します。[Certificate Templates] (証明書テンプレート) を右クリックし、[Manage] (管理) を選択します。
3. [Certificate Templates Console] (証明書テンプレートコンソール) ウィンドウで、[Kerberos Authentication] (Kerberos 認証) を右クリックし、[Duplicate Template] (テンプレートの複製) を選択します。
4. [Properties of New Template] (新しいテンプレートのプロパティ) ウィンドウがポップアップ表示されます。

5. [Properties of New Template] (新しいテンプレートのプロパティ) ウィンドウで、[Compatibility] (互換性) のタブを開いた上で以下を実行します。
 - a. [Certification Authority] (認証機関) を CA に適合する OS に変更します。
 - b. [Resulting changes] (変更の結果) ウィンドウが表示されたら、[OK] をクリックします。
 - c. [認証の受信者] を [Windows 10/Windows Server 2016] に変更します。
-  **Note**

AWS Managed Microsoft AD は Windows Server 2019 を使用しています。
- d. [Resulting changes] (変更の結果) ウィンドウが表示されたら、[OK] をクリックします。
 6. [General] (一般) タブをクリックし、[Template display name] (テンプレートの表示名) を、「LDAPOverSSL」、または自分が選択した他の名前に変更します。
 7. [Security] (セキュリティ) タブを開き、[Group or user names] (グループ名またはユーザー名) セクションで、[Domain Controllers] (ドメイン コントローラー) を選択します。[Permissions for Domain Controllers] (ドメインコントローラーのアクセス許可) セクションで、[Read] (読み取り)、[Enroll] (登録)、[Autoenroll] (自動登録) の [Allow] (許可) チェックボックスが、それぞれオンになっていることを確認します。
 8. [OK] をクリックして、「LDAPOverSSL」(または先に指定した独自の名前) として証明書テンプレートを作成します。[Certificate Templates Console] (証明書テンプレートコンソール) ウィンドウを閉じます。
 9. [Certificate Authority] (認証機関) ウィンドウで、[Certificate Templates] (証明書テンプレート) を右クリックした上で、[New > Certificate Template to Issue] (新規 > 発行する証明書テンプレート) を選択します。
 10. [Enable Certificate Templates] (証明書テンプレートの有効化) ウィンドウで、「LDAPOverSSL」(または先に指定した名前) を選択し、[OK] をクリックします。

ステップ 4: セキュリティグループのルールを追加する

最後のステップでは、Amazon EC2 コンソールを開き、セキュリティグループのルールを追加する必要があります。これらのルールにより、ドメインコントローラーはエンタープライズ CA に接続して証明書をリクエストできるようになります。これを行うには、ドメインコントローラーからの着信トラフィックをエンタープライズ CA が承認できるように、インバウンドのルールを追加します。次に、アウトバウンドのルールを追加して、ドメインコントローラーからエンタープライズ CA へのトラフィックを許可します。

両方のルールが設定されると、ドメインコントローラーは、エンタープライズ CA に対し証明書を自動的にリクエストし、さらにディレクトリの LDAPS を有効化します。これでドメインコントローラーの LDAP サービスで LDAPS 接続を受け入れる準備が整いました。

セキュリティグループのルールを設定するには

1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2>) にアクセスし、管理者の認証情報を使用してサインインを行います。
2. 左側のペインで、[Network & Security] (ネットワークとセキュリティ) の [Security Groups] (セキュリティセキュリティグループ) をクリックします。
3. メインペインで、CA AWS のセキュリティグループを選択します。
4. [Inbound] (インバウンド) タブを開き、[Edit] (編集) をクリックします。
5. Edit inbound rules (インバウンドのルールの編集) ダイアログボックスで、次の操作を行います。
 - [Add Rule] (ルールの追加) をクリックします。
 - [Type] (タイプ) では [All traffic] (すべてのトラフィック) を、[Source] (送信元) では [Custom] (カスタム) をそれぞれ選択します。
 - ディレクトリ AWS のセキュリティグループ (例: sg-123456789) を Source の横にあるボックスに入力します。
 - [保存] を選択します。
6. 次に、AWS Managed Microsoft AD ディレクトリ AWS のセキュリティグループを選択します。[Outbound] (アウトバウンド) タブを開き、[Edit] (編集) をクリックします。
7. [Edit outbound rules] (アウトバウンドルールの編集) ダイアログボックスで、次の操作を行います。
 - [Add Rule] (ルールの追加) をクリックします。
 - [Type] (タイプ) では [All traffic] (すべてのトラフィック) を、[Destination] (送信先) では [Custom] (カスタム) をそれぞれ選択します。
 - 送信先の横にあるボックスに CA AWS のセキュリティグループを入力します。
 - [保存] を選択します。

LDP ツールを使用して AWS Managed Microsoft AD ディレクトリへの LDAPS 接続をテストできます。LDP ツールは、Active Directory 管理ツールに付属しています。詳細については、「[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#)」を参照してください。

 Note

LDAPS 接続をテストする前に、下位 CA からドメインコントローラーに証明書が発行されるまで、最大 30 分間待機する必要があります。

サーバー側の LDAPS の詳細については、セキュリティ AWS ブログの[AWS 「Managed Microsoft AD Directory でサーバー側の LDAPS を有効にする方法」](#)を参照してください。

AWS Managed Microsoft AD を使用したクライアント側の LDAPS の有効化

AWS Managed Microsoft AD でのクライアント側の Lightweight Directory Access Protocol Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) サポートは、セルフマネージド (オンプレミス) Microsoft Active Directory (AD) と AWS アプリケーション間の通信を暗号化します。このようなアプリケーションの例には、WorkSpaces AWS IAM Identity Center、QuickSight、Amazon Chime などがあります。この暗号化は、組織の ID データをより適切に保護し、セキュリティ要件を満たすのに役立ちます。

前提条件

クライアント側 LDAPS を有効にする前に、次の要件を満たす必要があります。

トピック

- [AWS Managed Microsoft AD とセルフマネージドの間に信頼関係を作成する Microsoft Active Directory](#)
- [Active Directory にサーバー証明書をデプロイする](#)
- [認証機関の証明書要件](#)
- [ネットワーク要件](#)

AWS Managed Microsoft AD とセルフマネージドの間に信頼関係を作成する Microsoft Active Directory

まず、AWS Managed Microsoft AD とセルフマネージドの間に信頼関係を確立 Microsoft Active Directory して、クライアント側の LDAPS を有効にする必要があります。詳細については、「[the section called “信頼関係の作成”](#)」を参照してください。

Active Directory にサーバー証明書をデプロイする

クライアント側の LDAPS を有効にするには、Active Directory 内のドメインコントローラーごとに、サーバー証明書を取得しインストールする必要があります。これらの証明書は、LDAP サービスが LDAP クライアントからの SSL 接続をリッスンして自動的に承認するために使用されます。SSL 証明書は、社内の Active Directory 証明書サービス (ADCS) のデプロイから発行されたもの、または商用発行者から購入したものを使用できます。Active Directory サーバー証明書の要件の詳細については、Microsoft のウェブサイト「[LDAP over SSL \(LDAPS\) Certificate](#)」(LDAP over SSL (LDAPS) 証明書) を参照してください。

認証機関の証明書要件

クライアント側 LDAPS のオペレーションには、サーバー証明書の発行元を表す認証機関 (CA) 証明書が必要です。LDAP 通信を暗号化するために、CA 証明書は、Active Directory のドメインコントローラーから提示されるサーバー証明書と照合されます。次の CA 証明書の要件に注意してください。

- クライアント側 LDAPS を有効にするには、エンタープライズ認証機関 (CA) が必要です。Active Directory Certificate Service、サードパーティーの商用認証機関、または [AWS Certificate Manager](#) を使用できます。Microsoft Enterprise Certificate Authority の詳細については、「[Microsoft ドキュメント](#)」をご参照ください。
- 証明書を登録するには、有効期限までに 90 日超の期間があることが必要です。
- 証明書は、プライバシー強化メール (PEM) 形式である必要があります。Active Directory 内から CA 証明書をエクスポートする場合は、そのファイル形式として Base64 でエンコードされた X.509 (.CER) を選択します。
- AWS Managed Microsoft AD ディレクトリごとに最大 5 つの (5) CA 証明書を保存できます。
- RSASSA-PSS 署名アルゴリズムを使用する証明書はサポートされていません。
- 信頼される各ドメイン内の、すべてのサーバー証明書にチェーンされる CA 証明書は、登録を済ませておく必要があります。

ネットワーク要件

AWS アプリケーション LDAP トラフィックは TCP ポート 636 でのみ実行され、LDAP ポート 389 へのフォールバックはありません。ただし、レプリケーション、信頼などをサポートする Windows LDAP 通信は、Windows ネイティブセキュリティを備えた LDAP ポート 389 を引き続き使用します。AWS Managed Microsoft AD (アウトバウンド) とセルフマネージド Active Directory (インバウンド) のポート 636 で TCP 通信を許可するように AWS セキュリティグループとネットワーク

ファイアウォールを設定します。AWS Managed Microsoft AD と自己管理型 Active Directory の間で LDAP ポート 389 を、開いたままに維持します。

クライアント側 LDAPS を有効にする

クライアント側の LDAPS を使用するには、認証期間 (CA) 証明書を AWS Managed Microsoft AD にインポートした上で、ディレクトリの LDAPS を有効にします。この有効化により、AWS アプリケーションと自己管理型 Active Directory 間のすべての LDAP トラフィックには、Secure Sockets Layer (SSL) チャンネルの暗号化が使用されます。

2 つの異なる方法を使用して、ディレクトリのクライアント側 LDAPS を有効にできます。AWS Management Console メソッドまたは AWS CLI メソッドを使用できます。

Note

クライアント側の LDAPS は AWS Managed Microsoft AD のリージョン機能です。「[マルチリージョンレプリケーション](#)」を使用している場合、次の手順を各リージョンで個別に適用する必要があります。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

トピック

- [ステップ 1: で証明書を登録する AWS Directory Service](#)
- [ステップ 2: 登録ステータスを確認する](#)
- [ステップ 3: クライアント側 LDAPS を有効にする](#)
- [ステップ 4: LDAPS ステータスを確認する](#)

ステップ 1: で証明書を登録する AWS Directory Service

証明書を登録するには、次のいずれかの方法を使用します AWS Directory Service。

方法 1: 証明書を AWS Directory Service (AWS Management Console) に登録するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。

- [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合には、証明書を登録するリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションで、[Actions] (アクション) メニューを選択してから、[Register certificate] (証明書の登録) を選択します。
 5. [Register a CA certificate] (CA 証明書を登録する) ダイアログボックスで [Browse] (参照) をクリックしてから、証明書を選択し、[Open] (開く) をクリックします。
 6. [Register certificate] (証明書の登録) を選択します。

方法 2: 証明書を AWS Directory Service (AWS CLI) に登録するには

- 以下のコマンドを実行してください。証明書データについては、CA 証明書ファイルの場所を指定します。証明書 ID がレスポンスとして提供されます。

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

ステップ 2: 登録ステータスを確認する

証明書登録のステータスまたは登録済み証明書のリストを表示するには、次のいずれかの方法を使用します。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の登録ステータスを確認するには

1. [Directory details] (ディレクトリの詳細) ページの [Client-side LDAPS] (クライアント側 LDAPS) セクションに移動します。
2. [Registration status] (登録ステータス) 列に表示される現在の証明書登録状態を確認します。登録ステータスの値が [Registered] (登録済み) に変わると、証明書は正常に登録されています。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の登録ステータスを確認するには

- 次のコマンドを実行します。ステータス値として Registered が返される場合、証明書は正常に登録されています。

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

ステップ 3: クライアント側 LDAPS を有効にする

でクライアント側の LDAPS を有効にするには、次のいずれかの方法を使用します AWS Directory Service。

Note

クライアント側 LDAPS を有効にするには、1 つ以上の証明書が正常に登録されている必要があります。

方法 1: AWS Directory Service (AWS Management Console) でクライアント側の LDAPS を有効にするには

1. [Directory details] (ディレクトリの詳細) ページの [Client-side LDAPS] (クライアント側 LDAPS) セクションに移動します。
2. [Enable] (有効化) を選択します。このオプションを使用できない場合は、有効な証明書が正常に登録されていることを確認してから、もう一度やり直してください。
3. [Enable client-side LDAPS] (クライアント側 LDAPS を有効にする) ダイアログボックスで、[Enable] (有効化) を選択します。

方法 2: AWS Directory Service (AWS CLI) でクライアント側の LDAPS を有効にするには

- 以下のコマンドを実行してください。

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

ステップ 4: LDAPS ステータスを確認する

LDAPS ステータスを確認するには、次のいずれかの方法を使用します AWS Directory Service。

方法 1: LDAPS ステータスを確認するには AWS Directory Service (AWS Management Console)

1. [Directory details] (ディレクトリの詳細) ページの [Client-side LDAPS] (クライアント側 LDAPS) セクションに移動します。
2. ステータス値が [Enabled] (有効) と表示されている場合、LDAPS は正常に設定されています。

方法 2: LDAPS ステータスを確認するには AWS Directory Service (AWS CLI)

- 以下のコマンドを実行してください。ステータス値として Enabled が返される場合、LDAPS は正常に設定されています。

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

クライアント側 LDAPS を管理する

LDAPS 設定を管理するには、以下のコマンドを使用します。

2 つの異なる方法を使用して、クライアント側 LDAPS 設定を管理できます。AWS Management Console メソッドまたは AWS CLI メソッドを使用できます。

証明書の詳細を表示する

以下のいずれかの方法を使用して、証明書の有効期限を確認します。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の詳細を表示するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、証明書を表示するリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。

4. [Client-side LDAPS] (クライアント側 LDAPS) セクションの [CA certificates] (CA 証明書) に、証明書に関する情報が表示されます。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の詳細を表示するには

- 以下のコマンドを実行してください。証明書 ID として、register-certificate または list-certificates から返される識別子を使用します。

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

証明書の登録解除

以下のいずれかの方法を使用して、証明書を登録解除します。

Note

登録されている証明書が 1 つのみの場合は、証明書を登録解除する前に、まず LDAPS を無効にする必要があります。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の登録を解除するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、証明書の登録を解除するリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションで、[Actions] (アクション) を選択してから、[Deregister certificate] (証明書の登録解除) を選択します。

5. [Deregister a CA certificate] (CA 証明書を登録解除する) ダイアログボックスで、[Deregister] (登録解除) をクリックします。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の登録を解除するには

- 以下のコマンドを実行してください。証明書 ID として、register-certificate または list-certificates から返される識別子を使用します。

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

クライアント側 LDAPS の無効化

以下のいずれかの方法を使用して、クライアント側 LDAPS を無効にします。

方法 1: AWS Directory Service (AWS Management Console) でクライアント側の LDAPS を無効にするには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、クライアント側の LDAPS を無効にするリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションで、[Disable] (無効化) を選択します。
5. [Disable client-side LDAPS] (クライアント側 LDAPS を無効にする) ダイアログボックスで、[Disable] (無効化) をクリックします。

方法 2: AWS Directory Service (AWS CLI) でクライアント側の LDAPS を無効にするには

- 以下のコマンドを実行してください。

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

証明書登録に関する問題

AWS Managed Microsoft AD ドメインコントローラーを CA 証明書に登録するプロセスには、最大 30 分かかる場合があります。証明書の登録で問題が発生し、AWS Managed Microsoft AD ドメインコントローラーを再起動する場合は、お問い合わせください サポート。サポートケースの作成については、「[サポートケースの作成とケース管理](#)」を参照してください。

AWS Managed Microsoft AD のコンプライアンスを管理する

AWS Managed Microsoft AD を使用して、以下のコンプライアンス要件の対象となる、AWS クラウド内の Active Directory 対応アプリケーションをサポートできます。ただし、Simple AD を使用すると、アプリケーションはコンプライアンス要件に従いません。

サポートされるコンプライアンス標準

AWS Managed Microsoft AD は、以下の標準について監査済みであり、コンプライアンス認定を取得する必要があるソリューションの一部として使用できます。



AWS Managed Microsoft AD は、Federal Risk and Authorization Management Program (FedRAMP) のセキュリティ要件を満たしており、FedRAMP の Moderate and High Baseline で FedRAMP Joint Authorization Board (JAB) Provisional Authority to Operate (P-ATO) を取得しています。FedRAMP の詳細については、「[FedRAMP コンプライアンス](#)」を参照してください。



AWS Managed Microsoft AD は、クレジットカード業界 (PCI) データセキュリティ標準 (DSS) バージョン 3.2 をサービスプロバイダーレベル 1 で準拠証明書を取得しています。カード所有者データの保存、処理、または送信に製品およびサービスを使用する AWS お客様は、独自の PCI DSS コンプライアンス証明書を管理する際に AWS Managed Microsoft AD を使用できます。

PCI コンプライアンスパッケージのコピーをリクエストする方法など、AWS PCI DSS の詳細については、[「PCI DSS レベル 1」](#)を参照してください。重要なのは、PCI DSS バージョン 3.2 標準に準拠するように AWS Managed Microsoft AD できめ細かなパスワードポリシーを設定する必要があることです。適用する必要があるポリシーの詳細については、以下の AWS 「Managed Microsoft AD ディレクトリの PCI コンプライアンスを有効にする」というタイトルのセクションを参照してください。



AWS は、医療保険の相互運用性と説明責任に関する法律 (HIPAA) コンプライアンスプログラムを拡張し、AWS Managed Microsoft AD を [HIPAA 対応サービス](#)として含めました。と事業提携契約 (BAA) を締結している場合は AWS、AWS Managed Microsoft AD を使用して HIPAA 準拠のアプリケーションを構築できます。

AWS は、医療情報の処理と保存 AWS に活用する方法の詳細に関心のあるお客様向けに、[HIPAA に重点を置いたホワイトペーパー](#)を提供しています。詳細については、[「HIPAA コンプライアンス」](#)を参照してください。

責任共有

セキュリティ (FedRAMP、HIPAA、PCI へのコンプライアンスを含む) は[責任共有](#)の対象です。AWS Managed Microsoft AD のコンプライアンスステータスは、AWS クラウドで実行するアプリケーションに自動的に適用されないことを理解することが重要です。AWS サービスの使用が標準に準拠していることを確認する必要があります。

AWS Managed Microsoft AD がサポートするさまざまな AWS コンプライアンスプログラムの完全なリストについては、[AWS「コンプライアンスプログラムによる対象範囲内のサービス」](#)を参照してください。

AWS Managed Microsoft AD ディレクトリの PCI コンプライアンスを有効にする

AWS Managed Microsoft AD ディレクトリの PCI コンプライアンスを有効にするには、[AWS Managed Microsoft AD が提供する PCI DSS 準拠証明書 \(AOC\) および責任概要ドキュメント](#)で指定されているように、きめ細かなパスワードポリシーを設定する必要があります AWS Artifact。

詳細なパスワードポリシーの使用の詳細については、「[AWS Managed Microsoft AD パスワードポリシーについて](#)」を参照してください。

AWS Managed Microsoft AD ネットワークセキュリティ設定の強化

AWS Managed Microsoft AD ディレクトリ用にプロビジョニングされる AWS セキュリティグループは、AWS Managed Microsoft AD ディレクトリのすべての既知のユースケースをサポートするために必要な最小限のインバウンドネットワークポートで設定されます。プロビジョニングされた AWS セキュリティグループの詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。

AWS Managed Microsoft AD ディレクトリのネットワークセキュリティをさらに強化するために、以下の一般的なシナリオに基づいて AWS セキュリティグループを変更できます。

カスタマードメインコントローラー CIDR - この CIDR ブロックは、ドメインオンプレミスドメインコントローラーが存在する場所です。

カスタマークライアント CIDR - この CIDR ブロックは、コンピュータやユーザーなどのクライアントが AWS Managed Microsoft AD に対して認証する場所です。AWS Managed Microsoft AD ドメインコントローラーもこの CIDR ブロックにあります。

シナリオ

- [AWS アプリケーションはのみをサポートします](#)
- [AWS 信頼サポートのあるアプリケーションのみ](#)
- [AWS アプリケーションとネイティブ Active Directory ワークロードのサポート](#)
- [AWS アプリケーションとネイティブ Active Directory ワークロードのサポートと信頼サポート](#)

AWS アプリケーションは のみをサポートします

すべてのユーザーアカウントは AWS Managed Microsoft AD でのみプロビジョニングされ、次のようなサポートされている AWS アプリケーションで使用されます。

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

次の AWS セキュリティグループ設定を使用して、AWS Managed Microsoft AD ドメインコントローラーへの重要でないトラフィックをすべてブロックできます。

Note

- 以下は、この AWS セキュリティグループ設定と互換性がありません。
 - Amazon EC2 インスタンス
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Active Directory での信頼
 - ドメイン参加済みのクライアントまたはサーバー

インバウンドルール

なし。

アウトバウンドルール

なし。

AWS 信頼サポートのあるアプリケーションのみ

すべてのユーザーアカウントは AWS Managed Microsoft AD または信頼できる Active Directory にプロビジョニングされ、次のようなサポートされている AWS アプリケーションで使用されます。

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

Managed AWS Microsoft AD ドメインコントローラーへの重要でないトラフィックをすべてブロックするように、プロビジョニングされた AWS セキュリティグループ設定を変更できます。

Note

- 以下は、この AWS セキュリティグループ設定と互換性がありません。
 - Amazon EC2 インスタンス
 - Amazon FSx
 - Amazon RDS for MySQL
 - Amazon RDS for Oracle
 - Amazon RDS for PostgreSQL
 - Amazon RDS for SQL Server
 - WorkSpaces
 - Active Directory での信頼

- ドメイン参加済みのクライアントまたはサーバー
- この設定では、「カスタマードメインコントローラー CIDR」ネットワークが安全であることを確認する必要があります。
- TCP 445 は、信頼の作成時にだけ使用し、信頼の確立後は削除できます。
- TCP 636 は、SSL 経由で LDAP を使用している場合にのみ必要となります。

インバウンドルール

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
TCP と UDP	53	カスタマードメインコントローラー CIDR	DNS	ユーザーとコンピュータの認証、名前解決、信頼
TCP と UDP	88	カスタマードメインコントローラー CIDR	Kerberos	ユーザーとコンピュータの認証、フォレストレベルの信頼
TCP と UDP	389	カスタマードメインコントローラー CIDR	LDAP	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP と UDP	464	カスタマードメインコントローラー CIDR	Kerberos パスワードの変更 / 設定	レプリケーション、ユーザーとコンピュータの認証、信頼
TCP	445	カスタマードメインコントローラー CIDR	SMB / CIFS	レプリケーション、ユーザーとコンピュータの

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
				認証、グループ ポリシー、信頼
TCP	135	カスタマードメ インコントロー ラー CIDR	レプリケーショ ン	RPC、EPM
TCP	636	カスタマードメ インコントロー ラー CIDR	LDAP SSL	ディレクトリ、 レプリケーショ ン、ユーザーと コンピュータの 認証、グループ ポリシー、信頼
TCP	49152 - 65535	カスタマードメ インコントロー ラー CIDR	RPC	レプリケーショ ン、ユーザーと コンピュータの 認証、グループ ポリシー、信頼
TCP	3268 - 3269	カスタマードメ インコントロー ラー CIDR	LDAP GC および LDAP GC SSL	ディレクトリ、 レプリケーショ ン、ユーザーと コンピュータの 認証、グループ ポリシー、信頼
UDP	123	カスタマードメ インコントロー ラー CIDR	Windows タイム	Windows タイ ム、信頼

アウトバウンドルール

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directoryの使用
すべて	すべて	カスタマードメインコントローラ CIDR	すべてのトラフィック	

AWS アプリケーションとネイティブ Active Directory ワークロードのサポート

ユーザーアカウントは Managed Microsoft AD AWS でのみプロビジョニングされ、次のようなサポートされている AWS アプリケーションで使用されます。

- Amazon Chime
- Amazon Connect
- Amazon EC2 インスタンス
- Amazon FSx
- QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Managed AWS Microsoft AD ドメインコントローラへの重要でないトラフィックをすべてブロックするように、プロビジョニングされた AWS セキュリティグループ設定を変更できます。

Note

- Active Directory AWS Managed Microsoft AD ディレクトリとカスタマードメインコントローラー CIDR の間で信頼を作成および維持することはできません。
- これには、「顧客クライアント CIDR」ネットワークが安全であることを確認する必要があります。
- TCP 636 は、SSL 経由で LDAP を使用している場合にのみ必要となります。
- この設定で Enterprise CA を使用する場合は、アウトバウンドルール「TCP, 443, CA CIDR」を作成する必要があります。

インバウンドルール

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
TCP と UDP	53	顧客クライアント CIDR	DNS	ユーザーとコンピュータの認証、名前解決、信頼
TCP と UDP	88	顧客クライアント CIDR	Kerberos	ユーザーとコンピュータの認証、フォレストレベルの信頼
TCP と UDP	389	顧客クライアント CIDR	LDAP	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP と UDP	445	顧客クライアント CIDR	SMB / CIFS	レプリケーション、ユーザーとコンピュータの

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
				認証、グループポリシー、信頼
TCP と UDP	464	顧客クライアント CIDR	Kerberos パスワードの変更 / 設定	レプリケーション、ユーザーとコンピュータの認証、信頼
TCP	135	顧客クライアント CIDR	レプリケーション	RPC、EPM
TCP	636	顧客クライアント CIDR	LDAP SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	49152 - 65535	顧客クライアント CIDR	RPC	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	3268 - 3269	顧客クライアント CIDR	LDAP GC および LDAP GC SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	9389	顧客クライアント CIDR	SOAP	AD DS ウェブサービス
UDP	123	顧客クライアント CIDR	Windows タイム	Windows タイム、信頼

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
UDP	138	顧客クライアント CIDR	DFSN と NetLogon	DFS、グループポリシー

アウトバウンドルール

なし。

AWS アプリケーションとネイティブ Active Directory ワークロードのサポートと信頼サポート

すべてのユーザーアカウントは AWS Managed Microsoft AD または信頼できる Active Directory にプロビジョニングされ、次のようなサポートされている AWS アプリケーションで使用されます。

- Amazon Chime
- Amazon Connect
- Amazon EC2 インスタンス
- Amazon FSx
- QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- AWS IAM Identity Center
- WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

Managed AWS Microsoft AD ドメインコントローラーへの重要でないトラフィックをすべてブロックするように、プロビジョニングされた AWS セキュリティグループ設定を変更できます。

Note

- これには、「顧客ドメインコントローラー CIDR」ネットワークと「顧客クライアント CIDR」ネットワークが安全であることを確認する必要があります。
- 「カスタマードメインコントローラー CIDR」を含む TCP 445 は信頼の作成にのみ使用され、信頼が確立された後に削除できます。
- 「顧客クライアント CIDR」を含む TCP 445 は、グループポリシーの処理に必要なため、開いたままにしておく必要があります。
- TCP 636 は、SSL 経由で LDAP を使用している場合にのみ必要となります。
- この設定で Enterprise CA を使用する場合は、アウトバウンドルール「TCP, 443, CA CIDR」を作成する必要があります。

インバウンドルール

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
TCP と UDP	53	カスタマードメインコントローラー CIDR	DNS	ユーザーとコンピュータの認証、名前解決、信頼
TCP と UDP	88	カスタマードメインコントローラー CIDR	Kerberos	ユーザーとコンピュータの認証、フォレストレベルの信頼
TCP と UDP	389	カスタマードメインコントローラー CIDR	LDAP	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directory の使用
TCP と UDP	464	カスタマードメインコントローラー CIDR	Kerberos パスワードの変更 / 設定	レプリケーション、ユーザーとコンピュータの認証、信頼
TCP	445	カスタマードメインコントローラー CIDR	SMB / CIFS	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	135	カスタマードメインコントローラー CIDR	レプリケーション	RPC、EPM
TCP	636	カスタマードメインコントローラー CIDR	LDAP SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	49152 - 65535	カスタマードメインコントローラー CIDR	RPC	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	3268 - 3269	カスタマードメインコントローラー CIDR	LDAP GC および LDAP GC SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directoryの使用
UDP	123	カスタマードメインコントローラー CIDR	Windows タイム	Windows タイム、信頼
TCP と UDP	53	カスタマードメインコントローラー CIDR	DNS	ユーザーとコンピュータの認証、名前解決、信頼
TCP と UDP	88	カスタマードメインコントローラー CIDR	Kerberos	ユーザーとコンピュータの認証、フォレストレベルの信頼
TCP と UDP	389	カスタマードメインコントローラー CIDR	LDAP	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP と UDP	445	カスタマードメインコントローラー CIDR	SMB / CIFS	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP と UDP	464	カスタマードメインコントローラー CIDR	Kerberos パスワードの変更 / 設定	レプリケーション、ユーザーとコンピュータの認証、信頼
TCP	135	カスタマードメインコントローラー CIDR	レプリケーション	RPC、EPM

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directoryの使用
TCP	636	カスタマードメインコントローラー CIDR	LDAP SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	49152 - 65535	カスタマードメインコントローラー CIDR	RPC	レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	3268 - 3269	カスタマードメインコントローラー CIDR	LDAP GC および LDAP GC SSL	ディレクトリ、レプリケーション、ユーザーとコンピュータの認証、グループポリシー、信頼
TCP	9389	カスタマードメインコントローラー CIDR	SOAP	AD DS ウェブサービス
UDP	123	カスタマードメインコントローラー CIDR	Windows タイム	Windows タイム、信頼
UDP	138	カスタマードメインコントローラー CIDR	DFSN と NetLogon	DFS、グループポリシー

アウトバウンドルール

プロトコル	ポート範囲	ソース	トラフィックの種類	Active Directoryの使用
すべて	すべて	カスタマードメインコントローラー CIDR	すべてのトラフィック	

AWS Managed Microsoft AD ディレクトリのセキュリティ設定の編集

AWS Managed Microsoft AD の詳細なディレクトリ設定は、運用ワークロードを増やすことなく、コンプライアンスとセキュリティの要件を満たすように設定できます。ディレクトリ設定では、ディレクトリで使用されるプロトコルと暗号のセキュアチャネル設定を更新できます。たとえば、RC4 や DES などの個々のレガシー暗号、および SSL 2.0/3.0 や TLS 1.0/1.1 などのプロトコルを柔軟に無効にできます。AWS マネージド Microsoft AD は、ディレクトリ内のすべてのドメインコントローラーに設定をデプロイし、ドメインコントローラーの再起動を管理し、追加の をスケールアウトまたはデプロイするときこの設定を維持します AWS リージョン。使用できるすべての設定については、「[ディレクトリセキュリティ設定のリスト](#)」を参照してください。

ディレクトリセキュリティ設定の編集

任意のディレクトリ設定を構成および編集することができます。

ディレクトリ設定を編集するには

1. AWS マネジメントコンソールにサインインし、で AWS Directory Service コンソールを開きます <https://console.aws.amazon.com/directoryservicev2/>。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Networking & security] (ネットワークとセキュリティ) で、[Directory settings] (ディレクトリ設定) を見つけ、[Edit settings] (設定の編集) を選択します。
4. [Edit settings] (設定の編集) で、編集したい設定の [Value] (値) を変更します。設定を編集すると、そのステータスは [Default] (デフォルト) から [Ready to Update] (更新準備完了) に変わります。以前に設定を編集したことがある場合、そのステータスは [Updated] (更新済み) から [Ready to Update] (更新準備完了) に変わります。次に、[Review] (確認) を選択します。
5. [Review and update settings] (設定の確認と更新) で、[Directory settings] (ディレクトリ設定) を調べ、新しい値がすべて正しいことを確認します。設定にその他の変更を加えたい場合は、

[Edit settings] (設定の編集) を選択します。変更を加え、新しい値を実装する準備ができたなら、[Update settings] (設定の更新) を選択します。次に、ディレクトリ ID ページに戻ります。

 Note

[Directory settings] (ディレクトリ設定) で、更新された設定の [Status] (ステータス) を確認できます。設定が実装されている間、[Status] (ステータス) には [Updating] (更新中) と表示されます。設定で [Status] (ステータス) に [Updating] (更新中) と表示されている間は、他の設定を編集することができません。設定が編集内容で正常に更新された場合、[Status] (ステータス) に [Updated] (更新済み) と表示されます。設定が編集内容で更新されなかった場合、[Status] (ステータス) に [Failed] (失敗) と表示されます。

ディレクトリセキュリティ設定が失敗した

設定の更新中にエラーが発生した場合、[Status] (ステータス) に [Failed] (失敗) と表示されます。失敗ステータスでは、設定は新しい値に更新されず、元の値が実装されたままになります。これらの設定の更新を再試行するか、以前の値に戻すことができます。

更新が失敗した設定を解決するには

- [Directory settings] (ディレクトリ設定) で、[Resolve failed settings] (失敗した設定を解決する) を選択します。次に、以下のいずれかを行います。
 - 設定を失敗状態の前の値に戻すには、[Revert failed settings] (失敗した設定を元に戻す) を選択します。次に、ポップアップモーダルで [Revert] (元に戻す) を選択します。
 - ディレクトリ設定の更新を再試行するには、[Retry failed settings] (失敗した設定を再試行する) を選択します。失敗した更新を再試行する前に、ディレクトリ設定にさらに変更を加える場合は、[Continue editing] (編集を続行) を選択します。[Review and retry failed updates] (失敗した更新を確認して再試行する) で、[Update settings] (設定の更新) を選択します。

ディレクトリセキュリティ設定のリスト

以下のリストは、使用可能なすべてのディレクトリセキュリティ設定のタイプ、設定名、API 名、可能性のある値、および設定の説明を示しています。

他のすべてのセキュリティ設定が無効な場合、TLS 1.2 と AES 256/256 がデフォルトのディレクトリセキュリティ設定です。これらが無効にすることはできません。

タイプ	設定名	API 名	考えられる値	設定の説明
証明書ベース の認証	証明書 バック デー ト補 正	CERTIFICA TE_BACKDA TING_COMP ENSATION	年: 0～50	証明書 が Active Directory の ユーザーよ りも古いも のであり、引 き続き Active Directory での 認証に使用で きる期間を示 す値を指定し ます。デフォ ルト値は 10 分 です。この値 は 1 秒から 50 年の間で設定 できます。
			月: 0～11	
			日: 0～30	
			時間: 0～23	この設定を構 成するには、 「強力な証明 書バインディ ングの強制」 の「互換性」 タイプを選択 する必要があります。
			分: 0～59	
			秒: 0～59	
				詳細について は、Microsoft Support ド キュメントの 「 KB5014754 - Windows ド

タイプ	設定名	API 名	考えられる値	設定の説明
				メインコントローラーでの証明書ベースの認証の変更 を参照してください。

タイプ	設定名	API 名	考えられる値	設定の説明
	証明書の強力な強制	CERTIFICATE_STRONG_ENFORCEMENT	互換性、完全適用	次のいずれかの強制タイプを指定します。 • 互換性: 証明書をユーザーに強くマッピングできない場合、認証が許可されます。証明書が Active Directory のユーザーアカウントよりも前のものである場合は、証明書のバックデート補償も設定する必要があります。そうしないと、認証が失敗します。 • 完全な強制 (デフォルト): 証明書をユーザーに強くマッ

タイプ	設定名	API 名	考えられる値	設定の説明
				ピングできない場合、認証は許可されません。この強制タイプを選択した場合、証明書バックデート補正は設定できません。 詳細については、Microsoft Support ドキュメントの「KB5014754 - Windows ドメインコントローラーでの証明書ベースの認証の変更」を参照してください。

タイプ	設定名	API 名	考えられる値	設定の説明
セキュアチャネル: 暗号	AES 128/128	AES_128_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために AES 128/128 暗号による暗号化を有効または無効にします。
	DES 56/56	DES_56_56	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために DES 56/56 暗号による暗号化を有効または無効にします。
	RC2 40/128	RC2_40_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC2 40/128 暗号による暗号化を有効または無効にします。

タイプ	設定名	API 名	考えられる値	設定の説明
	RC2_56/128	RC2_56_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC2_56/128 暗号による暗号化を有効または無効にします。
	RC2_128/128	RC2_128_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC2_128/128 暗号による暗号化を有効または無効にします。
	RC4_40/128	RC4_40_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC4_40/128 暗号による暗号化を有効または無効にします。

タイプ	設定名	API 名	考えられる値	設定の説明
	RC4 56/128	RC4_56_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC4 56/128 暗号による暗号化を有効または無効にします。
	RC4 64/128	RC4_64_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC4 64/128 暗号による暗号化を有効または無効にします。
	RC4 128/128	RC4_128_128	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために RC4 128/128 暗号による暗号化を有効または無効にします。

タイプ	設定名	API 名	考えられる値	設定の説明
セキュアチャネル: プロトコル	Triple DES 168/168	3DES_168_168	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラー間の安全なチャネル通信のために Triple DES 168/168 暗号による暗号化を有効または無効にします。
	PCT 1.0	PCT_1_0	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラーでの安全なチャネル通信 (サーバーとクライアント) のために PCT 1.0 プロトコルを有効または無効にします。

タイプ	設定名	API 名	考えられる値	設定の説明
	SSL 2.0	SSL_2_0	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラーでの安全なチャネル通信 (サーバーとクライアント) のために SSL 2.0 プロトコルを有効または無効にします。
	SSL 3.0	SSL_3_0	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラーでの安全なチャネル通信 (サーバーとクライアント) のために SSL 3.0 プロトコルを有効または無効にします。

タイプ	設定名	API 名	考えられる値	設定の説明
	TLS 1.0	TLS_1_0	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラーでの安全なチャネル通信 (サーバーとクライアント) のために TLS 1.0 プロトコルを有効または無効にします。
	TLS 1.1	TLS_1_1	Enable/Disable (有効/無効)	ディレクトリ内のドメインコントローラーでの安全なチャネル通信 (サーバーとクライアント) のために TLS 1.1 プロトコルを有効または無効にします。

AWS Managed Microsoft AD の AWS Private CA Connector for AD をセットアップする

AWS Managed Microsoft AD を [AWS Private Certificate Authority \(CA\)](#) と統合して、Active Directory ドメインに参加しているユーザー、グループ、マシンの証明書を発行および管理できます。AWS Private CA Connector for Active Directoryを使用すると、ローカルエージェントやプロキシサーバーをデプロイ、パッチ適用、更新することなく、セルフマネージドエンタープライズ CAs のフルマネージド AWS Private CA ドロップインリプレイスメントを使用できます。

Note

AWS Private CA Connector for を使用した AWS Managed Microsoft AD ドメインコントローラーのサーバー側の LDAPS 証明書登録Active Directoryは、現時点ではサポートされていません。ディレクトリのサーバー側の LDAPS を有効にするには、[AWS 「Managed Microsoft AD ディレクトリのサーバー側の LDAPS を有効にする方法」](#) を参照してください。

ディレクトリと AWS Private CA の統合は、AWS Directory Service コンソール、Connector for Active Directoryコンソール、または [CreateTemplate](#) API AWS Private CA を呼び出すことで設定できます。AWS Private CA Connector for Active Directoryコンソールを使用してプライベート CA 統合を設定するには、[「コネクタテンプレートの作成」](#) を参照してください。AWS Directory Service コンソールからこの統合を設定する方法については、次の手順を参照してください。

AWS Private CA Connector for AD のセットアップ

1. にサインイン AWS Management Console し、 で AWS Directory Service コンソールを開きます <https://console.aws.amazon.com/directoryservicev2/>。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. アプリケーション管理タブとAWS アプリケーションとサービスセクションで、「AWS Private CA Connector for AD」を選択します。[Active Directory 用のプライベート CA 証明書の作成] ページが表示されます。コンソールの手順に従って Active Directory Connector 用のプライベート CA を作成し、ご使用のプライベート CA に登録します。詳細については、[「コネクタの作成」](#) を参照してください。
4. コネクタを作成したら、コネクタのステータスおよび関連するプライベート CA のステータスなど、AWS Private CA Connector for AD の詳細を表示する方法について説明します。

次に、AWS Private CA Connector for AD が証明書を発行できるように、AWS Managed Microsoft AD のグループポリシーオブジェクトを設定します。

AWS Private CA Connector for AD の表示

1. にサインイン AWS Management Console し、 で AWS Directory Service コンソールを開きます <https://console.aws.amazon.com/directoryservicev2/>。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。

3. アプリケーション管理タブとAWS アプリケーションとサービスセクションで、プライベート CA コネクタと関連するプライベート CA を表示できます。デフォルトでは、以下のフィールドが表示されます。
 - a. AWS Private CA コネクタ ID — AWS Private CA コネクタの一意的識別子。これを選択すると、その AWS Private CA コネクタの詳細ページが表示されます。
 - b. AWS Private CA subject — CA の識別名に関する情報。こちらをクリックすると、その AWS Private CA の詳細ページが表示されます。
 - c. ステータス — AWS Private CA Connector と のステータスチェックに基づきます AWS Private CA。両方のチェックに合格すると、[アクティブ] と表示されます。いずれかのチェックが失敗すると、[1/2 チェック失敗] と表示されます。両方のチェックが失敗すると、[失敗] と表示されます。失敗ステータスの詳細については、ハイパーリンクにカーソルを合わせると、どのチェックが失敗したか確認できます。コンソール内の指示に従い、修正します。
 - d. 作成日 — AWS Private CA Connector が作成された日。

詳細については、「[コネクタの詳細表示](#)」を参照してください。

AD ポリシーの設定

AWS Managed Microsoft AD オブジェクトが証明書をリクエストおよび受信できるように、CA Connector for AD を設定する必要があります。この手順では、が AWS Managed Microsoft AD オブジェクトに証明書 AWS Private CA を発行できるように、グループポリシーオブジェクト ([GPO](#)) を設定します。

1. AWS Managed Microsoft AD 管理者インスタンスに接続し、スタートメニューから [Server Manager](#) を開きます。
2. [ツール] で、[グループポリシー管理] を選択します。
3. [フォレストとドメイン] で、サブドメイン組織単位 (OU) を検索し (例えば、[AWS Managed Microsoft AD の作成](#) で説明されている手順に従っている場合、サブドメイン組織単位は corp になります)、サブドメイン OU を右クリックします。[このドメインに GPO を作成してここにリンクする...] を選択し、名前に PCA GPO を入力します。[OK] を選択します。
4. 新しく作成された GPO は、サブドメイン名の後に表示されます。PCA GPO を右クリックして [編集] を選択します。ダイアログボックスが開かれる間に、This is a link and that changes will be globally propagated というアラートメッセージが表示する場合は、[確認] を選択してメッセージを確認します。[グループポリシー管理エディター] が開きます。

5. [グループポリシー管理エディター] で、[コンピュータの設定] > [ポリシー] > [Windows 設定] > [セキュリティ設定] > [パブリックキーポリシー] (フォルダを選択) に移動します。
6. [オブジェクトのタイプ] で [証明書サービスクライアント - 証明書登録ポリシー] を選択します。
7. [証明書サービスクライアント - 証明書登録ポリシー] ウィンドウで、[設定モデル] を [有効] に変更します。
8. [Active Directory 登録ポリシー] が [選択済み]、そして [有効] になっていることを確認します。[Add] (追加) を選択します。
9. [証明書登録ポリシーサーバー] ダイアログボックスを開くはずです。コネクタを作成したときに生成された証明書登録ポリシーサーバーエンドポイントを [登録サーバーポリシー URI を入力] フィールドに入力します。[認証タイプ] は [Windows 統合] のままにします。
10. [検証] を選択します。検証が成功したら、[追加] を選択します。
11. [証明書サービスクライアント - 証明書登録ポリシー] に戻り、新しく作成したコネクタの横にあるダイアログボックスを選択して、コネクタをデフォルトの登録ポリシーにします。
12. 「Active Directory 登録ポリシー」を選択し、「削除」を選択します。
13. 確認ダイアログボックスで [はい] を選択して LDAP ベースの認証を削除します。
14. [証明書サービスクライアント] > [証明書登録ポリシー] ウィンドウで [適用] と [確認] を選択し、閉じます。次に、ウィンドウを閉じます。
15. [パブリックキーポリシー] フォルダの [オブジェクトの種類] で 「Certificate Services Client – 自動登録」を選択します。
16. [設定モデル] オプションを [有効] に変更します。
17. [期限切れの証明書を更新する] と [証明書を更新する] の両方がオンになっていることを確認します。他の設定はそのままにします。
18. [適用]、[確認] の順に選択し、ダイアログボックスを閉じます。

次に、ユーザー設定用のパブリックキーポリシーを設定します。

- [ユーザー設定] > [ポリシー] > [Windows 設定] > [セキュリティ設定] > [パブリックキーポリシー] に移動します。ステップ 6 からステップ 21 までの手順に従って、ユーザー設定用のパブリックキーポリシーを設定します。

GPOs とパブリックキーポリシーの設定が完了すると、ドメイン内のオブジェクトは AWS Private CA Connector for AD に証明書をリクエストし、 によって発行された証明書を取得します AWS Private CA。

証明書 AWS Private CA の発行の確認

AWS Managed Microsoft AD の証明書を発行 AWS Private CA するために を更新するプロセスには、最大 8 時間かかる場合があります。

次のいずれかを試すことができます。

- この期間を待つことができます。
- から証明書を受信するように設定された AWS Managed Microsoft AD ドメイン参加マシンを再起動できます AWS Private CA。その後、AWS Private CA が AWS Managed Microsoft AD ドメインのメンバーに証明書を発行したことを確認するには、[Microsoft ドキュメント](#)の手順に従ってください。
- 次のPowerShellコマンドを使用して、AWS Managed Microsoft AD の証明書を更新できます。

```
certutil -pulse
```

AWS Managed Microsoft AD のモニタリング

AWS Managed Microsoft AD を最大限に活用するには、さまざまな AWS Managed Microsoft AD ステータスと Managed Microsoft AD AWS の意味について詳しく説明します。Amazon Simple Notification Service や Amazon CloudWatch などの AWS サービスを使用して AWS Managed Microsoft AD をモニタリングすることもできます。Amazon Simple Notification Service は、AWS Managed Microsoft AD ディレクトリのステータスの通知を送信できます。Amazon CloudWatch は Managed Microsoft AD AWS ドメインコントローラーのパフォーマンスをモニタリングできます。

AWS Managed Microsoft AD をモニタリングするタスク

- [AWS Managed Microsoft AD ディレクトリのステータスについて](#)
- [Amazon Simple Notification Service による AWS Managed Microsoft AD ディレクトリのステータス通知の有効化](#)
- [AWS Managed Microsoft AD ディレクトリログについて](#)
- [AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#)
- [CloudWatch を使用した AWS Managed Microsoft AD ドメインコントローラーのパフォーマンスのモニタリング](#)
- [AWS Managed Microsoft AD の Amazon CloudWatch ログ転送を無効にする](#)
- [Microsoft イベントビューアーによる DNS サーバーの監視](#)

AWS Managed Microsoft AD ディレクトリのステータスについて

ディレクトリのステータスには以下の種類があります。

[Active] (アクティブ)

ディレクトリは正常に動作しています。ディレクトリには AWS Directory Service が検出した問題はありせん。

[Creating] (作成中)

ディレクトリは現在作成中です。ディレクトリの作成には通常 20〜45 分かかりますが、システムの負荷によって異なる場合があります。

[Deleted] (削除済み)

ディレクトリは削除されています。ディレクトリのリソースはすべて解放されています。ディレクトリがこの状態になったら、復元できません。

[Deleting] (削除中)

ディレクトリは削除中です。ディレクトリが完全に削除されるまでは、この状態です。ディレクトリがこの状態になると、削除操作を取り消すことができず、ディレクトリを回復できません。

[Failed] (失敗)

ディレクトリを作成できませんでした。このディレクトリを削除してください。問題が解決しない場合は、[AWS サポート センター](#)までお問い合わせください。

[Impaired] (障害)

ディレクトリがパフォーマンスが低下した状態で実行されています。1 つまたは複数の問題が検出され、すべてのディレクトリのオペレーションが最適に動作しているとは限りません。ディレクトリがこのステータスになるのは、さまざまな原因があり得ます。パッチ適用や EC2 インスタンスのローテーションなど通常の運用メンテナンス、いずれかのドメインコントローラーにおけるアプリケーションの一時的なホットスポットティング、あるいは、ネットワークに行った変更が意図せずディレクトリの通信を妨害するなどです。詳細については、「[AWS Managed Microsoft AD のトラブルシューティング](#)」、「[AD Connector のトラブルシューティング](#)」、「[Simple AD のトラブルシューティング](#)」のいずれかを参照してください。通常のメンテナンス関連の問題の場合、AWS は 40 分以内にこれらの問題を解決します。トラブルシューティングのトピックを確認した後も、ディレクトリの障害の状態が 40 分以上続く場合は、[AWS サポート センター](#)までお問い合わせください。

⚠ Important

ディレクトリが障害の状態あるときは、スナップショットを復元しないでください。障害の解消にスナップショットの復元が必要になることはほとんどありません。詳細については、「[スナップショットを使用した AWS Managed Microsoft AD の復元](#)」を参照してください。

[Requested] (リクエスト済み)

ディレクトリの作成リクエストは現在保留中です。

[RestoreFailed] (復元失敗)

スナップショットからのディレクトリの復元に失敗しました。復元操作を再試行してください。これが続く場合は、別のスナップショットを試すか、[AWS サポート センター](#)までお問い合わせください。

[Restoring] (復元中)

ディレクトリは現在、自動スナップショットまたは手動スナップショットから復元されています。スナップショットからの復元には、スナップショット内のディレクトリデータのサイズに応じて通常数分かかります。

Amazon Simple Notification Service による AWS Managed Microsoft AD ディレクトリのステータス通知の有効化

Amazon Simple Notification Service (Amazon SNS) を使用して、ディレクトリのステータスが変更されたときに E メールまたはテキストメッセージ (SMS) を受け取ることができます。ディレクトリが「有効」ステータスから「[障害ステータス](#)」に変わると通知されます。ディレクトリが Active ステータスに戻ったときも通知を受け取ります。

仕組み

Amazon SNS は「トピック」を使用してメッセージを収集および配信します。各トピックには、そのトピックに発行されたメッセージを受け取る 1 人または複数の受信者が存在します。以下のステップを使用して、Amazon SNS トピックにパブリッシャー AWS Directory Service としてを追加できます。がディレクトリのステータスの変更 AWS Directory Service を検出すると、そのトピックにメッセージを発行し、トピックのサブスクライバーに送信されます。

発行者として、複数のディレクトリを単一のトピックに関連付けることができます。以前に Amazon SNS で作成したトピックに、ディレクトリステータスのメッセージを追加することもできます。トピックの発行者と受信者は詳細に管理できます。Amazon SNS の詳細については、「[Amazon SNS とは](#)」を参照してください。

Note

ディレクトリステータス通知は、AWS Managed Microsoft AD のリージョン機能です。「[マルチリージョンレプリケーション](#)」を使用している場合、次の手順を各リージョンで個別に適用する必要があります。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

Amazon SNS の有効化

ここでは、AWS Managed Microsoft AD で Amazon SNS を有効にする方法について説明します。

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、SNS メッセージングを有効にするリージョンを選択し、[Maintenance] (メンテナンス) タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Maintenance] (メンテナンス) タブを選択します。
4. [Directory monitoring] (ディレクトリのモニタリング) セクションで [Actions] (アクション) をクリックし、[Create notification] (通知の作成) をクリックします。
5. [Create notification] (通知の作成) ページで、[Choose a notification type] (通知タイプを選択) をクリックしてから、[Create a new notification] (新しい通知の作成) を選択します。または、既存の SNS トピックがある場合は、[Associate with existing SNS topic] (既存の SNS トピックに関連付ける) を選択し、このディレクトリからそのトピックにステータスメッセージを送信できます。

Note

[Create a new notification] (新しい通知の作成) を選択した場合でも、既存の SNS トピックと同じトピック名を使用すると、Amazon SNS は新しいトピックを作成せずに、既存のトピックに新しいサブスクリプション情報を追加するだけです。

[Associate with existing SNS topic] (既存の SNS トピックに関連付ける) を選択した場合は、ディレクトリと同じリージョンにある SNS トピックのみを選択できます。

6. [Recipient type] (受信タイプ) を選択し、[Recipient] (受信者) の連絡先情報を入力します。SMS の電話番号を入力する場合は、数字のみを入力します。ハイフン、スペース、括弧を含めないでください。
7. (オプション) トピックの名前と SNS 表示名を入力します。表示名は、このトピックから送信されるすべての SMS メッセージに含まれる短縮名 (最大 10 文字) です。SMS オプションを使用する場合、表示名は必須です。

Note

[DirectoryServiceFullAccess](#) 管理ポリシーのみを持つ IAM ユーザーまたはロールを使用してログインしている場合、トピック名は「DirectoryMonitoring」で始まる必要があります。トピック名をさらにカスタマイズするには、SNS の権限が追加が必要です。

8. [Create] (作成) をクリックします。

追加の E メールアドレス、Amazon SQS キュー、など、追加の SNS サブスクライバーを指定する場合は AWS Lambda、[Amazon SNS コンソール](#)から指定できます。

Amazon SNS トピックからのディレクトリステータスメッセージの削除

ここでは、Amazon SNS トピックから AWS Managed Microsoft AD ディレクトリのステータスメッセージを削除する方法について説明します。

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ステータスメッセージを削除するリージョンを選択し、[Maintenance]

(メンテナンス) タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

- [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Maintenance] (メンテナンス) タブを選択します。
4. [Directory monitoring] (ディレクトリのモニタリング) セクションでリストから SNS トピック名を選択し、[Actions] (アクション) をクリックして、[Remove] (削除) を選択します。
 5. [Remove] (削除) をクリックします。

これで、選択した SNS トピックへの発行者であるディレクトリが削除されます。

Amazon SNS トピックの削除

トピック全体を削除する場合は、「[Amazon SNS コンソール](#)」から削除できます。

SNS コンソールを使用して Amazon SNS トピックを削除する前に、ディレクトリがそのトピックにステータスメッセージを送信していないことを確認する必要があります。

SNS コンソールを使用して Amazon SNS トピックを削除した場合、この変更は Directory Services コンソール内にはすぐに反映されません。ディレクトリが削除したトピックに通知を次回発行したときにのみ通知されます。その場合、ディレクトリのモニタリングタブに更新されたステータスが表示され、トピックが見つからないことが示されます。

したがって、重要なディレクトリステータスメッセージが欠落しないように、 からメッセージを受信するトピックを削除する前に AWS Directory Service、ディレクトリを別の Amazon SNS トピックに関連付けます。

Amazon SNS トピックを削除する方法の詳細については、「[Deleting an Amazon SNS topic and subscription](#)」を参照してください。

AWS Managed Microsoft AD ディレクトリログについて

AWS Managed Microsoft AD ドメインコントローラーインスタンスのセキュリティログは 1 年間アーカイブされます。Managed AWS Microsoft AD ディレクトリを設定して、ドメインコントローラーログをほぼリアルタイムで Amazon CloudWatch Logs に転送することもできます。詳細については、「[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#)」を参照してください。

AWS は、コンプライアンスのために次のイベントを記録します。

モニタリングカテゴリ	ポリシー設定	監査の状態
アカウントログオン	認証情報検証の監査	成功、失敗
	その他のアカウントログオンイベントの監査	成功、失敗
	Kerberos 認証サービスの監査	成功、失敗
アカウント管理	コンピュータアカウント管理の監査	成功、失敗
	その他のアカウント管理イベントの監査	成功、失敗
	セキュリティグループ管理の監査	成功、失敗
	ユーザーアカウント管理の監査	成功、失敗
詳細な追跡	DPAPI アクティビティの監査	成功、失敗
	PNP アクティビティの監査	成功
	プロセス作成の監査	成功、失敗
DS アクセス	ディレクトリサービスアクセスの監査	成功、失敗
	ディレクトリサービス変更の監査	成功、失敗
ログオン/ログオフ	アカウントロックアウトの監査	成功、失敗
	ログオフの監査	成功
	ログオンの監査	成功、失敗

モニタリングカテゴリ	ポリシー設定	監査の状態
	その他のログオン/ログオフイベントの監査	成功、失敗
	特殊なログオンの監査	成功、失敗
オブジェクトアクセス	その他のオブジェクトアクセスイベントの監査	成功、失敗
	リムーバブルストレージの監査	成功、失敗
	集約型アクセスポリシーステー징の監査	成功、失敗
ポリシー変更	ポリシー変更の監査	成功、失敗
	認証ポリシー変更の監査	成功、失敗
	許可ポリシー変更の監査	成功、失敗
	MPSSVC ルールレベルのポリシー変更の監査	成功
	その他のポリシー変更イベントの監査	失敗
特権使用	機密性の高い特権使用の監査	成功、失敗
システム	IPsec ドライバーの監査	成功、失敗
	その他のシステムイベントの監査	成功、失敗
	セキュリティ状態変更の監査	成功、失敗
	セキュリティシステム拡張の監査	成功、失敗
	システム完全性の監査	成功、失敗

AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化

AWS Directory Service コンソールまたは APIs を使用して、ドメインコントローラーのセキュリティイベントログを AWS Managed Microsoft AD の Amazon CloudWatch Logs に転送できます。これにより、ディレクトリのセキュリティイベントの透明性が得られ、セキュリティモニタリング、監査、およびログの保持ポリシーの要件を満たすために役立ちます。

CloudWatch Logs は、これらのイベントを他の AWS アカウント、AWS サービス、またはサードパーティーのアプリケーションに転送することもできます。これにより、一元的なアラートのモニタリングと設定、および、ほぼリアルタイムでの異常なアクティビティへの事前の対応が容易になります。

有効化されたら、CloudWatch Logs コンソールを使用して、このサービスを有効化したときに指定したロググループからデータを取得できます。このロググループには、ドメインコントローラーのセキュリティログが含まれます。

ロググループとそのデータの読み方の詳細については、「Amazon CloudWatch Logs ユーザーガイド」の「[ロググループとログストリームの操作](#)」を参照してください。

Note

ログ転送は AWS Managed Microsoft AD のリージョン機能です。「[マルチリージョンレプリケーション](#)」を使用している場合、次の手順を各リージョンで個別に適用する必要があります。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。有効にすると、ログ転送機能はドメインコントローラーから指定された CloudWatch ロググループへのログの送信を開始します。ログ転送が有効になる前に作成されたログは、CloudWatch ロググループに転送されません。

トピック

- [AWS Management Console を使用して Amazon CloudWatch Logs ログ転送を有効にする](#)
- [CLI または PowerShell を使用して Amazon CloudWatch Logs ログ転送を有効にする](#)

AWS Management Console を使用して Amazon CloudWatch Logs ログ転送を有効にする

Managed AWS Microsoft AD の Amazon CloudWatch Logs ログ転送は、で有効にできます AWS Management Console。

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、ディレクトリを選択します。
2. 共有する AWS Managed Microsoft AD ディレクトリのディレクトリ ID を選択します。
3. ディレクトリ詳細ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ログ転送を有効にするリージョンを選択し、[Networking & security] (ネットワークとセキュリティ) タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Log forwarding] (ログ転送) セクションで、[Enable] (有効化) を選択します。
5. [Enable log forwarding to CloudWatch] (CloudWatch へのログ転送を有効化する) ダイアログで、次のいずれかのオプションを選択します。
 - a. [Create a new CloudWatch log group] (新しい CloudWatch ロググループを作成) を選択し、[CloudWatch Log group name] (CloudWatch ロググループ名) で CloudWatch Logs で参照できる名前を指定します。
 - b. [Choose an existing CloudWatch log group] (既存の CloudWatch ロググループを選択) を選択し、[Existing CloudWatch log groups] (既存の CloudWatch ロググループ) でメニューからロググループを選択します。
6. 料金の情報とリンクを確認したら、[Enable] (有効化) をクリックします。

CLI または PowerShell を使用して Amazon CloudWatch Logs ログ転送を有効にする

[ds create-log-subscription](#) コマンドを使用するには、まず Amazon CloudWatch ロググループを作成し、そのグループに必要なアクセス許可を付与する IAM リソースポリシーを作成する必要があります。CLI または PowerShell を使用してログ転送を有効にするには、次の手順を完了します。

ステップ 1: CloudWatch Logs にロググループを作成する

ドメインコントローラーからセキュリティログを受信するために使用されるロググループを作成します。名前の先頭には /aws/directoryservice/ を付けることをお勧めしますが、必須ではありません。例:

CLI Command

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

PowerShell Command

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

CloudWatch Logs グループの作成方法については、「Amazon CloudWatch Logs ユーザーガイド」の「[CloudWatch Logs にロググループを作成します](#)」を参照してください。

ステップ 2: IAM で CloudWatch Logs リソースポリシーを作成する

ステップ 1 で作成した新しいロググループにログを追加する AWS Directory Service 権限を付与する CloudWatch Logs リソースポリシーを作成します。ロググループに正確な ARN を指定して、AWS Directory Service の他のロググループへのアクセスを制限するか、ワイルドカードを使用してすべてのロググループを含めることができます。次のサンプルポリシーでは、ワイルドカードメソッドを使用して、ディレクトリが存在する /aws/directoryservice/ AWS アカウントの で始まるすべてのロググループが含まれることを特定します。

JSON

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

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

CLI から実行する必要があるため、このポリシーをローカルワークステーションのテキストファイル (例えば、DSPolicy.json) に保存する必要があります。例:

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
```

ステップ 3: AWS Directory Service ログサブスクリプションを作成する

この最後のステップでは、ログのサブスクリプションを作成して、ログ転送を有効にできます。例 :

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'
```

CloudWatch を使用した AWS Managed Microsoft AD ドメインコントローラーのパフォーマンスのモニタリング

AWS Directory Service は Amazon CloudWatch と統合され、各ドメインコントローラーの重要なパフォーマンスメトリクスを提供します。Active Directory。つまり、ドメインコントローラーのパフォーマンスカウンターとして、CPU やメモリの使用率などをモニタリングできます。また、アラームを設定し、使用率の高い時間に対応するための自動アクションを起動させることもできます。例えば、ドメインコントローラーの CPU 使用率が 70% を超えた場合のアラーム設定し、その発生時に通知を送信するための SNS トピックを作成します。この SNS トピックを使用して、AWS Lambda 関数などの自動化を開始し、Active Directory のドメインコントローラーの数を増やすことができます。

ドメインコントローラーのモニタリングの詳細については、「[CloudWatch メトリクスを使用して、ドメインコントローラーを追加するタイミングを決定する](#)」を参照してください。

Amazon CloudWatch には料金がかかります。詳細については、「[CloudWatch の請求とコスト](#)」を参照してください。

Important

CloudWatch を使用したドメインコントローラーのパフォーマンスメトリクスは、カナダ西部 (カルガリー) リージョンでは利用できません。

CloudWatch を有効にするには、[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#) を参照してください。

CloudWatch でドメインコントローラーのパフォーマンスメトリクスを検索する

Amazon CloudWatch コンソールでは、特定のサービスのメトリクスは最初に、サービスのネームスペースによってグループ化されます。ユーザーは、その名前空間に從属するメトリクスフィルターを追加できます。次の手順を使用して、CloudWatch で AWS Managed Microsoft AD ドメインコントローラーメトリクスを設定するために必要な正しい名前空間と下位メトリクスを見つけます。

CloudWatch コンソールでドメインコントローラーのメトリクスを検索するには

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/cloudwatch/> で CloudWatch コンソールを開きます。
2. ナビゲーションペインで Metrics (メトリクス) を選択します。

3. メトリクスのリストから、[Directory Service] (ディレクトリサービス) の名前空間を選択し、さらにメトリクスとして [AWS Managed Microsoft AD] を選択します。

CloudWatch コンソールを使用してドメインコントローラーメトリクスを設定する方法については、セキュリティブログの「[使用率メトリクスに基づいて AWS Managed Microsoft AD のスケーリングを自動化する方法](#)」を参照してください。AWS

CloudWatch メトリクスを使用して、ドメインコントローラーを追加するタイミングを決定する

ドメインコントローラー全体での負荷分散は、Active Directory の耐障害性とパフォーマンスにとって重要です。AWS Managed Microsoft AD でのドメインコントローラーのパフォーマンスを最適化するために、先に CloudWatch の重要なメトリクスをモニタリングして、ベースラインを形成することをお勧めします。このプロセスでは、時間の経過とともに Active Directory を分析し、平均およびピーク時の Active Directory 使用率を特定します。ベースラインを決めた後に、これらのメトリクスを定期的にモニタリングすることで、ドメインコントローラーを Active Directory に追加するタイミングを判断しやすくなります。

次のメトリクスは、定期的なモニタリングには欠かせません。CloudWatch で利用できるドメインコントローラーのメトリクス一覧については、「[AWS Managed Microsoft AD パフォーマンスカウンター](#)」を参照してください。

- ドメインコントローラーに固有のメトリクスには、次のようなものがあります。
 - プロセッサ
 - メモリ
 - 論理ディスク
 - ネットワークインターフェイス
- AWS Managed Microsoft AD ディレクトリ固有のメトリクス：
 - LDAP 検索
 - バインド
 - DNS クエリ
 - ディレクトリ読み取り
 - ディレクトリ書き込み

CloudWatch コンソールを使用してドメインコントローラーメトリクスを設定する方法については、セキュリティブログの「[使用率メトリクスに基づいて AWS Managed Microsoft AD のスケーリングを自動化する方法](#)」を参照してください。AWS CloudWatch でのメトリクスに関する一般的な情報については、「Amazon CloudWatch ユーザーガイド」の「[Amazon CloudWatch メトリクスを使用する](#)」を参照してください。

ドメイン コントローラーの計画に関する一般的な情報については、Microsoft のウェブサイトにある「[Active Directory ドメインサービスの容量計画](#)」を参照してください。

AWS Managed Microsoft AD パフォーマンスカウンター

次の表に、AWS Managed Microsoft AD でドメインコントローラーとディレクトリのパフォーマンスを追跡するために Amazon CloudWatch で使用できるすべてのパフォーマンスカウンターを示します。

メトリクスカテゴリ	メトリクス名
データベース ==> インスタンス (NTDSA)	Database Cache % Hit
	I/O Database Reads Average Latency
	I/O Database Reads/sec
	I/O Log Writes Average Latency
DirectoryServices (NTDS)	LDAP Bind Time
	DRA Pending Replication Operations
	DRA Pending Replication Synchronizations
DNS	Recursive Queries/sec
	Recursive Query Failure/sec
	TCP Query Received/sec
	Total Query Received/sec
	Total Response Sent/sec

メトリクスカテゴリ	メトリクス名
	UDP Query Received/sec
LogicalDisk	Avg。 Disk Queue Length
	% Free Space
	% Committed Bytes in Use
メモリ	Long-Term Average Standby Cache Lifetime (s)
	Bytes Sent/sec
ネットワークインターフェイス	Bytes Received/sec
	Current Bandwidth
	ATQ Estimated Queue Delay
	ATQ Request Latency
	DS Directory Reads/Sec
NTDS	DS Directory Searches/Sec
	DS Directory Writes/Sec
	LDAP Client Sessions
	LDAP Searches/sec
	LDAP Successful Binds/sec
プロセッサ	% Processor Time
セキュリティシステム全体の統計	Kerberos Authentications
	NTLM Authentications

AWS Managed Microsoft AD の Amazon CloudWatch ログ転送を無効にする

で AWS Managed Microsoft AD の CloudWatch Logs ログ転送を無効にすることができます AWS Management Console。ログ転送の詳細については、「[the section called “CloudWatch を使用してディレクトリをモニタリングする”](#)」をご参照ください。

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、ディレクトリを選択します。
2. 共有する AWS Managed Microsoft AD ディレクトリのディレクトリ ID を選択します。
3. ディレクトリ詳細ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ログ転送を無効にするリージョンを選択し、[Networking & security] (ネットワークとセキュリティ) タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Log forwarding] (ログ転送) セクションで、[Disable] (無効化) を選択します。
5. [Disable log forwarding] (ログ転送の無効化) ダイアログの情報を確認したら、[Disable] (無効化) をクリックします。

Microsoft イベントビューアーによる DNS サーバーの監視

AWS Managed Microsoft AD DNS イベントを監査できるため、DNS の問題の特定とトラブルシューティングが容易になります。例えば、DNS レコードが見つからない場合は、DNS 監査イベントログを使用して根本原因を特定し問題を解決できます。さらに、不審な IP アドレスからのリクエストを検出しブロックすることでセキュリティの強化を図るために、DNS 監査イベントログを使用することもできます。

そのためには、[管理者] アカウント、または [AWS ドメインネームシステム管理者] グループのメンバーであるアカウントを使用して、ログインする必要があります。このグループの詳細については、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。

AWS Managed Microsoft AD DNS のイベントビューアーにアクセスするには

1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2/>) を開きます。
2. 左のナビゲーションペインの [インスタンス] を選択してください。

3. AWS Managed Microsoft AD デイレクトリに参加している Amazon EC2 インスタンスを見つけます。対象のインスタンスを選択し、[Connect] (接続) をクリックしてください。
4. Amazon EC2 インスタンスに接続したら、[スタート] メニューを開き、[Windows 管理ツール] フォルダを選択します。[管理ツール] フォルダ内で、[イベントビューアー] を選択します。
5. イベントビューアーウィンドウで [Action] (アクション) をクリックし、次に [Connect to Another Computer] (別のコンピュータに接続) をクリックします。
6. 別のコンピュータを選択し、AWS Managed Microsoft AD DNS サーバーの名前または IP アドレスのいずれかを入力し、OK を選択します。
7. 左側のペインで、[Applications and Services Logs] (アプリケーションとサービスのログ)、[Microsoft]、[Windows]、[DNS-Server] (DNS サーバー) の順に選択し、最後に [Audit] (監査) をクリックします。

AWS Managed Microsoft AD から AWS アプリケーションとサービスへのアクセス

Managed AWS Microsoft AD ユーザーにアクセスを許可して、AWS アプリケーションとサービスにアクセスできます。これらの AWS アプリケーションとサービスには、次のようなものがあります。

- Amazon Chime
- Amazon EC2
- QuickSight
- AWS Management Console
- Amazon WorkSpaces

AWS Managed Microsoft AD でアクセス URLs とシングルサインオンを使用することもできます。

AWS Managed Microsoft AD から AWS アプリケーションとサービスにアクセスするタスク

- [AWS Managed Microsoft AD のアプリケーションの互換性](#)
- [AWS Managed Microsoft AD の AWS アプリケーションとサービスへのアクセスの有効化](#)
- [AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化](#)
- [AWS Managed Microsoft AD のアクセス URL の作成](#)
- [AWS Managed Microsoft AD のシングルサインオンの有効化](#)

AWS Managed Microsoft AD のアプリケーションの互換性

AWS Directory Service for Microsoft Active Directory (AWS マネージド Microsoft AD) は、複数の AWS サービスおよびサードパーティーアプリケーションと互換性があります。

以下は、互換性のある AWS アプリケーションとサービスのリストです。

- Amazon Chime
- Amazon Connect
- Amazon EC2
- QuickSight
- Amazon RDS
- WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS IAM Identity Center
- AWS License Manager
- AWS Management Console
- FSx for Windows File Server
- WorkSpaces

詳細については、「[AWS Managed Microsoft AD の AWS アプリケーションとサービスへのアクセスの有効化](#)」を参照してください。

を使用するカスタムおよび商用off-the-shelfアプリケーションは多数あるためActive Directory、AWS は AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) とのサードパーティーアプリケーションの互換性を正式に検証することも、広範に検証することもできません。は、アプリケーションのインストールに関する潜在的な課題を克服するためにお客様と AWS 連携しますが、アプリケーションが AWS Managed Microsoft AD と互換性があること、または互換性が維持されることは保証できません。

以下のサードパーティーアプリケーションは AWS Managed Microsoft AD と互換性があります。

- Active Directory に基づくアクティベーション (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 (以前は Azure Active Directory (Azure AD) と呼ばれていました)
- Microsoft Entra Connect (以前は Azure Active Directory Connect と呼ばれていました)
- 分散ファイルシステムレプリケーション (DFSR)
- 分散ファイルシステム名前空間 (DFS-N)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server (Always On アベイラビリティーグループを含む)
- Microsoft System Center Configuration Manager (SCCM) - SCCM をデプロイするユーザーは、AWS 委任システム管理者グループのメンバーである必要があります。
- Microsoft Windows and Windows Server OS
- Office 365

これらのアプリケーションのすべての設定がサポートされているわけではありません。

互換性に関するガイドライン

アプリケーションには互換性のない設定が含まれていることがあります。多くの場合、アプリケーションのデプロイ設定により非互換性を解決できます。アプリケーションの互換性がなくなる原因として多いものを次に示します。お客様はこの情報を使用して、目的のアプリケーションの互換性の特性を調べ、デプロイを変更する場合、その方法を特定できます。

- ドメイン管理者などの特権アクセス許可 – 一部のアプリケーションは、ドメイン管理者としてインストールする必要があります。Active Directory をマネージドサービスとして配信するために、AWS はこのアクセス許可レベルの排他的な制御を保持する必要があるため、ドメイン管理者としてそのようなアプリケーションをインストールすることはできません。ただし、多くの場合、このようなアプリケーションをインストールするには、インストールを実行するユーザーに、特定の、権限の少ない、AWS サポートされているアクセス許可を委任します。アプリケーションに必要な正確なアクセス許可の詳細については、アプリケーションのプロバイダーにお問い合わせください。委任 AWS を許可するアクセス許可の詳細については、「」を参照してください [AWS Managed Microsoft AD で作成されるもの](#)。
- 特権 Active Directory コンテナへのアクセス – ディレクトリ内では、AWS マネージド Microsoft AD は組織単位 (OU) を提供しており、管理を完全に制御できます。Active Directory ツリー内でその OU よりも上位にあるコンテナに対しては、作成や書き込みのアクセス許可がなく、読み取りアク

セス許可がある場合でも限定的です。お客様にアクセス許可が付与されていないコンテナを作成したりそれらにアクセスしたりするアプリケーションは機能しない可能性があります。ただし、そのようなアプリケーションでは、多くの場合、OU 内で作成したコンテナを代替として使用できます。OU 内のコンテナを代替として作成して使用する方法については、アプリケーションのプロバイダーに確認してください。OU に関する詳細は、「[AWS Managed Microsoft AD で作成されるもの](#)」を参照してください。

- インストールワークフロー中のスキーマの変更 – 一部の Active Directory アプリケーションは、デフォルトの Active Directory スキーマを変更する必要があり、アプリケーションのインストールワークフロー中にそのような変更を試みる場合があります。スキーマ拡張は特権的であるため、AWS は AWS Directory Service コンソール、CLI、または SDK を介してのみ Lightweight Directory Interchange Format (LDIF) ファイルをインポートすることでこれを可能にします。このようなアプリケーションには、多くの場合、AWS Directory Service スキーマの更新プロセスを通じてディレクトリに適用できる LDIF ファイルが含まれています。LDIF のインポートプロセスの詳細については、「[チュートリアル: AWS Managed Microsoft AD スキーマの拡張](#)」を参照してください。インストールプロセス中にスキーマのインストールをバイパスすれば、アプリケーションをインストールできます。

互換性のない既知のアプリケーション

以下は、AWS Managed Microsoft AD と連携する設定が見つからない、一般的にリクエストされる市販 off-the-shelf アプリケーションの一覧です。は、お客様が非生産的な作業を回避できるように、独自の判断でこのリストを随時 AWS 更新します。AWS は、現在または将来の互換性に関する保証やクレームなしに、この情報を提供します。

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

AWS Managed Microsoft AD の AWS アプリケーションとサービスへのアクセスの有効化

ユーザーは Managed Microsoft AD AWS を承認して、Amazon WorkSpaces などの AWS アプリケーションやサービスへのアクセスを許可できます Active Directory。Managed Microsoft AD AWS と連携するには、次の AWS アプリケーションとサービスを有効または無効にできます。

AWS アプリケーション/サービス	詳細情報
Amazon Chime	詳細については、「 Active Directory への接続 」を参照してください。
Amazon Connect	詳細については、「 Amazon Connect 管理者ガイド 」を参照してください。
Amazon EC2	詳細については、「 Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法 」を参照してください。
Amazon FSx for Windows File Server	詳細については、「 Microsoft Active Directory 用 AWS Directory Service での Amazon FSx の使用 」を参照してください。
QuickSight	詳細については、 QuickSight Enterprise Edition での Active Directory の使用 」を参照してください。
Amazon Relational Database Service	詳細については次を参照してください: • MySQL での Kerberos 認証の使用 • Amazon RDS for Oracle での Kerberos 認証の使用 • Amazon RDS for PostgreSQL での Kerberos 認証の使用 • Amazon RDS for SQL Server での AWS Managed Microsoft AD の使用
Amazon WorkDocs	詳細については、「 Enable Amazon WorkDocs for AWS Managed Microsoft AD 」を参照してください。
Amazon WorkMail	詳細については、「 Creating an organization 」を参照してください。

AWS アプリケーション/サービス	詳細情報
Amazon WorkSpaces	WorkSpaces から、Simple AD、AWS Microsoft AD、または AD Connector を直接作成することが可能です。このためには単純に、Workspace の作成時に [Advanced Setup] (高度なセットアップ) を起動します。 詳細については、WorkSpaces で既存の AWS Directory Service ディレクトリを登録する Personal」を参照してください。
AWS Client VPN	詳細については、「クライアント VPN の Active Directory 認証」を参照してください。
AWS IAM Identity Center	詳細については、「Microsoft AD ディレクトリに接続する」を参照してください。
AWS License Manager	詳細については、「License Manager でのユーザーベースのサブスクリプションの管理」を参照してください。
AWS Management Console	詳細については、「AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化」を参照してください。
AWS Private Certificate Authority	詳細については、「Active Directory のAWS Private CA コネクタ」を参照してください。
AWS Transfer Family	詳細については、「SFTP、FTPS、または FTP サーバーエンドポイントの設定」を参照してください。

有効化の完了後は、ディレクトリへのアクセス権限を付与したアプリケーションまたはサービスのコンソールから、そのディレクトリへのアクセスを管理します。

AWS アプリケーションとサービスの検索

AWS Directory Service コンソールで前述のアプリケーションとサービスを検索する AWS には、次の手順を実行します。

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. [AWS apps & services] (AWS アプリおよびサービス) セクションでリストを確認します。

を使用して AWS アプリケーションとサービスを認可または認可解除する方法の詳細については AWS Directory Service、「」を参照してください [を使用した AWS アプリケーションとサービスの認可](#) [AWS Directory Service](#)。

AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化

AWS Directory Service では、ディレクトリのメンバーに へのアクセスを許可できます AWS Management Console。デフォルトでは、ディレクトリメンバーは AWS リソースにアクセスできません。ディレクトリメンバーに IAM ロールを割り当てて、さまざまな AWS サービスとリソースへのアクセスを許可します。IAM ロールでは、ディレクトリメンバーに付与するサービス、リソース、およびアクセス権限のレベルを定義します。

ディレクトリメンバーにコンソールへのアクセス権限を付与する際には、ディレクトリにアクセスするための URL を設定しておく必要があります。ディレクトリの詳細表示およびアクセス URL の取得に関する詳細は、「[AWS Managed Microsoft AD ディレクトリ情報の表示](#)」を参照してください。アクセス URL 作成方法の詳細については、「[AWS Managed Microsoft AD のアクセス URL の作成](#)」を参照してください。

IAM ロールを作成し、ディレクトリメンバーに割り当てる方法に関する詳細については「[AWS Managed Microsoft AD ユーザーとグループに IAM ロールを持つリソースへのアクセス権 AWS を付与する](#)」を参照してください。

トピック

- [AWS Management Console アクセスの有効化](#)

- [AWS Management Console アクセスの無効化](#)
- [AWS Management Console ログインセッションの長さの設定](#)

関連する AWS セキュリティブログ記事

- [AWS Managed Microsoft AD とオンプレミス認証情報 AWS Management Console を使用してにアクセスする方法](#)

関連 AWS re:Post 記事

- [AWS Management Console オンプレミスActive Directoryユーザーにへのアクセスを許可するにはどうすればよいですか？](#)

Note

へのアクセス AWS Management Console は、AWS Managed Microsoft AD のリージョン機能です。「[マルチリージョンレプリケーション](#)」を使用している場合、次の手順を各リージョンで個別に適用する必要があります。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

AWS Management Console アクセスの有効化

デフォルトでは、コンソールへのアクセスが有効化されたディレクトリはありません。ディレクトリのユーザーおよびグループによるコンソールアクセスを有効にするには、以下の手順を実行します。

コンソールアクセスを有効にするには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - マルチリージョンレプリケーションの下に複数のリージョンが表示されている場合は、へのアクセスを有効にするリージョンを選択し AWS Management Console、アプリケーション管理タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

- [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを開きます。
4. AWS Management Console セクションで、[Enable] (有効) をクリックします。ディレクトリに対するコンソールアクセスが有効になりました。

Important

ユーザーがアクセス URL を使用してコンソールにサインインできるようにするには、まず、そのユーザーを IAM ロールに追加しておく必要があります。IAM ロールへのユーザーの割り当てに関する一般情報については、「[既存の IAM ロールにユーザーまたはグループを割り当てる](#)」を参照してください。IAM ロールの割り当てが完了したユーザーは、アクセス URL を使用してコンソールにアクセスできるようになります。例えば、ディレクトリアクセス URL が `example-corp.awsapps.com` の場合 `example-corp.awsapps.com`、コンソールにアクセスする URL は `https://example-corp.awsapps.com/console/` です。

AWS Management Console アクセスの無効化

AWS Managed Microsoft AD ディレクトリのユーザーとグループの AWS Management Console アクセスを無効にするには、次の手順を実行します。

コンソールアクセスを無効化するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - マルチリージョンレプリケーションの下に複数のリージョンが表示されている場合は、へのアクセスを無効にするリージョンを選択し AWS Management Console、アプリケーション管理タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを開きます。
4. AWS Management Console セクションで、[Disable] (無効) をクリックします。これで、ディレクトリからのコンソールアクセスが無効化されます。

5. IAM ロールがディレクトリ内のユーザーまたはグループに割り当てられている場合、[Disable] (無効) ボタンは使用できない場合があります。この場合は、先に進む前に、ディレクトリのすべての IAM ロールの割り当てを削除します。これには、ディレクトリから削除されたユーザー ([Deleted User] (削除されたユーザー) に表示) またはグループ ([Deleted Group] (削除されたグループ) に表示) への割り当ても含まれます。

すべての IAM ロールの割り当てが削除されたら、上記の手順を繰り返します。

AWS Management Console ログインセッションの長さの設定

デフォルトでは、ユーザーは正常にサインインしてからログアウト AWS Management Console するまでに 1 時間セッションを使用できます。この場合、再度サインインしてセッションを開始する必要がありますが、1 時間後経過すると、再度このセッションからログオフされます。以下の手順により、使用期間をセッションごとに最大 12 時間に延長することができます。

AWS Management Console ログインセッションの長さを設定するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ログインセッション期間を設定するリージョンを選択した上で、[Application management] (アプリケーション管理) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを開きます。
4. [AWS apps & services] (AWS アプリおよびサービス) セクションで、[Management Console] (マネジメントコンソール) を選択します。
5. AWS リソースへのアクセスの管理ダイアログボックスで、続行を選択します。
6. [Assign users and groups to IAM roles] (ユーザーおよびグループの IAM ロールへの割り当て) ページの [Set login session length] (ログインセッション期間の設定) で数値を編集し、[Save] (保存) をクリックします。

AWS Managed Microsoft AD のアクセス URL の作成

アクセス URL は、Amazon WorkDocs などの AWS アプリケーションやサービスで使用され、ディレクトリに関連付けられているログインページにアクセスします。以下の手順を実行して、ディレクトリのアクセス URL を作成できます。

考慮事項

- URL はグローバルに一意である必要があります。
- マルチリージョンディレクトリを使用している場合、アクセス URL はプライマリリージョンからのみ設定できます。
- このディレクトリのアプリケーションアクセス URL は、作成した後では変更できません。アクセス URL が作成された後は、他のユーザーが使用することはできません。ディレクトリを削除すると、アクセス URL も削除され、他のアカウントで使用することができます。

アクセス URL を作成するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [マルチリージョンレプリケーション] に複数のリージョンが表示されている場合は、プライマリリージョンを選択して [アプリケーション管理] タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを選択します。
4. [Application access URL] (アプリケーションのアクセス URL) セクションで、ディレクトリにアクセス URL が割り当てられていない場合は、[Create] (作成) ボタンが表示されます。ディレクトリのエイリアスを入力し、[Create] (作成) をクリックします。「Entity Already Exists (エンティティは既に存在しています)」というエラーが返された場合は、指定したディレクトリのエイリアスは割り当て済みです。別のエイリアスを選択して、この手順を繰り返します。

アクセス URL は、`<alias>.awsapps.com` の形式で表示されます。デフォルトでは、この URL は WorkDocs のサインインページに移動します。

AWS Managed Microsoft AD のシングルサインオンの有効化

AWS Directory Service は、ユーザーが認証情報を個別に入力することなく、ディレクトリに参加しているコンピュータから WorkDocs にアクセスできるようにする機能を提供します。

シングルサインオンを有効にする前に、ユーザーのウェブブラウザでシングルサインオンをサポートさせるための、追加の手順を実行する必要があります。ユーザーは、シングルサインオンを有効にするために、ウェブブラウザで設定の変更が必要な場合があります。

Note

シングルサインオンは、AWS Directory Service ディレクトリに結合されているコンピュータで使用された場合にのみ機能します。このディレクトリに結合されていないコンピュータでは使用できません。

ディレクトリに AD Connector ディレクトリを使用しており、AD Connector サービスアカウントがそのサービスプリンシパル名属性を追加または削除するためのアクセス許可を持っていない場合、下記のステップ 5 とステップ 6 では、2 つのオプションが選択できます。

1. 続行した場合、AD Connector サービスアカウントのサービスプリンシパル名属性を追加または削除するアクセス許可を持つディレクトリユーザーのユーザー名とパスワードの入力を求められます。これらの認証情報は、シングルサインオンを有効にする目的でのみ使用され、サービスで保存されることはありません。AD Connector サービスアカウントのアクセス許可は変更されません。
2. AD Connector サービスアカウントには、それ自体のサービスプリンシパル名属性を追加または削除するための権限を委任できます。AD Connector サービスアカウントのアクセス許可を変更する権限を持つアカウントを使用して、ドメインに結合済みコンピュータから次の PowerShell コマンドを実行します。次のコマンドは、AD Connector サービスアカウントに対して、それ自体のサービスプリンシパル名属性のみを追加および削除することを許可します。

```
$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"
```

WorkDocs でシングルサインオンを有効または無効にするには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. アプリケーションアクセス URL セクションで、有効を選択して WorkDocs のシングルサインオンを有効にします。

[Enable] (有効) ボタンが表示されていない場合は、最初にアクセス URL を作成すると、このオプションが表示されます。アクセス URL 作成方法の詳細については、「[AWS Managed Microsoft AD のアクセス URL の作成](#)」を参照してください。

5. [Enable Single Sign-On for this directory] (このディレクトリのシングルサインオンの有効化) ダイアログボックスで、[Enable] (有効) をクリックします。ディレクトリのシングルサインオンが有効に設定されます。
6. 後で WorkDocs でシングルサインオンを無効にする場合は、Disable を選択し、このディレクトリの Single Sign-On を無効にするダイアログボックスでもう一度Disable を選択します。

トピック

- [IE および Chrome でのシングルサインオン](#)
- [Firefox でのシングルサインオン](#)

IE および Chrome でのシングルサインオン

Microsoft Internet Explorer (IE) および Google Chrome ブラウザでシングルサインオンを使用するには、クライアントコンピュータで以下のタスクを実行する必要があります。

- シングルサインオンが承認済みサイトのリストに、アクセス URL (例: `https://<alias>.awsapps.com`) を追加します。
- アクティブなスクリプト (JavaScript) を有効にします。
- 自動ログオンを許可します。
- 統合された認証を有効にします。

ユーザーは、これらのタスクを手動で実行するか、対象の設定を、グループポリシーの設定を通じて変更することができます。

トピック

- [Windows シングルサインオン用の手動アップデート](#)
- [OS X でシングルサインオンを設定するための手動アップデート](#)
- [シングルサインオンのグループポリシー設定](#)

Windows シングルサインオン用の手動アップデート

Windows コンピュータでのシングルサインオンを手動で有効にするには、クライアントコンピュータで以下の手順を行います。これらの設定の一部については、適切に事前設定が行われています。

Windows 上で Internet Explorer および Chrome のシングルサインオンを手動で有効にするには

1. [Internet Properties] (インターネットプロパティ) ダイアログボックスを開くには、[Start] (スタート) メニューを開き、検索ボックスに「Internet Options」と入力した上で、[Internet Options] (インターネットオプション) をクリックします。
2. 承認済みサイトのリストにアクセス URL を追加してシングルサインオンを設定するには、以下の手順を実行します。

- a. [Internet Properties] (インターネットプロパティ) ダイアログボックスで [Security] (セキュリティ) タブを開きます。
 - b. [Local intranet] (ローカルイントラネット)、[Sites] (サイト) の順に選択します。
 - c. [Local intranet] (ローカルイントラネット) ダイアログボックスで、[Advanced] (詳細) をクリックします。
 - d. ウェブサイトのリストにアクセス URL を追加した後、[Close] (閉じる) をクリックします。
 - e. [Local intranet] (ローカルイントラネット) ダイアログボックスで、[OK] をクリックします。
3. アクティブスクリプトを有効にするには、以下の手順を行います。
- a. [Internet Properties] (インターネットのプロパティ) ダイアログボックスの [Security] (セキュリティ) タブで、[Custom level] (カスタムレベル) をクリックします。
 - b. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、下部にある [Scripting] (スクリプト) までスクロールし、[Active scripting] (アクティブスクリプト) の下で [Enable] (有効) をクリックします。
 - c. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、[OK] をクリックします。
4. 自動ログオンを有効にするには、以下の手順を実行します。
- a. [Internet Properties] (インターネットのプロパティ) ダイアログボックスの [Security] (セキュリティ) タブで、[Custom level] (カスタムレベル) をクリックします。
 - b. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、下部の [User Authentication] (ユーザー認証) までスクロールし、[Logon] (ログオン) にある [Automatic logon only in Intranet zone] (イントラネットゾーン内のみで自動ログオンを認証する) をクリックします。
 - c. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、[OK] をクリックします。
 - d. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、[OK] をクリックします。
5. 統合された認証を有効にするには、以下の手順を行います。
- a. [Internet Properties] (インターネットのプロパティ) ダイアログボックスで、[Advanced] (詳細) タブを表示します。

- b. 下部にある [Security] (セキュリティ) までスクロールし、[Enable Integrated Windows Authentication] (Windows 認証の統合を有効化する) をクリックします。
 - c. [Internet Properties] (インターネットプロパティ) ダイアログボックスで、[OK] をクリックします。
6. これらの変更を適用するためにブラウザを再起動します。

OS X でシングルサインオンを設定するための手動アップデート

シングルサインオンを、OS X の Chrome 向けに手動で有効化するには、クライアントコンピュータで以下の手順を実行します。これらの手順を完了させるには、コンピュータの管理者権限が必要です。

OS X で Chrome 向けのシングルサインオンを手動で有効にするには

1. 次のコマンドを実行し、アクセス URL を [AuthServerAllowlist](#) ポリシーに追加します。

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. [System Preferences] (システム設定) を開き、[Profiles] (プロファイル) パネルに移動して、Chrome Kerberos Configuration プロファイルを削除します。
3. Chrome を再起動して `chrome://policy` を開き、新しい設定が適用されていることを確認します。

シングルサインオンのグループポリシー設定

ドメイン管理者は、グループポリシー設定を実装することで、ドメインに結合しているクライアントコンピュータでのシングルサインオンの設定を変更できるようになります。

Note

Chrome のポリシーを適用したドメインのコンピュータで Chrome ウェブブラウザを管理している場合は、アクセス URL を [AuthServerAllowlist](#) ポリシーに追加する必要があります。Chrome ポリシーの設定に関する詳細については、「[Policy Settings in Chrome](#)」(Chrome のポリシー設定) を参照してください。

グループポリシー設定を使用して Internet Explorer および Chrome のシングルサインオンを有効にするには

1. 以下の手順を実行し、新しいグループポリシーオブジェクトを作成します。
 - a. グループポリシー管理ツールを開き、対象のドメインに移動して [Group Policy Objects] (グループポリシーオブジェクト) をクリックします。
 - b. メインメニューで、[Action] (アクション)、[New] (新規) の順に選択します。
 - c. [New GPO] (新しい GPO) ダイアログボックスで、グループポリシーオブジェクトのために識別しやすい名前 (IAM Identity Center Policy など) を入力します。また、[Source Starter GPO] (ソース スターター GPO) は 「(none)」 のままにします。[OK] をクリックします。
2. アクセス URL を承認済みサイトのリストに追加してシングルサインオンを設定するには、以下の手順を実行します。
 - a. グループポリシー管理ツールで、使用するドメインに移動し、[Group Policy Objects] (グループポリシーオブジェクト) を選択します。次に、右クリックで IAM Identity Center ポリシーのコンテキスト メニューを開き、[Edit] (編集) を選択します。
 - b. ポリシーツリー内で、[User Configuration] (ユーザーの設定)、[Preferences] (設定)、[Windows Settings] (Windows の設定) の順に選択します。
 - c. [Windows Settings] (Windows の設定) リストから、[Registry] (レジストリ) のコンテキストメニューを右クリックで開き、[New registry item] (新規のレジストリ項目) を選択します。
 - d. [New Registry Properties] (新規レジストリ設定) ダイアログボックスで、以下の設定を入力した上で [OK] をクリックします。

[Action] (アクション)

Update

[Hive]

HKEY_CURRENT_USER

[Path] (パス)

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

`<alias>` の値は、アクセス URL から抽出します。アクセス URL が `https://examplecorp.awsapps.com` の場合、エイリアスは `examplecorp` となり、レジストリキーは `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp` になります。

[Value name] (値の名前)

https

[Value type] (値の型)

REG_DWORD

[Value data] (値のデータ)

1

3. アクティブスクリプトを有効にするには、以下の手順を行います。

- a. グループポリシー管理ツールで、使用するドメインに移動し、[Group Policy Objects] (グループポリシーオブジェクト) を選択します。次に、右クリックで IAM Identity Center ポリシーのコンテキストメニューを開き、[Edit] (編集) を選択します。
- b. ポリシーツリー内で、[Computer Configuration] (コンピュータの設定)、[Policies] (ポリシー)、[Administrative Templates] (管理テンプレート)、[Windows Components] (Windows コンポーネント)、[Internet Explorer]、[Internet Control Panel] (インターネットコントロールパネル)、[Security Page] (セキュリティページ)、[Intranet Zone] (イントラネットゾーン) の順に選択します。
- c. [Intranet Zone] (イントラネットゾーン) リストで、右クリックにより [Allow active scripting] (アクティブスクリプトの許可) のコンテキストメニューを開き、[Edit] (編集) を選択します。
- d. [Allow active scripting] (アクティブスクリプトの許可) ダイアログボックスで、以下の設定を入力した上で [OK] をクリックします。
 - [Enabled] (有効) ラジオボタンをオンにします。
 - [Options] (オプション) で、[Allow active scripting] (アクティブスクリプトを許可する) を「Enable」(有効) に設定します。

4. 自動ログオンを有効にするには、以下の手順を実行します。

- a. グループポリシー管理ツールで、対象のドメインに移動しグループポリシーオブジェクトを選択します。次に、右クリックで SSO ポリシーのコンテキストメニューを開き、[Edit] (編集) を選択します。
 - b. ポリシーツリー内で、[Computer Configuration] (コンピュータの設定)、[Policies] (ポリシー)、[Administrative Templates] (管理テンプレート)、[Windows Components] (Windows コンポーネント)、[Internet Explorer]、[Internet Control Panel] (インターネットコントロールパネル)、[Security Page] (セキュリティページ)、[Intranet Zone] (イントラネットゾーン) の順に選択します。
 - c. [Intranet Zone] (イントラネットゾーン) リストで、右クリックにより [Logon options] (ログオンオプション) のコンテキストメニューを開き、[Edit] (編集) を選択します。
 - d. [Logon options] (ログオンオプション) ダイアログボックスで、以下の設定を入力した上で [OK] を選択します。
 - [Enabled] (有効) ラジオボタンをオンにします。
 - [Options] (オプション) で、[Logon options] (ログオンオプション) に [Automatic logon only in Intranet zone] (イントラネットゾーン内のみで自動ログオンを認証する) を設定します。
5. 統合された認証を有効にするには、以下の手順を行います。
- a. グループポリシー管理ツールで、使用するドメインに移動し、[Group Policy Objects] (グループポリシーオブジェクト) を選択します。次に、右クリックで IAM Identity Center ポリシーのコンテキストメニューを開き、[Edit] (編集) を選択します。
 - b. ポリシーツリー内で、[User Configuration] (ユーザーの設定)、[Preferences] (設定)、[Windows Settings] (Windows の設定) の順に選択します。
 - c. [Windows Settings] (Windows の設定) リストから、[Registry] (レジストリ) のコンテキストメニューを右クリックで開き、[New registry item] (新規のレジストリ項目) を選択します。
 - d. [New Registry Properties] (新規レジストリ設定) ダイアログボックスで、以下の設定を入力した上で [OK] をクリックします。

[Action] (アクション)

Update

[Hive]

HKEY_CURRENT_USER

[Path] (パス)

Software\Microsoft\Windows\CurrentVersion\Internet Settings

[Value name] (値の名前)

EnableNegotiate

[Value type] (値の型)

REG_DWORD

[Value data] (値のデータ)

1

6. 開いている場合は、[Group Policy Management Editor] (グループポリシー管理エディタ) ウィンドウを閉じます。
7. 次の手順を実行し、ドメインに新しいポリシーを割り当てます。
 - a. [グループポリシーの管理] ツリーで、右クリックによりドメインのコンテキストメニューを開き、[Link an Existing GPO] (既存の GPO をリンク) を選択します。
 - b. [Group Policy Objects] (グループポリシーオブジェクト) リストで、IAM Identity Center ポリシーを選択し、[OK] を選択します。

この変更は、クライアントが次にグループポリシーを更新した後、または次回のユーザーログインの後に適用されます。

Firefox でのシングルサインオン

Mozilla Firefox ブラウザでシングルサインオンのサポートを許可するには、アクセス URL (例: <https://<alias>.awsapps.com>) を、シングルサインオン承認済みサイトのリストに追加します。この設定は、手動で行うことも、スクリプトを使用して自動で行うこともできます。

トピック

- [シングルサインオンのための手動による更新](#)
- [シングルサインオンのための自動によるアップデート](#)

シングルサインオンのための手動による更新

Firefox の承認済みサイトのリストに手動でアクセス URL を追加するには、クライアントコンピュータで以下の手順を実行します。

Firefox の承認済みサイトのリストに手動でアクセス URL を追加するには

1. Firefox を開いて、`about:config` ページに移動します。
2. `network.negotiate-auth.trusted-uris` の設定を開き、アクセス URL をサイトのリストに追加します。複数のエントリを設定するには、それぞれをカンマ (,) で区切ります。

シングルサインオンのための自動によるアップデート

ドメインの管理者であれば、ネットワークにあるすべてのコンピュータに対し、Firefox の `network.negotiate-auth.trusted-uris` ユーザー設定にアクセス URL を追加するためのスクリプトを使用できます。詳細については、<https://support.mozilla.org/en-US/questions/939037> にアクセスしてください。

AWS Managed Microsoft AD ユーザーとグループに IAM ロールを持つリソースへのアクセス権 AWS を付与する

AWS Directory Service は、AWS Managed Microsoft AD ユーザーとグループに Amazon EC2 コンソールへのアクセス AWS などの サービスやリソースへのアクセスを許可する機能を提供します。「」で説明されているように、ディレクトリを管理するためのアクセス権を IAM ユーザーに付与すると同様に[アイデンティティベースのポリシー \(IAM ポリシー\)](#)、ディレクトリ内のユーザーが Amazon EC2 などの他の AWS リソースにアクセスできるようにするには、それらのユーザーとグループに IAM ロールとポリシーを割り当てる必要があります。詳細については、「IAM ユーザーガイド」の「[IAM ロール](#)」を参照してください。

へのアクセス権をユーザーに付与する方法については AWS Management Console、「」を参照してください[AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化](#)。

トピック

- [新しい IAM ロールの作成](#)
- [既存の IAM ロールの信頼関係を編集する](#)
- [既存の IAM ロールにユーザーまたはグループを割り当てる](#)

- [ロールに割り当てられたユーザーとグループの表示](#)
- [IAM ロールからユーザーまたはグループを削除する](#)
- [での AWS マネージドポリシーの使用 AWS Directory Service](#)

新しい IAM ロールの作成

で使用する新しい IAM ロールを作成する必要がある場合は AWS Directory Service、IAM コンソールを使用して作成する必要があります。ロールが作成されたら、AWS Directory Service コンソールでそのロールを表示する前に、そのロールとの信頼関係を設定する必要があります。詳細については、「[既存の IAM ロールの信頼関係を編集する](#)」を参照してください。

Note

このタスクを実行するユーザーには、以下の IAM アクションを実行するためのアクセス許可が付与されている必要があります。詳細については、「[アイデンティティベースのポリシー \(IAM ポリシー\)](#)」を参照してください。

- iam:PassRole
- iam:GetRole
- iam:CreateRole
- iam:PutRolePolicy

IAM コンソールで新しいロールを作成するには

1. IAM コンソールのナビゲーションペインで [Roles] (ロール) をクリックします。詳細については、IAM ユーザーガイドの [Creating a role \(AWS Management Console\)](#) を参照してください。
2. [Create role] (ロールの作成) を選択します。
3. [Choose the service that will use this role] (このロールを使用するサービスを選択) で、[Directory Service] (ディレクトリサービス)、[Next] (次へ) の順に選択します。
4. ディレクトリユーザーに適用するポリシー (AmazonEC2FullAccess など) の横にあるチェックボックスをオンにして、[Next] (次へ) をクリックします。
5. 必要に応じてタグをロールに追加した上で、[Next] (次へ) をクリックします。
6. [Role name] ロール名を入力し、オプションで [Description] (説明) を入力した後、[Create role] (ロールを作成) をクリックします。

例: AWS Management Console へのアクセスを有効にするためのロールを作成する

次のチェックリストは、特定の AWS Managed Microsoft AD ユーザーに Amazon EC2 コンソールへのアクセスを許可する新しい IAM ロールを作成するために完了する必要があるタスクの例を示しています。

1. 上記の手順に従い、IAM コンソールを使用してロールを作成します。ポリシーが要求されたら、「AmazonEC2FullAccess」を選択します。
2. [既存の IAM ロールの信頼関係を編集する](#) の手順に従い作成したロールを編集した後、必要な信頼関係情報をポリシードキュメントに追加します。このステップは、次のステップ AWS Management Console へのアクセスを有効にした直後にロールを表示するために必要です。
3. [AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化](#) の手順に従って、AWS Management Consoleへの一般的なアクセスを設定します。
4. [既存の IAM ロールにユーザーまたはグループを割り当てる](#) の手順に従って、EC2 リソースへのフルアクセスを必要とするユーザーを新しいロールに追加します。

既存の IAM ロールの信頼関係を編集する

既存の IAM ロールを AWS Directory Service ユーザーとグループに割り当てることができます。ただし、これを行うには、ロールに どの信頼関係が必要です AWS Directory Service。AWS Directory Service を使用して の手順を使用してロールを作成すると [新しい IAM ロールの作成](#)、この信頼関係が自動的に設定されます。

Note

ユーザーがこの信頼関係を確立する必要があるのは、AWS Directory Serviceによって作成されない IAM ロールに対してのみです。

への既存の IAM ロールの信頼関係を確立するには AWS Directory Service

1. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. IAM コンソールのナビゲーションペインの [Access management] で、[Roles] を選択します。

コンソールには、アカウントにあるロールが表示されます。
3. 変更するロールの名前を選択した後、詳細ページの [Trust relationships] タブを開きます。
4. [Edit trust policy] (信頼ポリシーを編集) を選択します。

5. [Policy Document] の下に以下の内容を貼り付けた後、[Update policy] をクリックします。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

このポリシードキュメントは、AWS CLIを使用して更新することも可能です。詳細については、「AWS CLI コマンドリファレンス」の「[update-trust](#)」を参照してください。

既存の IAM ロールにユーザーまたはグループを割り当てる

Managed Microsoft AD ユーザーまたはグループに既存の IAM AWS ロールを割り当てることができます。そのため、次の手順を完了していることを確認してください。

前提条件

- [AWS Managed Microsoft AD を作成します](#)。
- 「[IAM ユーザーを作成する](#)」または「[IAM グループを作成する](#)」。
- 信頼関係を持つ[ロールを作成します](#) AWS Directory Service。既存の IAM ロールの場合、「[既存のロールの信頼関係を編集](#)」する必要があります。

⚠ Important

ディレクトリ内のネストされたグループの AWS Managed Microsoft AD ユーザーのアクセスはサポートされていません。親グループのメンバーにはコンソールへのアクセス権限がありますが、子グループのメンバーによるアクセスは無効です。

AWS Managed Microsoft AD ユーザーまたはグループを既存の IAM ロールに割り当てるには

1. [AWS Directory Service コンソール](#) のナビゲーションペインの [Active Directory] で、[Directories] を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - a. [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを開きます。
 - b. [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、割り当てを行うリージョンを選択した上で、[Application management] (アプリケーション管理) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
4. [AWS Management Console] セクションまで下にスクロールして、[アクション] と [有効にする] を選択します。
5. [コンソールアクセスの委任] セクションで、ユーザーに割り当てる既存の IAM ロールの IAM ロール名を選択します。
6. [Selected role] (選択されたロール) ページの [Manage users and groups for this role] (このロールのユーザーとグループの管理) で、[Add] (追加) をクリックします。
7. [Add users and groups to role] (ロールへのユーザーとグループの追加) ページの [Select Active Directory Forest] (Active Directory フォレストの選択) で、AWS Managed Microsoft AD フォレスト (このフォレスト) またはオンプレミスフォレスト (信頼されたフォレスト) の内、AWS Management Console へのアクセスが必要なアカウントが含まれている方を選択します。信頼されたフォレストの設定方法の詳細については、「[チュートリアル: AWS Managed Microsoft AD と自己管理型 Active Directory ドメイン間で信頼関係を作成する](#)」を参照してください。
8. [Specify which users or groups to add (追加するユーザーまたはグループを指定)] で、[Find by user (ユーザーで検索)] または [Find by group (グループで検索)] のいずれかを選択し、ユーザーまたはグループの名前を入力します。可能性のある結果のリストから、追加するユーザーまたはグループを選択します。

9. [Add] (追加) をクリックして、ユーザーとグループのロールへの割り当てを完了します。

ロールに割り当てられたユーザーとグループの表示

IAM ロールに割り当てられた AWS Managed Microsoft AD ユーザーとグループを表示するには、次の手順を実行します。

前提条件

- [AWS Managed Microsoft AD を作成します](#)。
- 「[IAM ユーザーを作成する](#)」または「[IAM グループを作成する](#)」。
- 信頼関係を持つ[ロールを作成します](#) AWS Directory Service。既存の IAM ロールの場合、「[既存のロールの信頼関係を編集](#)」する必要があります。
- [既存の IAM ロールにユーザーまたはグループを割り当てる](#)。

IAM ロールに割り当てられた AWS Managed Microsoft AD ユーザーとグループを表示するには

1. 「[AWS Directory Service コンソール](#)」のナビゲーションペインで、[Active Directory] の下の [ディレクトリ] を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - a. [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、割り当てを表示するリージョンを選択した上で、[Application management] (アプリケーション管理) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - b. [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを開きます。
4. [AWS Management Console] セクションまで下にスクロールします。[ステータス] は [有効] にする必要があります。そうでない場合は、[アクション] で [有効にする] を選択します。詳細については、「[AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化](#)」を参照してください。

 Note

AWS Management Console が無効になっている場合、グループやユーザーは表示されません。

5. [コンソールアクセスの委任] セクションで表示したい IAM ロールのハイパーリンクを選択します。または、[IAM でポリシーを表示] を選択して、IAM コンソールで IAM ポリシーを表示できます。
6. [選択されたロール] ページの [このロールのユーザーとグループの管理] セクションで、対象の IAM ロールに割り当てられたユーザーとグループを確認できます。

IAM ロールからユーザーまたはグループを削除する

Managed AWS Microsoft AD ユーザーまたはグループを IAM ロールから削除するには、次の手順を実行します。

ユーザーまたはグループから IAM ロールを削除するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - a. [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、割り当てを削除するリージョンを選択した上で、[Application management] (アプリケーション管理) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - b. [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Application management] (アプリケーション管理) タブを開きます。
4. AWS Management Console セクションで、ユーザーとグループを削除したい IAM ロールを選択する。
5. [Selected role] (選択されたロール) ページの [Manage users and groups for this role] (このロールのユーザーとグループの管理) で、ロールを削除するユーザーまたはグループを選択し、[Remove] (削除) を選択します。このロールは指定されたユーザーおよびグループから削除されますが、アカウントからは削除されません。

 Note

ロールを削除する場合は、「[ロールまたはインスタンスプロファイルの削除](#)」を参照してください。

での AWS マネージドポリシーの使用 AWS Directory Service

AWS Directory Service では、Amazon EC2 コンソールへのアクセスなど、AWS のサービスとリソースへのアクセス権をユーザーとグループに付与するために、以下の AWS 管理ポリシーが用意されています。これらのポリシーを確認するには、AWS Management Console にログインする必要があります。

- [読み取り専用アクセス](#)
- [パワーユーザーアクセス](#)
- [AWS Directory Service フルアクセス](#)
- [AWS Directory Service 読み取り専用アクセス](#)
- [AWS Directory Service Data へのフルアクセス](#)
- [AWS Directory Service Data の読み取り専用アクセス](#)
- [Amazon Cloud Directory フルアクセス](#)
- [Amazon Cloud Directory 読み取り専用アクセス](#)
- [Amazon EC2 フルアクセス](#)
- [Amazon EC2 読み取り専用アクセス](#)
- [Amazon VPC フルアクセス](#)
- [Amazon VPC 読み取り専用アクセス](#)
- [Amazon RDS フルアクセス](#)
- [Amazon RDS 読み取り専用アクセス](#)
- [Amazon DynamoDB フルアクセス](#)
- [Amazon DynamoDB 読み取り専用アクセス](#)
- [Amazon S3 フルアクセス](#)
- [Amazon S3 読み取り専用アクセス](#)
- [AWS CloudTrail フルアクセス](#)

- [AWS CloudTrail 読み取り専用アクセス](#)
- [Amazon CloudWatch フルアクセス](#)
- [Amazon CloudWatch 読み取り専用アクセス](#)
- [Amazon CloudWatch Logs フルアクセス](#)
- [Amazon CloudWatch Logs 読み取り専用アクセス](#)

独自のポリシーを作成する方法の詳細については、IAM ユーザーガイドの[AWS 「リソースを管理するポリシーの例」](#)を参照してください。

AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する

マルチリージョンレプリケーションを使用すると、複数のリージョンにまたがって AWS Managed Microsoft AD ディレクトリデータを自動的にレプリケートできます AWS リージョン。このレプリケーションにより、地理的に離れた場所にあるユーザーやアプリケーションのパフォーマンスを向上させることができます。AWS マネージド Microsoft AD は、ネイティブ Active Directory レプリケーションを使用してディレクトリのデータを新しいリージョンに安全にレプリケートします。

マルチリージョンレプリケーションは、AWS Managed Microsoft AD の Enterprise Edition でのみサポートされています。

AWS Managed Microsoft AD が利用可能なほとんどのリージョンで、自動マルチリージョンレプリケーションを使用できます。

Important

マルチリージョンレプリケーションは、オプトインリージョンでは利用できません。オプトインリージョンは次のとおりです。

- アフリカ (ケープタウン) af-south-1
- アジアパシフィック (香港) ap-east-1
- アジアパシフィック (ハイデラバード) ap-south-2
- アジアパシフィック (ジャカルタ) ap-southeast-3
- アジアパシフィック (メルボルン) ap-southeast-4
- アジアパシフィック (タイ) ap-southeast-7

- カナダ西部 (カルガリー) ca-west-1
- 欧州 (ミラノ) eu-south-1
- 欧州 (スペイン) eu-south-2
- 欧州 (チューリッヒ) eu-central-2
- イスラエル (テルアビブ) il-central-1
- 中東 (バーレーン) me-south-1
- 中東 (UAE) me-central-1
- メキシコ (中部) mx-central-1

詳細については、「AWS アカウント管理 リファレンスガイド」の「[アカウントで使用できる AWS リージョン リージョンを指定する](#)」を参照してください。

マルチリージョンレプリケーションの仕組み

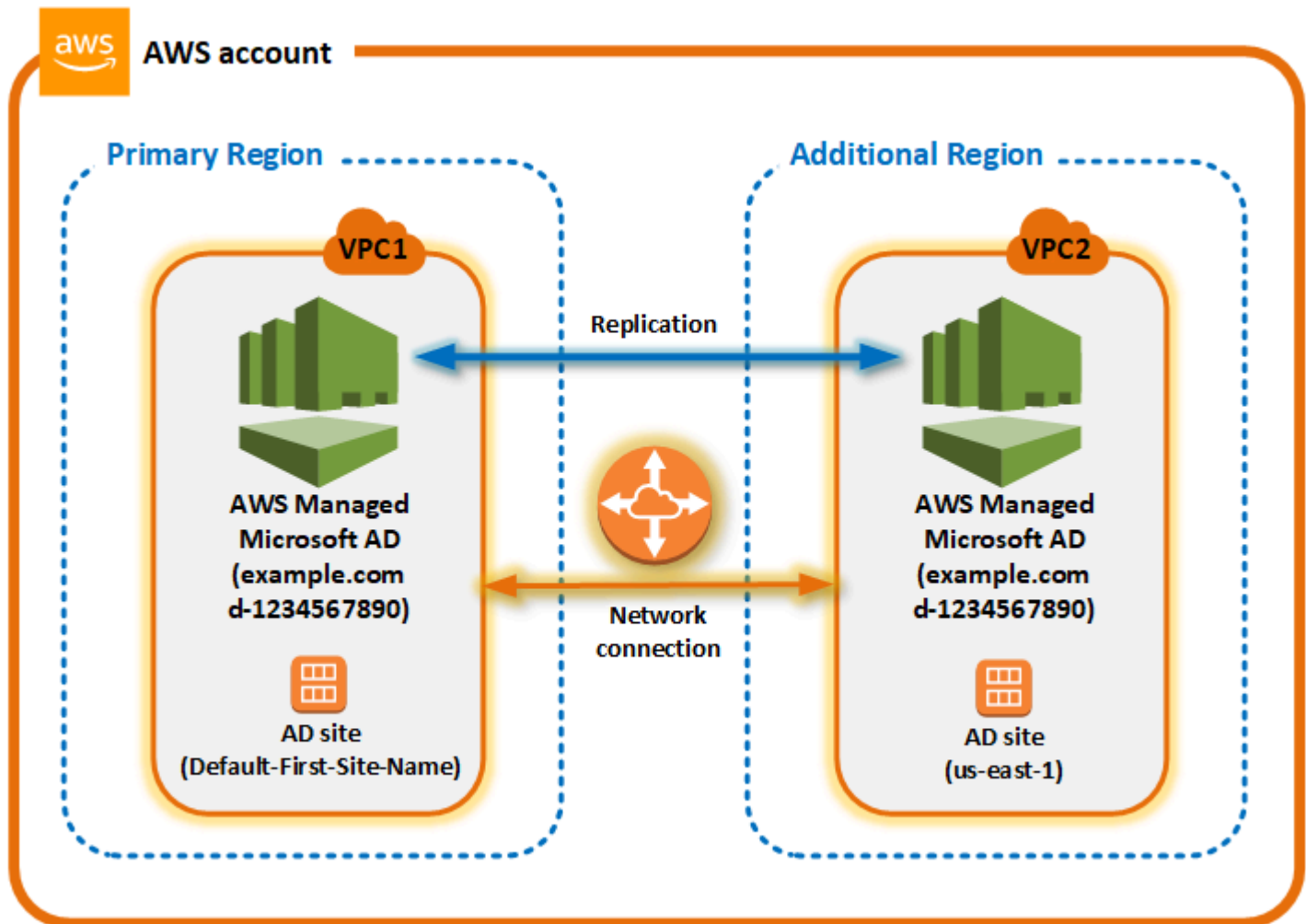
マルチリージョンレプリケーション機能を使用すると、AWS マネージド Microsoft AD はグローバル Active Directory インフラストラクチャの管理に伴う差別化されていない負担を排除します。設定すると、AWS ユーザー、グループ、グループポリシー、スキーマを含むすべてのカスタマーディレクトリデータが複数のリージョンにレプリケートされます AWS リージョン。

新しいリージョンが追加されると、図に示すように次の操作が自動的に実行されます。

- AWS Managed Microsoft AD は、選択した VPC に 2 つのドメインコントローラーを作成し、同じ AWS アカウントの新しいリージョンにデプロイします。ディレクトリ識別子 (directory_id) はすべてのリージョンで同じままです。必要に応じて、ドメインコントローラーを後から追加できます。
- AWS Managed Microsoft AD は、プライマリリージョンと新しいリージョン間のネットワーク接続を設定します。
- AWS Managed Microsoft AD は新しい Active Directory サイトを作成し、us-east-1 などのリージョンと同じ名前を付けます。この名前は、Active Directory サイトとサービスのツールを使用して後から変更することも可能です。
- AWS Managed Microsoft AD は、ユーザー、グループ、グループポリシー、Active Directory の信頼、組織単位、Active Directory スキーマなど、すべての Active Directory オブジェクトと設定を新しいリージョンにレプリケートします。Active Directory のサイトのリンクは、[変更通知](#)を使用するように設定されています。サイト間の変更通知を有効にすると、変更 (緊急のレプリケーション

を必要とする変更を含む) が、ソースサイト内で伝達される場合と同じ頻度でリモートサイトに伝達されます。

- 追加した最初のリージョンである場合、AWS マネージド Microsoft AD はすべての機能をマルチリージョン対応にします。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。



Active Directory サイト

マルチリージョンレプリケーションでは、複数の Active Directory サイト (リージョンごとに 1 つの Active Directory サイト) がサポートされます。新しいリージョンが追加されると、リージョンと同じ名前が付けられます (us-east-1 など)。この名前は、Active Directory サイトとサービスを使って後から変更することも可能です。

AWS サービス

AWS Amazon RDS for SQL Server や Amazon FSx などの サービスは、グローバルディレクトリのローカルインスタンスに接続します。これにより、ユーザーは、で実行される Active Directory対応アプリケーション AWS や、任意の AWS リージョンの Amazon RDS for SQL Server などの AWS サービスに一度サインインできます。そのためには、AWS Managed Microsoft AD と信頼Active Directoryしているユーザーが AWS Managed Microsoft AD またはオンプレミスの認証情報を必要とします。

マルチリージョンレプリケーション機能では、次の AWS サービスを使用できます。

- Amazon EC2
- Amazon FSx for Windows File Server
- SQL Server の Amazon Relational Database Service
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

フェイルオーバー

1 つのリージョン内のすべてのドメインコントローラーがダウンした場合、AWS マネージド Microsoft AD はドメインコントローラーを復元し、ディレクトリデータを自動的にレプリケートします。その間、他のリージョンのドメインコントローラーは稼働したままです。

マルチリージョンレプリケーションのメリット

AWS Managed Microsoft AD のマルチリージョンレプリケーションでは、Active Directory対応アプリケーションはディレクトリをローカルで使用するハイパフォーマンスを実現し、マルチリージョン機能を使用して回復性を実現します。マルチリージョンレプリケーションは、SharePoint や SQL Server Always On などの Active Directory対応アプリケーションだけでなく、Amazon RDS for SQL Server や FSx for Windows File Server などの AWS サービスでも使用できます。以下は、マルチリージョンレプリケーションのその他の利点です。

- これにより、単一の AWS Managed Microsoft AD インスタンスをグローバルにすばやくデプロイでき、グローバル Active Directory インフラストラクチャの自己管理の手間が省けます。
- これにより、Windows および Linux ワークロードを複数の AWS リージョンにデプロイして管理することが容易になり、コスト効率が向上します。自動マルチリージョンレプリケーションによって、グローバルな Active Directory 対応アプリケーションで最適なパフォーマンスを実現できます。Windows または Linux インスタンスにデプロイされたすべてのアプリケーションは、リージョンでローカルに AWS Managed Microsoft AD を使用します。これにより、可能な限り最も近いリージョンからのユーザーリクエストへの応答が可能になります。
- マルチリージョンの耐障害性が得られます。高可用性の AWS マネージドインフラストラクチャにデプロイされた AWS マネージド Microsoft AD は、すべてのリージョンで基盤となる Active Directory インフラストラクチャの自動ソフトウェア更新、モニタリング、復旧、セキュリティを処理します。ユーザーはアプリケーションの構築に専念できます。

トピック

- [グローバル機能とリージョン機能](#)
- [プライマリリージョンと追加のリージョン](#)
- [AWS Managed Microsoft AD のレプリケートされたリージョンの追加](#)
- [AWS Managed Microsoft AD のレプリケートされたリージョンの削除](#)

グローバル機能とリージョン機能

マルチ AWS リージョンレプリケーションを使用してリージョンをディレクトリに追加すると、AWS Directory Service はすべての機能の範囲を拡張し、リージョン対応になります。これらの機能は、AWS Directory Service コンソールでディレクトリの ID を選択したときに表示される、詳細ページのさまざまなタブに一覧表示されます。つまり、機能はすべて、コンソールの [Multi-Region replication] (マルチリージョンレプリケーション) のセクションで選択するリージョンに基づいて有効化され、設定され、管理されます。各リージョンで機能を変更すると、その変更はグローバルに、またはリージョンごとに適用されます。

マルチリージョンレプリケーションは、AWS Managed Microsoft AD の Enterprise Edition でのみサポートされています。

グローバル機能

[プライマリリージョン](#) が選択されている間にグローバル機能を変更すると、その変更はすべてのリージョンに適用されます。

グローバルに使用されている機能は、[Directory details] (ディレクトリの詳細) ページで、隣に [Applied to all replicated Regions] (レプリケートされたすべてのリージョンに適用) と表示されているので、それで識別できます。または、リストでプライマリリージョンではない別のリージョンを選択した場合は、グローバルに使用されている機能は、[Inherited from primary Region] (プライマリリージョンから継承済み) と表示されているので、それで識別できます。

リージョン機能

[追加のリージョン](#) で機能を変更すると、その変更はそのリージョンのみに適用されます。

リージョン機能は、[Directory details] (ディレクトリの詳細) ページで、隣に [Applied to all replicated Regions] (レプリケートされたすべてのリージョンに適用済み) または [Inherited from primary Region] (プライマリリージョンから継承済み) とは表示されないで、それで識別できます。

プライマリリージョンと追加のリージョン

マルチリージョンレプリケーションでは、AWS マネージド Microsoft AD は次の 2 種類のリージョンを使用して、ディレクトリ全体にグローバルまたはリージョンの機能を適用する方法を区別します。

プライマリリージョン

ディレクトリを初めて作成した最初のリージョンのことを、プライマリリージョンといいます。プライマリリージョンから実行できるのは、Active Directory の信頼の作成や AD スキーマの更新など、グローバルディレクトリレベルの操作のみです。

プライマリリージョンは、最初のリージョンとして [Multi-Region replication] (マルチリージョンレプリケーション) セクションで常にリストの一番上に表示され、最後に - Primary が付きます。例えば、米国東部 (バージニア北部) - Primary のようにです。

プライマリリージョンが選択されている間に [グローバル機能](#) を変更すると、その変更はすべてのリージョンに適用されます。

リージョンを追加できるのは、プライマリリージョンが選択されている間のみです。詳細については、「[AWS Managed Microsoft AD のレプリケートされたリージョンの追加](#)」を参照してください。

追加のリージョン

ディレクトリに追加したリージョンは、追加のリージョンといいます。

機能の中には、すべてのリージョンに対してグローバルに管理できるものもありますが、それ以外はリージョンごとに個別に管理されます。追加のリージョン (非プライマリリージョン) の機能を管理するには、まず、[Directory details] (ディレクトリの詳細) ページの [Multi-Region replication] (マルチリージョンレプリケーション) セクションにあるリストから、追加のリージョンを選択する必要があります。これで、機能の管理に進むことができます。

追加のリージョンが選択されている間に [リージョン機能](#) を変更すると、その変更はそのリージョンのみに適用されます。

AWS Managed Microsoft AD のレプリケートされたリージョンの追加

[AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#) 機能を使用してリージョンを追加すると、AWS マネージド Microsoft AD は、選択した AWS リージョンに Amazon Virtual Private Cloud (VPC) とサブネットの 2 つのドメインコントローラーを作成します。AWS マネージド Microsoft AD は、Windows ワークロードが新しいリージョンのディレクトリに接続できるようにする関連するセキュリティグループも作成します。また、ディレクトリが既にデプロイされている場合は、同じ AWS アカウントを使用してこれらのリソースを作成します。これを行うには、リージョンを選択し、VPC を指定し、新しいリージョンの設定を指定します。

マルチリージョンレプリケーションは、AWS Managed Microsoft AD の Enterprise Edition でのみサポートされています。

前提条件

新しいレプリケーションリージョンを追加する手順に進む前に、以下の前提条件タスクを確認しておくことをお勧めします。

- ディレクトリをレプリケートする新しいリージョンに必要な AWS Identity and Access Management (IAM) アクセス許可、Amazon VPC 設定、サブネット設定があることを確認します。
- 既存のオンプレミス Active Directory 認証情報を使用して Active Directory 対応ワークロードにアクセスして管理する場合は AWS、AWS Managed Microsoft AD とオンプレミス AD インフラストラクチャとの間に Active Directory 信頼を作成する必要があります。信頼の詳細については、「[AWS Managed Microsoft AD を既存の Active Directory インフラストラクチャに接続する](#)」を参照してください。
- オンプレミスの Active Directory 間に既存の信頼関係があり、レプリケートされたリージョンが追加される場合は、ディレクトリをレプリケートする新しいリージョンに、必要な Amazon VPC とサブネットのセットアップがあることを確認する必要があります。

AWS Managed Microsoft AD とオンプレミス AD インフラストラクチャの間に信頼関係を作成することもできます。これにより、既存のオンプレミス Active Directory 認証情報を使用して AD 対応ワークロードを管理できます。詳細については、「[AWS Managed Microsoft AD を既存の Active Directory インフラストラクチャに接続する](#)」を参照してください。

リージョンの追加

Managed AWS Microsoft AD ディレクトリにレプリケートされたリージョンを追加するには、次の手順に従います。

レプリケートされたリージョンを追加するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページの [Multi-Region replication] (マルチリージョンレプリケーション) で、リストから [Primary] (プライマリ) リージョンを選択し、[Add Region] (リージョンの追加) をクリックします。

Note

リージョンを追加できるのは、プライマリリージョンが選択されている間のみです。詳細については、「[プライマリリージョン](#)」を参照してください。

4. [Add Region] (リージョンの追加) ページの [Region] (リージョン) で、追加するリージョンをリストから選択します。
5. [VPC] で、このリージョンで使用する VPC を選択します。

Note

この VPC には、別のリージョンのこのディレクトリで使用されている VPC と重複する、Classless Inter-Domain Routing (CIDR) を含めることはできません。

6. [Subnets] (サブネット) で、このリージョンで使用するサブネットを選択します。
7. [Pricing] (料金) で情報を確認し、[Add] (追加) をクリックします。
8. AWS Managed Microsoft AD がドメインコントローラーのデプロイプロセスを完了すると、リージョンにアクティブステータスが表示されます。これで、必要に応じて、このリージョンを更新できるようになります。

次の手順

新しいリージョンを追加したら、以下に示す次に行う手順の実行を検討します。

- 必要に応じて、新しいリージョンに追加のドメインコントローラー (最大 20 まで) をデプロイします。新しいリージョンを追加するときのドメインコントローラーの数は、デフォルトで 2 です。これは、耐障害性と高可用性を確保するために最低限必要な数です。詳細については、「[AWS Management Consoleで追加のドメインコントローラーを追加または削除する](#)」を参照してください。

Note

AWS Managed Microsoft AD AWS リージョン にレプリケートされた を追加すると、デフォルトで 2 つのドメインコントローラーが作成されます。これは、耐障害性と高可用性に必要なドメインコントローラーの最小数です。

- ディレクトリをリージョンごとにより多くの AWS アカウントと共有します。ディレクトリの共有設定は、プライマリリージョンから自動的にレプリケートされません。詳細については、「[AWS Managed Microsoft AD を共有する](#)」を参照してください。

Note

ディレクトリの共有設定は、プライマリ AWS リージョンで自動的にレプリケートされません。

- ログ転送を有効にして、新しいリージョンから Amazon CloudWatch Logs を使用してディレクトリのセキュリティログを取得します。ログ転送を有効にするときは、ディレクトリをレプリケートした各リージョンでロググループ名を指定する必要があります。詳細については、「[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#)」を参照してください。

Note

ログ転送を有効にするときは、ディレクトリをレプリケートした各 AWS リージョン でロググループの名称を指定する必要があります。

- リージョンごとにディレクトリのヘルスステータスを追跡するために、新しいリージョンの Amazon Simple Notification Service (Amazon SNS) モニタリングを有効にします。詳細については、「[Amazon Simple Notification Service による AWS Managed Microsoft AD ディレクトリのステータス通知の有効化](#)」を参照してください。

AWS Managed Microsoft AD のレプリケートされたリージョンの削除

Managed AWS Microsoft AD ディレクトリのリージョンを削除するには、次の手順に従います。リージョンを削除する前に、それが次のいずれにも該当しないことを確認します。

- 認可されたアプリケーションがアタッチされている。
- 共有ディレクトリが関連付けられている。

レプリケートされたリージョンを削除するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. ナビゲーションバーで [リージョン] セレクターを選択し、ディレクトリが保存されているリージョンを選択します。
3. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
4. [Directory details] (ディレクトリの詳細) ページの [Multi-Region replication] (マルチリージョンレプリケーション) で、[Delete Region] (リージョンの削除) を選択します。
5. [Delete Region] (リージョンの削除) ダイアログボックスで、情報を確認し、リージョン名を入力して確定します。その後、[Delete] (削除) をクリックします。

Note

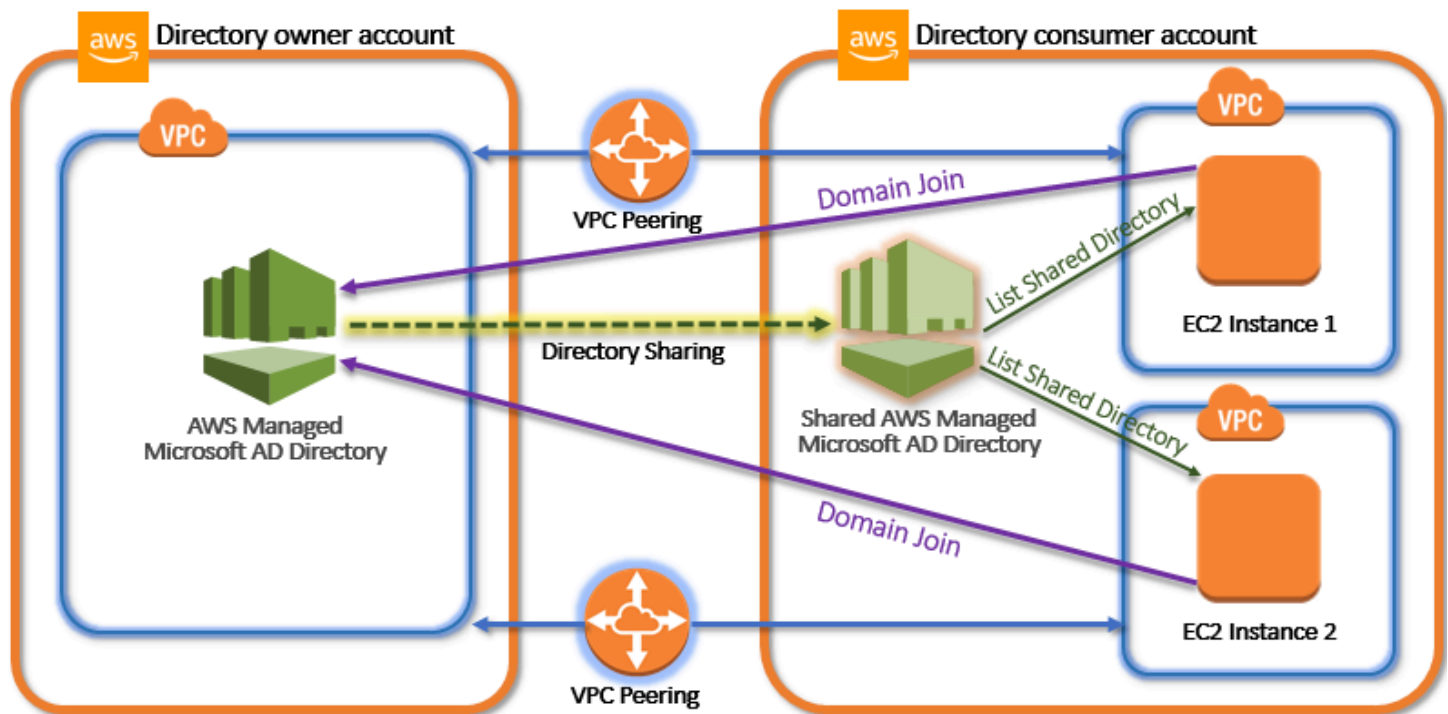
リージョンが削除されている間はリージョンを更新することはできません。

AWS Managed Microsoft AD を共有する

AWS Managed Microsoft AD は と緊密に統合 AWS Organizations され、複数の 間でシームレスなディレクトリ共有を可能にします AWS アカウント。1 つのディレクトリを同じ組織内で信頼 AWS アカウント AWS アカウント されている他のディレクトリと共有することも、組織外の他のディレクトリと共有することもできます。AWS アカウント が現在組織のメンバーでない場合にも、ディレクトリを共有できます。

主要なディレクトリ共有の概念

以下の主要な概念を理解すると、ディレクトリ共有機能をさらに活用できます。



ディレクトリ所有者アカウント

ディレクトリ所有者は、共有ディレクトリ関係で発信元ディレクトリを所有する AWS アカウント所有者です。このアカウントの管理者は、ディレクトリを共有する先を指定してディレクトリ AWS アカウント 共有ワークフローを開始します。ディレクトリの所有者は、AWS Directory Service コンソールの、特定のディレクトリの [Scale & Share] (スケーリングと共有) タブを使用して誰とディレクトリを共有したのかを確認することができます。

ディレクトリコンシューマーアカウント

共有したディレクトリ関係では、ディレクトリコンシューマーは、ディレクトリ所有者がディレクトリを共有した AWS アカウント を表します。使用する共有メソッドによって、このアカウントの管理者は、共有ディレクトリの使用を開始する前に、ディレクトリ所有者が送信する招待を受理する必要があります。

ディレクトリ共有プロセスでは、ディレクトリコンシューマーアカウント内に共有ディレクトリが作成されます。この共有ディレクトリには、EC2 インスタンスがシームレスにドメインを結合できるメタデータが含まれています。これは、ディレクトリ所有者アカウントの元のディレクトリにあります。ディレクトリコンシューマーアカウントの各共有ディレクトリには、一意の識別子 (共有ディレクトリ ID) があります。

共有メソッド

AWS Managed Microsoft AD には、次の 2 つのディレクトリ共有方法があります。

- AWS Organizations – このメソッドでは、ディレクトリコンシューマーアカウントを参照して検証できるため、組織内でのディレクトリの共有が容易になります。このオプションを組織で使用するには、[All features] (すべての機能) が有効であり、ユーザーのディレクトリが組織の管理アカウントにある必要があります。この共有メソッドではディレクトリコンシューマーアカウントがディレクトリの共有リクエストを受理する必要がないため、セットアップが簡素化されます。コンソールでは、このメソッドを組織 AWS アカウント 内でこのディレクトリをと共有と呼びます。
- ハンドシェイク – このメソッドでは、AWS Organizationsを使用していない場合でもディレクトリの共有が可能です。ハンドシェイクメソッドでは、ディレクトリコンシューマーアカウントがディレクトリの共有リクエストを受理することが必要となります。コンソールでは、このメソッドは [Share this directory with other AWS アカウント] (このディレクトリを他の AWS アカウントと共有) と表示されます。

ネットワーク接続

ネットワーク接続は、間でディレクトリ共有関係を使用するための前提条件です AWS アカウント。は、VPC を接続するための多くのソリューション AWS をサポートしています。これには、VPC [ピアリング](#)、[Transit Gateway](#)、[VPN](#) などがあります。VPCs 開始するには、「[チュートリアル: AWS Managed Microsoft AD ディレクトリを共有してシームレスな EC2 ドメイン結合を実現する](#)」を参照してください。

考慮事項

AWS Managed Microsoft AD でディレクトリ共有を使用する場合の考慮事項を次に示します。

料金

- AWS では、ディレクトリ共有に追加料金がかかります。共有 AWS Managed Microsoft AD AWS アカウント を使用している は、共有料金が請求されたアカウントです。詳細については、AWS Directory Service ウェブサイトの[料金](#)表ページを参照してください。
- ディレクトリ共有により、AWS Managed Microsoft AD は、複数のアカウントと VPC で Amazon EC2 と統合するコスト効率の高い方法になります。VPCs

利用可能なリージョン

- ディレクトリ共有は、[AWS Managed Microsoft AD が提供されているすべてのリージョン](#)で利用できます。
- AWS 中国 (寧夏) では、[AWS Systems Manager](#) (SSM) を使用して Amazon EC2 インスタンスをシームレスに結合する場合にのみこの機能を使用できます。

ディレクトリ共有の詳細と、AWS Managed Microsoft AD ディレクトリのアクセス範囲を AWS アカウントの境界を越えて拡張する方法については、以下のトピックを参照してください。

トピック

- [チュートリアル: AWS Managed Microsoft AD ディレクトリを共有してシームレスな EC2 ドメイン結合を実現する](#)
- [ディレクトリの共有解除](#)

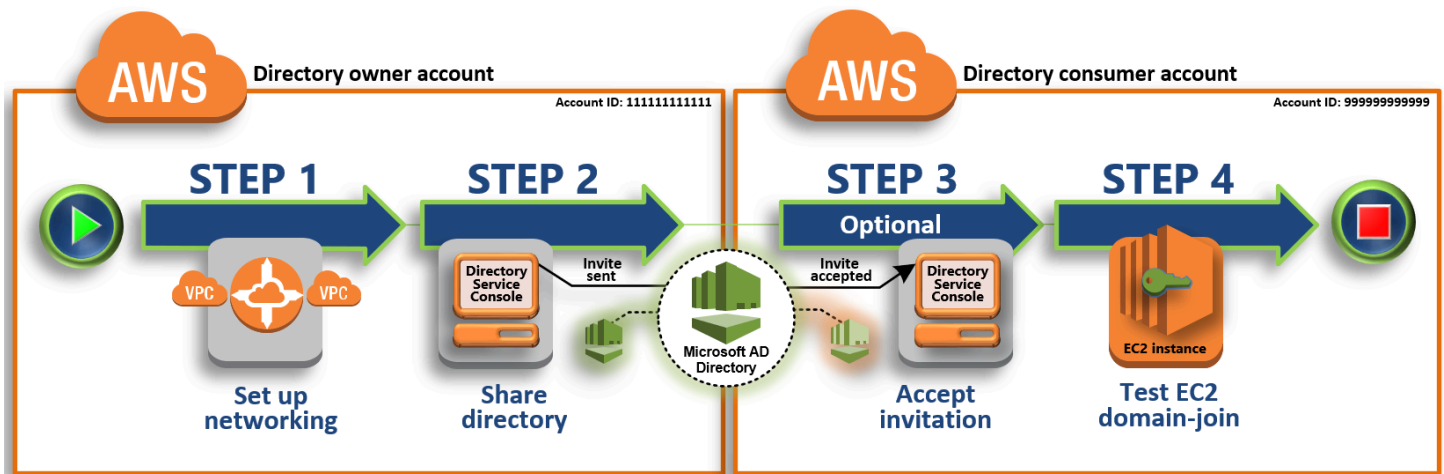
チュートリアル: AWS Managed Microsoft AD ディレクトリを共有してシームレスな EC2 ドメイン結合を実現する

このチュートリアルでは、AWS Managed Microsoft AD ディレクトリ (ディレクトリ所有者アカウント) を別の AWS アカウント (ディレクトリコンシューマーアカウント) と共有する方法を示します。ネットワークの前提条件が完了したら、2 つのディレクトリを共有します AWS アカウント。次に、ディレクトリのコンシューマーアカウントで EC2 インスタンスをドメインにシームレスに結合する方法を説明します。

このチュートリアルを開始する前にまず、ディレクトリ共有における主要な概念と、ユースケースの内容を確認しておくことをお勧めします。詳細については、「[主要なディレクトリ共有の概念](#)」を参照してください。

ディレクトリを共有するプロセスは、ディレクトリを同じ AWS 組織 AWS アカウント 内の別の と共有するか、AWS 組織外のアカウントと共有するかによって異なります。共有の仕組みについては、「[共有メソッド](#)」を参照してください。

このワークフローには 4 つの基本的な手順があります。



ステップ 1: ネットワーク環境をセットアップする

ディレクトリの所有者アカウントでは、ディレクトリの共有プロセスに必要なネットワークの前提条件のすべてを設定します。

ステップ 2: ディレクトリを共有する

ディレクトリ所有者の管理者認証情報でサインインしたら、AWS Directory Service コンソールを開き、ディレクトリのコンシューマーアカウントに招待を送信するために、ディレクトリ共有のワークフローを開始します。

ステップ 3: 共有ディレクトリの招待を受理する – (選択可能)

ディレクトリコンシューマー管理者の認証情報を使用してサインインしている間、AWS Directory Service コンソールを開き、ディレクトリ共有の招待を受け入れます。

ステップ 4: Windows Server 用の EC2 インスタンスとドメインとのシームレス結合をテストする

最後に、ディレクトリのコンシューマーの管理者として、EC2 インスタンスをドメインに結合し、これが動作することを確認します。

その他のリソース

- [ユースケース: Share your directory to seamlessly join Amazon EC2 instances to a domain across AWS アカウント](#)
- [AWS セキュリティブログ記事: 複数のアカウントと VPCs から単一の AWS Managed Microsoft AD ディレクトリに Amazon EC2 インスタンスを結合する方法](#)

ステップ 1: ネットワーク環境をセットアップする

AWS Managed Microsoft AD ディレクトリ (ディレクトリアカountの所有者) を別の (ディレクトリコンシューマーアカウント) AWS アカount と共有するには、Amazon VPC ピアリング接続を確立する必要があります。共有 AWS Managed Microsoft AD のネットワーク環境をセットアップする手順については、次の手順を参照してください。

前提条件

このチュートリアルの手順を開始する前に、まず次を完了してください。

- 同じリージョンでテスト AWS アカount 目的で 2 つの新しい を作成します。を作成すると AWS アカount、各アカountに専用の Virtual Private Cloud (VPC) が自動的に作成されます。各アカountの VPC ID を書き留めておきます。この情報は後で必要になります。
- [AWS Managed Microsoft AD を作成します](#)。
- VPC ピアリング接続を作成する場合、ディレクトリアカountの所有者とディレクトリコンシューマーアカウントの両方に、ピアリング接続を作成して受け入れるために必要なアクセス許可が必要です。詳細については、「[例: VPC ピアリング接続を作成する](#)」および「[例: VPC ピアリング接続を受け入れる](#)」を参照してください。

Note

ディレクトリ所有者とディレクトリコンシューマーのアカウントにある VPC を接続するためには多くの方法がありますが、このチュートリアルでは VPC ピアリング方式を使用します。その他の VPC 接続オプションについては、「[ネットワーク接続](#)」を参照してください。

ディレクトリの所有者アカウントとディレクトリのコンシューマーアカウント間の VPC ピアリング接続を設定する

作成する VPC ピアリング接続は、ディレクトリコンシューマーとディレクトリ所有者 VPCs。ここでの手順に従い、ディレクトリのコンシューマーアカウントと接続するための VPC ピアリング接続を設定します。この接続では、プライベート IP アドレスを使用して両方の VPC 間でトラフィックをルーティングできます。

ディレクトリの所有者アカウントとディレクトリのコンシューマーアカウント間に VPC ピアリング接続を作成するには

1. Amazon VPC コンソールの <https://console.aws.amazon.com/vpc/> を開いてください。必ず、VPC ピアリング接続を作成するために必要なアクセス許可を持つディレクトリ所有者アカウントの管理者認証情報を使用してユーザーとしてサインインします。詳細については「[前提条件](#)」を参照してください。
2. ナビゲーションペインで、[Peering Connections] (ピアリング接続) をクリックします。次に、[Create Peering Connection] (ピアリング接続の作成) をクリックします。
3. 以下の情報を設定します。
 - [Peering connection name tag] (ピアリング接続ネームタグ): ディレクトリのコンシューマーアカウントの VPC への接続を、明確に識別できるような名前を指定します。
 - [VPC (Requester)] (VPC (リクエスタ)): ディレクトリの所有者アカウントの VPC ID を選択します。
 - [Select another VPC to peer with] (ピア接続するもうひとつの VPC を選択) で、[My account] (マイアカウント) および [This region] (このリージョン) が選択されていることを確認します。
 - [VPC (Acceptor)] (VPC (アクセプタ)): ディレクトリのコンシューマーアカウントの VPC ID を選択します。
4. [Create Peering Connection] (ピアリング接続の作成) をクリックします。確認ダイアログボックスで [OK] をクリックします。

ディレクトリのコンシューマーアカウントに代わってピアリングリクエストを承諾するには

1. Amazon VPC コンソールの <https://console.aws.amazon.com/vpc/> を開いてください。ピアリングリクエストを受け入れるために必要なアクセス許可を持つユーザーとしてサインインします。詳細については「[前提条件](#)」を参照してください。
2. ナビゲーションペインで、[Peering Connections] (ピアリング接続) をクリックします。
3. 保留中の VPC ピアリング接続を選択します。(ステータスは「Pending Acceptance (承諾の保留中)」となっています)。
[Actions] (アクション)、[Accept Request] (リクエストの承諾) の順に選択します。
4. 確認ダイアログボックスで、[Yes, Accept] (はい、承諾します) を選択します。次の確認ダイアログボックスで、[Modify my route tables now] (ルートテーブルを今すぐ変更) を選択して、ルートテーブルページに直接移動します。

これで VPC ピアリング接続がアクティブ化されたので、ディレクトリの所有者アカウント内で、VPC のルートテーブルにエントリを追加する必要があります。これにより、ディレクトリのコンシューマーアカウントの VPC に、トラフィックを誘導することが可能になります。

ディレクトリの所有者アカウントで VPC のルートテーブルにエントリを追加するには

1. Amazon VPC コンソールの [Route Tables] (ルートテーブル) セクションで、ディレクトリ所有者 VPC のルートテーブルを選択します。
2. [Routes] (ルート) タブを開き、[Edit routes] (ルートの編集)、[Add route] (ルートの追加) の順に選択します。
3. [Destination] (送信先) 列で、ディレクトリのコンシューマー VPC のための CIDR ブロックを入力します。
4. [Target] (ターゲット) 列で、ディレクトリの所有者アカウントで前に作成した、VPC ピアリング接続用の接続 ID (**pcx-123456789abcde000** など) を入力します。
5. [Save changes] (変更の保存) をクリックします。

ディレクトリのコンシューマーアカウントで VPC のルートテーブルにエントリを追加するには

1. Amazon VPC コンソールの [Route Tables] (ルートテーブル) セクションで、ディレクトリコンシューマー VPC のルートテーブルを選択します。
2. [Routes] (ルート) タブを開き、[Edit routes] (ルートの編集)、[Add route] (ルートの追加) の順に選択します。
3. [Destination] (送信先) 列で、ディレクトリの所有者 VPC の CIDR ブロックを入力します。
4. [Target] (ターゲット) 列で、ディレクトリのコンシューマーアカウントで前に作成した、VPC ピアリング接続用の接続 ID (**pcx-123456789abcde001** など) を入力します。
5. [Save changes] (変更の保存) をクリックします。

ディレクトリのコンシューマー VPC のセキュリティグループの設定で、必ずアウトバウンドルートテーブルに Active Directory プロトコルとポートを追加して、アウトバウンドトラフィックを有効にします。詳細については、[VPC のセキュリティグループ](#) および [AWS Managed Microsoft AD prerequisites](#) を参照してください。

次のステップ

[ステップ 2: ディレクトリを共有する](#)

ステップ 2: ディレクトリを共有する

次の手順に従い、ディレクトリの所有者アカウント内からディレクトリ共有のワークフローを開始します。

Note

ディレクトリ共有は AWS Managed Microsoft AD のリージョン機能です。「[マルチリージョンレプリケーション](#)」を使用している場合、次の手順を各リージョンで個別に適用する必要があります。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

ディレクトリの所有者アカウントからディレクトリを共有するには

1. ディレクトリ所有者アカウントの管理者認証情報 AWS Management Console を使用して にサインインし、<https://console.aws.amazon.com/directoryservicev2/> で [AWS Directory Service コンソール](#)を開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. 共有する AWS Managed Microsoft AD ディレクトリのディレクトリ ID を選択します。
4. ディレクトリ詳細ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ディレクトリを共有するリージョンを選択した上で、[Scale & share] (スケール & 共有) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Scale & share] (スケールリングと共有) タブを選択します。
5. [Shared directories] (共有ディレクトリ) セクションで、[Actions] (アクション)、[Create new shared directory] (新しい共有ディレクトリの作成) の順に選択します。
6. 共有 AWS アカウント 先の選択ページで、ビジネスニーズに応じて次のいずれかの共有方法を選択します。
 - a. このディレクトリを組織 AWS アカウント 内で共有する – このオプションを使用すると、AWS 組織 AWS アカウント 内のすべての を示すリストから、ディレクトリ AWS アカウント を共有する を選択できます。ディレクトリを共有する AWS Directory Service 前に、との信頼されたアクセスを有効にする必要があります。詳細については、「[How to enable or](#)

[disable trusted access](#)」(信頼されたアクセスを有効または無効にする方法)を参照してください。

 Note

このオプションを組織で使用するには、[All features] (すべての機能) が有効であり、ユーザーのディレクトリが組織の管理アカウントにある必要があります。

- i. AWS アカウント 組織内 の、ディレクトリ AWS アカウント を共有する を選択し、追加 をクリックします。
 - ii. 料金の詳細を確認した上で、[Share] (共有) をクリックします。
 - iii. このガイドの[ステップ 4](#)に進みます。すべて同じ組織 AWS アカウント にあるため、ステップ 3 に従う必要はありません。
- b. このディレクトリを他の と共有 AWS アカウント - このオプションを使用すると、AWS 組織内外のアカウントとディレクトリを共有できます。このオプションは、ディレクトリが AWS 組織のメンバーではなく、別の と共有する場合にも使用できます AWS アカウント。
- i. [AWS アカウント ID] で、ディレクトリを共有するすべての AWS アカウント ID を入力し、[追加] をクリックします。
 - ii. [Send a note] (メモの送信) で、別の AWS アカウントの管理者へのメッセージを入力します。
 - iii. 料金の詳細を確認した上で、[Share] (共有) をクリックします。
 - iv. ステップ 3 に進みます。

次のステップ

[ステップ 3: 共有ディレクトリの招待を受理する – \(選択可能\)](#)

ステップ 3: 共有ディレクトリの招待を受理する – (選択可能)

前の手順でこのディレクトリを他の AWS アカウントと共有 (ハンドシェイクメソッド) オプションを選択した場合、この手順を使用して共有ディレクトリのワークフローを完了する必要があります。組織 AWS アカウント 内でこのディレクトリを と共有 オプションを選択した場合は、このステップをスキップしてステップ 4 に進みます。

共有ディレクトリの招待を受理するには

1. ディレクトリコンシューマーアカウントの管理者認証情報 AWS Management Console を使用して にサインインし、<https://console.aws.amazon.com/directoryservicev2/> で [AWS Directory Service コンソール](#)を開きます。
2. ナビゲーションペインで、[Directories shared with me] (自分と共有するディレクトリ) をクリックします。
3. [Shared directory ID] (共有ディレクトリ ID) 列で、[Pending acceptance] (承諾の保留中) 状態にあるディレクトリ ID を選択します。
4. [Shared directory details] (共有ディレクトリの詳細) ページで、[Review] (確認) をクリックします。
5. [Pending shared directory invitation] (保留中の共有ディレクトリの招待) ダイアログボックスで、記述、ディレクトリの所有者の詳細、および料金に関する情報を確認します。同意する場合には、[Accept] (承諾) をクリックしてディレクトリの使用を開始します。

次のステップ

[ステップ 4: Windows Server 用の EC2 インスタンスとドメインとのシームレス結合をテストする](#)

ステップ 4: Windows Server 用の EC2 インスタンスとドメインとのシームレス結合をテストする

次の 2 つのメソッドのいずれかを使用して、EC2 インスタンスをドメインにシームレスに結合するテストを行います。

方法 1: Amazon EC2 コンソールを使用してドメインの結合をテストする

これらの手順は、ディレクトリのコンシューマーアカウントで使います。

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
2. ナビゲーションバーで、既存のディレクトリ AWS リージョン と同じ を選択します。
3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Windows EC2 インスタンスに使用する名前を入力します。

5. (オプション) [補足タグを追加] で、タグとキーの値のペアを 1 つまたは複数追加して、この EC2 インスタンスのアクセスを整理、追跡、または制御します。
6. [アプリケーションと OS イメージ (Amazon マシンイメージ)] セクションの [クイックスタート] ペインで [Windows] を選択します。Windows Amazon マシンイメージ (AMI) は、[Amazon マシンイメージ (AMI)] ドロップダウンリストから変更できます。
7. [インスタンスタイプ] セクションで、[インスタンスタイプ] ドロップダウンリストから使用するインスタンスタイプを選択します。
8. キーペア (ログイン) セクションでは、[新しいキーペアを作成する](#) か、既存のキーペアを使用するか、キーペアなしで続行するかを選択できます。
9. [インスタンスを起動する] ページの [ネットワーク設定] セクションで、[編集] を選択します。[VPC に必須の] ドロップダウンリストから、ディレクトリが作成された [VPC] を選択します。
10. [サブネット] ドロップダウンリストから VPC 内のパブリックサブネットの 1 つを選択します。選択するサブネットで、すべての外部トラフィックがインターネットゲートウェイにルーティングされるように選択する必要があります。そうでない場合は、インスタンスにリモート接続できません。

インターネットゲートウェイへの接続方法の詳細については、Amazon VPC ユーザーガイドの「[インターネットゲートウェイを使用してサブネットをインターネットに接続する](#)」を参照してください。

11. [自動割り当てパブリック IP] で、[有効化] を選択します。

公開 IP アドレス指定とプライベート IP アドレス指定の詳細については、「Amazon EC2 インスタンスユーザーガイド」の「[Amazon EC2 インスタンスの IP アドレス指定](#)」を参照してください。

12. [ファイアウォール (セキュリティグループ)] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
13. [ストレージの設定] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
14. [高度な詳細] セクションを選択し、[ドメイン結合ディレクトリ] ドロップダウンリストからドメインを選択します。

 Note

ドメイン結合ディレクトリを選択すると、次のようになります:

 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. 

このエラーは、EC2 起動ウィザードが予期しないプロパティを持つ既存の SSM ドキュメントを識別した場合に発生します。次のいずれかを試すことができます。

- 以前に SSM ドキュメントを編集し、プロパティの存在が予想される場合は、[閉じる] を選択して EC2 インスタンスを変更せずに起動します。
- ここで既存の SSM ドキュメントを削除するリンクを選択して、SSM ドキュメントを削除します。これにより、正しいプロパティを使用する SSM ドキュメントを作成できます。EC2 インスタンスを起動すると、SSM ドキュメントが自動的に作成されます。

15. [IAM インスタンスプロファイル] には既存の IAM インスタンスプロファイルを選択するか、新しいプロファイルを作成できます。管理 AWS ポリシー AmazonSSMManagedInstanceCore と AmazonSSMDirectoryServiceAccess がアタッチされている IAM インスタンスプロファイルを IAM インスタンスプロファイルドロップダウンリストから選択します。新しい IAM プロファイルリンクを作成するには、[新しい IAM プロファイルを作成する] リンクを選択し、以下を実行します。

1. [ロールの作成] を選択してください。
2. [Select trusted entity] (信頼されたエンティティを選択) で、[AWS サービス] を選択します。
3. [ユースケース] で、[EC2] を選択してください。
4. ポリシーのリスト内の [アクセス許可を追加する] の下で、AmazonSSMManagedInstanceCore ポリシーと AmazonSSMDirectoryServiceAccess ポリシーを選択します。リストを絞り込むため、検索ボックスに **SSM** と入力します。[次へ] を選択します。

 Note

AmazonSSMDirectoryServiceAccess は、によって Active Directory 管理される にインスタンスを結合するアクセス許可を提供します AWS Directory Service。AmazonSSMManagedInstanceCore は、AWS Systems Manager サービスを使用するために必要な最小限のアクセス許可を提供します。これらのアクセス許

可を使用してロールを作成する方法、および IAM ロールに割り当てることができるその他のアクセス許可とポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。

5. [名前、確認、作成] ページで、[ロール名] を入力します。EC2 インスタンスにアタッチするには、このロール名が必要です。
 6. (オプション) IAM インスタンスプロファイルの説明を [説明] フィールドに入力できます。
 7. [ロールの作成] を選択してください。
 8. [インスタンスを起動する] ページに戻り、[IAM インスタンスプロファイル] の横にある更新アイコンを選択します。新しい IAM インスタンスプロファイルが [IAM インスタンスプロファイル] ドロップダウンリストに表示されるはずです。新しいプロファイルを選択し、残りの設定はデフォルト値のままにします。
16. [インスタンスを起動] を選択します。

方法 2: AWS Systems Managerを使用してドメインの結合をテストする

これらの手順は、ディレクトリのコンシューマーアカウントで使われます。この手順を完了するには、ディレクトリ ID、ディレクトリ名、DNS IP アドレスなど、ディレクトリ所有者のアカウントに関するいくつかの情報が必要となります。

前提条件

- セットアップ AWS Systems Manager。
 - Systems Manager の詳細については、「[AWS Systems Managerの一般的なセットアップ](#)」を参照してください。
- AWS Managed Microsoft Active Directory ドメインに参加するインスタンスには、AmazonSSMManagedInstanceCore と AmazonSSMDirectoryServiceAccess 管理ポリシーを含む IAM ロールがアタッチされている必要があります。
- これらのマネージドポリシーと、Systems Manager の IAM インスタンスプロファイルにアタッチできるその他のポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。管理ポリシーの詳細については、「IAM ユーザーガイド」の「[AWS 管理ポリシー](#)」を参照してください。

Systems Manager を使用して EC2 インスタンスを AWS Managed Microsoft Active Directory ドメインに結合する方法の詳細については、「[を使用して実行中の EC2 Windows インスタンス AWS Systems Manager を Directory Service ドメインに結合するにはどうすればよいですか？ AWS](#)」を参照してください。

1. で AWS Systems Manager コンソールを開きます <https://console.aws.amazon.com/systems-manager/>。
2. ナビゲーションペインの [Node Management] (ノード管理) で、[Run Command] (コマンドを実行) を選択します。
3. [Run command] (コマンドの実行) を選択します。
4. [Run a command] (コマンドの実行) ページで、AWS-JoinDirectoryServiceDomain を検索します。検索結果に表示されたら、AWS-JoinDirectoryServiceDomain オプションを選択します。
5. 下部にある [Command parameters] (コマンドのパラメータ) セクションまでスクロールします。以下のパラメーターを指定する必要があります。

 Note

ディレクトリ ID、ディレクトリ名、DNS IP アドレスを見つけるには、AWS Directory Service コンソールに戻り、共有されているディレクトリを選択し、ディレクトリを選択します。[ディレクトリ ID] は [共有ディレクトリの詳細] セクションにあります。[ディレクトリ名] と [DNS IP アドレス] の値は、[所有者ディレクトリの詳細] セクションにあります。

- [ディレクトリ ID] に AWS Managed Microsoft Active Directory の名前を入力します。
 - [ディレクトリ名] に AWS Managed Microsoft Active Directory の名前を入力します (ディレクトリ所有者アカウント用)。
 - DNS IP アドレスの場合は、AWS Managed Microsoft Active Directory (ディレクトリ所有者アカウント用) に DNS サーバーの IP アドレスを入力します。
6. [ターゲット] で [インスタンスを手動で選択する] を選択し、ドメインに参加させたいインスタンスを選択します。
 7. フォームの残りの設定はデフォルト値のままにしておき、ページを下方方向にスクロールして [Run] (実行) をクリックします。

8. インスタンスがドメインに正常に参加すると、コマンドステータスは [保留中] から [成功] に変わります。ドメインに参加したインスタンスの [インスタンス ID] と [出力を表示] を選択すると、コマンド出力を表示できます。

前述の手順のいずれかを完了すると、EC2 インスタンスをドメインに結合できるようになります。これを行うと、AWS Managed Microsoft AD ユーザーアカウントの認証情報を使用してリモートデスクトッププロトコル (RDP) クライアントを使用してインスタンスにログインできます。

ディレクトリの共有解除

AWS Managed Microsoft AD ディレクトリの共有を解除するには、次の手順に従います。

ディレクトリの共有を解除するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインの [Active Directory] で、[Directories] (ディレクトリ) を選択します。
2. 共有を解除する AWS Managed Microsoft AD ディレクトリのディレクトリ ID を選択します。
3. ディレクトリ詳細ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、ディレクトリの共有を解除するリージョンを選択し、[Scale & share] (スケーリングと共有) タブを選択します。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Scale & share] (スケーリングと共有) タブを選択します。
4. [Shared directories] (共有ディレクトリ) セクションで、共有を解除する共有ディレクトリを選択し、[Actions] (アクション) を選択後、[Unshare] (共有解除) を選択します。
5. [Unshare directory] (ディレクトリの共有解除) ダイアログボックスで、[Unshare] (共有解除) を選択します。

追加リソース

- [ユースケース: ディレクトリを共有して、Amazon EC2 インスタンスを AWS アカウント間でドメインにシームレスに結合する](#)
- [AWS セキュリティブログ記事: How to join Amazon EC2 instances from multiple accounts and VPCs to a single AWS Managed Microsoft AD directory](#)

- [「Joining your Amazon RDS DB instances across accounts to a single shared domain」](#) (アカウントをまたがった Amazon RDS DB インスタンスを単一の共有ドメインに結合する)

Active Directory ユーザーの AWS Managed Microsoft AD への移行

Active Directory Migration Toolkit (ADMT) と Password Export Service (PES) を使用して、セルフマネージド型から AWS Managed Microsoft AD ディレクトリ Active Directory にユーザーを移行できます。これにより、ユーザーの Active Directory オブジェクトと暗号化パスワードを簡単に移行できます。

詳細な手順については、AWS セキュリティブログの [「ADMT を使用してオンプレミスドメインを AWS Managed Microsoft AD に移行する方法」](#) を参照してください。

AWS Managed Microsoft AD を既存の Active Directory インフラストラクチャに接続する

このセクションでは、AWS Managed Microsoft AD と既存の Active Directory インフラストラクチャ間の信頼関係を設定する方法について説明します。

AWS Managed Microsoft AD を既存の に接続するタスク Active Directory :

- [AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)
- [AWS Managed Microsoft AD でパブリック IP アドレスを使用する場合の IP ルートの追加](#)
- [チュートリアル: AWS Managed Microsoft AD と自己管理型 Active Directory ドメイン間で信頼関係を作成する](#)
- [チュートリアル: 2 つの AWS Managed Microsoft AD ドメイン間に信頼関係を作成する](#)

AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成

AWS Directory Service for Microsoft Active Directory とセルフマネージド (オンプレミス) ディレクトリ間、および AWS クラウド内の複数の AWS Managed Microsoft AD ディレクトリ間で、1 方向と双方向の外部信頼関係とフォレスト信頼関係を設定できます。AWS マネージド Microsoft AD は、受信、送信、双方向 (双方向) の 3 つの信頼関係のすべての方向をサポートしています。

信頼関係の詳細については、[AWS 「Managed Microsoft AD との信頼について知っておくべきこと」](#) を参照してください。

Note

信頼関係を設定するときは、セルフマネージドディレクトリが AWS Directory Service と互換性があり、引き続き互換性があることを確認する必要があります。お客様の責任の詳細については、「[責任共有モデル](#)」を参照してください。

AWS Managed Microsoft AD は、外部信頼とフォレスト信頼の両方をサポートしています。フォレスト信頼の作成方法を示すシナリオの例については、「[チュートリアル: AWS Managed Microsoft AD と自己管理型 Active Directory ドメイン間で信頼関係を作成する](#)」を参照してください。

Amazon Chime、Amazon Connect、QuickSight、WorkDocs AWS IAM Identity Center、Amazon WorkMail、Amazon WorkSpaces、などの AWS エンタープライズアプリには双方向の信頼が必要です AWS Management Console。AWS マネージド Microsoft AD は、セルフマネージド のユーザーとグループをクエリできる必要があります Active Directory。

選択認証を有効にすると、AWS アプリケーション固有のサービスアカウントのみがセルフマネージド をクエリできます Active Directory。詳細については、[AWS 「Managed Microsoft AD との AWS アプリ統合のセキュリティを強化する」](#)を参照してください。

Amazon EC2、Amazon RDS、および Amazon FSx は、一方向または双方向のいずれかの信頼で動作します。

前提条件

信頼の作成は数ステップのみで完了しますが、信頼を設定する前に、いくつかの前提条件の手順を完了しておく必要があります。

Note

AWS Managed Microsoft AD は、[単一ラベルドメイン](#)との信頼をサポートしていません。

VPC に接続する

自己管理型ディレクトリとの信頼関係を作成する際には、まず、自己管理型ネットワークを AWS Managed Microsoft AD を含む Amazon VPC に接続しておく必要があります。セルフマネージドおよび AWS Managed Microsoft AD ネットワークのファイアウォールでは、Microsoft ドキュメントの[Windows Server 2008 以降のバージョン](#)に記載されているネットワークポートが開いている必要があります。

Amazon WorkDocs や Amazon QuickSight などの AWS アプリケーションで認証に完全なドメイン名の代わりに NetBIOS 名を使用するには、ポート 9389 を許可する必要があります。Active Directory ポートとプロトコルの詳細については、Microsoft ドキュメントの「[Windows のサービス概要およびネットワークポート要件](#)」を参照してください。

これらは、ディレクトリに接続するために必要な最小限のポートです。固有の設定によっては、追加ポートが開かれていることが必要です。

VPC の設定

AWS Managed Microsoft AD を含む VPC には、適切なアウトバウンドルールとインバウンドルールが必要です。

VPC のアウトバウンドルールを設定するには

1. [AWS Directory Service コンソール](#)のディレクトリの詳細ページで、AWS Managed Microsoft AD ディレクトリ ID を書き留めます。
2. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
3. [Security Groups] (セキュリティグループ) をクリックします。
4. AWS Managed Microsoft AD ディレクトリ ID を検索します。検索結果で、「ディレクトリ ID ディレクトリコントローラー用にAWS 作成されたセキュリティグループ」という説明の項目を選択します。

Note

選択したセキュリティグループは、最初にディレクトリを作成する際に自動的に作成されるセキュリティグループです。

5. そのセキュリティグループの [Outbound Rules] (アウトバウンドルール) タブを開きます。[Edit] (編集)、[Add another rule] (別のルールの追加) の順に選択します。新しいルールに、次の値を入力します。

- [Type] (タイプ): All Traffic
- [Protocol] (プロトコル): All
- [Destination] (送信先) は、ドメインコントローラーから発信されるトラフィックと、(自己管理型ネットワーク内にある) そのトラフィックの送信先を指定します。単一の IP アドレスまたは IP アドレス範囲を CIDR 表記で指定します (例: 203.0.113.5/32)。同じリージョン内にある別のセキュリティグループの、名前または ID を指定することもできます。詳細について

は、「[ディレクトリ AWS のセキュリティグループの設定と使用を理解する](#)」を参照してください。

6. [Save] (保存) をクリックします。

Kerberos 事前認証を有効にする

お客様のユーザーは、アカウント内で Kerberos 事前認証を有効にしておく必要があります。この設定の詳細については、Microsoft TechNet の「[Microsoft](#)」(事前認証) を参照してください。

自己管理型ドメインで DNS 条件付きフォワーダーを設定する

自己管理型ドメインでは、DNS 条件付きフォワーダーを設定する必要があります。条件付きフォワーダーの詳細については、Microsoft TechNet の「[Assign a Conditional Forwarder for a Domain Name](#)」(ドメイン名の条件フォワーダーの割り当て) を参照してください。

以下の手順を実行するには、以下の自己管理型ドメイン用 Windows Server ツールに対するアクセス権限が必要です。

- AD DS ツールと AD LDS ツール
- DNS

自己管理型ドメインで DNS の条件付きフォワーダーを設定するには

1. まず、AWS Managed Microsoft AD に関する情報を取得する必要があります。AWS Management Console にサインインして [AWS Directory Service コンソール](#)を開きます。
2. ナビゲーションペインで [Directories] (ディレクトリ) をクリックします。
3. AWS Managed Microsoft AD のディレクトリ ID を選択します。
4. 完全修飾ドメイン名 (FQDN) とディレクトリの DNS アドレスを書き留めます。
5. 次に、自己管理型ドメインコントローラーに戻ります。サーバーマネージャーを開きます。
6. [Tools] (ツール) メニューで、[DNS] を選択します。
7. 信頼関係を設定するドメインの DNS サーバーを、コンソールのツリーから展開します。
8. コンソールのツリー内で、[Conditional Forwarders] (条件付きフォワーダー) を選択します。
9. [Action] (アクション) メニューから、[New conditional forwarder] (新規の条件付きフォワーダー) を選択します。
10. DNS ドメインで、前述の AWS Managed Microsoft AD の完全修飾ドメイン名 (FQDN) を入力します。

11. プライマリサーバーの IP アドレスを選択し、前述の AWS Managed Microsoft AD ディレクトリの DNS アドレスを入力します。

DNS アドレスの入力後に、「timeout」または「unable」というエラーが表示される場合があります。通常、このエラーは無視できます。
12. [Store this conditional forwarder in Active Directory and replicate as follows: All DNS servers in this domain] (この条件付きフォワーダーを Active Directory 内に保存し次のようにレプリケートします: このドメインのすべての DNS サーバー) を選択します。[OK] をクリックします。

信頼関係のパスワード

既存のドメインとの間の信頼関係を作成している場合は、Windows Server 管理ツールを使用して、そのドメインに対する信頼関係を設定します。その際に、使用する信頼のパスワードを書き留めます。AWS Managed Microsoft AD で信頼関係を設定するときは、同じパスワードを使用する必要があります。詳細については、Microsoft TechNet の「[Managing Trusts](#)」(信頼の管理) を参照してください。

これで、AWS Managed Microsoft AD で信頼関係を作成する準備が整いました。

NetBIOS とドメイン名

信頼関係を確立するには、NetBIOS とドメインの名前は異なる一意のものである必要があります。

信頼関係を作成、検証、または削除する

Note

信頼関係は AWS Managed Microsoft AD のグローバル機能です。[AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#) を使用している場合、[プライマリリージョン](#) で次の手順を実行する必要があります。変更した内容は、レプリケートされたすべてのリージョンで自動的に適用されます。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

AWS Managed Microsoft AD との信頼関係を作成するには

1. [AWS Directory Service コンソール](#)を開きます。
2. ディレクトリページで、AWS Managed Microsoft AD ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。

- [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、[Actions] (アクション)、[Add trust relationship] (信頼関係の追加) の順に選択します。
 5. [Add a trust relationship] (信頼関係の追加) ページで、信頼タイプ、信頼されたドメインの完全修飾ドメイン名 (FQDN)、信頼パスワード、信頼の方向など、必要な情報を入力します。
 6. (オプション) Managed AWS Microsoft AD ディレクトリ内のリソースへのアクセスを許可されたユーザーのみに許可する場合は、オプションで Selective authentication チェックボックスを選択できます。選択的な認証に関する全般的な情報については、Microsoft TechNet の「[Security Considerations for Trusts](#)」(信頼のセキュリティ上の考慮事項) を参照してください。
 7. [Conditional forwarder] (条件付きフォワーダー) に、自己管理型 DNS サーバーの IP アドレスを入力します。すでに条件付きフォワーダを作成済みな場合は、DNS IP アドレスではなく、自己管理型ドメインの FQDN を入力できます。
 8. (オプション) [Add another IP address] (別の IP アドレスの追加) をクリックした後、追加する自己管理型 DNS サーバーの IP アドレスを入力します。このステップは、適用可能な DNS サーバーアドレスごとに、合計 4 つのアドレスまで繰り返すことができます。
 9. [Add] (追加) を選択します。
 10. 自己管理型ドメインの DNS サーバーまたはネットワークで、パブリックな (RFC 1918 を除く) IP アドレススペースを使用している場合は、[IP routing] (IP ルーティング) セクションで、[Actions] (アクション)、[Add route] (ルートの追加) の順に選択します。CIDR 形式 (例: 203.0.113.0/24) を使用して、DNS サーバーまたは自己管理型ネットワークの IP アドレスブロックを入力します。このステップは、DNS サーバーと自己管理型ネットワークの両方で、RFC 1918 IP アドレススペースを使用している場合は必要ありません。

 Note

パブリック IP アドレススペースを使用している場合、[AWS の IP アドレス範囲](#)を指定しないようにしてください。これらの範囲は使用できません。

11. (オプション) [Add routes] (ルートの追加) ページを表示している際は、同時に [Add routes to the security group for this directory's VPC] (このディレクトリの VPC のセキュリティグループに

ルートを追加します) も選択することを推奨します。これにより、上記の「VPC を設定する」に記述したセキュリティグループが設定されます。これらのセキュリティルールは、パブリックに公開されていない内部ネットワークインターフェイスに影響します。このオプションを使用できない場合は、セキュリティグループをすでにカスタマイズしていることを示すメッセージが表示されます。

信頼関係は、双方のドメインで設定する必要があります。この関係は、補完的であることが必要です。例えば、片側のドメインで送信の信頼を作成した場合は、もう一方のドメインでは受信の信頼を作成します。

既存のドメインとの間の信頼関係を作成している場合は、Windows Server 管理ツールを使用して、そのドメインに対する信頼関係を設定します。

AWS Managed Microsoft AD とさまざまな Active Directory ドメインの間に複数の信頼を作成できます。ただし、各ペアが一度に保持できる信頼関係は 1 つのみです。たとえば、「受信方向」に既存の一方方向の信頼があり、「送信方向」に別の信頼関係を設定する場合は、既存の信頼関係を削除し、新しい「双方向」の信頼を作成する必要があります。

送信の信頼関係を確認するには

1. [AWS Directory Service コンソール](#)を開きます。
2. ディレクトリページで、AWS Managed Microsoft AD ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで検証する信頼を選択した後、[Actions] (アクション)、[Verify trust relationship] (信頼関係の検証) の順に選択します。

このプロセスでは、双方向信頼の送信方向のみを検証します。AWS は受信信頼の検証をサポートしていません。自己管理型 Active Directory との間で信頼関係を確認する方法の詳細については、Microsoft TechNet の「[Verify a Trust](#)」(信頼を検証する) を参照してください。

既存の信頼関係を削除するには

1. [AWS Directory Service コンソール](#)を開きます。
2. ディレクトリページで、AWS Managed Microsoft AD ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、削除する信頼を選択した上で、[Actions] (アクション)、[Delete trust relationship] (信頼関係の削除) の順に選択します。
5. [Delete] (削除) をクリックします。

AWS Managed Microsoft AD でパブリック IP アドレスを使用する場合の IP ルートの追加

AWS Directory Service for Microsoft Active Directory を使用すると、他のディレクトリとの信頼を確立するなど、多くの強力なActive Directory機能を活用できます。ただし、他のディレクトリのネットワークの DNS サーバーでパブリック (RFC 1918 ではない) IP アドレスを使用している場合は、信頼の設定の一部として、その IP アドレスを指定する必要があります。この手順については、「[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)」を参照してください。

同様に、VPC がパブリック IP 範囲を使用している場合、上の AWS Managed Microsoft AD からピア AWS VPC AWS にトラフィックをルーティングするときにも IP アドレス情報を入力する必要があります。

「[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)」に説明があるように、IP アドレスの追加時に [Add routes to the security group for this directory's VPC] (このディレクトリの VPC のセキュリティグループにルートを追加する) オプションを選択できます。このオプションは選択する必要があります。ただし、以下に示すように、必要なトラフィックを許可するように[セキュリティグループ](#)をカスタマイズ済みである場合は除きます。詳細については、「[ディレクトリ AWS のセキュリティグループの設定と使用を理解する](#)」を参照してください。

チュートリアル: AWS Managed Microsoft AD と自己管理型 Active Directory ドメイン間で信頼関係を作成する

このチュートリアルでは、AWS Directory Service for Microsoft Active Directory とセルフマネージド (オンプレミス) Microsoft 間の信頼関係を設定するために必要なすべての手順について説明します Active Directory。数ステップで信頼関係を作成できますが、その前に以下の手順を完了させる必要があります。

トピック

- [前提条件](#)
- [ステップ 1: 自己管理型 AD ドメインを準備する](#)
- [ステップ 2: AWS Managed Microsoft AD を準備する](#)
- [ステップ 3: 信頼関係を作成する](#)

以下の資料も参照してください。

[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)

前提条件

このチュートリアルでは、以下をすでに使用していることを前提とします。

Note

AWS Managed Microsoft AD は、[単一ラベルドメイン](#)との信頼をサポートしていません。

- で作成された AWS Managed Microsoft AD ディレクトリ AWS。この手順に関するサポートが必要な場合は、「[AWS Managed Microsoft AD の開始方法](#)」を参照してください。
- 実行中の EC2 インスタンスが AWS Managed Microsoft AD に追加Windowsされました。この手順に関するサポートが必要な場合は、「[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)」を参照してください。

Important

AWS Managed Microsoft AD の管理者アカウントには、このインスタンスへの管理アクセス権が必要です。

- 以下の Windows Server ツールが、対象のインスタンスにインストールされています:
 - AD DS ツールと AD LDS ツール
 - DNS

この手順に関するサポートが必要な場合は、「[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#)」を参照してください。

- 自己管理型 (オンプレミスオンプレミス) の Microsoft Active Directory

このディレクトリに対する管理アクセス権限が必要です。また、前述と同じ Windows Server ツールも、このディレクトリでの使用が可能な状態にする必要があります。

- セルフマネージドネットワークと AWS Managed Microsoft AD を含む VPC 間のアクティブな接続。この手順に関するサポートが必要な場合は、「[Amazon Virtual Private Cloud Connectivity Options](#)」(Amazon Virtual Private Cloud での接続性オプション) を参照してください。
- ローカルセキュリティポリシーが正しく設定されていること。Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously をチェックして、少なくとも次の 3 つの名前が付けられたパイプが含まれていることを確認します。
 - netlogon
 - samr
 - lsarpc
- 信頼関係を確立するには、NetBIOS とドメインの名前は異なる一意のものである必要があります。

信頼関係を作成するための前提条件の詳細については、「[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)」を参照してください。

チュートリアルの設定

このチュートリアルでは、AWS Managed Microsoft AD とセルフマネージドドメインをすでに作成しています。セルフマネージドネットワークは AWS Managed Microsoft AD の VPC に接続されています。2 つのディレクトリのプロパティを以下に示します。

AWS で実行されている Managed Microsoft AD AWS

- ドメイン名 (FQDN): MyManagedAD.example.com
- NetBIOS 名: MyManagedAD

- DNS アドレス: 10.0.10.246、10.0.20.121
- VPC CIDR: 10.0.0.0/16

AWS Managed Microsoft AD は VPC ID: vpc-12345678 にあります。

セルフマネージドまたは AWS Managed Microsoft AD ドメイン

- ドメイン名 (FQDN): corp.example.com
- NetBIOS 名: CORP
- DNS アドレス: 172.16.10.153
- 自己管理型 CIDR: 172.16.0.0/16

次のステップ

[ステップ 1: 自己管理型 AD ドメインを準備する](#)

ステップ 1: 自己管理型 AD ドメインを準備する

まず、自己管理型 (オンプレミス) ドメインで、前提条件のための手順をいくつか完了する必要があります。

自己管理型ファイアウォールを設定する

Managed AWS Microsoft AD を含む VPC で使用されるすべてのサブネットの CIDRs に対して次のポートが開かれるように、セルフマネージドファイアウォールを設定する必要があります。このチュートリアルでは、次のポートで 10.0.0.0/16 (AWS Managed Microsoft AD の VPC の CIDR ブロック) からの送受信トラフィックの両方を許可します。

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 認証
- TCP/UDP 389 - Lightweight Directory Access Protocol (LDAP)
- TCP 445 – サーバーメッセージブロック (SMB)
- TCP 9389 - Active Directory Web Services (ADWS) (オプション - Amazon WorkDocs や Amazon QuickSight などの AWS アプリケーションでの認証に完全なドメイン名の代わりに NetBIOS 名を使用する場合は、このポートを開く必要があります)。

 Note

SMBv1 のサポートは終了しました。

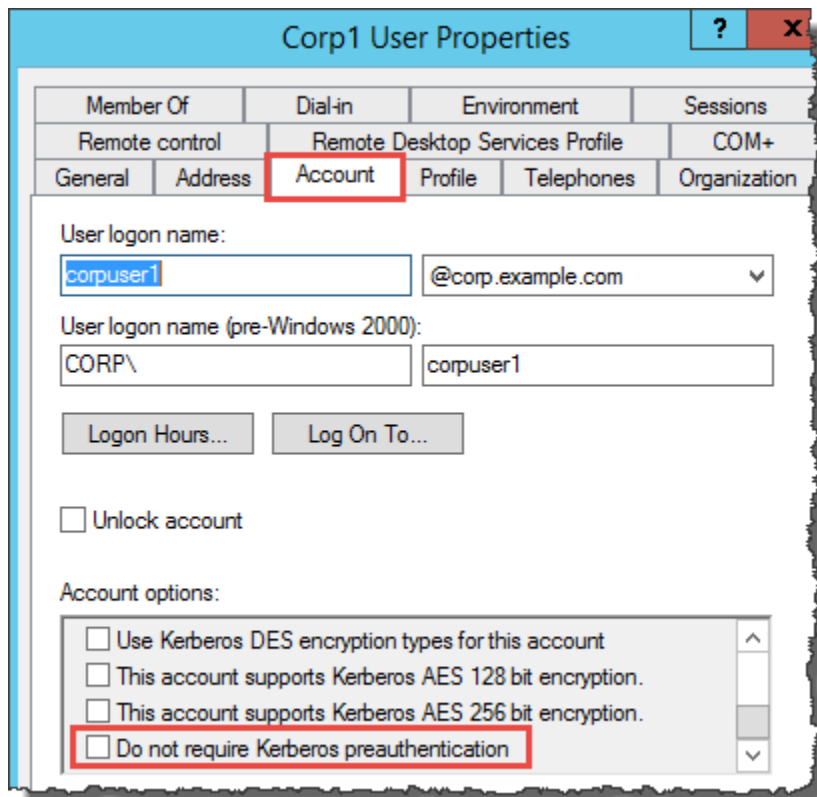
これらは、VPC を自己管理型のディレクトリに接続するために最低限必要となるポートです。固有の設定によっては、追加ポートが開かれていることが必要です。

Kerberos の事前認証が有効化されていることを確認する

Kerberos の事前認証は、両方のディレクトリのユーザアカウントで有効にする必要があります。これはデフォルト設定ですが、いずれかのユーザーのプロパティをチェックして、何も変更されていないことを確認します。

ユーザーの Kerberos 設定を表示するには

1. 自己管理型ドメインコントローラーで、サーバーマネージャーを開きます。
2. [Tools] (ツール) メニューで、[Active Directory Users and Computers] (Active Directory ユーザーとコンピュータ) を選択します。
3. [Users] フォルダを選択し、右クリックによりコンテキストメニューを開きます。右側のペインに表示されるユーザーアカウントを無作為に選択します。[Properties] (プロパティ) をクリックします。
4. [Account] (アカウント) タブを開きます。[Account options] (アカウントオプション) リストで下にスクロールし、[Do not require Kerberos preauthentication] (Kerberos 事前認証を要求しない) がオンになっていないことを確認します。



自己管理型ドメインのための DNS 条件付きフォワーダーを設定する

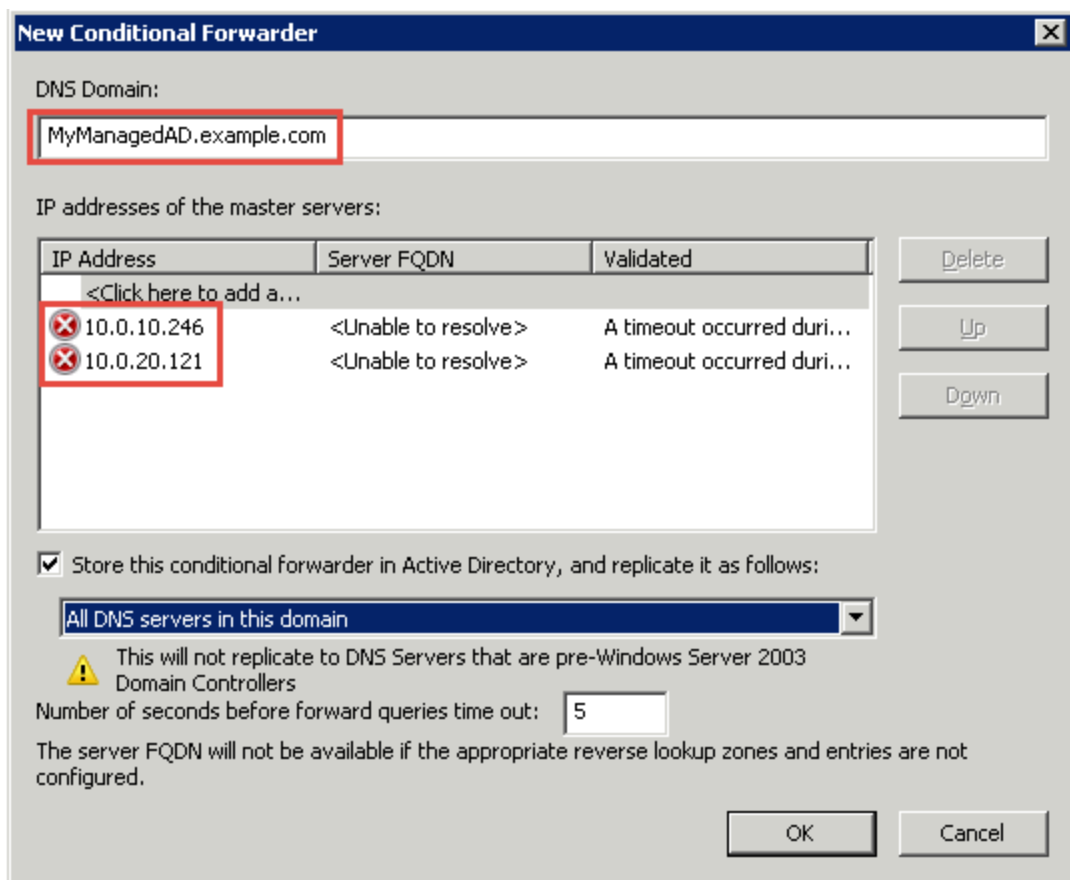
DNS の条件付きフォワーダーは、各ドメインで設定する必要があります。セルフマネージドドメインでこれを行う前に、まず AWS Managed Microsoft AD に関する情報を取得します。

自己管理型ドメインで DNS の条件付きフォワーダーを設定するには

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. ナビゲーションペインで [Directories] (ディレクトリ) をクリックします。
3. AWS Managed Microsoft AD のディレクトリ ID を選択します。
4. [Details] (詳細) ページで、ディレクトリの [Directory name] (ディレクトリ名) と [DNS address] (DNS アドレス) の値をメモします。
5. 次に、自己管理型ドメインコントローラーに戻ります。サーバーマネージャーを開きます。
6. [Tools] (ツール) メニューで、[DNS] を選択します。
7. 信頼関係を設定するドメインの DNS サーバーを、コンソールのツリーから展開します。ここで使用するサーバーは、WWIN-5V70CN7VJ0.corp.example.com です。
8. コンソールのツリー内で、[Conditional Forwarders] (条件付きフォワーダー) を選択します。

9. [Action] (アクション) メニューから、[New conditional forwarder] (新規の条件付きフォワーダー) を選択します。
10. DNS ドメインで、前にメモした AWS Managed Microsoft AD の完全修飾ドメイン名 (FQDN) を入力します。この例では、FQDN は MyManagedAD.example.com です。
11. プライマリサーバーの IP アドレスを選択し、前に書き留めた AWS Managed Microsoft AD ディレクトリの DNS アドレスを入力します。この例では、これらの DNS アドレスは 10.0.10.246 と、10.0.20.121 です。

DNS アドレスの入力後に、「timeout」または「unable」というエラーが表示される場合があります。通常、このエラーは無視できます。



12. [Store this conditional forwarder in Active Directory, and replicate it as follows] (この条件付きフォワーダーを Active Directory に保存し次に従いレプリケートします) をクリックします。
13. [All DNS servers in this domain] (このドメイン内のすべての DNS サーバー)、[OK] の順に選択します。

次のステップ

[ステップ 2: AWS Managed Microsoft AD を準備する](#)

ステップ 2: AWS Managed Microsoft AD を準備する

次に、AWS Managed Microsoft AD を信頼関係の準備を整えます。以下の手順の多くは、自己管理型ドメインで行ったものとほぼ同じです。ただし、今回は AWS Managed Microsoft AD を使用します。

VPC サブネットとセキュリティグループを設定する

セルフマネージドネットワークから AWS Managed Microsoft AD を含む VPC へのトラフィックを許可する必要があります。これを行うには、AWS Managed Microsoft AD のデプロイに使用されるサブネットに関連付けられた ACLs とドメインコントローラーに設定されたセキュリティグループルールの両方が、信頼をサポートするために必要なトラフィックを許可していることを確認する必要があります。

ポート要件は、ドメインコントローラーが使用する Windows Server のバージョン、および、信頼を利用するサービスやアプリケーションの種類によって変化します。このチュートリアルでは、次のポートを開く必要があります。

インバウンド

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 認証
- UDP 123 – NTP
- TCP 135 – RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 – SMB
- TCP/UDP 464 – Kerberos 認証
- TCP 636 – LDAPS (TLS/SSL 経由の LDAP)
- TCP 3268-3269 – グローバルカタログ
- TCP/UDP 49152-65535 – RPC 用のエフェメラルポート

Note

SMBv1 のサポートは終了しました。

アウトバウンド

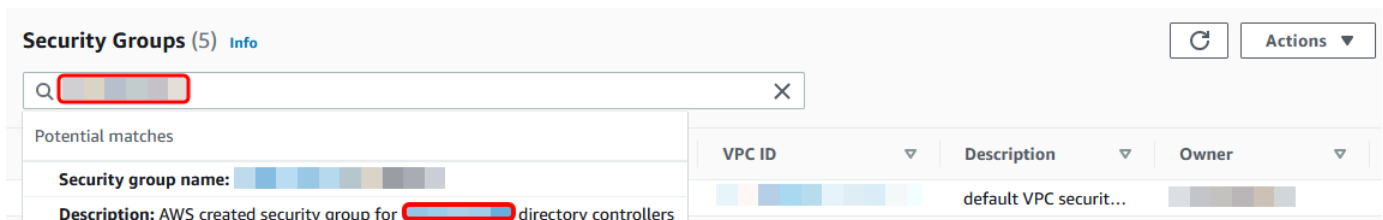
- すべて

Note

これらは、VPC と自己管理型ディレクトリを接続するために最低限と必要なるポートです。固有の設定によっては、追加ポートが開かれていることが必要です。

AWS Managed Microsoft AD ドメインコントローラーのアウトバウンドルールとインバウンドルールを設定するには

1. [AWS Directory Service コンソール](#) に戻ります。ディレクトリのリストで、AWS Managed Microsoft AD ディレクトリのディレクトリ ID を書き留めます。
2. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
3. ナビゲーションペインで、[Security Groups] を選択します。
4. 検索ボックスを使用して Managed Microsoft AD ディレクトリ ID AWS を検索します。検索結果で、**AWS created security group for *yourdirectoryID* directory controllers** セキュリティグループの説明に該当する項目を選択します。



5. 対象のセキュリティグループの [Outbound Rules] (アウトバウンドルール) タブを開きます。[Edit outbound rules]、[Add rule] の順に選択します。新しいルールに、次の値を入力します。
 - [Type] (タイプ): ALL Traffic
 - [Protocol] (プロトコル): ALL
 - [Destination] (送信先) では、ドメインコントローラーから発信されるトラフィックと、その送信先を指定します。単一の IP アドレスまたは IP アドレス範囲を CIDR 表記で指定します (例: 203.0.113.5/32)。同じリージョン内にある別のセキュリティグループの、名前または ID を指定することもできます。詳細については、「[ディレクトリ AWS のセキュリティグループの設定と使用を理解する](#)」を参照してください。
6. [Save Rule] をクリックします。

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

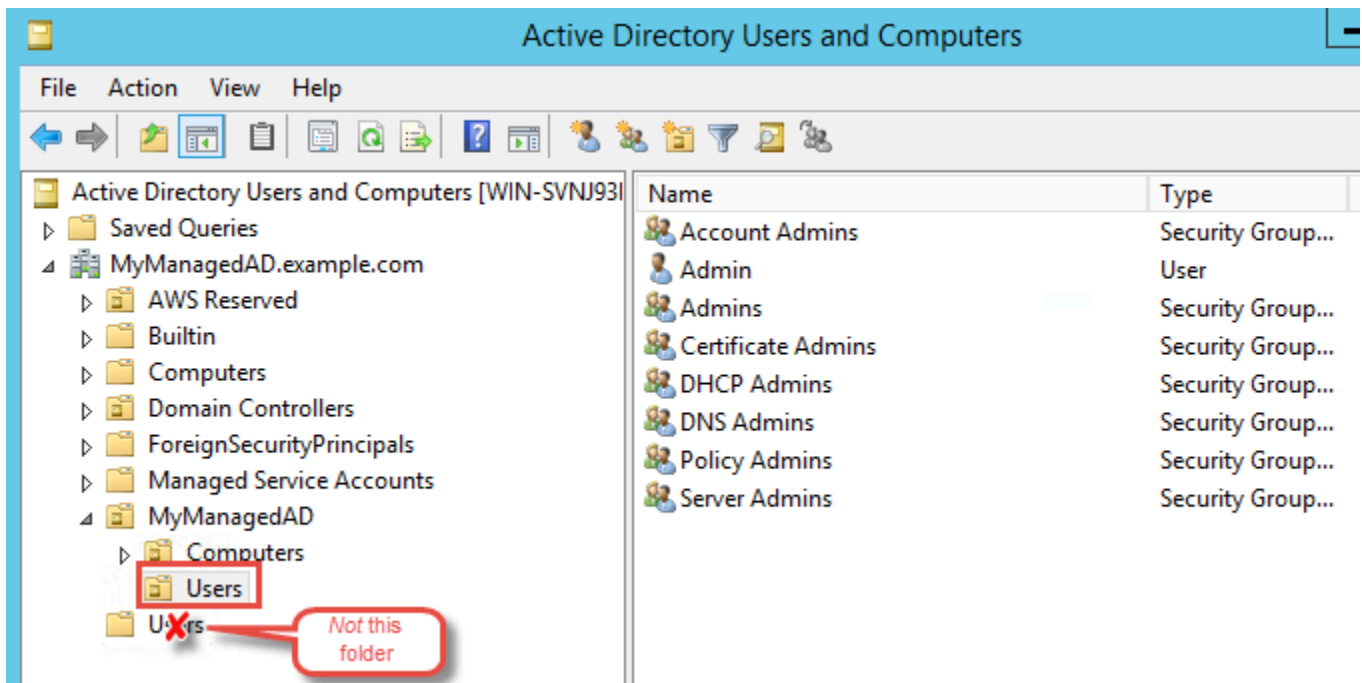
Cancel Preview changes Save rules

Kerberos の事前認証が有効化されていることを確認する

次に、AWS Managed Microsoft AD のユーザーでも Kerberos 事前認証が有効になっていることを確認します。これは、自己管理型ディレクトリで実施したものと同一プロセスです。これはデフォルト設定ですが、何も変更されていないことを確認します。

ユーザーの Kerberos 設定を表示するには

1. ドメインの または [AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#) ドメイン内のユーザーを管理するアクセス許可が委任されたアカウントを使用して、AWS Managed Microsoft AD ディレクトリのメンバーであるインスタンスにログインします。
2. まだインストールされていない場合は、Active Directory ユーザーと、コンピュータツール、および DNS ツールをインストールします。これらのツールをインストールする方法については、「[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#)」を参照してください。
3. サーバーマネージャーを開きます。[Tools] (ツール) メニューで、[Active Directory Users and Computers] (Active Directory ユーザーとコンピュータ) を選択します。
4. 使用しているドメイン内の、[Users] フォルダを選択します。これは、NetBIOS 名を使用する [Users] フォルダであり、完全修飾ドメイン名 (FQDN) の [Users] フォルダではないことに注意してください。



5. ユーザーのリストで、ユーザーを右クリックし、[Properties] (プロパティ) を選択します。
6. [Account] (アカウント) タブを開きます。[Account options] (アカウントオプション) リストで、[Do not require Kerberos preauthentication] (Kerberos 事前認証は不要) がオンになっていないことを確認します。

次のステップ

ステップ 3: 信頼関係を作成する

ステップ 3: 信頼関係を作成する

ここまでで準備作業が完了しました。最後の手順では、信頼関係を作成していきます。最初にセルフマネージドドメインに信頼を作成し、最後に AWS Managed Microsoft AD に信頼を作成します。信頼関係の作成処理中に問題が発生した場合は、「[信頼作成ステータスの理由](#)」のガイドを参照してください。

自己管理型 Active Directory で信頼を設定する

このチュートリアルでは、双方向フォレストの信頼を設定します。ただし、一方向フォレストの信頼を作成する場合、各ドメインの信頼には、それぞれ補完的な方向を持たせる必要があることにご注意ください。例えば、セルフマネージドドメインで一方向の送信信頼を作成する場合は、AWS Managed Microsoft AD で一方向の送信信頼を作成する必要があります。

 Note

AWS Managed Microsoft AD は、外部信頼もサポートしています。ただし、このチュートリアルは、双方向フォレストの信頼を作成することを目的とします。

自己管理型 Active Directory で信頼を設定するには

1. サーバーマネージャーを開き、[Tools] (ツール) メニューから、[Active Directory Domains and Trusts] (Active Directory のドメインと信頼) を選択します。
2. ドメインのコンテキスト (右クリック) メニューを開き、[Properties] (プロパティ) を選択します。
3. [Trusts] (信頼) タブを開き、[New trust] (新規の信頼) をクリックします。AWS Managed Microsoft AD の名前を入力し、次へを選択します。
4. [Forest trust] (フォレストの信頼) を選択します。[Next] (次へ) をクリックします。
5. [Two-way] を選択します。[Next] (次へ) をクリックします。
6. [This domain only] (このドメインのみ) を選択します。[Next] (次へ) をクリックします。
7. [Forest-wide authentication] (フォレスト全体の認証) を選択します。[Next] (次へ) をクリックします。
8. [Trust password] (信頼のパスワード) にパスワードを入力します。AWS Managed Microsoft AD の信頼を設定するときに必要になるため、このパスワードを覚えておいてください。
9. 次のダイアログボックスで設定を確認した上で、[Next] (次へ) をクリックします。信頼が正常に作成されたことを確認し、[Next] (次へ) を再度クリックします。
10. [No, do not confirm the outgoing trust] (いいえ、送信の信頼を確認しません) を選択します。[Next] (次へ) をクリックします。
11. [No, do not confirm the incoming trust] (いいえ、受信の信頼の確認は行いません) を選択します。[Next] (次へ) を選択します。

AWS Managed Microsoft AD ディレクトリで信頼を設定する

最後に、AWS Managed Microsoft AD ディレクトリとのフォレストの信頼関係を設定します。セルフマネージドドメインに双方向のフォレスト信頼を作成しているため、AWS Managed Microsoft AD ディレクトリを使用して双方向の信頼も作成します。

Note

信頼関係は AWS Managed Microsoft AD のグローバル機能です。[AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#) を使用している場合、[プライマリリージョン](#) で次の手順を実行する必要があります。変更した内容は、レプリケートされたすべてのリージョンで自動的に適用されます。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

AWS Managed Microsoft AD ディレクトリで信頼を設定するには

1. [AWS Directory Service コンソール](#) に戻ります。
2. ディレクトリページで、AWS Managed Microsoft AD ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、[Actions] (アクション)、[Add trust relationship] (信頼関係の追加) の順に選択します。
5. [Add a trust relationship] (信頼関係の追加) ページで、信頼のタイプを指定します。この例では、[Forest trust] (フォレストの信頼) を選択します。自己管理型ドメインの FQDN を入力します (このチュートリアルでは **corp.example.com**)。自己管理型ドメインで信頼を作成した際に使用したものと同一、信頼パスワードを入力します。方向を指定します。この例では、[Two-way] (双方向) を選択します。
6. [Conditional forwarder] (条件付きフォワーダー) フィールドに、自己管理型 DNS サーバーの IP アドレスを入力します。この例では、172.16.10.153 と入力します。
7. (オプション) [Add another IP address] (別の IP アドレスの追加) を選択し、自己管理型 DNS サーバーの 2 番目の IP アドレスを入力します。指定できる DNS サーバー数は最大で合計 4 台です。
8. [Add] (追加) を選択します。

おつかれ様でした。これで、セルフマネージドドメイン (corp.example.com) と AWS Managed Microsoft AD (MyManagedAD.example.com). これらの 2 つのドメイン間に設定できるのは、1 つの信頼関係だけです。例えば、設定を一方向の信頼に変更する場合は、まず既存の信頼関係を削除した上で、新しい信頼関係を作成する必要があります。

信頼の確認や削除に関する手順を含む詳細については、「[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)」を参照してください。

チュートリアル: 2 つの AWS Managed Microsoft AD ドメイン間に信頼関係を作成する

このチュートリアルでは、2 つの AWS Directory Service for Microsoft Active Directory ドメイン間の信頼関係を設定するために必要なすべての手順について説明します。

トピック

- [ステップ 1: AWS Managed Microsoft AD を準備する](#)
- [ステップ 2: 別の AWS Managed Microsoft AD ドメインとの信頼関係を作成する](#)

以下の資料も参照してください。

[AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)

ステップ 1: AWS Managed Microsoft AD を準備する

このセクションでは、AWS Managed Microsoft AD を別の AWS Managed Microsoft AD との信頼関係に備えます。以下のステップの多くは、[チュートリアル: AWS Managed Microsoft AD と自己管理型 Active Directory ドメイン間で信頼関係を作成する](#) で実行したものとほぼ同じです。ただし、今回は、相互に連携するように AWS Managed Microsoft AD 環境を設定します。

VPC サブネットとセキュリティグループを設定する

1 つの AWS Managed Microsoft AD ネットワークから、他の AWS Managed Microsoft AD を含む VPC へのトラフィックを許可する必要があります。これを行うには、AWS Managed Microsoft AD のデプロイに使用されるサブネットに関連付けられた ACLs とドメインコントローラーに設定されたセキュリティグループルールの両方が、信頼をサポートするために必要なトラフィックを許可していることを確認する必要があります。

ポート要件は、ドメインコントローラーが使用する Windows Server のバージョン、および、信頼を利用するサービスやアプリケーションの種類によって変化します。このチュートリアルでは、次のポートを開く必要があります。

インバウンド

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 認証
- UDP 123 – NTP
- TCP 135 – RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 – SMB

Note

SMBv1 のサポートは終了しました。

- TCP/UDP 464 – Kerberos 認証
- TCP 636 – LDAPS (TLS/SSL 経由の LDAP)
- TCP 3268-3269 – グローバルカタログ
- TCP/UDP 1024-65535 – RPC 用のエフェメラルポート

アウトバウンド

- すべて

Note

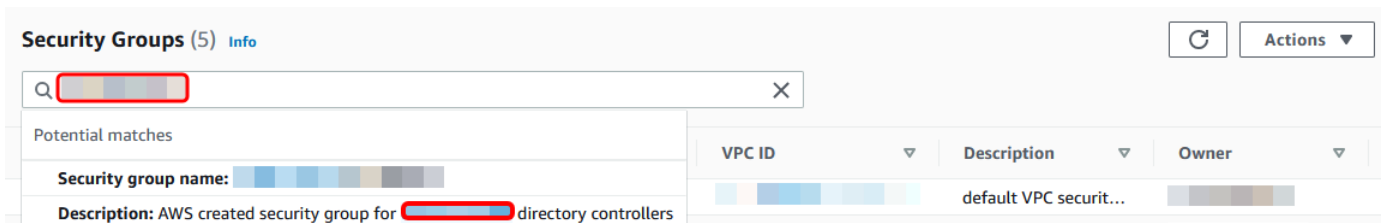
これらは、両方の AWS Managed Microsoft AD から VPC に接続できるようにするために最低限必要となるポートです。固有の設定によっては、追加ポートが開かれていることが必要です。詳細については、Microsoft ウェブサイトの「[How to configure a firewall for Active Directory domains and trusts](#)」(Active Directory ドメインと信頼用にファイアウォールを設定する方法)を参照してください。

AWS Managed Microsoft AD ドメインコントローラーのアウトバウンドルールを設定するには

Note

それぞれのディレクトリに対して、以下の 1~6 のステップを繰り返します。

1. [AWS Directory Service コンソール](#)に移動します。ディレクトリのリストで、AWS Managed Microsoft AD ディレクトリのディレクトリ ID を書き留めます。
2. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
3. ナビゲーションペインで、[Security Groups] を選択します。
4. 検索ボックスを使用して Managed Microsoft AD ディレクトリ ID AWS を検索します。検索結果で、**AWS created security group for *yourdirectoryID* directory controllers** の説明を持つ項目を選択します。



5. 対象のセキュリティグループの [Outbound Rules] (アウトバウンドルール) タブを開きます。[Edit] (編集)、[Add another rule] (別のルールの追加) の順に選択します。新しいルールに、次の値を入力します。
 - [Type] (タイプ): ALL Traffic
 - [Protocol] (プロトコル): ALL
 - [Destination] (送信先) では、ドメインコントローラーから発信されるトラフィックと、その送信先を指定します。単一の IP アドレスまたは IP アドレス範囲を CIDR 表記で指定します (例: 203.0.113.5/32)。同じリージョン内にある別のセキュリティグループの、名前または ID を指定することもできます。詳細については、「[ディレクトリ AWS のセキュリティグループの設定と使用を理解する](#)」を参照してください。
6. [Save] (保存) をクリックします。

Edit outbound rules^{info}

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

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

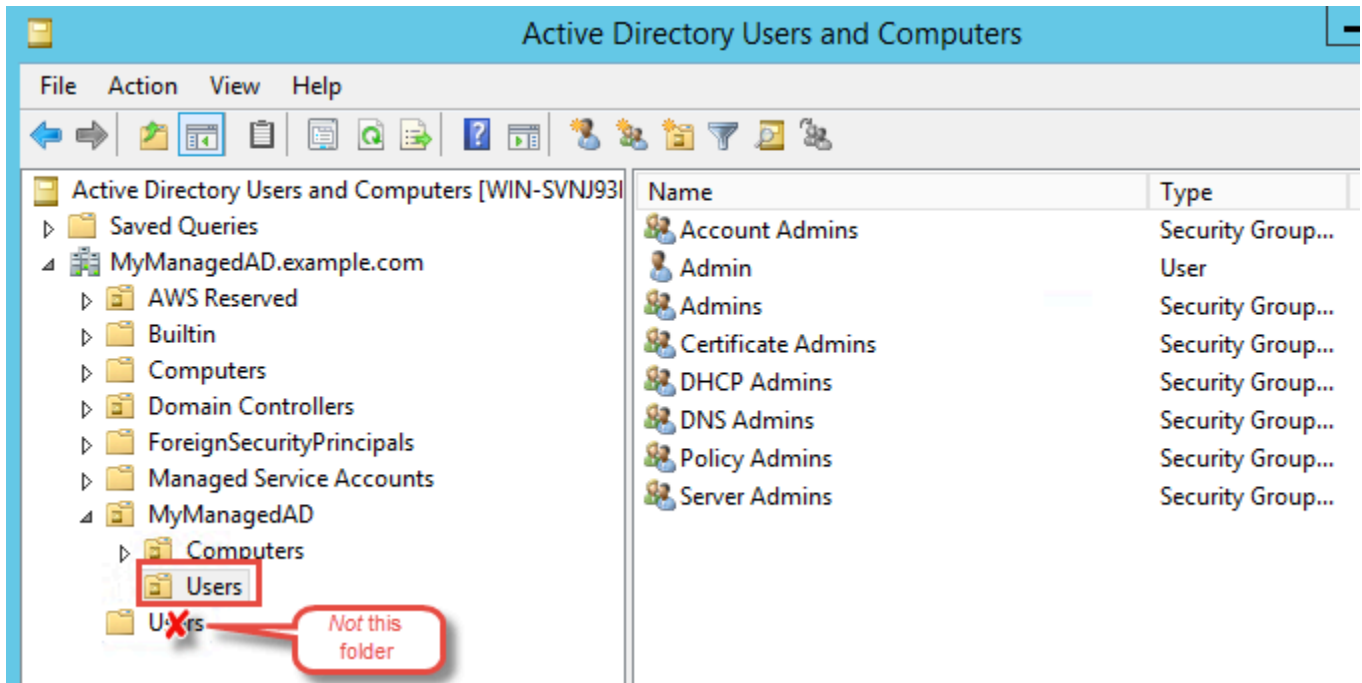
Cancel Preview changes Save rules

Kerberos の事前認証が有効化されていることを確認する

次に、AWS Managed Microsoft AD のユーザーでも Kerberos 事前認証が有効になっていることを確認します。これは、オンプレミスディレクトリで実施したものと同一プロセスです。これはデフォルト設定ですが、何も変更されていないことを確認します。

ユーザーの Kerberos 設定を表示するには

1. ドメインの または [AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#) ドメイン内のユーザーを管理するアクセス許可が委任されたアカウントを使用して、AWS Managed Microsoft AD ディレクトリのメンバーであるインスタンスにログインします。
2. まだインストールされていない場合は、Active Directory ユーザーと、コンピュータツール、および DNS ツールをインストールします。これらのツールをインストールする方法については、「[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#)」を参照してください。
3. サーバーマネージャーを開きます。[Tools] (ツール) メニューで、[Active Directory Users and Computers] (Active Directory ユーザーとコンピュータ) を選択します。
4. 使用しているドメイン内の、[Users] フォルダを選択します。これは、NetBIOS 名を使用する [Users] フォルダであり、完全修飾ドメイン名 (FQDN) の [Users] フォルダではないことに注意してください。



5. ユーザーのリストで、ユーザーを右クリックし、[Properties] (プロパティ) を選択します。
6. [Account] (アカウント) タブを開きます。[Account options] (アカウントオプション) リストで、[Do not require Kerberos preauthentication] (Kerberos 事前認証は不要) がオンになっていないことを確認します。

次のステップ

[ステップ 2: 別の AWS Managed Microsoft AD ドメインとの信頼関係を作成する](#)

ステップ 2: 別の AWS Managed Microsoft AD ドメインとの信頼関係を作成する

準備作業が完了したので、最後のステップは、2 つの AWS Managed Microsoft AD ドメイン間に信頼を作成することです。信頼関係の作成処理中に問題が発生した場合は、「[信頼作成ステータスの理由](#)」のガイドを参照してください。

最初の AWS Managed Microsoft AD ドメインで信頼を設定する

このチュートリアルでは、双方向フォレストの信頼を設定します。ただし、一方向フォレストの信頼を作成する場合、各ドメインの信頼には、それぞれ補完的な方向を持たせる必要があることにご注意ください。例えば、この最初のドメインで一方向の送信信頼を作成する場合は、2 番目の AWS Managed Microsoft AD ドメインで一方向の送信信頼を作成する必要があります。

 Note

AWS Managed Microsoft AD は、外部信頼もサポートしています。ただし、このチュートリアルは、双方向フォレストの信頼を作成することを目的とします。

最初の AWS Managed Microsoft AD ドメインで信頼を設定するには

1. [AWS Directory Service コンソール](#)を開きます。
2. ディレクトリページで、最初の AWS Managed Microsoft AD ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、[Actions] (アクション)、[Add trust relationship] (信頼関係の追加) の順に選択します。
5. 信頼関係の追加ページで、2 番目の AWS Managed Microsoft AD ドメインの FQDN を入力します。2 番目の AWS Managed Microsoft AD の信頼を設定するときに必要になるため、このパスワードを覚えておいてください。方向を指定します。この例では、[Two-way] (双方向) を選択します。
6. 条件付きフォワーダーフィールドに、2 番目の AWS Managed Microsoft AD DNS サーバーの IP アドレスを入力します。
7. (オプション) 別の IP アドレスを追加を選択し、2 番目の AWS Managed Microsoft AD DNS サーバーの 2 番目の IP アドレスを入力します。指定できる DNS サーバー数は最大で合計 4 台です。
8. [Add] (追加) を選択します。信頼はこの時点では失敗しますが、反対側の信頼が作成されていないので、この現象は想定内です。

2 番目の AWS Managed Microsoft AD ドメインで信頼を設定する

次に、2 番目の AWS Managed Microsoft AD ディレクトリとのフォレストの信頼関係を設定します。最初の AWS Managed Microsoft AD ドメインで双方向のフォレスト信頼を作成したため、この AWS Managed Microsoft AD ドメインを使用して双方向の信頼も作成します。

2 番目の AWS Managed Microsoft AD ドメインで信頼を設定するには

1. [AWS Directory Service コンソール](#) に戻ります。
2. ディレクトリページで、2 番目の AWS Managed Microsoft AD ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、[Actions] (アクション)、[Add trust relationship] (信頼関係の追加) の順に選択します。
5. 信頼関係の追加ページで、最初の AWS Managed Microsoft AD ドメインの FQDN を入力します。オンプレミスドメインで信頼を作成した際に使用したのと同じ信頼パスワードを入力します。方向を指定します。この例では、[Two-way] (双方向) を選択します。
6. [Conditional forwarder] (条件付きフォワーダー) フィールドに、1 番目の AWS Managed Microsoft AD DNS サーバーの IP アドレスを入力します。
7. (オプション) 別の IP アドレスを追加を選択し、最初の AWS Managed Microsoft AD DNS サーバーの 2 番目の IP アドレスを入力します。指定できる DNS サーバー数は最大で合計 4 台です。
8. [Add] (追加) を選択します。信頼は、この後すぐに検証する必要があります。
9. 1 番目のドメインで作成した信頼に戻り、信頼関係を再度確認します。

おつかれ様でした。これで、2 つの AWS Managed Microsoft AD ドメイン間に信頼関係ができました。これらの 2 つのドメイン間に設定できるのは、1 つの信頼関係だけです。例えば、設定を一方方向の信頼に変更する場合は、まず既存の信頼関係を削除した上で、新しい信頼関係を作成する必要があります。

AWS Managed Microsoft AD スキーマを拡張する

AWS Managed Microsoft AD は、スキーマを使用してディレクトリデータの保存方法を整理し、適用します。スキーマに定義を追加するプロセスは、「スキーマを拡張する」と呼ばれます。スキーマ拡張を使用すると、有効な LDAP データ交換形式 (LDIF) ファイルを使用して AWS Managed Microsoft AD ディレクトリのスキーマを変更できます。AD スキーマおよびスキーマを拡張する方法の詳細については、以下に一覧されたトピックを参照してください。

AWS Managed Microsoft AD スキーマを拡張するタイミング

AWS Managed Microsoft AD スキーマを拡張するには、新しいオブジェクトクラスと属性を追加します。例えば、シングルサインオン機能をサポートするためにスキーマの変更が必要なアプリケーションに対して、この作業を行います。

また、スキーマの拡張を使用して、特定の Active Directory のオブジェクトクラスと属性に依存するアプリケーションのサポートを、有効にすることもできます。これは、AWS Managed Microsoft AD に依存する企業アプリケーションをクラウドに移行する必要がある場合に AWS 特に役立ちます。

既存の Active Directory スキーマに追加されている各属性またはクラスは、一意の ID を使用して定義される必要があります。こうすることで、企業がスキーマを拡張する際にも一意であることが保証され、また互いに競合することはありません。これらの IDs は AD オブジェクト識別子 (OIDs と呼ばれ、AWS Managed Microsoft AD に保存されます。

開始するには、「[チュートリアル: AWS Managed Microsoft AD スキーマの拡張](#)」を参照してください。

関連トピック

- [AWS Managed Microsoft AD スキーマを拡張する](#)
- [スキーマの要素](#)

トピック

- [チュートリアル: AWS Managed Microsoft AD スキーマの拡張](#)

チュートリアル: AWS Managed Microsoft AD スキーマの拡張

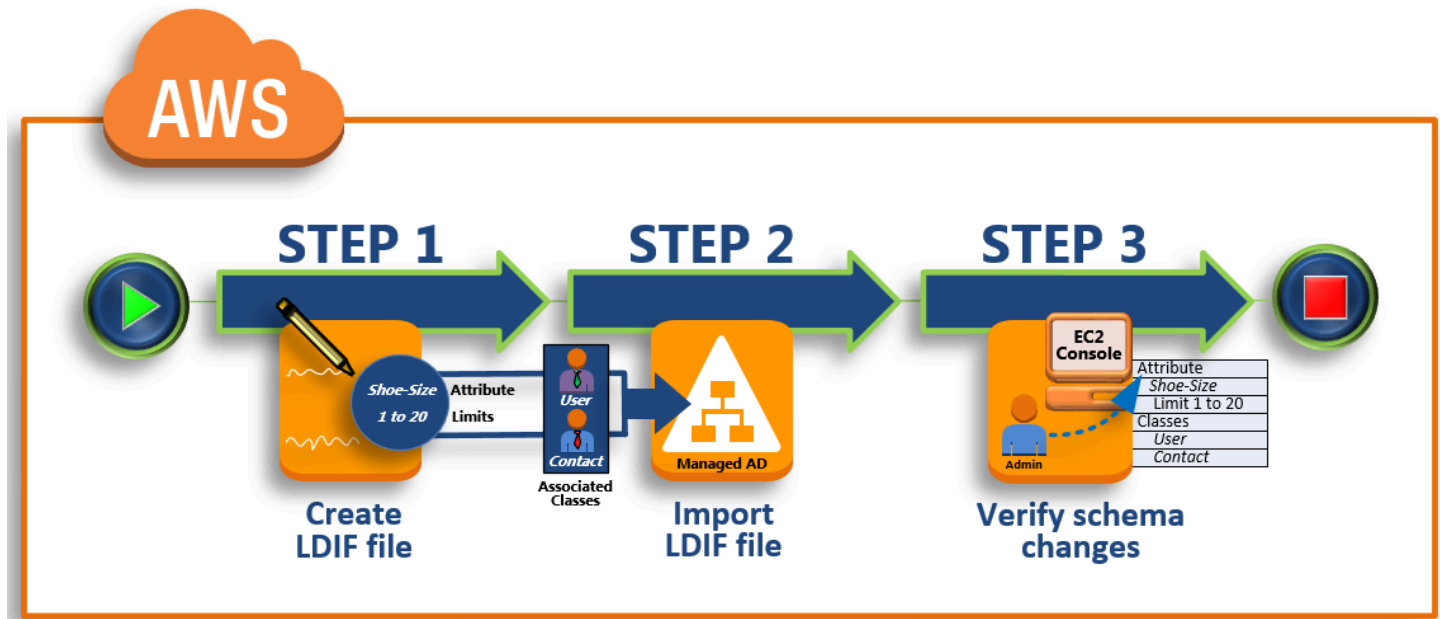
このチュートリアルでは、特定の要件を満たす一意の属性とクラスを追加して、AWS Managed Microsoft AD と呼ばれる AWS Directory Service for Microsoft Active Directory ディレクトリのス

スキーマを拡張する方法について説明します。AWS マネージド Microsoft AD スキーマ拡張は、有効な LDIF (Lightweight Directory Interchange Format) スクリプトファイルを使用してのみアップロードおよび適用できます。

属性 (attributeSchema) はデータベース内のフィールドを定義し、クラス (classSchema) はデータベース内のテーブルを定義します。例えば、Active Directory 内のすべてのユーザーオブジェクトは User というスキーマクラスによって定義され、ユーザーの個々のプロパティ (E メールアドレスや電話番号など) は属性ごとに定義されます。

Shoe-Size などの新しいプロパティを追加する場合は、整数型の新しい属性を定義します。また、1 ~ 20 のように下限と上限を定義することもできます。Shoe-Size attributeSchema オブジェクトが作成されたら、User classSchema オブジェクトをその属性を含むように変更します。属性は複数のクラスにリンクすることが可能です。例えば、Shoe-Size を Contact クラスに追加することもできます。Active Directory スキーマの詳細については、「[AWS Managed Microsoft AD スキーマを拡張するタイミング](#)」を参照してください。

このワークフローには 3 つの基本的な手順が含まれます。



ステップ 1: LDIF ファイルを作成する

最初に、LDIF ファイルを作成し、新しい属性と、その属性を追加するクラスを定義します。このファイルは、ワークフローの次の段階で使用します。

ステップ 2: LDIF ファイルをインポートする

このステップでは、AWS Directory Service コンソールを使用して LDIF ファイルを Microsoft Active Directory 環境にインポートします。

ステップ 3: スキーマ拡張が成功したかどうかを確認する

最後に、管理者は EC2 インスタンスを使用して、新しい拡張が Active Directory のスキーマスナップインに表示されることを確認します。

ステップ 1: LDIF ファイルを作成する

LDIF ファイルは、[LDAP](#) (Lightweight Directory Access Protocol) デイレクトリの内容と更新リクエストを示す、標準のプレーンテキストデータ交換形式です。LDIF は、ディレクトリの内容を、各オブジェクトまたは各エントリごとに 1 つのレコードが対応する、レコードのセットとして伝達します。また、追加、変更、削除、名前変更などの更新リクエストを、更新リクエストごとに 1 つのレコードが対応する、レコードのセットとして表します。

は、AWS Managed Microsoft AD デイレクトリで `ldifde.exe` アプリケーションを実行して、スキーマの変更を含む LDIF ファイル AWS Directory Service をインポートします。つまり、LDIF スクリプトの構文を理解しておくことは有用です。詳細については、「[LDIF Scripts](#)」(LDIF スクリプト)を参照してください。

一部のサードパーティ製 LDIF ツールは、スキーマの更新を抽出、クリーンアップ、および更新するために使用できます。いずれのツールを使用する場合でも、LDIF ファイルで使用されるすべての識別子は一意でなければならないことに注意してください。

LDIF ファイルを作成する前に、下記に示す概念とヒントを確認しておくことを強くお勧めします。

- スキーマの要素 – 属性、クラス、オブジェクト ID、リンクされた属性などのスキーマ要素について説明します。詳細については、「[スキーマの要素](#)」を参照してください。
- アイテムのシーケンス – LDIF ファイル内で項目が配置される順序が、降順で「[ディレクトリ情報ツリー \(DIT\)](#)」に従っていることを確認します。LDIF ファイルのシーケンシングの一般的なルールは以下のとおりです。
 - 空白行で項目を区切ります。
 - 子項目は、親項目の後にリストします。

- 属性やオブジェクトクラスなどの項目は、スキーマ内に置かれる必要があります。これらが存在しない場合は、使用する前にスキーマに追加する必要があります。例えば、属性をクラスに割り当てる前に、その属性を必ず作成します。
- DN の形式 – LDIF ファイルの新しい命令ごとに、その最初の行に識別名 (DN) を定義します。DN は Active Directory オブジェクトのツリー内で Active Directory オブジェクトを識別し、ディレクトリのドメインコンポーネントを含める必要があります。例えば、このチュートリアルでのディレクトリのドメインコンポーネントは DC=example,DC=com です。

DN には、Active Directory オブジェクトの共通名 (CN) も含める必要があります。最初の CN エントリは、属性またはクラスの名前です。次に、CN=Schema,CN=Configuration を使用する必要があります。この CN により、Active Directory スキーマを拡張できるようになります。前述のとおり、Active Directory オブジェクトの内容を追加または変更することはできません。DN の一般的な形式は以下のとおりです。

```
dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
```

このチュートリアルでは、新しい Shoe-Size 属性の DN は以下のようになります。

```
dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
```

- Warnings (警告) – スキーマを拡張する前に、以下の警告を確認します。
 - Active Directory スキーマを拡張する前に、この操作の影響に関する Microsoft の警告を確認することは重要です。詳細については、「[What You Must Know Before Extending the Schema](#)」(スキーマを拡張する前に知っておくべきこと)を参照してください。
 - スキーマの属性またはクラスを削除することはできません。したがって、誤操作をしたものの、バックアップからの復元を実行したくない場合は、オブジェクトを無効にするだけで済みます。詳細については、「[Disabling Existing Classes and Attributes](#)」(既存のクラスと属性の無効化)を参照してください。
 - デフォルトのセキュリティ記述子への変更はサポートされていません。

Managed Microsoft AD スキーマ拡張のテストに使用できる LDIF ファイルの構築方法とサンプル LDIF ファイルの詳細については、AWS セキュリティブログの AWS 「[How to Extend your AWS Managed Microsoft AD Directory Schema](#)」を参照してください。

次のステップ

[ステップ 2: LDIF ファイルをインポートする](#)

ステップ 2: LDIF ファイルをインポートする

AWS Directory Service コンソールから LDIF ファイルをインポートするか、API を使用してスキーマを拡張できます。スキーマ拡張 API でこれを行う方法の詳細については、[AWS Directory Service API Reference](#) を参照してください。現時点において AWS では、Microsoft Exchange などの外部アプリケーション使用した、スキーマの直接的な更新をサポートしていません。

Important

AWS Managed Microsoft AD ディレクトリスキーマを更新すると、オペレーションは元に戻されません。つまり、Active Directory で新しいクラスまたは属性を作成した場合は、それらを削除することができません。ただし、無効にすることは可能です。

スキーマの変更を削除する必要がある場合は、以前のスナップショットからディレクトリを復元するという方法もあります。スナップショットを復元すると、スキーマとディレクトリデータの両方が、過去のある時点でロールバックされています。スナップショットの最長保持期間は 180 日です。詳細については、Microsoft ウェブサイトの「[Active Directory のシステム状態バックアップの有効な保存期間](#)」を参照してください。

更新プロセスを開始する前に、AWS マネージド Microsoft AD はスナップショットを作成し、ディレクトリの現在の状態を保持します。

Note

スキーマ拡張機能は Managed Microsoft AD AWS のグローバル機能です。[AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#) を使用している場合、[プライマリリージョン](#) で次の手順を実行する必要があります。変更した内容は、レプリケートされたすべてのリージョンで自動的に適用されます。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

LDIF ファイルをインポートするには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。

- [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Maintenance] (メンテナンス) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Maintenance] (メンテナンス) タブを選択します。
4. [Schema extensions] (スキーマ拡張) セクションで、[Actions] (アクション)、[Upload and update schema] (スキーマのアップロードと更新) の順に選択します。
 5. ダイアログボックスで、[Browse] (参照) をクリックし、有効な LDIF ファイルを選択し説明を入力します。次に、[Update Schema] (スキーマの更新) をクリックします。

 Important

スキーマの拡張は危険性のある操作です。開発環境またはテスト環境のアプリケーションで初期テストを行っていないスキーマ更新を、そのまま本番環境に適用しないでください。

LDIF ファイルの適用方法

LDIF ファイルがアップロードされると、AWS Managed Microsoft AD は次の順序で変更を適用するため、ディレクトリをエラーから保護する手順を実行します。

1. LDIF ファイルを検証します。LDIF スクリプトはドメイン内の任意のオブジェクトを操作できるため、AWS Managed Microsoft AD はアップロード直後にチェックを実行して、インポートオペレーションが失敗しないようにします。これには、以下を確認するためのチェックが含まれます。
 - 更新されるオブジェクトは、スキーマコンテナにのみ保持されていること
 - DC (ドメインコントローラー) の部分は、LDIF スクリプトが実行されているドメインの名前と一致していること
2. ディレクトリのスナップショットを取得します。スキーマの更新後にアプリケーションに問題が発生した場合、スナップショットを使用してディレクトリを復元することができます。
3. 変更を単一の DC に適用します。AWS マネージド Microsoft AD は DCs の 1 つを分離し、LDIF ファイル内の更新を分離された DC に適用します。次に、1 つの DC をプライマリースキーマとして選択し、その DC をディレクトリレプリケーションから削除した上で、Ldifde.exe を使用して LDIF ファイルを適用します。

4. レプリケーションはすべての DCs に発生します。AWS マネージド Microsoft AD は、分離された DC をレプリケーションに追加して更新を完了します。この間も、ディレクトリは、Active Directory のサービスを中断することなくアプリケーションに提供し続けます。

次のステップ

[ステップ 3: スキーマ拡張が成功したかどうかを確認する](#)

ステップ 3: スキーマ拡張が成功したかどうかを確認する

インポート処理が完了したら、スキーマの更新がディレクトリに適用されたことを確認してください。このことは、スキーマの更新に依存するアプリケーションを移行または更新する際に特に重要となります。さまざまな LDAP ツールを使用するか、または適切な LDAP コマンドを発行するテストツールを作成して、これを実行できます。

この手順では、Active Directory スキーマのスナップインおよび (または) PowerShell を使用して、スキーマ更新が適用されたことを確認します。これらのツールは、AWS Managed Microsoft AD にドメイン結合されているコンピュータから実行する必要があります。このコンピュータとは、仮想プライベートクラウド (VPC) または仮想プライベートネットワーク (VPN) 接続を介したアクセスが可能な、オンプレミスネットワーク上で実行されている Windows サーバーです。また、これらのツールは、Amazon EC2 Windows のインスタンスでも実行できます ([How to launch a new EC2 instance with seamless domain join](#) (シームレスなドメイン結合を使用する新しい EC2 インスタンスの起動方法) を参照)。

Active Directory スキーマスナップインを使用して検証を行うには

1. [TechNet](#) ウェブサイトの手順に従って、Active Directory スキーマのスナップインをインストールします。
2. Microsoft 管理コンソール (MMC) を開き、ディレクトリの AD スキーマツリーを展開します。
3. 前に行ったスキーマの変更が見つかるまで、[Classes] フォルダと [Attributes] フォルダを調べます。

PowerShell 使用して検証を行うには

1. PowerShell ウィンドウを開きます。
2. 次に示すように、Get-ADObject コマンドレットを使用して、スキーマの変更を確認します。
例:

```
get-adobject -Identity 'CN=Shoe-  
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

オプションのステップ

[新しい属性に値を追加する – \(選択可能\)](#)

新しい属性に値を追加する – (選択可能)

新しい属性を作成し、AWS Managed Microsoft AD ディレクトリの属性に新しい値を追加する場合は、このオプションのステップを使用します。

属性に値を追加するには

1. PowerShell コマンドラインユーティリティを開き、次のコマンドを使用して新しい属性を設定します。この例では、特定のコンピュータの属性に新しい EC2InstanceID 値を追加します。

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

2. 次のコマンドを実行すると、EC2InstanceID 値がコンピュータオブジェクトに追加されたかどうかを検証できます。

```
PS C:\> get-adcomputer -Identity computer name -Property example-  
EC2InstanceID
```

関連リソース

以下のリソースリンクから、関連情報を提供している Microsoft のウェブサイト内に移動できます。

- [スキーマの拡張 \(Windows\)](#)
- [Active Directory スキーマ \(Windows\)](#)
- [Active Directory スキーマ](#)
- [Windows 管理: Active Directory スキーマの拡張](#)
- [スキーマ拡張での制約事項 \(Windows\)](#)
- [Ldifde](#)

Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法

インスタンスを起動したときに Amazon EC2 インスタンスを Active Directory ドメインにシームレスに結合できます。詳細については、「[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)」を参照してください。EC2 インスタンスを起動し、[AWS Systems Manager オートメーション](#)を使用して AWS Directory Service コンソールから直接 Active Directory ドメインに参加することもできます。

手動で EC2 インスタンスを Active Directory ドメインに結合する必要がある場合は、適切なリージョン、セキュリティグループまたはサブネットでインスタンスを起動して、そのインスタンスをドメインに結合する必要があります。

これらのインスタンスにリモート接続できるようにするには、接続元のネットワークからインスタンスへの IP 接続が必要です。ほとんどの場合、これには、インターネットゲートウェイが VPC にアタッチされていることと、インスタンスにパブリック IP アドレスがあることが必要です。

トピック

- [AWS Managed Microsoft AD Active Directory でディレクトリの管理インスタンスを起動する](#)
- [Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)
- [Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)
- [Amazon EC2 Mac インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)
- [AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)
- [AWS Managed Microsoft AD の DHCP オプションセットの作成または変更](#)

AWS Managed Microsoft AD Active Directory でディレクトリの管理インスタンスを起動する

この手順では、AWS Systems Manager オートメーション AWS Management Console を使用してディレクトリを管理する Amazon EC2 ディレクトリ管理 Windows インスタンスを起動します。これを行うには、オートメーションコンソールで AWS Systems Manager オートメーション [AWS-CreateDSManagementInstance](#) を直接実行します。

詳細については、以下のリンクを参照してください。

- [による Active Directory ドメイン結合の簡素化 AWS Systems Manager](#)

- [AWS Systems Manager を使用して実行中の EC2 Windows インスタンスをドメイン AWS Directory Service に結合するにはどうすればよいですか？](#)

前提条件

このチュートリアルを完了するには、次の前提条件が必要です。

- をセットアップする必要があります AWS Systems Manager。詳細については、「[セットアップ AWS Systems Manager](#)」を参照してください。
- Systems Manager と AWS Managed Microsoft AD を許可する [IAM インスタンスプロファイルロール](#)が必要です。
 - Systems Manager の詳細については、「[Systems Manager に必要なインスタンスのアクセス許可を設定する](#)」を参照してください。
 - EC2 ディレクトリ管理インスタンスが Managed Microsoft AD にドメイン参加できるようにするには、IAM Windows インスタンスロールに次の AWS 管理 AWS ポリシーが必要です。
 - **AmazonSSMManagedInstanceCore**
 - **AmazonSSMDirectoryServiceAccess**
 - AWS Managed Microsoft AD に接続されている VPC は、パブリック AWS Directory Service エンドポイントへのアクセスを許可する必要があります。詳細については、「[AWS Managed Microsoft AD を作成するための前提条件](#)」を参照してください。
 - コンソールからディレクトリ管理 EC2 インスタンスを起動するには、アカウントで次のアクセス許可を有効にする必要があります。
 - 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`

でのディレクトリ管理 EC2 インスタンスの起動 AWS Management Console

1. [AWS Directory Service コンソール](#) にサインインします。
2. [Active Directory] で [ディレクトリ] を選択します。
3. Active Directory 管理 EC2 インスタンスを起動するディレクトリの [ディレクトリ ID] を選択します。
4. ディレクトリページの右上隅にある [アクション] を選択します。
5. [アクション] ドロップダウンで、[ディレクトリ管理 EC2 インスタンスを起動する] を選択します。
6. [ディレクトリ管理 EC2 インスタンスを起動する] ページの [入力パラメータ] のフィールドに入力します。
 - a. (選択可能) インスタンスのキーペアを指定できます。[キーペア名 - オプションの] ドロップダウンリストから、キーペアを選択します。
 - b. (オプション) View AWS CLI コマンドを選択すると、このオートメーションを実行する AWS CLI ために 使用する例が表示されます。
7. [Submit] を選択してください。
8. ディレクトリページに戻ります。起動処理が正常に開始されたことを示す緑色のフラッシュバーが画面の上部に表示されます。

ディレクトリ管理 EC2 インスタンスを表示する

ディレクトリの EC2 インスタンスが起動していない場合は、[ディレクトリ管理 EC2 インスタンス] の下にダッシュ (-) が表示されます。

1. [Active Directory] で [ディレクトリ] を選択し、表示するディレクトリを選択します。
2. [ディレクトリの詳細] の [ディレクトリ管理 EC2 インスタンス] で、表示する 1 つまたはすべてのインスタンスを選択します。
3. インスタンスを選択すると、リモートデスクトップをインスタンスに接続するための EC2 の [インスタンスに接続] ページにルーティングされます。

Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory

Amazon EC2 Windows インスタンスを起動して AWS Managed Microsoft AD に参加できます。または、既存の EC2 Windows インスタンスを AWS Managed Microsoft AD に手動で結合することもできます。

Seamlessly join EC2 Windows instance

この手順では、Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD にシームレスに結合します。複数の でシームレスなドメイン結合を実行する必要がある場合は AWS アカウント、「」を参照してください[チュートリアル: AWS Managed Microsoft AD ディレクトリを共有してシームレスな EC2 ドメイン結合を実現する](#)。Amazon EC2 の詳細については、「[Amazon EC2 とは](#)」を参照してください。

前提条件

EC2 インスタンスをシームレスにドメイン結合するには、以下を完了する必要があります。

- AWS Managed Microsoft AD がある。詳細については[AWS Managed Microsoft AD の作成](#)を参照してください。
- EC2 Windows インスタンスをシームレスに結合するには、次の IAM アクセス許可が必要です。
 - 次の IAM アクセス許可を持つ IAM インスタンスプロファイル：
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - EC2 を AWS Managed Microsoft AD にシームレスに結合するユーザーには、次の IAM アクセス許可が必要です。
 - AWS Directory Service アクセス許可：
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Amazon VPC のアクセス許可：
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"

- "ec2:AttachNetworkInterface"
- EC2 アクセス許可 :
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
- AWS Systems Manager アクセス許可 :
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

AWS Managed Microsoft AD が作成されると、インバウンドルールとアウトバウンドルールを使用してセキュリティグループが作成されます。これらのルールとポートの詳細については、「」を参照してください[AWS Managed Microsoft AD で作成されるもの](#)。EC2 Windows インスタンスをシームレスにドメイン結合するには、インスタンスを起動する VPC で、AWS Managed Microsoft AD セキュリティグループのインバウンドルールとアウトバウンドルールで許可されているのと同じポートを許可する必要があります。

- ネットワークセキュリティとファイアウォールの設定によっては、追加のアウトバウンドトラフィックを許可する必要がある場合があります。このトラフィックは、次のエンドポイントへの HTTPS (ポート 443) 用になります。

Endpoint	ロール
ec2messages. <i>region</i> .amazonaws.com	Session Manager サービスを使用してセッションチャネルを作成および削除します。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。

Endpoint	ロール
ssm. <i>region</i> .amazonaws.com	のエンドポイント AWS Systems Manager Session Manager。詳細については、 「AWS Systems Manager エンドポイントとクォータ」 を参照してください。
ssmmessages. <i>region</i> .amazonaws.com	Session Manager サービスを使用してセッションチャネルを作成および削除します。詳細については、 「AWS Systems Manager エンドポイントとクォータ」 を参照してください。
ds. <i>region</i> .amazonaws.com	のエンドポイント AWS Directory Service。詳細については、 「のリージョンの可用性 AWS Directory Service」 を参照してください。

- AWS Managed Microsoft AD ドメイン名を解決する DNS サーバーを使用することをお勧めします。そのためには、DHCP オプションセットを作成できます。詳細については「[AWS Managed Microsoft AD の DHCP オプションセットの作成または変更](#)」を参照してください。
- DHCP オプションセットを作成しない場合、DNS サーバーは静的になり、AWS Managed Microsoft AD によって設定されます。

Amazon EC2 Windows インスタンスをシームレスに結合するには

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
2. ナビゲーションバーで、既存のディレクトリ AWS リージョン と同じ を選択します。
3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Windows EC2 インスタンスに使用する名前を入力します。
5. (オプション) [補足タグを追加] で、タグとキーの値のペアを 1 つまたは複数追加して、この EC2 インスタンスのアクセスを整理、追跡、または制御します。

6. [アプリケーションと OS イメージ (Amazon マシンイメージ)] セクションの [クイックスタート] ペインで [Windows] を選択します。Windows Amazon マシンイメージ (AMI) は、[Amazon マシンイメージ (AMI)] ドロップダウンリストから変更できます。
7. [インスタンスタイプ] セクションで、[インスタンスタイプ] ドロップダウンリストから使用するインスタンスタイプを選択します。
8. キーペア (ログイン) セクションでは、[新しいキーペアを作成する](#)か、既存のキーペアを使用するか、キーペアなしで続行するかを選択できます。
9. [インスタンスを起動する] ページの [ネットワーク設定] セクションで、[編集] を選択します。[VPC に必須の] ドロップダウンリストから、ディレクトリが作成された [VPC] を選択します。
10. [サブネット] ドロップダウンリストから VPC 内のパブリックサブネットの 1 つを選択します。選択するサブネットで、すべての外部トラフィックがインターネットゲートウェイにルーティングされるように選択する必要があります。そうでない場合は、インスタンスにリモート接続できません。

インターネットゲートウェイへの接続方法の詳細については、Amazon VPC ユーザーガイドの「[インターネットゲートウェイを使用してサブネットをインターネットに接続する](#)」を参照してください。

11. [自動割り当てパブリック IP] で、[有効化] を選択します。

公開 IP アドレス指定とプライベート IP アドレス指定の詳細については、「Amazon EC2 インスタンスユーザーガイド」の「[Amazon EC2 インスタンスの IP アドレス指定](#)」を参照してください。

12. [ファイアウォール (セキュリティグループ)] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
13. [ストレージの設定] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
14. [高度な詳細] セクションを選択し、[ドメイン結合ディレクトリ] ドロップダウンリストからドメインを選択します。

 Note

ドメイン結合ディレクトリを選択すると、次のようになります:

 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. 

このエラーは、EC2 起動ウィザードが予期しないプロパティを持つ既存の SSM ドキュメントを識別した場合に発生します。次のいずれかを試すことができます。

- 以前に SSM ドキュメントを編集し、プロパティの存在が予想される場合は、[閉じる] を選択して EC2 インスタンスを変更せずに起動します。
- ここで既存の SSM ドキュメントを削除するリンクを選択して、SSM ドキュメントを削除します。これにより、正しいプロパティを使用する SSM ドキュメントを作成できます。EC2 インスタンスを起動すると、SSM ドキュメントが自動的に作成されます。

15. [IAM インスタンスプロファイル] には既存の IAM インスタンスプロファイルを選択するか、新しいプロファイルを作成できます。管理 AWS ポリシー AmazonSSMManagedInstanceCore と AmazonSSMDirectoryServiceAccess がアタッチされている IAM インスタンスプロファイルを IAM インスタンスプロファイルドロップダウンリストから選択します。新しい IAM プロファイルリンクを作成するには、[新しい IAM プロファイルを作成する] リンクを選択し、以下を実行します。
 1. [ロールの作成] を選択してください。
 2. [Select trusted entity] (信頼されたエンティティを選択) で、[AWS サービス] を選択します。
 3. [ユースケース] で、[EC2] を選択してください。
 4. ポリシーのリスト内の [アクセス許可を追加する] の下で、AmazonSSMManagedInstanceCore ポリシーと AmazonSSMDirectoryServiceAccess ポリシーを選択します。リストを絞り込むため、検索ボックスに **SSM** と入力します。[次へ] を選択します。

 Note

AmazonSSMDirectoryServiceAccess は、 によって Active Directory 管理される にインスタンスを結合するためのアクセス許可を提供します AWS Directory Service。 AmazonSSMManagedInstanceCore は、 AWS Systems Manager サー

ビスを使用するために必要な最小限のアクセス許可を提供します。これらのアクセス許可を使用してロールを作成する方法、および IAM ロールに割り当てることができるその他のアクセス許可とポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。

5. [名前、確認、作成] ページで、[ロール名] を入力します。EC2 インスタンスにアタッチするには、このロール名が必要です。
 6. (オプション) IAM インスタンスプロファイルの説明を [説明] フィールドに入力できます。
 7. [ロールの作成] を選択してください。
 8. [インスタンスを起動する] ページに戻り、[IAM インスタンスプロファイル] の横にある更新アイコンを選択します。新しい IAM インスタンスプロファイルが [IAM インスタンスプロファイル] ドロップダウンリストに表示されるはずです。新しいプロファイルを選択し、残りの設定はデフォルト値のままにします。
16. [インスタンスを起動] を選択します。

Manually join EC2 Windows instance

既存の Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合するには、[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#) で指定したパラメータを使用して、インスタンスを起動する必要があります。

AWS Managed Microsoft AD DNS サーバーの IP アドレスが必要です。この情報は、お使いのディレクトリ > [ディレクトリの詳細] セクションと [ネットワークとセキュリティ] セクションの、[ディレクトリサービス] > [ディレクトリ] > [ディレクトリ ID] リンクの下にあります。

The screenshot displays the AWS Directory Service console for a specific directory instance. The left sidebar shows the navigation menu with 'Active Directory' and 'Cloud Directory' sections. The main content area is titled 'd-1234567890' and contains two main sections: 'Directory details' and 'Networking details'. The 'Directory details' section lists various attributes of the directory, including its type, edition, operating system version, DNS name, NetBIOS name, and EC2 instances used for administration. The 'Networking details' section provides information about the VPC, subnets, availability zones, and DNS addresses associated with the directory.

Directory details	
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)	-

Networking details	
VPC	Subnets
Availability zones	DNS address
us-east-2a	192.0.2.1
us-east-2b	198.51.100.1

Windows インスタンスを AWS Managed Microsoft AD に結合するには Active Directory

1. リモートデスクトッププロトコルクライアントを使用してインスタンスに接続します。
2. インスタンスの TCP / IPv4 プロパティダイアログボックスを開きます。
 - a. ネットワーク接続を開きます。

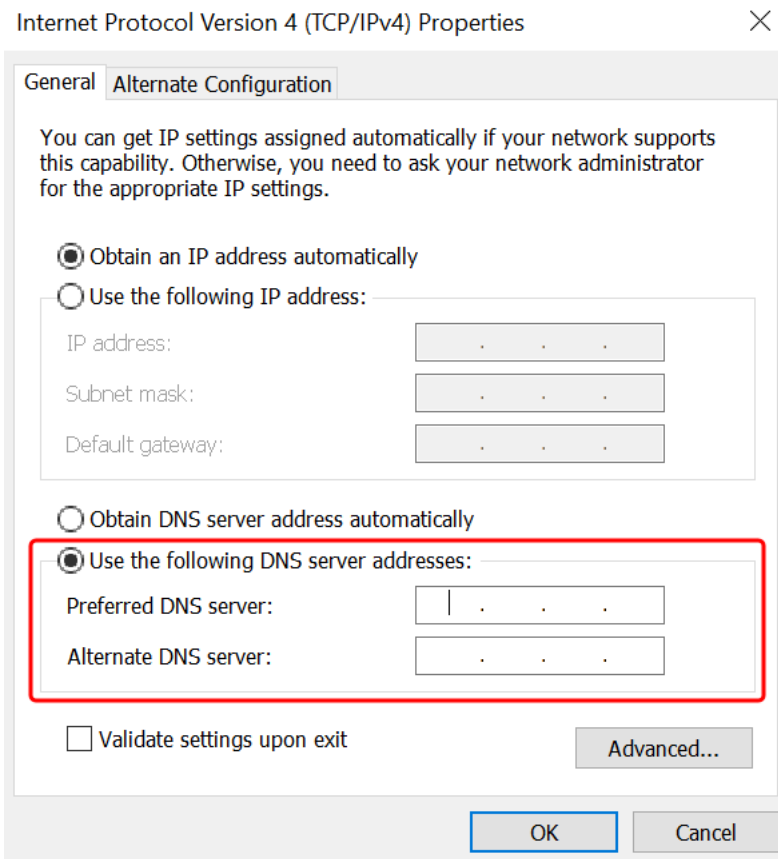
Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、[Network Connections] (ネットワーク接続) を直接開くことができます。

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. 有効になっているネットワーク接続のコンテキストメニュー (右クリック) を開き、[Properties] (プロパティ) を選択します。
- c. 接続のプロパティダイアログボックスで、[Internet Protocol Version 4] をダブルクリックして開きます。

3. 選択 次の DNS サーバーアドレスを使用し、優先 DNS サーバーと代替 DNS サーバーアドレスを AWS Managed Microsoft AD 提供の DNS サーバーの IP アドレスに変更し、OK を選択します。



4. インスタンスの [System Properties] (システムプロパティ) ダイアログボックスを開き、[Computer Name] (コンピュータ名) タブを選択して、[Change] (変更) をクリックします。

i Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、[System Properties] (システムプロパティ) ダイアログボックスを直接開くことができます。

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. フィールドのメンバーで、ドメインを選択し、AWS Managed Microsoft AD Active Directory の完全修飾名を入力し、OK を選択します。
6. ドメイン管理者の名前とパスワードの入力を求められたら、ドメイン結合権限を持つアカウントのユーザー名とパスワードを入力します。これらの権限の委任に関する詳細について

は、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

 Note

ドメインの完全修飾名または NetBIOS 名のいずれかを入力できます。これに続けて、バックスラッシュ (\)、ユーザー名の順に入力します。ユーザー名は [Admin] になります。例えば、**corp.example.com\admin**、**corp\admin** です。

7. ドメインへのアクセスを歓迎するメッセージを受け取ったら、インスタンスを再起動して変更を有効にします。

インスタンスが AWS Managed Microsoft AD Active Directory ドメインに結合されたので、そのインスタンスにリモートでログインし、ユーザーやグループの追加など、ディレクトリを管理するユーティリティをインストールできます。Active Directory 管理ツールを使用して、ユーザーとグループを作成できます。詳細については、「[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#)」を参照してください。

 Note

Amazon EC2 インスタンスの DNS アドレスを手動で変更する代わりに、Amazon Route 53 を使用して DNS クエリを処理することもできます。詳細については、「[Directory Service の DNS 解決策を Amazon Route 53 Resolver と統合する](#)」および「[アウトバウンド DNS クエリをネットワークに転送する](#)」を参照してください。

Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD に結合する Active Directory

EC2 Linux インスタンスを起動して、の AWS Managed Microsoft AD に参加できます AWS Management Console。EC2 Linux インスタンスを AWS Managed Microsoft AD に手動で結合することもできます。Winbind などのツールを使用して、EC2 Linux インスタンスを AWS Managed Microsoft AD にドメイン結合することもできます。

以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

- Amazon Linux AMI 2018.03.0

- Amazon Linux 2 (64 ビット x86)
- Red Hat Enterprise Linux 8 (HVM) (64 ビット x86)
- Ubuntu Server 18.04 LTS および Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

 Note

Ubuntu 14 および Red Hat Enterprise Linux 7 および 8 より前のディストリビューションは、シームレスなドメイン結合機能をサポートしていません。

EC2 Linux インスタンスをドメイン結合する方法：

- [Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory にシームレスに結合する](#)
- [Amazon EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合する](#)
- [Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合します。](#)
- [Winbind を使用して Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合する](#)

Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory にシームレスに結合する

この手順では、Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory にシームレスに結合します。この手順を完了するには、追加コストが発生する可能性のある AWS Secrets Manager シークレットを作成する必要があります。詳細については、「[AWS Secrets Manager 料金](#)」を参照してください。

複数の AWS アカウントでシームレスなドメイン結合を実行する必要がある場合は、オプションで[ディレクトリ共有](#)を有効にするように選択できます。

以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

- Amazon Linux AMI 2018.03.0

- Amazon Linux 2 (64 ビット x86)
- Red Hat Enterprise Linux 8 (HVM) (64 ビット x86)
- Ubuntu Server 18.04 LTS および Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

Ubuntu 14 および Red Hat Enterprise Linux 7 および 8 より前のディストリビューションは、シームレスなドメイン結合機能をサポートしていません。

Linux インスタンスを AWS Managed Microsoft AD Active Directory にシームレスに結合するプロセスのデモについては、以下の YouTube ビデオを参照してください。

Amazon EC2 for Linux のシームレスな AD ドメイン結合のデモ

前提条件

EC2 Linux インスタンスへのシームレスなドメイン結合を設定する前に、これらのセクションの手順を完了する必要があります。

シームレスなドメイン結合のためのネットワーク前提条件

EC2 Linux インスタンスをシームレスにドメイン結合するには、以下を完了する必要があります。

- AWS Managed Microsoft AD がある。詳細については[AWS Managed Microsoft AD の作成](#)を参照してください。
- EC2 Linux インスタンスをシームレスに結合するには、次の IAM アクセス許可が必要です。
 - AWS Managed Microsoft AD がある。詳細については[AWS Managed Microsoft AD の作成](#)を参照してください。
 - EC2 Windows インスタンスをシームレスに結合するには、次の IAM アクセス許可が必要です。
 - 次の IAM アクセス許可を持つ IAM インスタンスプロファイル：
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - EC2 を AWS Managed Microsoft AD にシームレスに結合するユーザーには、次の IAM アクセス許可が必要です。

- AWS Directory Service アクセス許可 :
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
- Amazon VPC のアクセス許可 :
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
- EC2 アクセス許可 :
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"
 - "ec2:DescribeInstanceTypes"
 - "ec2:RunInstances"
 - "ec2:CreateTags"
- AWS Systems Manager アクセス許可 :
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"
- AWS Managed Microsoft AD が作成されると、インバウンドルールとアウトバウンドルールを使用してセキュリティグループが作成されます。これらのルールとポートの詳細については、「」を参照してください[AWS Managed Microsoft AD で作成されるもの](#)。EC2 Linux インスタンスをシームレスにドメイン結合するには、インスタンスを起動する VPC で、AWS Managed Microsoft AD セキュリティグループのインバウンドルールとアウトバウンドルールで許可されているのと同じポートを許可する必要があります。
- ネットワークセキュリティとファイアウォールの設定によっては、追加のアウトバウンドトラフィックを許可する必要がある場合があります。このトラフィックは、次のエンドポイントへの HTTPS (ポート 443) 用になります。

Endpoint	ロール
ec2messages. <i>region</i> .amazonaws.com	Session Manager サービスを使用してセッションチャネルを作成および削除します。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。
ssm. <i>region</i> .amazonaws.com	のエンドポイント AWS Systems Manager Session Manager。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。
ssmmessages. <i>region</i> .amazonaws.com	Session Manager サービスを使用してセッションチャネルを作成および削除します。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。
ds. <i>region</i> .amazonaws.com	のエンドポイント AWS Directory Service。詳細については、「 のリージョンの可用性 AWS Directory Service 」を参照してください。
secretsmanager. <i>region</i> .amazonaws.com	のエンドポイント AWS Secrets Manager。詳細については、「 AWS Secrets Manager エンドポイントとクォータ 」を参照してください。

- AWS Managed Microsoft AD ドメイン名を解決する DNS サーバーを使用することをお勧めします。そのためには、DHCP オプションセットを作成できます。詳細については「[AWS Managed Microsoft AD の DHCP オプションセットの作成または変更](#)」を参照してください。
- DHCP オプションセットを作成しない場合、DNS サーバーは静的になり、AWS Managed Microsoft AD によって に設定されます。

シームレスなドメイン結合のサービスアカウントを選択する

Linux コンピュータを AWS Managed Microsoft AD Active Directory ドメインにシームレスに結合できます。これを行うには、マシンをドメインに結合するためのコンピュータアカウントの作成アクセス許可を持つユーザーアカウントを使用する必要があります。AWS が委任した管理者または他のグループのメンバーが、コンピュータをドメインに結合する十分な権限を持っている場合でも、これらを使用することは推奨されません。ベストプラクティスとして推奨されるのは、コンピュータをドメインに結合するために必要な、最小限の権限を持ったサービスアカウントを使用することです。

コンピュータをドメインに結合するために必要な最小限の権限をアカウントに委任するには、次の PowerShell コマンドを実行します。これらのコマンドは、ドメインに結合され、[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#) がインストールされている Windows コンピュータから実行する必要があります。また、コンピュータ OU またはコンテナのアクセス許可を変更するアクセス許可を持つアカウントを使用する必要があります。PowerShell コマンドは、サービスアカウントがドメインのデフォルトコンピュータコンテナにコンピュータオブジェクトを作成できるようにするアクセス許可を設定します。

```
$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"
```


グラフィカルユーザーインターフェイス (GUI) を使用する場合は、[権限をサービスアカウントに委任する](#) で説明している手動プロセスを使用できます。

ドメインサービスアカウントを保存するシークレットを作成する

を使用して AWS Secrets Manager ドメインサービスアカウントを保存できます。詳細については、「[AWS Secrets Manager シークレットの作成](#)」を参照してください。

 Note

Secrets Manager には料金がかかります。詳細については、「AWS Secrets Manager ユーザーガイド」の「[料金表](#)」を参照してください。

ドメインサービスアカウントの情報を保存するシークレットを作成するには

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/secretsmanager/> で AWS Secrets Manager コンソールを開きます。
2. [Store a new secret] (新しいシークレットの保存) を選択します。
3. [Store a new secret] (新しいシークレットを保存する) のページで、次の操作を行います：
 - a. [シークレットのタイプ] で、[その他のシークレットのタイプ] を選択します。
 - b. [Key/value pairs] (キー/値ペア) で、次のように実行します。
 - i. 最初のボックスに **awsSeamlessDomainUsername** と入力します。同じ行の次のボックスに、サービスアカウントのユーザー名を入力します。例えば、以前に PowerShell コマンドを使用した場合、サービスアカウント名は **awsSeamlessDomain** になります。

 Note

awsSeamlessDomainUsername を正確に入力する必要があります。先頭または末尾にスペースがないことを確認します。スペースがあると、ドメイン結合が失敗します。

The screenshot shows the AWS Secrets Manager console interface. On the left, a sidebar lists the steps: Step 1: Choose secret type, Step 2: Configure secret, Step 3 - optional: Configure rotation, and Step 4: Review. The main area is titled 'Choose secret type'. It has three sections: 'Secret type', 'Key/value pairs', and 'Encryption key'. In the 'Secret type' section, four radio buttons are present: '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). Below this, the 'Key/value pairs' section has a table with two columns: 'Key/value' and 'Plaintext'. The first row has 'awsSeamlessDomainUsername' in the 'Key/value' column (highlighted with a red box) and an empty 'Plaintext' column. Below the table is a '+ Add row' button. The 'Encryption key' section shows a dropdown menu with 'aws/secretsmanager' selected and a refresh button. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. [Add row] (行の追加) を選択します。
- iii. 新しい行で、最初のボックスに **awsSeamlessDomainPassword** と入力します。同じ行の次のボックスに、サービスアカウントのパスワードを入力します。

 Note

awsSeamlessDomainPassword を正確に入力する必要があります。先頭または末尾にスペースがないことを確認します。スペースがあると、ドメイン結合が失敗します。

- iv. 暗号化キーの下で、デフォルト値 `aws/secretsmanager` のままにしておきます。このオプションを選択すると、AWS Secrets Manager は常に秘密を暗号化します。自身で作成したキーを選択することもできます。
- v. [次へ] を選択します。

4. [Secret name]の下に、**d-xxxxxxxxxx**をディレクトリIDに置き換えて、以下のフォーマットでディレクトリIDを含むsecret nameを入力します：

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

これは、アプリケーション内のシークレットを取得するために使用されます。

 Note

aws/directory-services/d-xxxxxxxxxx**/seamless-domain-join** は正確に入力する必要がありますが、**d-xxxxxxxxxx** はディレクトリ ID に置き換えてください。先頭または末尾にスペースがないことを確認します。スペースがあると、ドメイン結合が失敗します。

The screenshot shows the AWS Secrets Manager console. The breadcrumb navigation is 'AWS Secrets Manager > Secrets > Store a new secret'. The left sidebar shows a progress indicator with four steps: Step 1 (Choose secret type), Step 2 (Configure secret), Step 3 (optional, Configure rotation), and Step 4 (Review). The main content area is titled 'Configure secret'. It contains several sections: 'Secret name and description' with a text input for the secret name (containing 'aws/directory-services/d-xxxxxxx/seamless-domain-join') and an optional description text area (containing 'Access to MYSQL prod database for my AppBeta'); 'Tags - optional' with a message 'No tags associated with the secret.' and an 'Add' button; 'Resource permissions - optional' with an 'Edit permissions' button; and 'Replicate secret - optional' with a description of creating read-only replicas. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons, with 'Next' being highlighted in orange.

5. それ以外はすべてデフォルトのままにして、[Next] (次へ) をクリックします。
6. [Configure automatic rotation] (自動ローテーションを設定) で [Disable automatic rotation] (自動ローテーションを無効にする) を選択し、[Next] (次へ) をクリックします。

このシークレットの保存後にローテーションを有効にすることができます。

7. 設定を確認し、[Store] (保存) をクリックして変更を保存します。Secrets Manager コンソールがアカウントのシークレットリストに戻ります。リストには、新しいシークレットが追加されています。
8. 新しく作成したシークレット名をリストから選択し、[Secret ARN] (シークレット ARN) 値をメモします。これは次のセクションで必要になります。

ドメインサービスアカウントシークレットのローテーションを有効にする

セキュリティ体制を改善するために、シークレットを定期的にローテーションすることをお勧めします。

ドメインサービスアカウントシークレットのローテーションを有効にするには

- 「AWS Secrets Manager ユーザーガイド」の「[シー AWS Secrets Manager クレットの自動ローテーションを設定する](#)」の手順に従います。

ステップ 5 では、「AWS Secrets Manager ユーザーガイド」のローテーションテンプレート「[Microsoft Active Directory 認証情報](#)」を使用します。

ヘルプについては、「AWS Secrets Manager ユーザーガイド」の「[ロー AWS Secrets Manager テーションのトラブルシューティング](#)」を参照してください。

必要な IAM ポリシーとロールを作成する

次の前提条件の手順に従い、Secrets Manager のシームレスなドメイン結合シークレット (先ほど作成したもの) への読み取り専用アクセスを許可するカスタムポリシーを作成し、新しい LinuxEC2DomainJoin IAM ロールを作成します。

Secrets Manager の IAM 読み取りポリシーを作成する

IAM コンソールを使用して、Secrets Manager シークレットへの読み取り専用アクセスを許可するポリシーを作成します。

Secrets Manager の IAM 読み取りポリシーを作成するには

1. IAM ポリシーを作成する権限を持つユーザー AWS Management Console として にサインインします。次に、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. ナビゲーションペインの [アクセス管理] で、[ポリシー] を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [JSON] タブを選択し、以下の JSON ポリシードキュメントからテキストをコピーします。これを、[JSON] テキストボックスに貼り付けます。

Note

リージョンとリソース ARN を、先ほど作成したシークレットの実際のリージョンと ARN に置き換えていることを確認してください。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
      "Resource": [
        "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
        services/d-xxxxxxxxx/seamless-domain-join"
      ]
    }
  ]
}
```

5. 完了したら、[Next] を選択します。構文エラーがある場合は、Policy Validator によってレポートされます。詳細については、「[IAM ポリシーの検証](#)」を参照してください。
6. [Review policy] (ポリシーの確認) ページで、ポリシー名を入力します (**SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read** など)。[Summary] (概要) セクションで、ポリシーで付与されているアクセス許可を確認します。[Create Policy] (ポリシーの作成) をクリックし、変更を保存します。新しいポリシーが管理ポリシーのリストに表示されます。これで ID にアタッチする準備は完了です。

Note

シークレットごとに 1 つのポリシーを作成することをお勧めします。そうすることで、インスタンスが適切なシークレットにのみアクセスできるようになり、インスタンスが侵害された場合の影響を最小限に抑えることができます。

LinuxEC2DomainJoin ロールを作成する

IAM コンソールを使用して、Linux EC2 インスタンスへのドメイン結合に使用するロールを作成します。

LinuxEC2DomainJoin ロールを作成するには

1. IAM ポリシーを作成する権限を持つユーザー AWS Management Console として にサインインします。次に、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. ナビゲーションペインの [Access Management] (アクセス管理) で、[Roles] (ロール) を選択します。
3. コンテンツペインで、[Create role] (ロールの作成) を選択します。
4. [Select type of trusted entity] (信頼されたエンティティの種類を選択) の下で、[AWS Service] を選択します。
5. [Use case] (ユースケース) で EC2 を選択し、[Next] (次へ) を選択します。

The screenshot shows the 'Create role' wizard in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected. The 'Filter policies' section is partially visible at the bottom.

6. [Filter policies] (フィルターポリシー) で、以下を実行します。
 - a. **AmazonSSMManagedInstanceCore** と入力します。次に、リスト内のその項目のチェックボックスをオンにします。
 - b. **AmazonSSMDirectoryServiceAccess** と入力します。次に、リスト内のその項目のチェックボックスをオンにします。
 - c. **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read** (または前の手順で作成したポリシーの名前) を入力します。次に、リスト内のその項目のチェックボックスをオンにします。

- d. 上記の 3 つのポリシーを追加したら、[ロールを作成] を選択します。

 Note

AmazonSSMDirectoryServiceAccess は、 によってActive Directory管理される にインスタンスを結合するアクセス許可を提供します AWS Directory Service。AmazonSSMManagedInstanceCore は、 AWS Systems Manager サービスを使用するために必要な最小限のアクセス許可を提供します。これらのアクセス許可を使用してロールを作成する方法、および IAM ロールに割り当てることができるその他のアクセス許可とポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。

7. **LinuxEC2DomainJoin**[Role name] (ロール名)欄 に、 適宜の別の名前など 新しいロールの名前を入力します。
8. (オプション) [Role description] (ロールの説明) に、説明を入力します。
9. (オプション) [ステップ 3: タグの追加] で [新しいタグの追加] を選択してタグを追加します。タグのキーと値のペアは、このロールのアクセスを整理、追跡、または制御するために使用されます。
10. [ロールの作成] を選択してください。

Linux インスタンスをシームレスに結合する

Linux インスタンスをシームレスに結合するには

1. にサインイン AWS Management Console し、 <https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
2. ナビゲーションバーのリージョンセレクターから、既存のディレクトリ AWS リージョン と同じ を選択します。
3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Linux EC2 インスタンスに使用する名前を入力します。
5. (選択可能) [補足タグを追加] で、タグとキーの値のペアを 1 つまたは複数追加して、この EC2 インスタンスのアクセスを整理、追跡、またはコントロールします。

6. Application and OS Image (Amazon Machine Image)セクションで、起動したいLinux AMIを選択します。

 Note

使用する AMI には AWS Systems Manager、(SSM Agent) バージョン 2.3.1644.0 以降が必要です。その AMI からインスタンスを起動して AMI にインストールされている SSM Agent のバージョンを確認するには、「[現在インストールされている SSM Agent バージョンを取得するには](#)」を参照してください。SSM Agent をアップグレードする必要がある場合は、「[Linux の EC2 インスタンスで SSM Agent をインストールして設定する](#)」を参照してください。

SSM は Linux インスタンスを Active Directory ドメインに結合する際にプラグイン aws:domainJoin を使用します。プラグインは、Linux インスタンスのホスト名を EC2AMAZ-XXXXXXX の形式に変更します。aws:domainJoinの詳細については、[AWS Systems Manager ユーザーガイド]の「[AWS Systems Manager コマンド・ドキュメント・プラグイン・リファレンス](#)」を参照してください。

7. [インスタンスタイプ] セクションで、[インスタンスタイプ] ドロップダウンリストから使用するインスタンスタイプを選択します。
8. [キーペア (ログイン)] セクションで、新しいキーペアを作成するか、既存のキーペアから選択します。新しいキーペアを作成するには、[新しいキーペアの作成] を選択します。キーペアの名前を入力し、[キーペアタイプ] と [プライベートキーファイル形式] のオプションを選択します。OpenSSH で使用できる形式でプライベートキーを保存するには、[.pem] を選択します。プライベートキーを PuTTY で使用できる形式で保存するには、[.ppk] を選択します。[キーペアの作成] を選択します。ブラウザによって秘密キーファイルが自動的にダウンロードされます。ダウンロードしたプライベートキーのファイルを安全な場所に保存します。

 Important

プライベートキーのファイルを保存できるのはこのタイミングだけです。

9. [インスタンスを起動する] ページの [ネットワーク設定] セクションで、[編集] を選択します。[VPC に必須の] ドロップダウンリストから、ディレクトリが作成された [VPC] を選択します。
10. [サブネット] ドロップダウンリストから VPC 内のパブリックサブネットの 1 つを選択します。選択するサブネットで、すべての外部トラフィックがインターネットゲートウェイにルーティングされるように選択する必要があります。そうでない場合は、インスタンスにリモート接続できません。

インターネットゲートウェイへの接続方法の詳細については、Amazon VPC ユーザーガイドの「[インターネットゲートウェイを使用してサブネットをインターネットに接続する](#)」を参照してください。

11. [自動割り当てパブリック IP] で、[有効化] を選択します。

公開 IP アドレス指定とプライベート IP アドレス指定の詳細については、「Amazon EC2 インスタンスユーザーガイド」の「[Amazon EC2 インスタンスの IP アドレス指定](#)」を参照してください。

12. [ファイアウォール (セキュリティグループ)] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
13. [ストレージの設定] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
14. [高度な詳細] セクションを選択し、[ドメイン結合ディレクトリ] ドロップダウンリストからドメインを選択します。

 Note

ドメイン結合ディレクトリを選択すると、次のようになります:

 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. 

このエラーは、EC2 起動ウィザードが予期しないプロパティを持つ既存の SSM ドキュメントを識別した場合に発生します。次のいずれかを試すことができます。

- 以前に SSM ドキュメントを編集し、プロパティの存在が予想される場合は、[閉じる] を選択して EC2 インスタンスを変更せずに起動します。
- ここで既存の SSM ドキュメントを削除するリンクを選択して、SSM ドキュメントを削除します。これにより、正しいプロパティを使用する SSM ドキュメントを作成できます。EC2 インスタンスを起動すると、SSM ドキュメントが自動的に作成されます。

15. [IAM インスタンスプロファイル] には、前提条件のセクションで以前に作成した IAM ロールを選択します ステップ 2: LinuxEC2DomainJoin ロールを作成します

16. [インスタンスを起動] を選択します。

Note

SUSE Linux でシームレスなドメイン結合を実行する場合は、認証が機能する前に再起動する必要があります。Linux ターミナルから SUSE を再起動するには、「sudo reboot」と入力します。

Amazon EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合する

この手順では、Amazon EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合します。これを行うには、EC2 Linux AWS Secrets Manager インスタンスを起動するアカウントの EC2 インスタンスロールに IAM 読み取りポリシーを作成します。この手順で、これは Account 2 と呼ばれます。このインスタンスは、Account 1 と呼ばれる他のアカウントから共有されている AWS Managed Microsoft AD を使用します。

前提条件

Amazon EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合する前に、以下を完了する必要があります。

- チュートリアルステップ 1~3、[チュートリアル: AWS Managed Microsoft AD ディレクトリを共有してシームレスな EC2 ドメイン結合を実現する](#)。このチュートリアルでは、ネットワークの設定と AWS Managed Microsoft AD の共有について説明します。
- [Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory にシームレスに結合する](#) に概説されている手順。

ステップ 1. アカウント 2 で LinuxEC2DomainJoin ロールを作成する

このステップでは、Account 2 にサインインした状態で IAM コンソールを使用し、EC2 Linux インスタンスをドメイン結合するための IAM ロールを作成します。

LinuxEC2DomainJoin ロールを作成する

1. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左のナビゲーションペインにある [アクセス管理] で、[ロール] を選択します。

3. [ロール] ページで、[ロールの作成] を選択してください。
4. 信頼されたエンティティの種類を選択 の下で、AWS サービス () を選択します。
5. [ユースケース] で [EC2] を選択し、[次へ] を選択します。
6. [Filter policies] (フィルターポリシー) で、以下を実行します。
 - a. AmazonSSMManagedInstanceCore と入力します。次に、リスト内のその項目のチェックボックスを選択します。
 - b. AmazonSSMDirectoryServiceAccess と入力してください。次に、リスト内のその項目のチェックボックスを選択します。
 - c. これらのポリシーを追加した後、[ロールを作成] を選択します。

 Note

AmazonSSMDirectoryServiceAccess は、によってActive Directory管理される にインスタンスを結合するためのアクセス許可を提供します AWS Directory Service。AmazonSSMManagedInstanceCoreは、を使用するために必要な最小限のアクセス許可を提供します AWS Systems Manager。これらのアクセス許可を使用してロールを作成する方法、および IAM ロールに割り当てることができるその他のアクセス許可とポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager に必要なインスタンスのアクセス許可を設定する](#)」を参照してください。

7. LinuxEC2DomainJoin[Role name] (ロール名) 欄 に、適宜の別の名前など 新しいロールの名前を入力します。
8. (選択可能) [ロールの説明] に、説明を入力します。
9. (選択可能) [ステップ 3: タグの追加] で [新しいタグの追加] を選択して、タグを追加します。タグのキーと値のペアは、このロールのアクセスを整理、追跡、または制御するために使用されます。
10. [ロールの作成] を選択してください。

ステップ 2. シー AWS Secrets Manager クレットを共有するためのクロスアカウントリソースアクセスを作成する

次のセクションでは、EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合するために満たす必要がある追加要件について説明します。これらの要件には、リソースポリシーの作成と、適切なサービスとリソースへのアタッチが含まれます。

アカウントのユーザーが別のアカウントの AWS Secrets Manager シークレットにアクセスできるようにするには、リソースポリシーと ID ポリシーの両方でアクセスを許可する必要があります。このタイプのアクセスは「[クロスアカウントリソースアクセス](#)」と呼ばれます。

このタイプのアクセスは、シークレットと同じアカウントのアイデンティティにアクセスを許可することとは異なります。また、シークレットの暗号化に使用されている [AWS Key Management Service](#) (KMS) キーをアイデンティティでできるようにする必要があります。クロスアカウントアクセスに AWS マネージドキー (aws/secretsmanager) を使用できないため、このアクセス許可が必要です。代わりに、作成した KMS キーを使用してシークレットを暗号化し、キーポリシーをそれにアタッチする必要があります。シークレットの暗号化キーを変更するには、「[AWS Secrets Manager シークレットを変更する](#)」を参照してください。

Note

使用するシークレットに応じて AWS Secrets Manager、に関連する料金が発生します。現在の価格の詳細なリストについては、「[AWS Secrets Manager 料金表](#)」を参照してください。Secrets Manager AWS マネージドキー aws/secretsmanager が作成する を使用して、シークレットを無料で暗号化できます。シークレットを暗号化するために独自の KMS キーを作成すると、は現在の KMS AWS レートで AWS 課金します。詳細については、「[AWS Key Management Service 料金](#)」を参照してください。

次の手順では、ユーザーが EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合できるようにするリソースポリシーを作成できます。

アカウント 1 のシークレットにリソースポリシーをアタッチします。

1. Secrets Manager のコンソール (<https://console.aws.amazon.com/secretsmanager/>) を開きます。
2. シークレットのリストから、[前提条件](#) の間に作成した [シークレット] を選択します。
3. [概要] タブの [シークレットの詳細ページ] で、[リソースアクセス許可] までスクロールダウンします。
4. [アクセス許可を編集する] を選択します。
 - ポリシーフィールドに次のポリシーを入力します。次のポリシーでは、Account 2 の [LinuxEC2DomainJoin] が Account 1 のシークレットにアクセスすることを許可しています。ARN 値を、「[ステップ 1](#)」で作成した LinuxEC2DomainJoin ロールである

Account 2 の ARN 値に置き換えます。このポリシーを使用するには、「[AWS Secrets Manager シークレットにアクセス許可ポリシーをアタッチする](#)」を参照してください。

```
{
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::Account2:role/LinuxEC2DomainJoin"
      },
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "*"
    }
  ]
}
```

Account 1 の KMS キーのキーポリシーにステートメントを追加します。

1. Secrets Manager のコンソール (<https://console.aws.amazon.com/secretsmanager/>) を開きます。
2. 左のナビゲーションバーで、[カスタマーマネージドキー] を選択します。
3. [カスタマーマネージドキー] ページで、作成したキーを選択します。
4. [キーの詳細] ページで、[キーポリシー] に移動し、[編集] を選択します。
5. 次のキーポリシーステートメントにより、Account 2 の ApplicationRole が Account 1 で KMS キーを使用して Account 1 のシークレットを復号化できるようにします。このステートメントを使用するには、それを KMS キーのキーポリシーに追加します。詳細については、[キーポリシーの変更](#)を参照してください。

```
{
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::Account2:role/ApplicationRole"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ]
}
```



```
],  
  "Resource": "*" }  
}
```

Account 2 のアイデンティティにアイデンティティポリシーを作成する

1. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. 左のナビゲーションペインにある [アクセス管理] で、[ポリシー] を選択します。
3. [ポリシーの作成] を選択します。[ポリシーエディター] で、[JSON] を選択します。
4. 次のポリシーにより、Account 2 の ApplicationRole が Account 1 のシークレットにアクセスし、同じく Account 1 にある暗号化キーを使用してシークレットの値を復号化できるようになります。Secrets Manager コンソールで、[シークレットの詳細] ページの [シークレットの ARN] の下に、シークレットの ARN を見つけられます。または、[describe-secret](#) を呼び出してシークレットの ARN を識別することもできます。リソース ARN をシークレット ARN と Account 1 のリソース ARN に置き換えます。このポリシーを使用するには、「[AWS Secrets Manager シークレットにアクセス許可ポリシーをアタッチする](#)」を参照してください。

```
{  
  {  
    "Version" : "2012-10-17",  
    "Statement" : [  
      {  
        "Effect": "Allow",  
        "Action": "secretsmanager:GetSecretValue",  
        "Resource": "SecretARN"  
      },  
      {  
        "Effect": "Allow",  
        "Action": [  
          "kms:Decrypt",  
          "kms:Describekey"  
        ],  
        "Resource": "arn:aws:kms:Region:Account1:key/Your_Encryption_Key"  
      }  
    ]  
  }  
}
```

5. [次へ] を選択し、[変更の保存] を選択します。

6. [Attach a resource policy to the secret in Account 1](#) の Account 2 で作成したロールを検索して選択します。
7. [アクセス許可を追加する] の下で、[ポリシーを追加する] を選択します。
8. 検索バーで、[Add a statement to the key policy for the KMS key in Account 1](#) で作成したポリシーを検索し、チェックボックスを選択してポリシーをロールに追加します。[アクセス許可を追加する] を選択します。

ステップ 3. Linux インスタンスをシームレスに結合する

次の手順を使用して、EC2 Linux インスタンスを共有 AWS Managed Microsoft AD にシームレスに結合できるようになりました。

Linux インスタンスをシームレスに結合するには

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
2. ナビゲーションバーのリージョンセレクターから、既存のディレクトリ AWS リージョンと同じを選択します。
3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Linux EC2 インスタンスに使用する名前を入力します。
5. (選択可能) [補足タグを追加] で、タグとキーの値のペアを 1 つまたは複数追加して、この EC2 インスタンスのアクセスを整理、追跡、またはコントロールします。
6. Application and OS Image (Amazon Machine Image) セクションで、起動したい Linux AMI を選択します。

Note

使用する AMI には AWS Systems Manager、(SSM Agent) バージョン 2.3.1644.0 以降が必要です。その AMI からインスタンスを起動して AMI にインストールされている SSM Agent のバージョンを確認するには、「[現在インストールされている SSM Agent バージョンを取得するには](#)」を参照してください。SSM Agent をアップグレードする必要がある場合は、「[Linux の EC2 インスタンスで SSM Agent をインストールして設定する](#)」を参照してください。

SSM は Linux インスタンスを Active Directory ドメインに結合する際にプラグイン `aws:domainJoin` を使用します。プラグインは、Linux インスタンスのホスト名を `EC2AMAZ-XXXXXX` の形式に変更します。`aws:domainJoin`の詳細については、[AWS Systems Manager ユーザーガイド]の「[AWS Systems Manager コマンド・ドキュメント・プラグイン・リファレンス](#)」を参照してください。

7. [インスタンスタイプ] セクションで、[インスタンスタイプ] ドロップダウンリストから使用するインスタンスタイプを選択します。
8. [キーペア (ログイン)] セクションで、新しいキーペアを作成するか、既存のキーペアから選択します。新しいキーペアを作成するには、[新しいキーペアの作成] を選択します。キーペアの名前を入力し、[キーペアタイプ] と [プライベートキーファイル形式] のオプションを選択します。OpenSSH で使用できる形式でプライベートキーを保存するには、[.pem] を選択します。プライベートキーを PuTTY で使用できる形式で保存するには、[.ppk] を選択します。[キーペアの作成] を選択します。ブラウザによって秘密キーファイルが自動的にダウンロードされます。ダウンロードしたプライベートキーのファイルを安全な場所に保存します。

 Important

プライベートキーのファイルを保存できるのはこのタイミングだけです。

9. [インスタンスを起動する] ページの [ネットワーク設定] セクションで、[編集] を選択します。[VPC に必須の] ドロップダウンリストから、ディレクトリが作成された [VPC] を選択します。
10. [サブネット] ドロップダウンリストから VPC 内のパブリックサブネットの 1 つを選択します。選択するサブネットで、すべての外部トラフィックがインターネットゲートウェイにルーティングされるように選択する必要があります。そうでない場合は、インスタンスにリモート接続できません。

インターネットゲートウェイへの接続方法の詳細については、Amazon VPC ユーザーガイドの「[インターネットゲートウェイを使用してサブネットをインターネットに接続する](#)」を参照してください。

11. [自動割り当てパブリック IP] で、[有効化] を選択します。

公開 IP アドレス指定とプライベート IP アドレス指定の詳細については、「Amazon EC2 インスタンスユーザーガイド」の「[Amazon EC2 インスタンスの IP アドレス指定](#)」を参照してください。

12. [ファイアウォール (セキュリティグループ)] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。

13. [ストレージの設定] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
14. [高度な詳細] セクションを選択し、[ドメイン結合ディレクトリ] ドロップダウンリストからドメインを選択します。

 Note

ドメイン結合ディレクトリを選択すると、次のようになります:

 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. 

このエラーは、EC2 起動ウィザードが予期しないプロパティを持つ既存の SSM ドキュメントを識別した場合に発生します。次のいずれかを試すことができます。

- 以前に SSM ドキュメントを編集し、プロパティの存在が予想される場合は、[閉じる] を選択して EC2 インスタンスを変更せずに起動します。
- ここで既存の SSM ドキュメントを削除するリンクを選択して、SSM ドキュメントを削除します。これにより、正しいプロパティを使用する SSM ドキュメントを作成できます。EC2 インスタンスを起動すると、SSM ドキュメントが自動的に作成されます。

15. [IAMインスタンスプロファイル]には、前提条件のセクションで以前に作成したIAMロールを選択します ステップ2: LinuxEC2DomainJoinロールを作成します
16. [インスタンスを起動] を選択します。

 Note

SUSE Linux でシームレスなドメイン結合を実行する場合は、認証が機能する前に再起動する必要があります。Linux ターミナルから SUSE を再起動するには、「sudo reboot」と入力します。

Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合します。

Amazon EC2 Windows インスタンスに加えて、特定の Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD に結合することもできます。以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 ビット x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64 ビット x86)
- Ubuntu Server 18.04 LTS および Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

他の Linux ディストリビューションとバージョンも動作する可能性があります、まだテストされていません。

Linux インスタンスを AWS Managed Microsoft AD に結合する

Amazon Linux、CentOS、Red Hat、または Ubuntu インスタンスをディレクトリに結合するときは、先に、[Linux インスタンスをシームレスに結合する](#) で指定したとおりにインスタンスを起動する必要があります。

Important

次の手順は、正しく実行しないと、インスタンスに到達不可能になったり、インスタンスが使用できなくなったりする可能性があります。したがって、これらの手順を実行する前に、バックアップを作成するか、インスタンスのスナップショットを作成することを強くお勧めします。

Linux インスタンスをディレクトリに結合するには

個々の Linux インスタンスについて、次のいずれかのタブの手順に従います。

Amazon Linux

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. Amazon Linux - 64 bit インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な Amazon Linux パッケージを Linux インスタンスにインストールします。

Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli  
krb5-workstation
```

Note

使用している Amazon Linux のバージョンを確認する方法については、「[Amazon EC2 Linux インスタンス用ユーザーガイド](#)」の「Identifying Amazon Linux images」(Amazon Linux イメージの特定) を参照してください。

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

ドメイン結合権限を持つ *example.com* ドメインのアカウント。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...  
* Successfully enrolled machine in realm
```

6. SSH サービスを設定して、パスワード認証を許可します。

- a. テキストエディタで `/etc/ssh/sshd_config` ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. `PasswordAuthentication` 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

7. インスタンスが再起動したら、任意の SSH クライアントを使用してインスタンスに接続し、次の手順を実行して AWS 委任管理者グループを `sudoers` リストに追加します。

- a. 次のコマンドを使用して `sudoers` ファイルを開きます。


```
sudo visudo
```

- b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

CentOS

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. CentOS 7 インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な CentOS 7 パッケージを Linux インスタンスにインストールします。

Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

ドメイン結合権限を持つ *example.com* ドメインのアカウント。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...  
* Successfully enrolled machine in realm
```

6. SSH サービスを設定して、パスワード認証を許可します。

- a. テキストエディタで `/etc/ssh/sshd_config` ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. `PasswordAuthentication` 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

7. インスタンスが再起動したら、任意の SSH クライアントを使用してインスタンスに接続し、次の手順を実行して AWS 委任管理者グループを `sudoers` リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

Red Hat

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. Red Hat - 64 bit インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な Red Hat パッケージを Linux インスタンスにインストールします。

Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -v -U join_account example.com --install=/  
  
join_account
```

ドメイン結合権限を持つ example.com ドメインのアカウントの *sAMAccountName*。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...  
* Successfully enrolled machine in realm
```

6. SSH サービスを設定して、パスワード認証を許可します。

- a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

7. インスタンスが再起動したら、任意の SSH クライアントを使用してインスタンスに接続し、次の手順を実行して AWS 委任管理者グループを sudoers リストに追加します。

- a. 次のコマンドを使用して `sudoers` ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を `sudoers` ファイルの下部に追加して保存します。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

SUSE

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの DNS サーバー IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定する場合は、AWS ナレッジセンターの「How [do I assign a static DNS server to a private Amazon EC2 instance](#)」を参照して、特定の Linux ディストリビューションとバージョンの永続 DNS サーバーを設定する方法を確認してください。
3. SUSE Linux 15 インスタンスが最新であることを確認します。
 - a. パッケージリポジトリを接続します。

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

- b. SUSE を更新します。

```
sudo zypper update -y
```

4. 必要な SUSE Linux 15 パッケージを Linux インスタンスにインストールします。

Note

これらのパッケージの一部が既にインストールされている可能性があります。

パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままで構いません。

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
```

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account example.com --verbose
```

join_account

ドメイン結合権限を持つ *example.com* ドメインの sAMAccountName。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

次の両方の戻り値が想定されることに注意してください。

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. SSSD を PAM で、手動で有効化します。

```
sudo pam-config --add --sss
```

7. nsswitch.conf を編集して nsswitch.conf の SSSD を有効にする

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
```

```
shadow: compat sss
```

8. /etc/pam.d/common-session に次の行を追加し、最初のログイン時にホームディレクトリを自動的に作成します。

```
sudo vi /etc/pam.d/common-session
```

```
session optional          pam_mkhomedir.so skel=/etc/skel umask=077
```

9. インスタンスを再起動して、ドメイン結合プロセスを完了します。

```
sudo reboot
```

10. 任意の SSH クライアントを使用してインスタンスに再接続し、ドメイン結合が正常に完了したことを確認し、追加の手順を完了します。

- a. インスタンスがドメインに登録済みであることを確認するには

```
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. SSSD デーモンのステータスを確認するには

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
  Loaded: loaded (/usr/lib/systemd/system/sss.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/sss.service
        ##479 /usr/sbin/sss -i --logger=files
        ##505 /usr/lib/sss/sss_be --domain example.com --uid 0 --gid 0 --
logger=files
        ##548 /usr/lib/sss/sss_nss --uid 0 --gid 0 --logger=files
        ##549 /usr/lib/sss/sss_pam --uid 0 --gid 0 --logger=files
```

11 SSH とコンソールを介したアクセスをユーザーに許可するには

```
sudo realm permit join_account@example.com
```

SSH とコンソールを介したアクセスをドメイングループに許可するには

```
sudo realm permit -g 'AWS Delegated Administrators'
```

または、すべてのユーザーにアクセスを許可するには

```
sudo realm permit --all
```

12 SSH サービスを設定して、パスワード認証を許可します。

- テキストエディタで `/etc/ssh/sshd_config` ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

13.13. インスタンスが再起動したら、任意の SSH クライアントを使用してインスタンスに接続し、次の手順を実行して AWS 委任管理者グループを sudoers リストに追加します。

a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "Domain Admins" group from the awsad.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. Ubuntu - 64 bit インスタンスが最新であることを確認します。

```
sudo apt-get update  
sudo apt-get -y upgrade
```

4. 必要な Ubuntu パッケージを Linux インスタンスにインストールします。

Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 逆引き DNS 解決を無効にし、デフォルトのレルムをドメインの FQDN に設定します。Ubuntu インスタンスは、レルムが稼働する前に DNS で逆引き解決可能になっている必要があります。なっていない場合、次のように /etc/krb5.conf で逆引き DNS を無効にする必要があります。

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

ドメイン結合権限を持つ example.com ドメインのアカウントの *sAMAccountName*。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...
* Successfully enrolled machine in realm
```

7. SSH サービスを設定して、パスワード認証を許可します。

- a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

8. インスタンスが再起動したら、任意の SSH クライアントを使用してインスタンスに接続し、次の手順を実行して AWS 委任管理者グループを `sudoers` リストに追加します。

- a. 次のコマンドを使用して `sudoers` ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を `sudoers` ファイルの下部に追加して保存します。

```
## Add the "AWS Delegated Administrators" group from the example.com domain.  
%AWS\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

アカウントのログインアクセスの制限

デフォルトでは、すべてのアカウントは Active Directory で定義されているため、ディレクトリのすべてのユーザーがインスタンスにログインできます。sssd.conf の `ad_access_filter` を使用して、特定のユーザーのみにインスタンスへのログインを許可できます。例:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

ユーザーは、特定のグループのメンバーである場合にのみ、インスタンスへのアクセスを許可されることを示しています。

cn

アクセス権限のあるグループの共通名。この例では、グループ名は、*admins* です。

ou

これは、上記のグループが配置される組織単位です。この例では、OU は、*Testou* です。

dc

これは、ドメインのドメインコンポーネントです。この例では、*example* です。

dc

これは、追加のドメインコンポーネントです。この例では、*com* です。

`ad_access_filter` を手動で `/etc/sss/sss.conf` に追加する必要があります。

テキストエディタで `/etc/sss/sss.conf` ファイルを開きます。

```
sudo vi /etc/sss/sss.conf
```

この操作を行った後、`sss.conf` は次のようになります。

```
[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)
```

設定を有効にするには、`sss` サービスを次のように再起動する必要があります。

```
sudo systemctl restart sssd.service
```

または、次のコマンドを使用できます。

```
sudo service sssd restart
```

デフォルトでは、すべてのアカウントは Active Directory で定義されているため、ディレクトリのすべてのユーザーがインスタンスにログインできます。sssd.conf の `ad_access_filter` を使用して、特定のユーザーのみにインスタンスへのログインを許可できます。

例:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

ユーザーは、特定のグループのメンバーである場合にのみ、インスタンスへのアクセスを許可されることを示しています。

cn

アクセス権限のあるグループの共通名。この例では、グループ名は、*admins* です。

ou

これは、上記のグループが配置される組織単位です。この例では、OU は、*Testou* です。

dc

これは、ドメインのドメインコンポーネントです。この例では、*example* です。

dc

これは、追加のドメインコンポーネントです。この例では、*com* です。

`ad_access_filter` を手動で `/etc/sssds/sssds.conf` に追加する必要があります。

1. テキストエディタで `/etc/sssds/sssds.conf` ファイルを開きます。

```
sudo vi /etc/sssds/sssds.conf
```

2. この操作を行った後、`sssds.conf` は次のようになります。

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admin,ou=Testou,dc=example,dc=com)
```

3. 設定を有効にするには、sssd サービスを次のように再起動する必要があります。

```
sudo systemctl restart sssd.service
```

または、次のコマンドを使用できます。

```
sudo service sssd restart
```

ID マッピング

ID マッピングは 2 つの方法で実行でき、UNIX/Linux ユーザー識別子 (UID) とグループ識別子 (GID)、Windows ID と Active Directory セキュリティ識別子 (SID) の ID 間の統一されたエクスペリエンスを維持できます。これらのメソッドは次のとおりです。

1. 一元化
2. 分散型

 Note

Active Directory での集中型ユーザーアイデンティティマッピングには、ポータブルオペレーティングシステムインターフェイス (POSIX) が必要です。

一元化されたユーザ ID マッピング

Active Directory または別の Lightweight Directory Access Protocol (LDAP) サービスは Linux ユーザーに UID と GID を提供します。では Active Directory、POSIX 拡張機能が設定されている場合、これらの識別子はユーザーの属性に保存されます。

- UID-Linux ユーザー名 (文字列)
- UID 番号-Linux ユーザー ID 番号 (整数)
- GID 番号-Linux グループ ID 番号 (整数)

Active Directory の UID と GID を使用するように Linux インスタンスを設定するには、`sssd.conf` ファイルに `ldap_id_mapping = False` を設定します。この値を設定する前に、UID、UID 番号、および GID 番号が Active Directory 内のユーザーとグループに追加されていることを確認してください。

分散型ユーザー ID マッピング

Active Directory に POSIX 拡張がない場合や、ID マッピングを集中的に管理しないことを選択した場合、Linux は UID と GID の値を計算できます。Linux はユーザー固有のセキュリティ識別子 (SID) を使用して一貫性を保ちます。

分散ユーザー ID マッピングを設定するには、`ldap_id_mapping = True` `sssd.conf` ファイルで設定します。

一般的な問題

を設定すると `ldap_id_mapping = False`、SSSD サービスの開始が失敗することがあります。この失敗の理由は、UIDs の変更がサポートされていないためです。ID マッピングから POSIX 属性、または POSIX 属性から ID マッピングに変更するたびに、SSSD キャッシュを削除することをお勧めします。ID マッピングと `ldap_id_mapping` パラメータの詳細については、Linux コマンドラインで「`sssd-ldap(8) man`」ページを参照してください。

Linux インスタンスへの接続

ユーザーの SSH クライアントを使用してインスタンスに接続し、ユーザー名の入力が求められます。ユーザーは、username@example.com または EXAMPLE\username のいずれかの形式でユーザー名を入力することができます。使用している Linux ディストリビューションに応じて、レスポンスは次のように表示されます。

Amazon Linux、Red Hat Enterprise Linux、および 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%

Winbind を使用して Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合する

Winbind サービスを使用して、Amazon EC2Linux インスタンスを AWS Managed Microsoft AD ドメインに手動で結合できます。これにより、既存のオンプレミス Active Directory ユーザーは、AWS Managed Microsoft AD Active Directory に参加している Linux インスタンスにアクセスするときに Active Directory 認証情報を使用できます。以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 ビット x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64 ビット x86)
- Ubuntu Server 18.04 LTS および Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

他の Linux ディストリビューションとバージョンも動作する可能性がありますが、まだテストされていません。

Linux インスタンスを AWS Managed Microsoft AD Active Directory に結合する

Important

次の手順は、正しく実行しないと、インスタンスに到達不可能になったり、インスタンスが使用できなくなったりする可能性があります。したがって、これらの手順を実行する前に、バックアップを作成するか、インスタンスのスナップショットを作成することを強くお勧めします。

Linux インスタンスをディレクトリに結合するには

個々の Linux インスタンスについて、次のいずれかのタブの手順に従います。

Amazon Linux/CENTOS/REDHAT

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの DNS サーバー IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定する場合は、AWS ナレッジセンターの「[How do I assign a static DNS server to a private Amazon EC2 instance](#)」を参照して、特定の Linux ディストリビューションとバージョンの永続 DNS サーバーを設定する方法を確認してください。
3. Linux インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な Samba / Winbind パッケージを Linux インスタンスにインストールします。

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
```

5. 障害が発生した場合に元に戻せるよう、メインの smb.conf ファイルのバックアップを作成します。

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 元の設定ファイル [/etc/samba/smb.conf] をテキストエディタで開きます。

```
sudo vim /etc/samba/smb.conf
```

次の例に示すように、Active Directory ドメイン環境情報を入力します。

```
[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. テキストエディタでホストファイル [/etc/hosts] を開きます。

```
sudo vim /etc/hosts
```

Linux インスタンスのプライベート IP アドレスを次のように追加します。

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

/etc/hosts ファイルで IP アドレスを指定しなかった場合、インスタンスをドメインに結合しているときに次の DNS エラーが発生することがあります。

No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER

このエラーは、結合は成功したが、[net ads] コマンドが DNS レコードを DNS に登録できなかったことを意味します。

8. net ユーティリティを使用して Linux インスタンスを Active Directory に結合します。

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

ドメイン結合権限を持つ *example.com* ドメインのアカウント。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
Enter join_account@example.com's password:
Using short domain name -- example
```

```
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. PAM 設定ファイルを変更します。以下のコマンドを使用して、winbind 認証に必要なエントリを追加します。

```
sudo authconfig --enablewinbind --enablewinbindauth --enablemkhomedir --update
```

10. /etc/ssh/sshd_config ファイルを編集して、SSH サービスを設定し、パスワード認証を許可します。

- a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

11. インスタンスが再起動したら、任意の SSH クライアントを使用してこれに接続し、次の手順を実行してドメインユーザーまたはグループのルート権限を sudoers リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 信頼するドメインまたは信頼されたドメインから必要なグループまたはユーザーを次のように追加し、保存します。

```
## 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
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

SUSE

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの DNS サーバー IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定する場合は、AWS ナレッジセンターの「How [do I assign a static DNS server to a private Amazon EC2 instance](#)」を参照して、特定の Linux ディストリビューションとバージョンの永続 DNS サーバーを設定する方法を確認してください。
3. SUSE Linux 15 インスタンスが最新であることを確認します。
 - a. パッケージリポジトリに接続します。

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

- b. SUSE を更新します。

```
sudo zypper update -y
```

4. 必要な Samba / Winbind パッケージを Linux インスタンスにインストールします。

```
sudo zypper in -y samba samba-winbind
```

5. 障害が発生した場合に元に戻せるよう、メインの smb.conf ファイルのバックアップを作成します。

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 元の設定ファイル [/etc/samba/smb.conf] をテキストエディタで開きます。

```
sudo vim /etc/samba/smb.conf
```

次の例に示すように、Active Directory ドメイン環境情報を入力します。

```
[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. テキストエディタでホストファイル [/etc/hosts] を開きます。

```
sudo vim /etc/hosts
```

Linux インスタンスのプライベート IP アドレスを次のように追加します。

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

/etc/hosts ファイルで IP アドレスを指定しなかった場合、インスタンスをドメインに結合しているときに次の DNS エラーが発生することがあります。

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

このエラーは、結合は成功したが、[net ads] コマンドが DNS レコードを DNS に登録できなかったことを意味します。

8. 次のコマンドを使用して Linux インスタンスをディレクトリに結合します。

```
sudo net ads join -U join_account@example.com
```

join_account

ドメイン結合権限を持つ *example.com* ドメインの sAMAccountName。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
Enter join_account@example.com's password:  
Using short domain name -- example  
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. PAM 設定ファイルを変更します。以下のコマンドを使用して、Winbind 認証に必要なエントリを追加します。

```
sudo pam-config --add --winbind --mkhomedir
```

- 10 Name Service Switch 設定ファイル [/etc/nsswitch.conf] をテキストエディタで開きます。

```
vim /etc/nsswitch.conf
```

以下に示すように Winbind ディレクティブを追加します。

```
passwd: files winbind  
shadow: files winbind  
group: files winbind
```

- 11 /etc/ssh/sshd_config ファイルを編集して、SSH サービスを設定し、パスワード認証を許可します。

- a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vim /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

12. インスタンスが再起動したら、任意の SSH クライアントを使用してこれに接続し、次の手順を実行してドメインユーザーまたはグループのルート権限を sudoers リストに追加します。

a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

b. 信頼するドメインまたは信頼されたドメインから必要なグループまたはユーザーを次のように追加し、保存します。

```
## 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
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

Ubuntu

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Service が提供する DNS サーバーの DNS サーバー IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定する場合は、AWS ナレッジセンターの「[How do I assign a static DNS server to a private Amazon EC2 instance](#)」を参照して、特定の Linux ディストリビューションとバージョンの永続 DNS サーバーを設定する方法を確認してください。
3. Linux インスタンスが最新であることを確認します。

```
sudo apt-get -y upgrade
```

4. 必要な Samba / Winbind パッケージを Linux インスタンスにインストールします。

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. 障害が発生した場合に元に戻せるよう、メインの `smb.conf` ファイルのバックアップを作成します。

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 元の設定ファイル [/etc/samba/smb.conf] をテキストエディタで開きます。

```
sudo vim /etc/samba/smb.conf
```

次の例に示すように、Active Directory ドメイン環境情報を入力します。

```
[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. テキストエディタでホストファイル [/etc/hosts] を開きます。

```
sudo vim /etc/hosts
```

Linux インスタンスのプライベート IP アドレスを次のように追加します。

```
10.x.x.x Linux_hostname.example.com Linux_hostname
```

Note

/etc/hosts ファイルで IP アドレスを指定しなかった場合、インスタンスをドメインに結合しているときに次の DNS エラーが発生することがあります。

```
No DNS domain configured for linux-instance. Unable to perform
DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER
```

このエラーは、結合は成功したが、[net ads] コマンドが DNS レコードを DNS に登録できなかったことを意味します。

8. net ユーティリティを使用して Linux インスタンスを Active Directory に結合します。

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

ドメイン結合権限を持つ *example.com* ドメインのアカウント。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
Enter join_account@example.com's password:  
Using short domain name -- example  
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. PAM 設定ファイルを変更します。以下のコマンドを使用して、Winbind 認証に必要なエントリを追加します。

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

- 10 Name Service Switch 設定ファイル [/etc/nsswitch.conf] をテキストエディタで開きます。

```
vim /etc/nsswitch.conf
```

以下に示すように Winbind ディレクティブを追加します。

```
passwd: compat winbind  
group:  compat winbind  
shadow: compat winbind
```

- 11 /etc/ssh/sshd_config ファイルを編集して、SSH サービスを設定し、パスワード認証を許可します。

- a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vim /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

12. インスタンスが再起動したら、任意の SSH クライアントを使用してこれに接続し、次の手順を実行してドメインユーザーまたはグループのルート権限を sudoers リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 信頼するドメインまたは信頼されたドメインから必要なグループまたはユーザーを次のように追加し、保存します。

```
## 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
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

Linux インスタンスへの接続

ユーザーの SSH クライアントを使用してインスタンスに接続し、ユーザー名の入力が求められます。ユーザーは、username@example.com または EXAMPLE\username のいずれかの形式でユー

ザー名を入力することができます。使用している Linux ディストリビューションに応じて、レスポンスは次のように表示されます。

Amazon Linux、Red Hat Enterprise Linux、および 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%		

Amazon EC2 Mac インスタンスを AWS Managed Microsoft AD に結合する Active Directory

この手順では、Amazon EC2 Mac インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合します。

前提条件

- Amazon EC2 Mac インスタンスには[Amazon EC2 専用ホスト](#)が必要です。専用ホストを割り当て、そのホスト上でインスタンスを起動する必要があります。詳細については、「Amazon EC2 ユーザーガイド」の「[Mac インスタンスを起動する](#)」を参照してください。
- AWS Managed Microsoft AD Active Directory の DHCP オプションセットを作成することをお勧めします。これにより、Amazon VPC 内のすべてのインスタンスで指定のドメインおよび DNS サーバーを参照し、ドメイン名を解決できるようになります。詳細については「[AWS Managed Microsoft AD の DHCP オプションセットの作成または変更](#)」を参照してください。

Note

このリソースの整理、またはアクセスの制御に使用されるタグ。詳細については、「Amazon EC2 ユーザーガイド」の「[料金と請求](#)」を参照してください。

Mac インスタンスを手動で結合する

- インスタンスに接続するには、次のSSHコマンドを使用して、Macインスタンスに接続します。詳細については、「Mac インスタンスへの接続」または「[Mac インスタンスへの接続](#)」を参照してください。

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

- Mac インスタンスに接続したら、以下のコマンドを使用して **ec2-user** アカウントのパスワードを作成します。

```
sudo passwd ec2-user
```

- コマンドラインでプロンプトが表示されたら、**ec2-user** アカウントのパスワードを入力します。オペレーティングシステムとソフトウェアを更新するには、「Amazon EC2 ユーザーガイド」の「[オペレーティングシステムとソフトウェアの更新](#)」の手順に従います。

- 次の ***dsconfigad*** コマンドを使用して、Mac インスタンスを AWS Managed Microsoft AD Active Directory ドメインに結合します。ドメイン名、コンピュータ名、組織単位を AWS Managed Microsoft AD Active Directory ドメイン情報に置き換えてください。詳細については、Apple Web サイトの [Mac のディレクトリユーティリティの「ドメインアクセスの設定」](#) を参照してください。

⚠ Warning

コンピュータ名にはハイフンを含めないでください。ハイフンは AWS Managed Microsoft AD Active Directory へのバインドを妨げる場合があります。

```
sudo dsconfigad -add domainName -computer computerName -username Username -  
ou "Your-AWS-Delegated-Organizational-Unit"
```

次の例は、ドメインに指定された名前の Mac **myec2mac01 example.com** インスタンスの管理ユーザーに参加させる場合のコマンドの外観を示しています。

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -  
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

- 以下のコマンドを使用して、Mac AWS インスタンスの管理ユーザーに委任管理者を追加します。

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators"
```

- 次のコマンドを使用して、AWS Managed Microsoft AD Active Directory ドメイン結合が成功したことを確認します。

```
dsconfigad -show
```

Mac インスタンスが AWS Managed Microsoft AD Active Directory に正常に参加しました。AWS Managed Microsoft AD Active Directory 認証情報を使用して Mac インスタンスにログインできるようになりました。

Mac インスタンスに初めてログインすると、「その他」ユーザーとしてログインするオプションが表示されるはずです。この時点で、Active Directory ドメイン認証情報を使用して Mac インスタン

スにログインできます。これらの手順を完了してもログイン画面に「その他」が表示されない場合は、ec2-user としてログインしてからログアウトします。

ドメインユーザーのグラフィカルユーザーインターフェイスを使用してログインするには、「Amazon EC2 ユーザーガイド」の「[インスタンスのグラフィカルユーザーインターフェイス \(GUI\) への接続](#)」の手順に従います。

AWS Managed Microsoft AD のディレクトリ結合権限を委任する

コンピュータを AWS Managed Microsoft AD に結合するには、コンピュータを ディレクトリに結合する権限を持つアカウントが必要です。

AWS Directory Service for Microsoft Active Directory では、管理者グループとAWS 委任サーバー管理者グループのメンバーにこれらの権限があります。

ただし、ベストプラクティスとして、必要な最小限の権限のみを持つアカウントを使用してください。次の手順は、Joiners という新しいグループを作成し、コンピュータをディレクトリに結合するために必要な権限をこのグループに委任する方法を示しています。

この手順は、ディレクトリに結合され、[Active Directory User and Computers] (Active Directory ユーザーとコンピュータ) MMC スナップインがインストールされたコンピュータで実行する必要があります。また、ドメイン管理者としてログインする必要があります。

AWS Managed Microsoft AD の参加権限を委任するには

1. [Active Directory ユーザーとコンピュータ] を開き、ナビゲーションツリーに NetBIOS 名が表示されている組織単位 (OU) を選択し、[ユーザー] OU を選択します。

Important

AWS Directory Service for Microsoft Active Directory を起動すると、 はディレクトリのすべてのオブジェクトを含む組織単位 (OU) AWS を作成します。この OU はドメインルートにあります。OU にはディレクトリを作成する際に入力した NetBIOS 名があります。ドメインルートは によって所有および管理されます AWS。ドメインルート自体に変更を加えることはできません。したがって、NetBIOS 名がある OU 内に **Joiners** グループを作成する必要があります。

2. [Users] (ユーザー) のコンテキスト (右クリック) メニューを開き、[New] (新規)、[Group] (グループ) の順に選択します。

3. [New Object - Group] (新しいオブジェクト - グループ) ボックスで、次の内容を入力し、[OK] をクリックします。
 - [Group name] (グループ名) に「**Joiners**」と入力します。
 - [Group scope] (グループのスコープ) で、[Global] (グローバル) を選択します。
 - [Group type] (グループの種類) で、[Security] (セキュリティ) を選択します。
4. ナビゲーションツリーで、NetBIOS 名の下の [Computers] (コンピュータ) コンテナを選択します。[Action] (アクション) メニューで、[Delegate Control] (制御の委任) を選択します。
5. [Delegation of Control Wizard] (制御の委任ウィザード) ページで、[Next] (次へ)、[Add] (追加) の順に選択します。
6. [Select Users, Computers, or Groups] (ユーザー、コンピュータ、またはグループの選択) ボックスで「Joiners」と入力し、[OK] をクリックします。複数のオブジェクトがある場合は、上記で作成した Joiners グループを選択します。[Next] (次へ) をクリックします。
7. [Tasks to Delegate] (委任するためのタスク) ページで、[Create a custom task to delegate] (委任するためのカスタムタスクを作成) を選択し、[Next] (次へ) をクリックします。
8. [Only the following objects in the folder] (フォルダ内の次のオブジェクトのみ) を選択し、[Computer objects] (コンピュータオブジェクト) を選択します。
9. [Create selected objects in this folder] (選択したオブジェクトをこのフォルダに作成) を選択し、[Delete selected objects in this folder] (このフォルダ内の選択したオブジェクトを削除) を選択します。続いて、[Next] (次へ) をクリックします。

The screenshot shows the 'Delegation of Control Wizard' window with the title bar 'Delegation of Control Wizard' and a close button. The main heading is 'Active Directory Object Type' with a subinstruction 'Indicate the scope of the task you want to delegate.' and a key icon. Below this, the 'Delegate control of:' section has two radio button options: 'This folder, existing objects in this folder, and creation of new objects in this folder' (unselected) and 'Only the following objects in the folder:' (selected). The selected option leads to a list box containing several object types with checkboxes: 'Computer objects' (checked), 'Connection objects' (unchecked), 'Contact objects' (unchecked), 'document objects' (unchecked), 'documentSeries objects' (unchecked), and 'domainRelatedObject objects' (unchecked). Below the list box, there are two checked checkboxes: 'Create selected objects in this folder' and 'Delete selected objects in this folder'. At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

10. [Read] (読み取り) と [Write] (書き込み) を選択し、[Next] (次へ) をクリックします。

The screenshot shows the 'Delegation of Control Wizard' window with the title bar 'Delegation of Control Wizard' and a close button. The main heading is 'Permissions' with a subinstruction 'Select the permissions you want to delegate.' and a key icon. Below this, the 'Show these permissions:' section has three checkboxes: 'General' (checked), 'Property-specific' (checked), and 'Creation/deletion of specific child objects' (unchecked). The 'Property-specific' checkbox is selected, leading to a 'Permissions:' list box. This list box contains several permissions with checkboxes: 'Full Control' (unchecked), 'Read' (checked), 'Write' (checked), 'Create All Child Objects' (unchecked), 'Delete All Child Objects' (unchecked), and 'Read All Properties' (unchecked). At the bottom, there are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

11. [Completing the Delegation of Control Wizard] (制御の委任の完了ウィザード) ページで情報を確認し、[Finish] (完了) を選択します。
12. 強力なパスワードでユーザーを作成し、そのユーザーを Joiners グループに追加します。このユーザーは、NetBIOS 名の下 [Users] (ユーザー) コンテナにある必要があります。このユーザーには、ディレクトリにインスタンスを接続するために十分な権限が与えられます。

AWS Managed Microsoft AD の DHCP オプションセットの作成または変更

AWS では、AWS Directory Service ディレクトリの DHCP オプションセットを作成し、ディレクトリがある VPC に DHCP オプションセットを割り当てることをお勧めします。これにより、VPC 内のすべてのインスタンスで指定のドメインおよび DNS サーバーを参照し、ドメイン名を解決できるようになります。

DHCP オプションセットの詳細については、「Amazon VPC ユーザーガイド」の「[DHCP options sets](#)」(DHCP オプションセット) を参照してください。

ディレクトリの DHCP オプションセットを作成するには

1. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
2. ナビゲーションペインで [DHCP Options Sets] (DHCP オプションセット) を選択し、[Create DHCP options set] (DHCP オプションセットの作成) を選択します。
3. [Create DHCP options set] (DHCP オプションセットの作成) ページで、ディレクトリの次の値を入力します。

名前

オプションセットのオプションタグ。

ドメイン名

ディレクトリの完全修飾名 (例: corp.example.com)。

ドメインネームサーバー

AWS指定したディレクトリの DNS サーバーの IP アドレス。

 Note

この IP アドレスは、[AWS Directory Service コンソール](#)のナビゲーションペインに移動し、[Directories] (ディレクトリ) を選択して正しいディレクトリ ID を選択すると確認できます。

NTP サーバー

このフィールドは空白のままにします。

NetBIOS ネームサーバー

このフィールドは空白のままにします。

NetBIOS ノードタイプ

このフィールドは空白のままにします。

4. [Create DHCP options set] を選択します。新しい DHCP オプションのセットが DHCP オプションの一覧に表示されます。
5. 新しい DHCP オプションセットの ID (dopt-**xxxxxxxx**) を書き留めておきます。これは、新しいオプションセットを VPC に関連付けるときに使用します。

VPC に関連付けられた DHCP オプションセットを変更するには

DHCP オプションセットを作成後に変更することはできません。VPC で異なる DHCP オプションセットを使用するには、新しいセットを作成して VPC に関連付ける必要があります。DHCP オプションを使用しないように VPC を設定することもできます。

1. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
2. ナビゲーションペインで、[Your VPCs (お使いの VPC)] を選択します。
3. VPC を選択して、[アクション]、[DHCP オプションセットの編集] を順番に選択します。
4. [DHCP options set] (DHCP オプションセット) で、オプションセットを選択するか、[No DHCP options set] (DHCP オプションセットなし) を選択し、[Save] (保存) をクリックします。

コマンドラインを使用して、VPC に関連付けられた DHCP オプションセットを変更するには、次の内容を参照してください:

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

AWS Managed Microsoft AD ユーザーとグループの管理

AWS Managed Microsoft AD でユーザーとグループを管理できます。ディレクトリにアクセスできる個人またはエンティティを表すユーザーを作成します。また、一度に複数のユーザーに許可を付与および拒否するグループを作成することもできます。ユーザーをグループに追加するだけでなく、グループをグループに追加することもできます。ユーザーをグループに追加すると、ユーザーはグループに割り当てられたロールとアクセス許可を継承します。グループにグループを追加すると、グループは親子関係を共有し、子グループは親グループに割り当てられたロールとアクセス許可を継承します。ユーザーのグループメンバーシップを別のユーザーにコピーすることもできます。

[the section called “Directory Service Data”](#) でユーザーとグループを管理するには、次の方法を使用します:

- [AWS Management Console](#)
- [AWS CLI](#)
- [AWS Directory Service Data API](#)
- [AWS Tools for Windows PowerShell](#)

AWS Directory Service Data CLI のデモについては、次のYouTube動画を参照してください。

[CRUD API を使用して AWS Managed Microsoft AD でユーザーとグループを管理する](#)

または、「[ドメイン結合インスタンス](#)」を使用することもできます。

AWS Management Consoleでユーザーとグループを管理する

AWS Directory Service Data を使用して AWS Management Console でユーザーとグループを管理できます。Directory Service Data は、組み込みオブジェクト管理タスクを実行する機能 AWS Directory Service を提供する の拡張機能です。これらのタスクには、ユーザーとグループの作成、グループへのユーザーの追加、グループへのグループの追加などがあります。

詳細については、「[AWS Management Consoleで AWS Managed Microsoft AD ユーザーとグループの管理](#)」を参照してください。

Note

この機能を使用するには、それを有効にする必要があります。詳細については、「[ユーザーおよびグループ管理の有効化](#)」を参照してください。

ディレクトリのプライマリ AWS Management Console AWS リージョン から 使用してのみ、ユーザーとグループを管理できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#) や などの AWS マネージドポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。

AWS CLIでユーザーとグループを管理する

[AWS Directory Service Data API](#) AWS CLI を使用して、でユーザーとグループを管理できます。Directory Service Data は、ds-data名前空間を使用して組み込みオブジェクト管理タスクを実行する機能 AWS Directory Service を提供する の拡張機能です。これらのタスクには、ユーザーとグループの作成、グループへのユーザーの追加、グループへのグループの追加などがあります。

AWS Directory Service Data CLI を使用してユーザーを作成する

以下は、ds-data名前空間を使用してユーザーを作成する AWS CLI コマンドの例です。

```
aws ds-data create-user --directory-id d-1234567890 --sam-account-name "jane.doe" --region your-Primary-Region-name
```

Note

これを使用するには AWS CLI、有効にする必要があります。詳細については、「[ユーザーとグループの管理または AWS Directory Service Data の有効化または無効化](#)」を参照してください。

ディレクトリのプライマリから AWS Directory Service Data CLI を使用してのみ、ユーザーとグループを管理 AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)やなどの AWS マネージドポリシーを使用できます。[AWSDirectoryServiceDataReadOnlyAccess](#)詳細については、[IAM のセキュリティのベストプラクティス](#)を参照してください。

詳細については、「[AWS CLIで AWS Managed Microsoft AD ユーザーとグループの管理](#)」を参照してください。

でユーザーとグループを管理する AWS Tools for PowerShell

[AWS Tools for PowerShell](#) には、(DS) と AWS Directory Service `AWS.Tools.DirectoryService (DSD)` の 2 つの管理用モジュール `AWS.Tools.DirectoryServiceData` があります。を使用する場合は AWS Directory Service、目的のオペレーションに適したモジュールを使用していることを確認してください。

- `DirectoryService` モジュールには、`Enable-DSDirectoryDataAccess`、`Disable-DSDirectoryDataAccess` と管理を管理するためのコマンドレットが含まれています `Reset-DSUserPassword`。
- `DirectoryServiceData` モジュールには、特にユーザーとグループの管理に焦点を当てた、ディレクトリ内でオペレーションを実行するためのコマンドレットが含まれています。これらの DSD コマンドレットには、ユーザー管理オペレーション (`New-DSDUser`、`Get-DSDUser`、`Update-DSDUser`、および `Remove-DSDUser`)、グループ管理オペレーション (`Get-DSDGroup`、`Update-DSDGroup`、`Remove-DSDGroup`)、グループメンバーシップ管理 (`Add-DSDGroupMember`、および `Remove-DSDGroupMember`)、検索機能 (`Search-DSDUser` および `Search-DSDGroup`) が含まれます。

オンプレミスインスタンスまたは Amazon EC2 インスタンスを使用してユーザーとグループを管理する

AWS Directory Service Data がユースケースをサポートしていない場合は、オンプレミスまたは EC2 インスタンスを使用してユーザーとグループを管理することをお勧めします。

AWS Managed Microsoft AD でユーザーとグループを作成するには、Managed Microsoft AD に結合された任意のインスタンス (オンプレミスまたは EC2) AWS を使用できます。また、ユーザーと

グループを作成する権限を持つユーザーとしてログインしている必要があります。インスタンスに Active Directory ツールをインストールする必要もあります。これにより、Active Directory ユーザーとコンピュータツールを使用してユーザーやグループを追加できます。

- Active Directory 管理 AWS Directory Service コンソールから、管理ツールがプリインストールされた事前設定済みの EC2 インスタンスをデプロイできます。詳細については、「[AWS Managed Microsoft AD Active Directory でディレクトリの管理インスタンスを起動する](#)」を参照してください。
- 管理ツールを使用してセルフマネージド EC2 インスタンスをデプロイし、必要なツールをインストールする必要がある場合は、「[ステップ 3: Amazon EC2 インスタンスをデプロイして AWS Managed Microsoft AD Active Directory を管理する](#)」を参照してください。

トピック

- [AWS Management ConsoleAWS CLIまたは を使用して AWS Managed Microsoft AD ユーザーとグループを管理する AWS Tools for PowerShell](#)
- [Amazon EC2 インスタンスを使用してユーザーとグループを管理する](#)

AWS Management ConsoleAWS CLIまたは を使用して AWS Managed Microsoft AD ユーザーとグループを管理する AWS Tools for PowerShell

、または を使用して AWS Management Console AWS CLI、AWS Managed Microsoft AD ユーザーとグループを で AWS Tools for PowerShell 管理できます[AWS Directory Service データ](#)。AWS Directory Service Data CLI は ds-data名前空間を使用します。の詳細については AWS CLI、「[の開始方法 AWS CLI](#)」を参照してください。詳細については AWS Tools for PowerShell、[AWS Tools for Windows PowerShell 「ユーザーガイド」](#)を参照してください。

AWS Managed Microsoft AD ユーザーとグループの作成、表示、更新、削除の詳細については、次の手順を参照してください。

ユーザーとグループの管理手順

- [ユーザーとグループの管理または AWS Directory Service Data の有効化または無効化](#)
- [AWS Managed Microsoft AD ユーザーの作成](#)
- [AWS Managed Microsoft AD ユーザーの表示と更新](#)
- [AWS Managed Microsoft AD ユーザーの削除](#)
- [AWS Managed Microsoft AD ユーザーの無効化](#)

- [AWS Managed Microsoft AD ユーザーのパスワードのリセットと有効化](#)
- [AWS Managed Microsoft AD グループの作成](#)
- [AWS Managed Microsoft AD グループの詳細の表示と更新](#)
- [AWS Managed Microsoft AD グループの削除](#)
- [グループへの AWS Managed Microsoft AD メンバーの追加と削除、グループへのグループの削除](#)
- [での AWS Managed Microsoft AD グループメンバーシップのコピー AWS Management Console](#)

ユーザーとグループの管理または AWS Directory Service Data の有効化または無効化

ユーザーとグループの管理または AWS Directory Service Data を使用するには、有効にする必要があります。有効にすると、AWS Management Console、AWS CLI、または からユーザーとグループを管理できます AWS Tools for PowerShell。

Important

- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data をサポートするリージョンのリストについては、「」を参照してください [Directory Service Data AWS リージョン でサポート](#)。
- AWS Directory Service Data のアクセスコントロールは、Amazon WorkSpaces、Amazon QuickSight、Amazon WorkMail AWS のサービス などの のアクセスコントロールとは異なります。詳細については、「[AWS Directory Service Data を使用したアプリケーション認可](#)」を参照してください。

AWS Directory Service Data の有効化

または を使用して、既存の AWS Managed Microsoft AD のユーザーとグループの管理または AWS Directory Service Data を有効にするには AWS Management Console AWS CLI、次の手順に従います AWS Tools for PowerShell。

AWS Management Console

AWS Management Consoleを使用して、ユーザーとグループの管理を有効にできます。

ユーザーとグループの管理を有効にするには

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. [ディレクトリの詳細] ページで、ユーザーとグループの管理を有効にするには、[有効にする] を選択します。
3. [ユーザーとグループの管理を有効にする] ダイアログボックスで、[有効にする] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を有効にするリクエストをフォーマットする方法について説明します。ディレクトリ ID 番号をリクエストに含める必要があります。

Note

AWS ディレクトリサービスデータを有効にする CLI コマンドは `aws ds` を使用します。

AWS Directory Service Data CLI を有効にするには

- を開き AWS CLI、次のコマンドを実行して、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

```
aws ds enable-directory-data-access --directory-id d-1234567890
```

AWS Tools for PowerShell

Tools for PowerShell で Directory Service Data を有効にするには

- を開き PowerShell、次のコマンドを実行して、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

```
Enable-DSDirectoryDataAccess -DirectoryId d-1234567890
```

AWS Directory Service データの無効化

または を使用して、既存の AWS Managed Microsoft AD のユーザーとグループの管理または AWS Directory Service Data を無効にするには AWS Management Console AWS CLI、次の手順に従います AWS Tools for PowerShell。

AWS Management Console

AWS Management Consoleを使用して、ユーザーとグループの管理を無効にできます。

ユーザーとグループの管理を無効にするには

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ユーザーとグループの管理を無効にするには、[ディレクトリの詳細] ページで [無効にする] を選択します。
3. [ユーザーとグループの管理を無効にする] ダイアログボックスで、[無効にする] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を無効にするリクエストをフォーマットする方法について説明します。ディレクトリ ID 番号をリクエストに含める必要があります。

Note

AWS ディレクトリサービスデータを無効にする CLI コマンドは を使用しますaws ds。

AWS Directory Service Data CLI を無効にするには

- を開き AWS CLI、次のコマンドを実行して、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

```
aws ds disable-directory-data-access --directory-id d-1234567890
```

AWS Tools for PowerShell

Tools for PowerShell で Directory Service Data を無効にするには

- を開き PowerShell、次のコマンドを実行して、ディレクトリ ID を AWS Managed Microsoft AD Directory ID に置き換えます。

```
Disable-DSDirectoryDataAccess -DirectoryId d-123456789
```

AWS Managed Microsoft AD ユーザーの作成

次の手順を使用して、AWS Management Console AWS CLI、または のいずれかで、ユーザーとグループの管理または AWS Directory Service Data を持つ新しい AWS Managed Microsoft AD ユーザーを作成します AWS Tools for PowerShell。

いずれの手順を開始する前に、以下を完了する必要があります。

- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#) や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。

AWS Management Console

で新しい AWS Managed Microsoft AD ユーザーアカウントを作成できます AWS Management Console。新しいユーザーアカウントを作成するときは、新しいユーザーの詳細を指定し、新しいユーザーをグループに追加するか、別のユーザーのグループメンバーシップを新しいユーザーにコピーするかを決定します。

詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

を使用して AWS Managed Microsoft AD ユーザーを作成するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [ディレクトリの詳細] ページで、[ユーザー] セクションで[ユーザーアカウントの作成] を選択します。
5. [ユーザーの詳細を指定] ページが表示されます。[必要な情報] セクションで、ユーザーログオン名とパスワードを入力します。ユーザーログオン名は、次の条件を満たす必要があります。
 - 一意のログオン名を使用する必要がある
 - 最大 20 文字
 - 英数字のみ含めることは可能
 - 次の文字は含めてはいけません: / \ [] : ; | , + * ? < > @
 - パスワードは、パスワードポリシーの要件に従う必要があります。詳細については、AWS 管理者にお問い合わせください。

 Warning

ユーザーが作成されたら、ユーザーログオン名を変更することはできません。

- a. (選択可能) [プライマリ情報] セクションで、ユーザーの姓名を入力できます。ユーザーの表示名と説明を入力することもできます。
- b. (選択可能) [連絡方法] セクションで、ユーザーのメールアドレスと電話番号を入力できます。
- c. (選択可能) [ジョブ関連情報] セクションで、ユーザーの部門、マネージャー、オフィス、会社を入力できます。

- d. (選択可能) [アドレス] セクションで、ユーザーのアドレスを入力できます。
- e. (選択可能) [アカウント設定] セクションで、ユーザーのメモ、優先言語、およびサービスプリンシパル名を入力できます。

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

- 6. ユーザーアカウントの詳細を指定したら、[次へ] を選択します。
- 7. [ユーザーをグループに追加 - 選択可能] ページで、ユーザーを新しいグループまたは既存のグループに追加できます。既存のユーザーのグループメンバーシップを新しいユーザーにコピーすることもできます。ユーザーをグループに追加したくない場合は、[次へ] を選択します。この手順を続行するには、ステップ 12 に進んでください。
- 8. (オプション) 新しいグループを作成するには、[AWS 「Managed Microsoft AD グループの作成」](#) を参照してください。
- 9. (選択可能) 既存のグループに新しいユーザーを追加するには:
 - 新しいユーザーを追加したいグループを[グループ] セクションで選択します。グループを検索するには、検索ボックスにグループ名を入力します。
- 10. (選択可能) 既存のユーザーのグループメンバーシップを新しいユーザーにコピーするには:
 - a. [ユーザーからグループメンバーシップをコピーする] タブを選択します。コピーしたいグループメンバーシップのあるユーザーを検索するには、[ユーザー] セクションの検索ボックスにユーザーログオン名を入力します。
 - b. [選択したグループ] セクションで、新しいユーザーがどのグループのメンバーになるかを選択します。
- 11. 新しいユーザーアカウントを作成する準備ができたなら、[次へ] を選択します。
- 12. [ユーザーの確認と更新] ページで、選択した内容を確認します。[ユーザーの作成] を選択します。
- 13. ユーザーを設定した後、新しいユーザーの詳細ページに移動します。ユーザーが正常に作成されたことを示すバナーが表示されます。

⚠ Important

ユーザーを作成するアクセス許可がないというエラーメッセージが表示された場合は、エラーメッセージの指示に従って、管理者にアクセス許可を付与するようリクエストしてください。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して新しい AWS Managed Microsoft AD ユーザーアカウントを作成するリクエストをフォーマットする方法について説明します。ディレクトリ ID 番号とユーザーログオン名をリクエストに含める必要があります。DisplayName 属性には、ユーザー表示名など他の属性を含めることもできます。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

を使用して AWS Managed Microsoft AD ユーザーを作成するには AWS CLI

- を開き AWS CLI、次のコマンドを実行して、ディレクトリ ID、ユーザー名、表示名を AWS Managed Microsoft AD Directory ID と必要な認証情報に置き換えます。

```
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 for PowerShell

次に、で新しい AWS Managed Microsoft AD ユーザーアカウントを作成するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。ディレクトリ ID 番号とユーザーログオン名をリクエストに含める必要があります。DisplayName 属性には、ユーザー表示名など他の属性を含めることもできます。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

Tools for PowerShell を使用して AWS Managed Microsoft AD ユーザーを作成するには

- を開き PowerShell、次のコマンドを実行し、ディレクトリ ID、ユーザー名、表示名を AWS Managed Microsoft AD Directory ID と必要な認証情報に置き換えます。

```
New-DSUser `
  -DirectoryId d-1234567890 `
  -SAMAccountName "jane.doe" `
  -OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'jane.doe' }
    Department = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'Legal' }
  }
```

AWS Managed Microsoft AD ユーザーの表示と更新

次の手順を使用して、、、または のユーザーとグループの管理または AWS Directory Service Data を使用して AWS Management Console AWS CLI Managed AWS Microsoft AD ユーザーの詳細を表示または更新します AWS Tools for PowerShell。

AWS Managed Microsoft AD ユーザーの詳細の表示

ユーザーの詳細は、AWS Management Console または で表示できます AWS CLI。ユーザーの詳細には、プロフィールとアカウント情報、グループメンバーシップが含まれます。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#) や などの AWS 管理ポリシーを使用できま

す[AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。

- [AWS Managed Microsoft AD ユーザーの作成](#).

AWS Management Console

AWS Managed Microsoft AD ユーザーの詳細については、「」を参照してください AWS Management Console。

を使用して AWS Managed Microsoft AD ユーザーの詳細とアカウントの詳細を表示するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ダイレクトリ] を選択します。ダイレクトリのリストを表示できるダイレクトリ画面が表示されます AWS リージョン。
3. [ダイレクトリ] を選択します。[ダイレクトリの詳細] 画面に移動します。
4. [ユーザー] を選択します。タブには、ダイレクトリ内のユーザーのリストが表示されます。
5. [ユーザーを追加] を選択します。[ユーザーの詳細] 画面が表示されます。[ユーザーの詳細] 画面では、以下の情報が表示されます。
 - ユーザーがメンバーであるグループ (グループメンバーシップ)
 - プロファイルの詳細 (ユーザーログオン名、名、姓などのプライマリ情報など)
 - アカウント設定 (ユーザープリンシパル名、サービスプリンシパル名、識別名などのアカウント情報など)
 - アカウントステータス

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

AWS CLI

を使用すると AWS CLI、プロファイル、アカウント情報、グループメンバーシップなど、ユーザーの詳細を表示できます。

を使用して AWS Managed Microsoft AD ユーザーのプロファイルとアカウントの詳細を表示するには AWS CLI

ここでは、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD ユーザーの詳細を表示する方法について説明します。

- ユーザーの詳細を表示するには、 を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
aws ds-data describe-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

ユーザーのグループメンバーシップを表示するには

ここでは、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD ユーザーのグループメンバーシップを表示する方法について説明します。

- ユーザーのグループメンバーシップを表示するには、 を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
aws ds-data list-groups-for-member --directory-id d-1234567890 --sam-account-name "jane.doe"
```

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

AWS Tools for PowerShell

Tools for PowerShell を使用すると、プロファイル、アカウント情報、グループメンバーシップなど、ユーザーの詳細を表示できます。

Tools for PowerShell を使用して AWS Managed Microsoft AD ユーザーのプロファイルとアカウントの詳細を表示するには

Tools for PowerShell を使用して AWS Managed Microsoft AD ユーザーの詳細を表示する方法を以下に示します。

- ユーザーの詳細を表示するには、 を開き PowerShell、次のコマンドを実行し、ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
Get-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

ユーザーのグループメンバーシップを表示するには

以下に、Tools for PowerShell を使用して AWS Managed Microsoft AD ユーザーのグループメンバーシップを表示する方法について説明します。

- ユーザーのグループメンバーシップを表示するには、を開きPowerShell、次のコマンドを実行します。ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
(Get-DSDGroupsForMemberList -DirectoryId d-1234567890 -SAMAccountName "jane.doe") .Groups
```

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

AWS Managed Microsoft AD ユーザーの詳細の更新

ユーザーとグループの管理または AWS Directory Service Data で AWS Managed Microsoft AD ユーザーを更新するには AWS Management Console AWS CLI、次の手順を使用します AWS Tools for PowerShell。

Note

属性の最小長は 1 です。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)やなどの AWS 管理ポリシーを使用できます。[AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD ユーザーの作成](#).

AWS Management Console

AWS Managed Microsoft AD ユーザーの詳細は、「」で更新できます AWS Management Console。

AWS Managed Microsoft AD ユーザーの詳細を で更新するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ダイレクトリ] を選択します。ダイレクトリのリストを表示できるダイレクトリ画面が表示されます AWS リージョン。
3. [ダイレクトリ] を選択します。[ダイレクトリの詳細] 画面に移動します。
4. [ユーザー] を選択します。タブには、ダイレクトリ内のユーザーのリストが表示されます。
5. [ユーザーを追加] を選択します。ユーザーを検索するには、ユーザーセクションの検索ボックスにユーザーログオン名を入力します。[ユーザーの詳細] 画面が表示されます。
6. ユーザーがメンバーであるグループを編集するには、[グループ] を選択します。このタブから、ユーザーをグループに追加またはグループから削除できます。詳細については、「[グループに AWS Managed Microsoft AD メンバーを追加する](#)」を参照してください。
7. ユーザープロファイルの詳細を編集するには、[プロファイル] を選択し、[編集] を選択します。または、[アクション] を選択して、[ユーザーの編集] を選択します。更新を行って確認した後、[保存] を選択します。

Warning

ユーザーが作成されたら、ユーザーログオン名を変更することはできません。

8. ユーザーのアカウント設定を編集するには、[ユーザーアカウント設定] を選択します。または、[アクション] を選択して、[ユーザーの編集] を選択します。更新を行って確認した後、[保存] を選択します。

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD ユーザーの詳細を更新するリクエストをフォーマットする方法について説明します。

ユーザーのアカウントを更新するときは、ディレクトリ ID 番号とユーザーログイン名を含める必要があります。また、Surname パラメータを持つユーザーの姓など、更新したい更新タイプと属性をリクエストに含める必要があります。詳細については、「[AWS Directory Service Data 属性](#)」を参照してください。

- ユーザーの詳細を更新するには、を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID、ユーザー名、ユーザータイプ、属性値を AWS Managed Microsoft AD Directory ID、ユーザー名、必要なユーザータイプと属性値に置き換えます。

```
aws ds-data update-user --directory-id d-1234567890 --sam-account-name "jane.doe" --update-type "REPLACE" --surname "Doe"
```

Note

[update-user](#) CLI コマンドでユーザー属性を削除する場合は、削除する属性と正確な値を指定する必要があります。ユーザー属性を確認するには、[describe-user](#) コマンドを使用します。

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

AWS Tools for PowerShell

次に、AWS Managed Microsoft AD ユーザーの詳細を更新するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

ユーザーのアカウントを更新するときは、ディレクトリ ID 番号とユーザーログオン名を含める必要があります。また、Surname パラメータを持つユーザーの姓など、更新したい更新タイプと属性をリクエストに含める必要があります。詳細については、「[AWS Directory Service Data 属性](#)」を参照してください。

- ユーザーの詳細を更新するには、 を開き PowerShell、次のコマンドを実行します。ディレクトリ ID、ユーザー名、ユーザータイプ、属性値を AWS Managed Microsoft AD Directory ID、ユーザー名、必要なユーザータイプと属性値に置き換えます。

```
Update-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe" -UpdateType  
"REPLACE" -Surname "Doe"
```

ユーザー属性の詳細については、[AWS Directory Service Data 属性](#) および「[Microsoft ドキュメント](#)」を参照してください。

AWS Managed Microsoft AD ユーザーの削除

ユーザーとグループの管理または AWS Directory Service Data を持つ AWS Managed Microsoft AD ユーザーを削除するには AWS Management Console AWS CLI、次の手順を使用します AWS Tools for PowerShell。

Important

ディレクトリからユーザーのアカウントを削除すると、ユーザーがアカウントとアプリケーションにアクセスするためのアクセス許可など、ユーザーに関するすべての情報が削除されます。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます。[AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD ユーザーの作成](#)。

AWS Management Console

AWS Managed Microsoft AD ユーザーアカウントは、で削除できます AWS Management Console。

を使用して AWS Managed Microsoft AD ユーザーアカウントを削除するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [ユーザー] を選択します。タブには、ディレクトリ内のユーザーのリストが表示されます。
5. アカウントを削除するユーザーを選択します。ユーザーを検索するには、ユーザーセクションの検索ボックスにユーザーログオン名を入力します。[ユーザーの詳細] 画面が表示されます。
6. [アクション] を選択します。次に[ユーザーアカウントの削除] を選択し、再び [ユーザーアカウントの削除] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD ユーザーのアカウントを削除するリクエストをフォーマットする方法について説明します。

を使用して AWS Managed Microsoft AD ユーザーアカウントを削除するには AWS CLI

- を開き AWS CLI、次のコマンドを実行して、ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
aws ds-data delete-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

AWS Tools for PowerShell

次に、AWS Managed Microsoft AD ユーザーのアカウントを削除するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

を使用して AWS Managed Microsoft AD ユーザーアカウントを削除するには AWS Tools for PowerShell

- を開きPowerShell、次のコマンドを実行して、ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
Remove-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

AWS Managed Microsoft AD ユーザーの無効化

次の手順を使用して、AWS Management Console AWS CLI、またはでユーザーとグループの管理または AWS Directory Service Data を使用する AWS Managed Microsoft AD ユーザーを無効にします AWS Tools for PowerShell。

Important

ユーザーのアカウントを無効にすると、ユーザーはアカウントとアプリケーションにアクセスするためのアクセス許可を失います。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#)。
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リ](#)

[ファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)やなどの AWS 管理ポリシーを使用できます。[AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。

- [AWS Managed Microsoft AD ユーザーの作成](#).

AWS Management Console

で AWS Managed Microsoft AD ユーザーアカウントを無効にすることができます AWS Management Console。

で AWS Managed Microsoft AD ユーザーアカウントを無効にするには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [ユーザー] を選択します。タブには、ディレクトリ内のユーザーのリストが表示されます。
5. 無効にするユーザーを選択します。[ユーザーの詳細] 画面が表示されます。
6. [アクション] を選択します。次に、[ユーザーアカウントを無効にする] を選択し、再度 [ユーザーアカウントを無効にする] を選択します。

Note

ユーザーのアカウントを再度有効にするには、ユーザーのパスワードをリセットする必要があります。詳細については、「[AWS Managed Microsoft AD ユーザーのパスワードのリセットと有効化](#)」を参照してください。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD ユーザーアカウントを無効にするリクエストをフォーマットする方法について説明します。

で AWS Managed Microsoft AD ユーザーアカウントを無効にするには AWS CLI

- を開き AWS CLI、次のコマンドを実行して、ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
aws ds-data disable-user --directory-id d-1234567890 --sam-account-name "jane.doe"
```

 Note

ユーザーアカウントを再度有効にするには、ユーザーのパスワードをリセットする必要があります。詳細については、「[AWS Managed Microsoft AD ユーザーのパスワードのリセットと有効化](#)」を参照してください。

AWS Tools for PowerShell

次に、を使用して AWS Managed Microsoft AD ユーザーアカウントを無効にするリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

で AWS Managed Microsoft AD ユーザーアカウントを無効にするには AWS Tools for PowerShell

- PowerShellを開き、次のコマンドを実行して、ディレクトリ ID とユーザー名を AWS Managed Microsoft AD Directory ID とユーザー名に置き換えます。

```
Disable-DSDUser -DirectoryId d-1234567890 -SAMAccountName "jane.doe"
```

 Note

ユーザーアカウントを再度有効にするには、ユーザーのパスワードをリセットする必要があります。詳細については、「[AWS Managed Microsoft AD ユーザーのパスワードのリセットと有効化](#)」を参照してください。

AWS Managed Microsoft AD ユーザーのパスワードのリセットと有効化

Managed AWS Microsoft AD ユーザーのパスワードをリセットして、AWS Management Console、のいずれかでユーザーとグループの管理または AWS Directory Service Data を使用してアカウントを有効にするには AWS CLI、次の手順に従います AWS Tools for PowerShell。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#)。
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD ユーザーの作成](#)。

AWS Management Console

AWS Managed Microsoft AD ユーザーのパスワードをリセットして、でアカウントを有効にできます AWS Management Console。このタスクは、[ディレクトリ] 画面または [ディレクトリの詳細] 画面から実行できます。

ディレクトリ

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [アクション] を選択し、[ユーザーパスワードのリセットしてアカウントを有効にする] を選択します。

- a. [ユーザーログオン名] に、パスワードをリセットしたいユーザーのユーザーログオン名を入力します。
 - b. [新しいパスワード] で、ユーザーの新しいパスワードを入力します。
 - c. [パスワードを確認する] に、ユーザーの新しいパスワードをもう一度入力します。
4. ユーザーの新しいパスワードを確認した後、[パスワードをリセットしてアカウントを有効にする] を選択します。

ディレクトリの詳細

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [ユーザー] を選択します。タブには、ディレクトリ内のユーザーのリストが表示されます。
5. パスワードをリセットしたいユーザーを選択します。
6. [アクション] を選択し、[ユーザーパスワードのリセットしてアカウントを有効にする] を選択します。
 - a. [新しいパスワード] で、ユーザーの新しいパスワードを入力します。
 - b. [パスワードを確認する] に、ユーザーの新しいパスワードをもう一度入力します。
7. ユーザーの新しいパスワードを確認した後、[パスワードをリセットしてアカウントを有効にする] を選択します。

AWS CLI

AWS Managed Microsoft AD のパスワードをリセットして、AWS Directory Service Data CLI でアカウントを有効にできます。

Note

ユーザーのパスワードリセットコマンドは `aws ds` を使用します。

を使用して AWS Managed Microsoft AD ユーザーのパスワードをリセットするには AWS CLI

- ユーザーのパスワードをリセットするには、を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID、ユーザー名、パスワードを AWS Managed Microsoft AD Directory ID、ユーザー名、および必要な認証情報に置き換えます。

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

AWS Tools for PowerShell

AWS Managed Microsoft AD のパスワードをリセットして、でアカウントを有効にできます
AWS Tools for PowerShell。

を使用して AWS Managed Microsoft AD ユーザーのパスワードをリセットするには AWS Tools
for PowerShell

- ユーザーのパスワードをリセットするには、PowerShell を開き、次のコマンドを実行して、ディレクトリ ID、ユーザー名、AWS Managed Microsoft AD Directory ID 付きのパスワード、ユーザー名、および必要な認証情報に置き換えます。

```
Reset-DSUserPassword -DirectoryId d-1234567890 -UserName "jane.doe" -NewPassword "your-password"
```

AWS Managed Microsoft AD グループの作成

次の手順を使用して、ユーザーとグループの管理または AWS Directory Service Data を持つ AWS Managed Microsoft AD グループを AWS Management Console、AWS CLI、または のいずれかで作成します AWS Tools for PowerShell。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。

- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。

AWS Management Console

で新しい AWS Managed Microsoft AD グループを作成できます AWS Management Console。新しいグループを作成するときは、グループの詳細を指定し、「[グループのタイプと範囲](#)」を決定します。ユーザーと子グループを新しいグループに追加するか、新しいグループを親グループに追加するオプションもあります。

を使用して AWS Managed Microsoft AD グループを作成するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] の選択 このタブには、AWS リージョン内のグループのリストが表示されます。
5. [グループの作成] を選択してください。新しいグループの作成を完了する手順に移動します。
6. [スタック詳細の指定] ページが表示されます。[グループ名] を入力します。グループ名は、次の条件を満たす必要があります:
 - 一意のグループ名にする必要がある
 - 最大 64 文字
 - 英数字のみ含めることは可能
 - 次の文字は含めてはいけません: / \ [] : ; | , + * ? < > @

⚠ Warning

グループの作成後にグループ名を変更することはできません。

7. 次のいずれかから [グループタイプ] を選択します。
 - セキュリティ
 - 配信
 - 詳細については [the section called “グループのタイプ”](#) を参照してください。
8. 次のいずれかから [グループ範囲] を選択します。
 - ドメインローカル
 - Universal
 - グローバル
 - [範囲の比較] をオンにすると、グループ範囲の間の類似点と相違点をグラフで表示できます。詳細については [the section called “グループのスコープ”](#) を参照してください。
9. プライマリ情報と問い合わせ方法を指定した後、[次へ] を選択します。
10. [グループにユーザーを追加する – 選択可能] ページが表示され、新しいグループにユーザーを追加できます。グループに追加するユーザーを検索するには、ユーザーセクションの検索ボックスにユーザーログオン名を入力します。グループに追加したいユーザーを選択し、[次へ] を選択します。
11. [子グループの追加 – 選択可能] ページが表示され、既存のグループを新しいグループに追加できます。既存のグループは、新しく作成されたグループの子グループになります。グループに子グループを追加すると、グループは親グループになり、子グループはグループのすべてのロールとアクセス許可を継承します。追加するグループを検索するには、[子グループの追加] セクションの検索ボックスにグループ名を入力します。新しいグループに追加する子グループを選択し、[次へ] を選択します。
12. [親グループの追加 – 選択可能] ページが表示され、新しいグループを既存のグループに追加できます。新しいグループは、既存グループの親グループになります。グループを親グループに追加すると、グループは子グループになり、親グループのすべてのロールとアクセス許可を継承します。追加するグループを検索するには、[親グループの追加] セクションの検索ボックスにグループ名を入力します。新しいグループに追加する親グループを選択し、[次へ] を選択します。
13. [グループの確認と作成] ページで選択内容を確認し、[グループを作成] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD グループを作成するリクエストをフォーマットする方法について説明します。新しいグループを作成するときは、ディレクトリ ID 番号とグループ名を含める必要があります。DisplayName 属性を持つグループ表示名など、他の属性を追加することもできます。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

を使用して AWS Managed Microsoft AD グループを作成するには AWS CLI

- を開き AWS CLI、次のコマンドを実行し、ディレクトリ ID、ユーザー名、グループ表示名を AWS Managed Microsoft AD Directory ID、ユーザー名、および目的のグループ表示名に置き換えます。

```
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 for PowerShell

次に、で AWS Managed Microsoft AD グループを作成するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。新しいグループを作成するときは、ディレクトリ ID 番号とグループ名を含める必要があります。DisplayName 属性を持つグループ表示名など、他の属性を追加することもできます。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

を使用して AWS Managed Microsoft AD グループを作成するには AWS Tools for PowerShell

- を開き PowerShell、次のコマンドを実行し、ディレクトリ ID、ユーザー名、グループ表示名を AWS Managed Microsoft AD Directory ID、ユーザー名、および目的のグループ表示名に置き換えます。

```
New-DSDGroup `\  
  -DirectoryId d-1234567890 `\  
  -SAMAccountName "your-group-name" `
```

```
-OtherAttribute @{
    DisplayName = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'myGroupDisplayName' }
    Description = [Amazon.DirectoryServiceData.Model.AttributeValue]@{S =
'myGroupDescription' }
}
```

AWS Managed Microsoft AD グループの詳細の表示と更新

次の手順を使用して、、、または のユーザーとグループの管理または AWS Directory Service Data を使用して AWS Managed Microsoft AD グループの詳細を表示 AWS Management Console AWS CLIまたは更新します AWS Tools for PowerShell。

AWS Managed Microsoft AD グループの詳細の表示

グループの詳細を表示または更新するには AWS Management Console、AWS CLI、、、または を使用します AWS Tools for PowerShell。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#)。
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD グループの作成](#)。

AWS Management Console

AWS Managed Microsoft AD グループの詳細については、「」を参照してください AWS Management Console。

を使用して AWS Managed Microsoft AD グループの詳細を表示するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] の選択 このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。[グループの詳細] 画面に移動します。[グループの詳細] ページでは、以下の情報が表示されます。
 - [メンバー] タブには、グループのメンバーであるユーザーと子グループが一覧表示されます。
 - [親グループ] タブには、グループがメンバーである親グループが一覧表示されます。
 - [プロパティ] タブには、グループプロパティ (グループ名、グループ表示名などのプライマリ情報など) が一覧表示されます。

AWS CLI

AWS Directory Service Data CLI を使用して、AWS Managed Microsoft AD グループの詳細を表示できます。

を使用して AWS Managed Microsoft AD グループの詳細を表示するには AWS CLI

次に、を使用して AWS Managed Microsoft AD グループの詳細を表示する方法について説明します AWS CLI。

- グループの詳細を表示するには、を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID とグループ名を AWS Managed Microsoft AD Directory ID とグループ名に置き換えます。

```
aws ds-data describe-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

を使用して AWS Managed Microsoft AD グループのグループメンバーを表示するには AWS CLI

次に、 を使用して AWS Managed Microsoft AD グループのメンバーを表示する方法について説明します AWS CLI。

- グループの詳細を表示するには、 を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID とグループ名を AWS Managed Microsoft AD Directory ID とグループ名に置き換えます。

```
aws ds-data list-group-members --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Tools for PowerShell

AWS Managed Microsoft AD グループの詳細を表示するには、 を使用します AWS Tools for PowerShell。

を使用して AWS Managed Microsoft AD グループの詳細を表示するには AWS Tools for PowerShell

Tools for PowerShell を使用して AWS Managed Microsoft AD グループの詳細を表示する方法を以下に示します。

- グループの詳細を表示するには、PowerShell を開き、次のコマンドを実行して、ディレクトリ ID とグループ名を AWS Managed Microsoft AD Directory ID とグループ名に置き換えます。

```
Get-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

を使用して AWS Managed Microsoft AD グループのグループメンバーを表示するには AWS Tools for PowerShell

Tools for PowerShell を使用して AWS Managed Microsoft AD グループのメンバーを表示する方法を以下に示します。

- グループの詳細を表示するには、PowerShell を開き、次のコマンドを実行して、ディレクトリ ID とグループ名を AWS Managed Microsoft AD Directory ID とグループ名に置き換えます。

```
(Get-DSDGroupMemberList -DirectoryId d-1234567890 -SAMAccountName "your-group-name").Members
```

AWS Managed Microsoft AD グループの詳細の更新

Managed AWS Microsoft AD グループの詳細を、、、または のユーザーとグループの管理または AWS Directory Service Data で更新するには AWS Management Console AWS CLI、次の手順に従います AWS Tools for PowerShell。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#)。
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD グループの作成](#)。

AWS Management Console

AWS Management Consoleを使用してグループの詳細を更新できます。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

Managed AWS Microsoft AD グループの詳細を で更新するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。

3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] の選択 このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。[グループの詳細] 画面に移動します。
6. グループのメンバーであるユーザーと子グループを編集するには、[メンバー] を選択します。このタブから、ユーザーと子グループをグループに追加、またはグループから削除できます。詳細については、「[グループへのメンバーとグループの追加と削除](#)」を参照してください。
7. グループがメンバーである親グループを編集するには、[親グループ] を選択します。このタブから、親グループからグループを追加および削除できます。詳細については、「[グループへのメンバーとグループの追加と削除](#)」を参照してください。
8. グループプロパティを編集するには、[プロパティ] を選択し、[編集] を選択します。[アクション] を選択して、[グループの編集] を選択します。更新を行って確認した後、[保存] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD グループの詳細を更新するリクエストをフォーマットする方法について説明します。

グループを更新するときは、ディレクトリ ID 番号とグループ名を含める必要があります。また、EmailAddress パラメータを含むグループのメールアドレスなど、更新する更新タイプと属性をリクエストに含める必要があります。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

- Managed AWS Microsoft AD グループの詳細を で更新するには AWS CLI

グループの詳細を更新するには、 を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID、グループ名、更新タイプ、属性を AWS Managed Microsoft AD Directory ID、グループ名、および必要な更新タイプと属性に置き換えます。

```
aws ds-data update-group --directory-id d-1234567890 --sam-account-name "your-group-name" --update-type "REPLACE" --group-scope "global"
```


AWS Tools for PowerShell

以下に、AWS Managed Microsoft AD グループの詳細を更新するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

グループを更新するときは、ディレクトリ ID 番号とグループ名を含める必要があります。また、EmailAddress パラメータを含むグループのメールアドレスなど、更新する更新タイプと属性をリクエストに含める必要があります。詳細については、「[AWS Directory Service Data 属性](#)」および「[グループタイプとグループスコープ](#)」を参照してください。

- AWS Managed Microsoft AD グループの詳細を で更新するには AWS Tools for PowerShell

グループの詳細を更新するには、 を開き PowerShell、次のコマンドを実行します。ディレクトリ ID、グループ名、更新タイプ、属性を AWS Managed Microsoft AD Directory ID、グループ名、および必要な更新タイプと属性に置き換えます。

```
Update-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name" -  
UpdateType "REPLACE" -GroupScope "global"
```

AWS Managed Microsoft AD グループの削除

ユーザーとグループの管理または AWS Directory Service Data を持つ AWS Managed Microsoft AD グループを、 または で削除するには AWS Management Console AWS CLI、次の手順に従います AWS Tools for PowerShell。

Important

グループを削除すると、グループメンバーが継承するアクセス許可など、グループに関するすべての情報が削除されます。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。

- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD グループを作成します。](#)

AWS Management Console

で AWS Managed Microsoft AD グループを削除できます AWS Management Console。

を使用して AWS Managed Microsoft AD グループを削除するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] の選択 このタブには、AWS リージョン内のグループのリストが表示されます。
5. 削除したいグループを選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。[グループの詳細] 画面に移動します。
6. [Delete group (グループの削除)] を選択します。ダイアログボックスが表示され、[確認] を選択してグループを削除できます。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD グループを削除するリクエストをフォーマットする方法について説明します。

を使用して AWS Managed Microsoft AD グループを削除するには AWS CLI

- を開き AWS CLI、次のコマンドを実行し、ディレクトリ ID とグループ名を AWS Managed Microsoft AD Directory ID とグループ名に置き換えます。

```
aws ds-data delete-group --directory-id d-1234567890 --sam-account-name "your-group-name"
```

AWS Tools for PowerShell

次に、を使用して AWS Managed Microsoft AD グループを削除するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

を使用して AWS Managed Microsoft AD グループを削除するには AWS Tools for PowerShell

- を開きPowerShell、次のコマンドを実行して、ディレクトリ ID とグループ名を AWS Managed Microsoft AD Directory ID とグループ名に置き換えます。

```
Remove-DSDGroup -DirectoryId d-1234567890 -SAMAccountName "your-group-name"
```

グループへの AWS Managed Microsoft AD メンバーの追加と削除、グループへのグループの削除

「[AWS Directory Service Data API](#)」では、メンバーはユーザー、グループ、またはコンピュータにすることができます。個人またはエンティティを代表するユーザーは、ディレクトリにアクセスできます。グループを使用すると、一度に複数のユーザーにアクセス許可を付与および拒否できます。

Managed AWS Microsoft AD ユーザーをグループに追加または削除するには AWS Management Console AWS CLI、次の手順を使用して、、、または のユーザーとグループ管理または AWS Directory Service Data を持つ別のグループに追加または削除します AWS Tools for PowerShell。

ユーザーをグループに追加する

次の手順を使用して、、、AWS Management Console AWS CLI、または でユーザーとグループ管理または AWS Directory Service Data を持つグループに AWS Managed Microsoft AD ユーザーを追加します AWS Tools for PowerShell。

Important

AWS Managed Microsoft AD ユーザーをグループに追加すると、ユーザーはグループに割り当てられたロールとアクセス許可を継承します。これらのロールとアクセス許可は、ユーザーのグループメンバーシップの一部です。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD ユーザーを作成します](#)。
- [AWS Managed Microsoft AD グループを作成します](#)。

AWS Management Console

AWS Managed Microsoft AD メンバーは、 を使用してグループに追加できます AWS Management Console。

を使用して AWS Managed Microsoft AD ユーザーをグループに追加するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] を選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。タブには、 内のグループのリストが表示されます AWS リージョン。
5. グループを選択します。[グループの詳細] 画面に移動します。

6. [メンバー] を選択します。タブには、グループ内のメンバータイプ別のユーザーと子グループのリストが表示されます。
7. [メンバー] タブで、[メンバーの追加] を選択します。
8. [メンバー] で、グループに追加するユーザーを選択し、[グループにメンバーを追加する] を選択します。メンバーを検索するには、[メンバー] セクションの検索ボックスにユーザーのユーザーログオン名とグループのグループ名を入力します。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD メンバーをグループに追加するリクエストをフォーマットする方法について説明します。

を使用して AWS Managed Microsoft AD ユーザーをグループに追加するには AWS CLI

- ユーザーをグループに追加するには、 を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えます。

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Tools for PowerShell

次に、AWS Managed Microsoft AD メンバーをグループに追加するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

を使用して AWS Managed Microsoft AD ユーザーをグループに追加するには AWS Tools for PowerShell

- ユーザーをグループに追加するには、PowerShell を開き、次のコマンドを実行して、ディレクトリ ID、グループ名、メンバー名を AWS Managed Microsoft AD Directory ID、グループ名、メンバー名に置き換えます。

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

グループからのユーザーの削除

「[AWS Directory Service Data API](#)」では、メンバーはユーザー、グループ、またはコンピュータにすることができます。個人またはエンティティを代表するユーザーは、ディレクトリにアクセスできます。グループを使用すると、一度に複数のユーザーにアクセス許可を付与および拒否できます。

次の手順を使用して、AWS Management Console AWS CLI、または のいずれかで、AWS Managed Microsoft AD ユーザーをユーザーとグループの管理または AWS Directory Service Data を持つグループから削除します AWS Tools for PowerShell。

Important

Managed AWS Microsoft AD ユーザーをグループから削除すると、そのユーザーはグループに割り当てられたロールとアクセス許可にアクセスできなくなります。これらのロールとアクセス許可は、グループのメンバーシップの一部です。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#)や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD ユーザーを作成します](#)。
- [AWS Managed Microsoft AD グループを作成します](#)。

AWS Management Console

AWS Managed Microsoft AD メンバーは、 を使用してグループから削除できます AWS Management Console。

を使用してグループから AWS Managed Microsoft AD ユーザーを削除するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ダイレクトリ] を選択します。ダイレクトリのリストを表示できるダイレクトリ画面が表示されます AWS リージョン。
3. [ダイレクトリ] を選択します。[ダイレクトリの詳細] 画面に移動します。
4. [グループ] を選択します。このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。[グループの詳細] 画面に移動します。
6. [メンバー] を選択します。タブには、グループ内のメンバータイプ別のユーザーと子グループのリストが表示されます。
7. 削除したいユーザーまたはグループを選択し、[削除] をクリックします。ユーザーを検索するには、[メンバー] セクションの検索ボックスにユーザー名を入力します。
8. グループからユーザーを削除することを確認し、再度 [削除] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を使用してグループから AWS Managed Microsoft AD メンバーを削除するリクエストをフォーマットする方法について説明します。

を使用してグループから AWS Managed Microsoft AD ユーザーを削除するには AWS CLI

- ユーザーをグループから削除するには、 を開き AWS CLI、次のコマンドを実行します。ダイレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えます。


```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "your-group-name" --member-name "jane.doe"
```

AWS Tools for PowerShell

次に、を使用してグループから AWS Managed Microsoft AD メンバーを削除するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

を使用してグループから AWS Managed Microsoft AD ユーザーを削除するには AWS Tools for PowerShell

- ユーザーをグループから削除するには、PowerShell を開き、次のコマンドを実行して、ディレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えます。

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "your-group-name" -MemberName "jane.doe"
```

グループへのグループの追加

AWS Managed Microsoft AD グループを別のグループに追加すると、グループは親子関係を共有します。子グループには、親グループに割り当てられたロールとアクセス許可が利用できます。子グループをグループに、グループを親グループに追加できます。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#)。
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#) や などの AWS 管理ポリシーを使用できま

す [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。

- [AWS Managed Microsoft AD グループを作成します](#)。

AWS Management Console

AWS Managed Microsoft AD グループは、を使用してグループに追加できます AWS Management Console。

を使用してグループに子グループを追加するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] を選択します。このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。[グループの詳細] 画面に移動します。
6. [メンバー] を選択します。タブには、グループ内のメンバータイプ別のユーザーと子グループのリストが表示されます。
7. [メンバーの追加] を選択します。
8. [メンバー] で、グループに追加したい子グループを選択し、[グループにメンバーを追加する] を選択します。

を使用して親グループをグループに追加するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。

4. [グループ] を選択します。このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。[グループの詳細] 画面に移動します。
6. [親グループ] を選択します。タブには、グループがメンバーであるグループのリストが表示されます。
7. [親グループの追加] を選択します。
8. [グループ] で、グループを追加するグループを選択し、再度 [親グループを追加] を選択します。

AWS CLI

以下に、AWS Directory Service Data CLI を使用して AWS Managed Microsoft AD グループをグループに追加するリクエストをフォーマットする方法について説明します。

を使用してグループに子グループを追加するには AWS CLI

- 親グループに子グループを追加するには、 を開き AWS CLI、次のコマンドを実行します。ディレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えます。

```
aws ds-data add-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Tools for PowerShell

次に、AWS Managed Microsoft AD グループをグループに追加するリクエストをフォーマットする方法について説明します AWS Tools for PowerShell。

を使用してグループに子グループを追加するには AWS Tools for PowerShell

- 親グループに子グループを追加するには、 を開き PowerShell、次のコマンドを実行します。ディレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えます。

```
Add-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -  
MemberName "child-group-name"
```

グループからグループを削除する

AWS Managed Microsoft AD グループを別のグループから削除すると、グループは親子関係を共有しなくなります。子グループには、親グループに割り当てられたロールとアクセス許可を利用できなくなります。グループから子グループを削除し、親グループからグループを削除できます。

いずれの手順を開始する前に、以下を完了する必要があります。

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。
- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#) や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD グループを作成します](#)。

AWS Management Console

AWS Managed Microsoft AD グループは、を使用してグループから削除できます AWS Management Console。

を使用してグループから子グループを削除するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ダイレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。

3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] を選択します。このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。[グループの詳細] 画面に移動します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。
6. [メンバー] を選択します。タブには、グループ内のメンバータイプ別のユーザーと子グループのリストが表示されます。
7. グループから削除したい子グループを選択し、[削除] を選択します。
8. グループから削除したい子グループを確認し、もう一度 [削除] を選択します。

を使用して親グループからグループを削除するには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. 左のナビゲーションペインから、[Active Directory] を選択し、[ディレクトリ] を選択します。ディレクトリのリストを表示できるディレクトリ画面が表示されます AWS リージョン。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] を選択します。このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループを選択します。[グループの詳細] 画面に移動します。グループを見つけるには、[グループ] セクションの検索ボックスにグループ名を入力します。
6. [親グループ] を選択します。タブには、グループがメンバーであるグループのリストが表示されます。
7. グループを削除したい親グループを選択し、[親グループの削除] を選択します。
8. グループを削除したい親グループを確認し、[親グループの削除] を再度選択します。

AWS CLI

以下に、AWS Managed Microsoft AD グループを削除するリクエストを AWS Directory Service Data CLI を使用してグループにフォーマットする方法について説明します。

- を使用して親グループから子グループを削除するには AWS CLI

親グループから子グループを削除するには、 を開き AWS CLI、ディレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えて次のコマンドを実行します。

```
aws ds-data remove-group-member --directory-id d-1234567890 --group-name "parent-group-name" --member-name "child-group-name"
```

AWS Tools for PowerShell

次に、AWS Managed Microsoft AD グループを削除するリクエストを のグループにフォーマットする方法について説明します AWS Tools for PowerShell。

- を使用して親グループから子グループを削除するには AWS Tools for PowerShell

親グループから子グループを削除するには、 を開き PowerShell、次のコマンドを実行します。ディレクトリ ID、グループ、メンバー名を AWS Managed Microsoft AD Directory ID、グループ、メンバー名に置き換えます。

```
Remove-DSDGroupMember -DirectoryId d-1234567890 -GroupName "parent-group-name" -MemberName "child-group-name"
```

での AWS Managed Microsoft AD グループメンバーシップのコピー AWS Management Console

グループメンバーシップは、ある AWS Managed Microsoft AD ユーザーから の別のユーザーにコピーできます AWS Management Console。グループメンバーシップは、グループに追加したときにユーザーが継承するロールとアクセス許可です。

いずれの手順を開始する前に、以下を完了する必要があります:

- [AWS Managed Microsoft AD の作成](#).
- ユーザーとグループの管理または AWS Directory Service Data CLI を使用するには、有効にする必要があります。詳細については、「[ユーザーとグループの管理を有効にする](#)」または「[ディレクトリサービスデータ](#)」を参照してください。

- この機能は、ディレクトリのプライマリからのみ有効に AWS リージョン できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
- AWS Directory Service Data を使用するには、必要な IAM アクセス許可が必要です。詳細については、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください。ユーザーとワークロードへのアクセス許可の付与を開始するには、[AWSDirectoryServiceDataFullAccess](#) や などの AWS 管理ポリシーを使用できます [AWSDirectoryServiceDataReadOnlyAccess](#)。詳細については、「[IAM のセキュリティのベストプラクティス](#)」を参照してください。
- [AWS Managed Microsoft AD グループを作成します](#)。

を使用して AWS Managed Microsoft AD グループメンバーシップをコピーするには AWS Management Console

1. <https://console.aws.amazon.com/directoryservicev2/> で AWS Directory Service コンソールを開きます。
2. ナビゲーションペインから [Active Directory] を選択し、[ディレクトリ] を選択します。[ディレクトリ] 画面が表示され、そこで AWS リージョン内のディレクトリのリストが表示されます。
3. [ディレクトリ] を選択します。[ディレクトリの詳細] 画面に移動します。
4. [グループ] を選択します。このタブには、AWS リージョン内のグループのリストが表示されます。
5. グループメンバーシップをコピーするアカウントを持つユーザーを選択します。ユーザーを検索するには、ユーザーセクションの検索ボックスにユーザーログオン名を入力します。[ユーザーの詳細] 画面が表示されます。
6. [すべてのグループメンバーシップをコピー] を選択します。コピーしたいグループを指定できる手順に移動します。
 - a. [コピーしたいグループを確認] の場合、[コピーするグループ] で、コピーしたいロールとアクセス許可を所有するグループを選択し、[次へ] を選択します。
 - b. [送信先アカウントの選択] の場合、[アカウントタイプ] で [既存のユーザーアカウント] を選択して、グループメンバーシップを既存のユーザーアカウントにコピーします。また、[新しいユーザーアカウント] を選択して新しいユーザーを作成し、グループメンバーシップを新しいユーザーアカウントにコピーします。グループを検索するには、[選択されたグループ] セクションの検索ボックスにグループの名前を入力します。
 - i. (選択可能) [既存のユーザーアカウント] を選択した場合は、ロールとアクセス許可をコピーする送信先アカウントを選択し、[次へ] を選択します。

- ii. (選択可能) [新しいユーザーアカウント] を選択した場合は、手順を完了し、[次へ] を選択します。ユーザー作成の詳細については、[ユーザーの作成](#) を参照してください。
- c. [グループメンバーシップの確認とコピー] については、選択を確認してから、[グループメンバーシップのコピー] を選択します。

Amazon EC2 インスタンスを使用してユーザーとグループを管理する

このセクションでは、AWS Managed Microsoft AD に参加している Amazon EC2 インスタンスを使用してユーザーとグループを管理する手順について説明します。

Directory Service Data API がユースケースをサポートしていない場合は、Amazon EC2 インスタンスを使用してユーザーとグループを管理することをお勧めします。詳細については、「[AWS Directory Service Data API 参照](#)」を参照してください。

Note

ユーザーを作成する前に、「Active Directory 管理ツールのインストール」の手順を完了する必要があります。詳細については、「[Active Directory 管理ツールのインストール](#)」を参照してください。

トピック

- [AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#)
- [AWS Managed Microsoft AD ユーザーの作成](#)
- [Amazon EC2 インスタンスを使用してユーザーのアカウントを削除する](#)
- [AWS Managed Microsoft AD ユーザーパスワードのリセット](#)
- [AWS Managed Microsoft AD グループの作成](#)
- [AWS Managed Microsoft AD ユーザーをグループに追加する](#)

AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール

Managed Microsoft AD AWS は、Active Directoryを使用して管理できますActive Directory Domain Services and Active Directory Lightweight Directory Services Tools。Active Directory Domain Services and Active Directory Lightweight Directory Services Tools を使用するには、それらをインストールする必要があります。次の手順では、これらのツールを Amazon EC2 Windows Server イン

タンスまたは PowerShell コマンドでインストールする方法について説明します。または、これらのツールが既にインストールされているディレクトリ管理 EC2 インスタンスを起動することもできます。

EC2 Windows Server instance

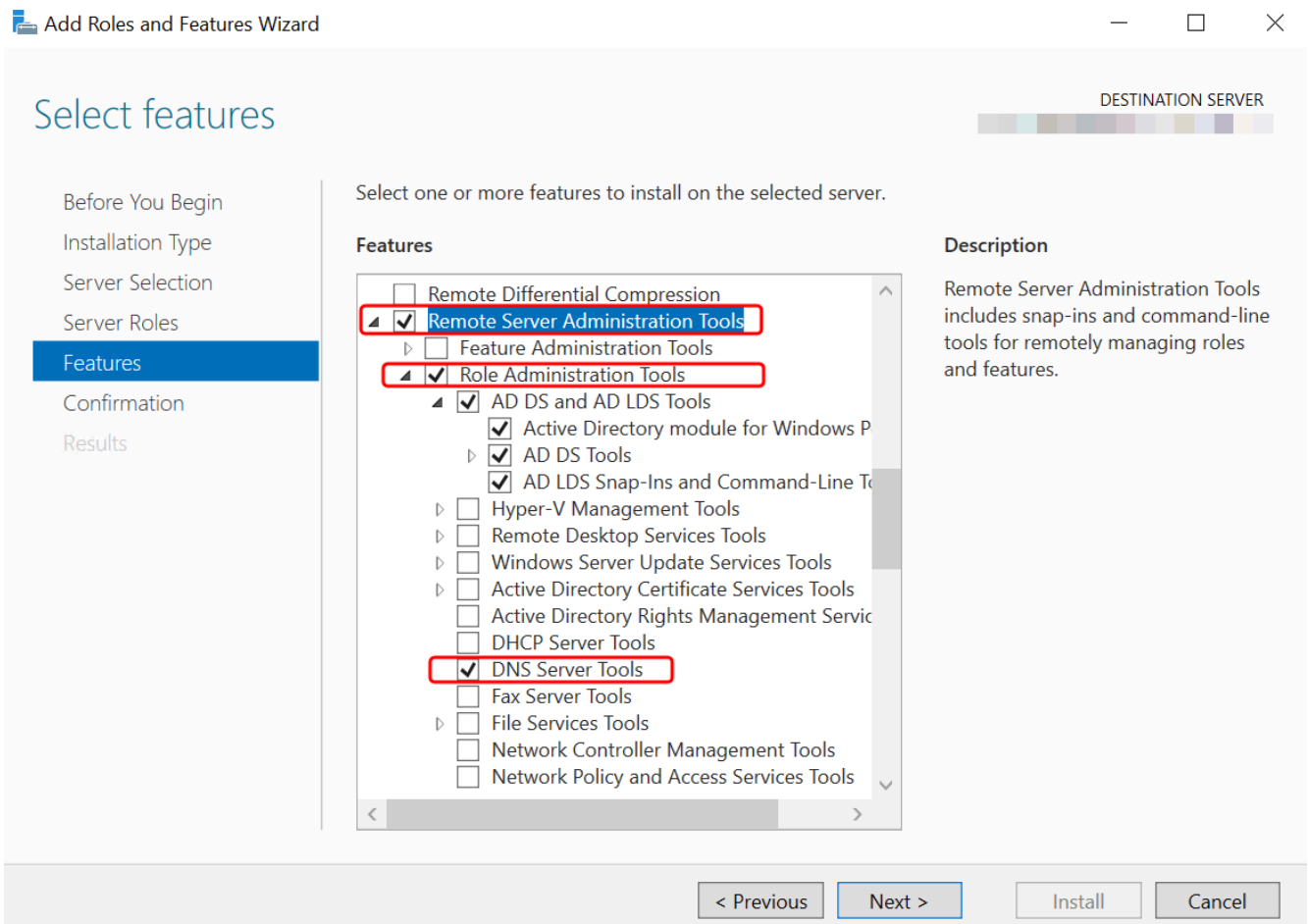
この手順を開始する前に、以下を完了してください。

1. AWS Managed Microsoft AD を作成しますActive Directory。詳細については、「[AWS Managed Microsoft AD の作成](#)」を参照してください。
2. EC2 Windows Server インスタンスを起動して AWS Managed Microsoft AD Active Directory に結合します。EC2 インスタンスでユーザーとグループを作成するには、以下のポリシーが必要です **AmazonSSMDirectoryServiceAccess** と **AmazonSSMManagedInstanceCore**。詳細については、「[AWS Managed Microsoft AD Active Directory でディレクトリの管理インスタンスを起動する](#)」および「[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)」を参照してください。
3. Active Directory ドメイン管理者の認証情報が必要になります。これらの認証情報は、AWS Managed Microsoft AD の作成時に作成されました。[AWS Managed Microsoft AD の作成](#)の手順に従った場合、管理者ユーザー名には NetBIOS 名 **corp\admin**が含まれます。

EC2 Windows Server インスタンスで Active Directory 管理ツールをインストールする

1. Amazon EC2 コンソールの <https://console.aws.amazon.com/ec2/> を開いてください。
2. Amazon EC2 コンソールで [インスタンス] を選択し、Windows Server インスタンスを選択して、[接続] を選択します。
3. [インスタンスに接続] ページで [RDP クライアント] を選択します。
4. [RDP クライアント] タブで [リモートデスクトップファイルのダウンロード] を選択し、[パスワードを取得] を選択してパスワードを取得します。
5. [Windows パスワードを取得] で、[プライベートキーファイルのアップロード] を選択します。Windows Server インスタンスに関連付けられている .pem プライベートキーファイルを選択します。プライベートキーファイルをアップロードしたら、[パスワードの復号化] を選択します。
6. [Windows セキュリティ] ダイアログボックスで、Windows Server コンピュータのローカル管理者の認証情報 をコピーしてサインインします。ユーザー名を **NetBIOS-Name\admin** または **DNS-Name\admin** の形式にすることができます。たとえば、[AWS Managed Microsoft AD の作成](#) の手順に従った場合**corp\admin**はユーザー名になります。

7. Windows Server インスタンスにサインインしたら、[スタート] メニューから [サーバーマネージャー] を選択して [サーバーマネージャー] を開きます。
8. [サーバー マネージャー] ダッシュボードで、[役割と機能の追加] を選択します。
9. [Add Roles and Features Wizard] (ロールと機能の追加ウィザード) で、[Installation Type] (インストールのタイプ) として [Role-based or feature-based installation] (ロールベースまたは機能ベースのインストール) を選択し、[Next] (次へ) をクリックします。
10. [Server Selection] (サーバーの選択) で、ローカルサーバーが選択されていることを確認し、左のナビゲーションペインの [Features] (機能) を選択します。
11. [機能] ツリーで、[リモートサーバー管理ツール]、[ロール管理ツール] の順に開き、[AD DS および AD LDS ツール] を選択します。[AD DS および AD LDS ツール] を選択すると、[PowerShell のための Active Directory もジュール]、[AD DS ツール]、および [AD LDS スナップインとコマンドラインツール] が選択されます。下にスクロールして [DNS サーバーツール] を選択し、[次へ] を選択します。



12. 情報を確認して [Install] (インストール) を選択します。機能のインストールが終了すると、Active Directory Domain Services と Active Directory Lightweight Directory Services ツールが [スタート] 画面の [管理ツール] フォルダから利用できるようになります。

PowerShell

PowerShell を使用して Active Directory 管理ツールをインストールできます。例えば、PowerShell プロンプトから `Install-WindowsFeature RSAT-ADDs` を使用して Active Directory リモート管理ツールをインストールすることが可能です。詳細については、Microsoft のウェブサイトの「[Install-WindowsFeature](#)」を参照してください。

Directory administration instance

[AWS Managed Microsoft AD Active Directory でディレクトリの管理インスタンスを起動する](#) の手順に従って、Active Directory Domain Services と Active Directory Lightweight Directory Services ツールが既にインストールされている AWS Management Console でディレクトリ管理 EC2 インスタンスを起動することができます。

AWS Managed Microsoft AD ユーザーの作成

AWS Managed Microsoft AD ユーザーを作成するには、Active Directory 管理ツールとを使用します PowerShell。Active Directory 管理ツールでユーザーを作成する前に、[AWS Managed Microsoft AD 用の Active Directory 管理ツールのインストール](#) の手順を完了する必要があります。

アクティブディレクトリ Administration Tools

Active Directory 管理ツールを使用して AWS Managed Microsoft AD ユーザーを作成するには、次の手順に従います。

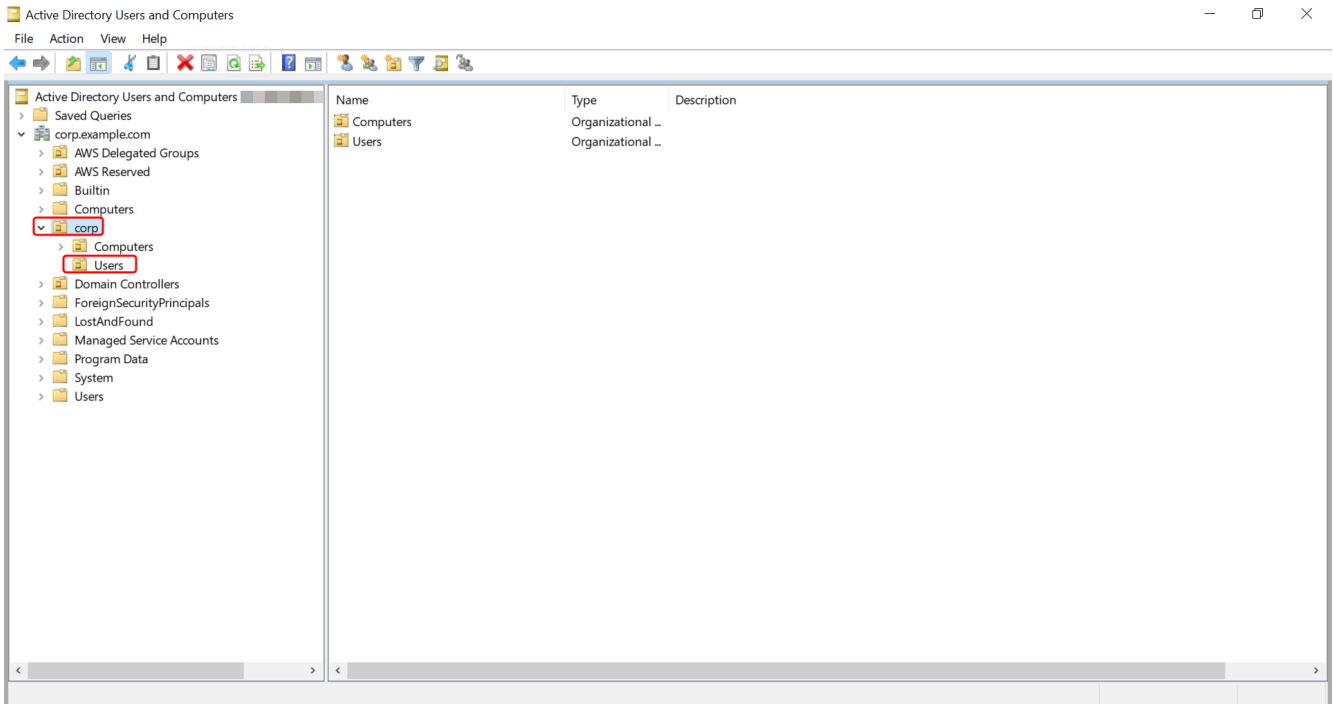
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Windows のスタートメニューから Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Windows Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリーで、ディレクトリの NetBIOS 名を持つ OU の下で、ユーザーを保存する OU (**corp\Users** など) を選択します。のディレクトリで使用される OU 構造の詳細については AWS、「」を参照してください[AWS Managed Microsoft AD で作成されるもの](#)。



4. [Action] メニューで、[New]、[User] の順に選択し、新規ユーザーのウィザードを開きます。
5. ウィザードの最初のページで、以下のフィールドに入力し、[Next] をクリックします。
 - [First name] (名)
 - [Last name] (姓)
 - [User logon name] (ユーザーのログオン名)
6. ウィザードの 2 番目のページで、[Password] と [Confirm Password] に、仮パスワードを入力します。[User must change password at next logon] (ユーザーは次回ログオン時にパスワードの変更が必要) オプションが選択されていることを確認します。その他のオプションは選択しないでください。[次へ] を選択します。
7. ウィザードの 3 番目のページで、新しいユーザーの情報が正しいことを確認し、[Finish] をクリックします。新しいユーザーが [Users] フォルダに表示されます。

PowerShell

を使用して AWS Managed Microsoft AD ユーザーを作成するには、次の手順に従います
PowerShell。

1. Active Directory 管理者として Active Directory ドメインと結合しているインスタンスに接続します。
2. PowerShell を開きます。
3. ユーザー名を、作成するユーザーの **jane.doe** ユーザー名に置き換えるコマンドを入力します。PowerShell によって新しいユーザーのパスワードを入力するよう求められます。Active Directory パスワードの複雑さの要件の詳細については、「[Microsoft ドキュメント](#)」を参照してください。New-ADUser コマンドの詳細については、[Microsoft ドキュメント](#)を参照してください。

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

Amazon EC2 インスタンスを使用してユーザーのアカウントを削除する

Managed AWS Microsoft AD に参加している Amazon EC2 インスタンスを持つユーザーを削除するには、次の手順に従います。

Note

この手順を完了する前に、Active Directory 管理ツールをインストールする必要があります。詳細については、「[Active Directory 管理ツールのインストール](#)」を参照してください。

ユーザーを削除するには

1. Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Windows Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

2. ディレクトリツリーで、削除するユーザーを含む OU (Corp\Users など) を選択します。
3. 削除するユーザーを選択します。[アクション] メニューで、[削除] を選択します。
4. ユーザーを削除するかどうかを確認するダイアログボックスが表示されます。[はい] を選択してユーザーを削除します。

削除されたユーザーは AD のごみ箱に一時的に保存されます。AD のごみ箱について詳しくは、Microsoft の「Ask the Directory Services Team」ブログにある「[The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting](#)」を参照してください。

AWS Managed Microsoft AD ユーザーパスワードのリセット

ユーザーは、Active Directory で定義されているパスワードポリシーに従う必要があります。時々、Active Directory 管理者などのユーザーであってもこのルールを覚えなくなり、パスワードを忘れてしまうこともあります。この場合、ユーザーが AWS Managed Microsoft AD に属する AWS Directory Service している場合は、を使用してユーザーのパスワードをすばやくリセットできます。

パスワードをリセットするには、リセットに必要な権限を持つユーザーとしてサインインする必要があります。権限の詳細については、「[AWS Directory Service リソースへのアクセス許可の管理の概要](#)」を参照してください。

Active Directory 内のユーザーのパスワードを、以下の例外を除きリセットすることが可能です：

- Active Directory の作成時に使用した NetBIOS 名に基づく組織単位 (OU) 内の任意のユーザーのパスワードをリセットできます。例えば、[AWS Managed Microsoft AD の作成](#) の手順に従った場合、NetBIOS 名は CORP になり、リセットできるユーザーのパスワードは Corp/Users OU のメンバーになります。
- Active Directory の作成時に使用した NetBIOS 名に基づく OU 以外のユーザーのパスワードをリセットすることはできません。例えば、[AWS 予約済みの OU] にいるユーザーのパスワードはリセットできません。AWS Managed Microsoft AD の OU 構造の詳細については、「」を参照してください。[AWS Managed Microsoft AD で作成されるもの](#)。

AWS Managed Microsoft AD でパスワードがリセットされたときにパスワードポリシーを適用する仕組みの詳細については、[パスワードポリシーの適用方法](#) を参照してください。

Managed AWS Microsoft AD ユーザーパスワードをリセットするには、次のいずれかのツールを使用できます。

- AWS Management Console
- AWS CLI
- PowerShell

AWS Management Console

で AWS Managed Microsoft AD ユーザーパスワードをリセットするには、次の手順に従います AWS Management Console。

1. [\[AWS Directory Service コンソール\]](#) のナビゲーションペインで、[Active Directory] の下にある [ディレクトリ] を選択し、リスト内でパスワードをリセットしたい Active Directory を選択します。
2. [ディレクトリの詳細] ページで、[アクション] を選択して [ユーザーパスワードのリセット] をクリックします。
3. [Reset user password] ダイアログで、[Username] に、パスワードの変更が必要なユーザーの名前を入力します。
4. [New password] (新しいパスワード) と [Confirm Password] (パスワードの確認) にパスワードを入力した上で、[Reset password] (パスワードをリセットする) をクリックします。

AWS CLI

で AWS Managed Microsoft AD ユーザーパスワードをリセットするには、次の手順に従います AWS CLI。

1. をインストールするには AWS CLI、[「 の最新バージョンのインストールまたは更新 AWS CLI」](#) を参照してください。
2. を開きます AWS CLI。
3. 次のコマンドを入力し、ディレクトリ ID、ユーザー名 **jane.doe**、パスワード **P@ssw0rd** を自分の Active Directory ディレクトリ ID と必要な認証情報に置き換えます。詳細については、「AWS CLI コマンドリファレンス」の [「reset-user-password」](#) を参照してください。

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

PowerShell

で AWS Managed Microsoft AD ユーザーパスワードをリセットするには、次の手順に従います PowerShell。

1. Active Directory 管理者として Active Directory ドメインと結合しているインスタンスに接続します。
2. PowerShell を開きます。
3. 次のコマンドを入力し、ユーザー名 **jane.doe**、ディレクトリ ID、およびパスワード **P@ssw0rd** を自分の Active Directory ディレクトリ ID と必要な認証情報に置き換えます。詳細については、「[Reset-DSUserPassword Cmdlet](#)」(Reset-DSUserPassword コマンドレット) を参照してください。

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

AWS Managed Microsoft AD グループの作成

AWS Managed Microsoft AD でグループを作成できます。Managed Microsoft AD ディレクトリに参加している Amazon EC2 AWS インスタンスを使用してセキュリティグループを作成するには、次の手順に従います。セキュリティグループを作成する前に、「Active Directory 管理ツールのインストール」の手順を完了する必要があります。

アクティブディレクトリ Administration Tools

Active Directory 管理ツールを使用して AWS Managed Microsoft AD グループを作成するには、次の手順に従います。

グループを作成するには

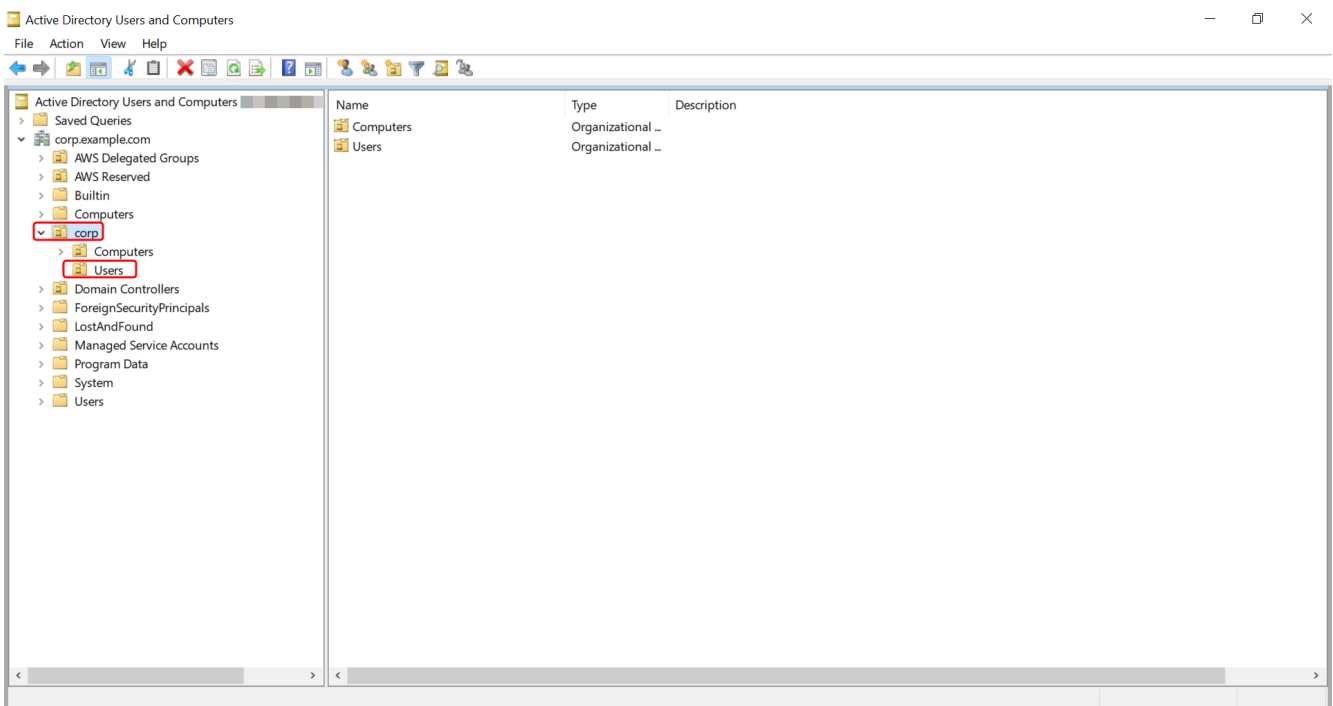
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリー内で、ディレクトリの NetBIOS 名を持つ OU の下から、グループを保存する OU (Corp\ Users など) を選択します。のディレクトリで使用する OU 構造の詳細については AWS、「」を参照してください[AWS Managed Microsoft AD で作成されるもの](#)。



4. [Action] (アクション) メニューで、[New] (新規)、[Group] (グループ) の順に選択し、新規グループのウィザードを開きます。
5. [グループ名] にグループの名前を入力し、[グループのスコープ] を選択します。[グループの種類] から [セキュリティ] を選択します。Active Directory グループのスコープとセキュリティグループの詳細については、Microsoft Windows Server ドキュメントの「[Active Directory セキュリティグループ](#)」を参照してください。
6. [OK] をクリックします。新しいセキュリティグループが [Users] フォルダに表示されます。

PowerShell

PowerShell コマンドを使用してグループを作成できます。詳細については、Windows Server 2022 PowerShell ドキュメントの「[New-ADGroup](#)」を参照してください。

AWS Managed Microsoft AD ユーザーをグループに追加する

AWS Managed Microsoft AD ユーザーをグループに追加できます。Managed Microsoft AD ディレクトリに参加している Amazon EC2 AWS インスタンスを持つセキュリティグループにユーザーを追加するには、次の手順に従います。

アクティブディレクトリ Administration Tools

ユーザーをグループに追加するには

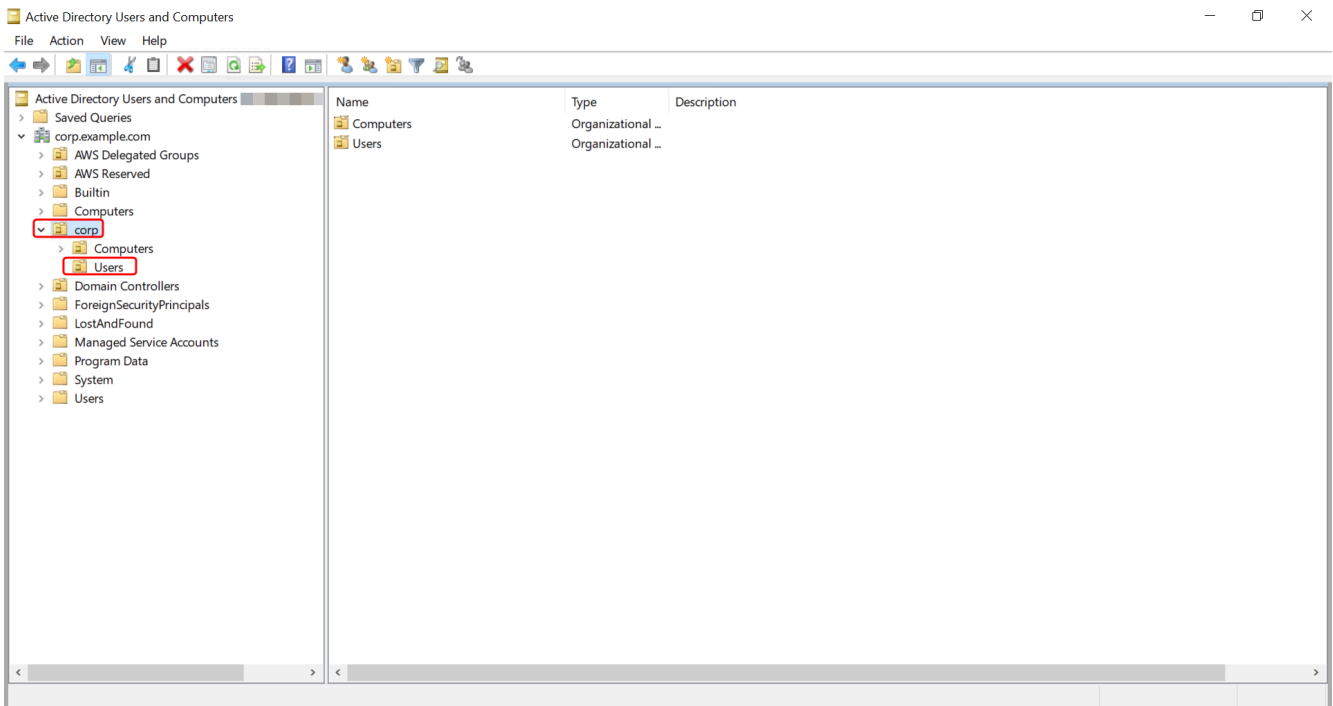
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリーで、グループを保存したディレクトリの NetBIOS 名を持つ OU の下にある OU を選択し、ユーザーをメンバーとして追加するグループを選択します。



4. [Action] (アクション) メニューで、[Properties] (プロパティ) をクリックしてグループのプロパティダイアログボックスを開きます。
5. [Members] (メンバー) タブを開き、[Add] (追加) をクリックします。
6. [Enter the object names to select] で、追加するユーザー名を入力した後、[OK] をクリックします。対象の名前が [Members] (メンバー) リストに表示されます。もう一度 [OK] をクリックしてグループのメンバーシップを更新します。
7. [Users] フォルダでこのユーザーを選択し、[Action] (操作) メニューの [Properties] (プロパティ) をクリックしてプロパティダイアログボックスを開いて、ユーザーがグループのメンバーになっていることを確認します。[Member Of] (所属するグループ) タブを開きます。ユーザーが所属するグループのリストに、グループの名前が表示されます。

AWS Directory Service データ

AWS Directory Service Data は の拡張機能です AWS Directory Service。Amazon EC2 インスタンスに専用の AD 管理インスタンスをデプロイすることなく、Microsoft Active Directory 用 AWS Directory Service からユーザー、グループ、メンバーシップを作成、読み取り、更新、および Active Directory (AD) できます。また、直接ネットワーク接続なしで、ディレクトリ間で組み込みのオブジェクト管理タスクを実行することもできます。これにより、プロビジョニングとアクセス管理が簡素化され、完全に自動化されたデプロイが実現します。詳細については、「[AWS Directory Service Data API Reference](#)」を参照してください。

Directory Service Data は、組織単位 (OU) にある AWS Managed Microsoft AD 内で CreateGroup、CreateUser やなどのユーザーおよびグループの書き込みオペレーションをサポートします。Directory Service Data は、AWS Managed Microsoft AD 内のすべてのユーザー ListGroups、グループ、グループメンバーシップ、および信頼できる領域にわたる ListUsers やなどの読み取りオペレーションをサポートします。Directory Service Data は、OU および AWS 委任グループ OU 内のグループへのグループメンバーの追加と削除をサポートしているため、特定の委任グループオブジェクトにユーザーを追加することでアクセス許可を委任できます。詳細については、「[AWS Managed Microsoft AD でのユーザーとグループの管理](#)」を参照してください。

Note

Directory Service Data は、プライマリリージョンでのみ使用できます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

トピック

- [レプリケーションと整合性](#)
- [AWS Directory Service Data 属性](#)
- [グループタイプとグループスコープ](#)

レプリケーションと整合性

Directory Service Data API は AWS Managed Microsoft AD ドメインコントローラーに接続して、基盤となるディレクトリオブジェクトに対してオペレーションを実行します。Active Directory は結果整合性のあるプラットフォームであり、AWS Directory Service ディレクトリドメインコントローラー間でレプリケーションが継続的に発生しています。デフォルトでは、すべての AWS Directory Service ディレクトリは 2 つのドメインコントローラーで作成されます。

Directory Service Data は、リクエスト間で同じドメインコントローラーを使用することで、整合的なエクスペリエンスを維持しようとします。ドメインコントローラーが使用できない場合、Directory Service Data は代替ドメインコントローラーに切り替えます。これらのイベント中に、オブジェクトがドメインコントローラー間でレプリケートされている間、ドメインコントローラー間で最終的な整合性に気付くことがあります。

ディレクトリの制限は AWS Managed Microsoft AD エディションによって異なります。

- Standard Edition – ディレクトリごとに読み取りオペレーションで 1 秒あたり 8 トランザクション、書き込みオペレーションで 4 TPS をサポートします。

- Enterprise Edition – ディレクトリごとに読み取りオペレーションで 1 秒あたり 16 のトランザクション、書き込みオペレーションで 8 TPS をサポートします。

 Note

Standard Edition と Enterprise Edition の両方で、同時リクエストは 10 件に制限されています。

- AWS アカウント – すべてのディレクトリで、Directory Service Data オペレーションに対して 1 秒あたり合計 100 件のトランザクションをサポートします。

AWS Directory Service Data 属性

このトピックでは、「[AWS Directory Service Data API 参照](#)」の属性を操作する方法について説明します。

リクエスト属性

リクエスト本文のパラメータでは、次の属性を定義する必要があります。これらの属性を定義する方法の例については、「AWS Directory Service Data API Reference」の「[CreateGroup](#)」を参照してください。

Directory Service Data 属性名	LDAP 表示名	AWS Management Console	PowerShell イエイリアス	アクセスタイプ	オブジェクトの種類	属性値	検索可能
DistinguishedName	distinguishedName	識別名	なし	ReadOnly	ユーザー、グループ	String	いいえ
EmailAddress	mail	E メールアドレス	EmailAddress	作成可能	ユーザー	String	はい
有効	なし	有効	有効	Mutable	ユーザー	ブール値	いいえ

Directory Service Data 属性名	LDAP 表示名	AWS Management Console	PowerShell エイリアス	アクセスタイプ	オブジェクトの種類	属性値	検索可能
GivenName	givenName	[First Name] (名)	GivenName	作成可能	ユーザー	String	はい
GroupScope	groupScope	グループのスコープ	なし	作成可能	グループ	列挙型	いいえ
GroupType	groupType	グループのタイプ	なし	作成可能	グループ	列挙型	いいえ
SamAccountName	sAMAccountName	[User login name] (ユーザーのログオン名)	sAMAccountName	作成可能	ユーザー、グループ	String	はい
SID	objectSid	ユーザー/グループのセキュリティ識別子 (SID)	SID	ReadOnly	ユーザー、グループ	String	いいえ
Surname	sn	姓	Surname	作成可能	ユーザー	String	はい
UserPrincipalName	userPrincipalName	ユーザープリンシパル名	UserPrincipalName	ReadOnly	ユーザー	String	いいえ

その他の属性

次の属性は `OtherAttributes` で定義する必要があり、リクエスト本文パラメータにはマッピングされません。リクエストで他の属性を定義する場合は、属性名、データタイプ、および各属性の値を指定する必要があります。これらの属性を定義する方法の例については、「AWS Directory Service Data API Reference」の「[CreateUser](#)」を参照してください。

Note

これらの属性の名前は入力として提供され、LDAP 表示名と同等である場合、大文字と小文字を区別しません。

Directory Service Data 属性名	LDAP 表示名	AWS Management Console	PowerShell エイリアス	アクセスタイプ	オブジェクトの種類	属性値	検索可能
Assistant	assistant	Assistant	なし	ReadOnly	ユーザー	String	いいえ
Cn	cn	共通名	なし	ReadOnly	ユーザー、グループ	String	いいえ
Co	co	国/リージョン	国	Mutable	ユーザー	String	いいえ
Company	company	Company	Company	作成可能	ユーザー	String	いいえ
Department	department	Department	Department	作成可能	ユーザー	String	いいえ
説明	description	説明	説明	作成可能	ユーザー、グループ	String	いいえ
DirectReports	directReports	直属部下	なし	ReadOnly	ユーザー	文字列セット	いいえ

Directory Service Data 属性名	LDAP 表示名	AWS Management Console	PowerShell エイリアス	アクセスタイプ	オブジェクトの種類	属性値	検索可能
DisplayName	displayName	Display name (表示名)	DisplayName	作成可能	ユーザー、グループ	String	はい
FacsimileTelephoneNumber	facsimileTelephoneNumber	Fax	Fax	作成可能	ユーザー、グループ	String	いいえ
HomePhone	homePhone	自宅の電話番号	HomePhone	作成可能	ユーザー	String	いいえ
情報	情報	メモ	なし	Mutable	ユーザー、グループ	String	いいえ
Initials	initials	Initials	Initials	ReadOnly	ユーザー	String	いいえ
IpPhone	ipPhone	IP 電話	なし	Mutable	ユーザー	String	いいえ
L	l	市町村	市町村	作成可能	ユーザー	String	はい
Manager	manager	Manager	Manager	Mutable	ユーザー	String	いいえ
Mail	mail	E メールアドレス	EmailAddress	Mutable	グループ	String	はい
モバイル	モバイル	携帯電話番号	MobilePhone	Mutable	ユーザー	String	いいえ
ObjectClass	objectClass	ユーザー/グループ	なし	ReadOnly	グループ	String	いいえ

Directory Service Data 属性名	LDAP 表示名	AWS Management Console	PowerShell エイリアス	アクセスタイプ	オブジェクトの種類	属性値	検索可能
ObjectGUID	objectGUID	グローバル一意識別子 (GUID)	なし	ReadOnly	ユーザー、グループ	String	いいえ
Pager	pager	ページャー	なし	Mutable	ユーザー	String	いいえ
PhysicalDeliveryOfficeName	physicalDeliveryOfficeName	Office	なし	作成可能	ユーザー	String	はい
PostalCode	postalCode	郵便番号	PostalCode	作成可能	ユーザー	String	いいえ
PreferredLanguage	preferredLanguage	優先言語	なし	Mutable	ユーザー	String	いいえ
ProxyAddresses	proxyAddresses	プロキシアドレス	なし	ReadOnly	ユーザー、グループ	複数値の文字列	はい
ServicePrincipalName	servicePrincipalName	サービスプリンシパル名	ServicePrincipalName	Mutable	ユーザー	複数値の文字列	いいえ
State	st	都道府県	状態	作成可能	ユーザー	String	いいえ
StreetAddress	streetAddress	番地	StreetAddress	作成可能	ユーザー	String	いいえ
TelephoneNumber	telephoneNumber	電話番号	OfficePhone	作成可能	ユーザー	String	いいえ

Directory Service Data 属性名	LDAP 表示名	AWS Management Console	PowerShell エイリアス	アクセスタイプ	オブジェクトの種類	属性値	検索可能
タイトル	title	役割	タイトル	ReadOnly	ユーザー	String	いいえ
WhenChanged	whenChanged	最終更新日	なし	ReadOnly	ユーザー、グループ	String	いいえ
WWWHomepage	wWWHomepage	ホームページ URL	wWWHomepage	Mutable	ユーザー、グループ	String	いいえ

グループタイプとグループスコープ

AWS Managed Microsoft AD のグループには、グループタイプとグループスコープの両方があります。それぞれの詳細については、以下のセクションを参照してください。

トピック

- [グループのタイプ](#)
- [グループのスコープ](#)

グループのタイプ

グループタイプは、グループがアクセスできる Active Directory 内の共有リソースを決定します。グループタイプは 2 つあります:

- セキュリティ – グループメンバーが共有された Active Directory リソースにアクセスできるように、これらのグループのアクセス権限を割り当てることができます。
- ディストリビューション – このタイプを使用してメールディストリビューションリストを作成できます。これらのグループメンバーは、Active Directory の共有リソースにアクセスできません。

グループタイプ間での変更には制限はありません。

グループタイプの詳細については、「[Microsoft ドキュメント](#)」を参照してください。

グループのスコープ

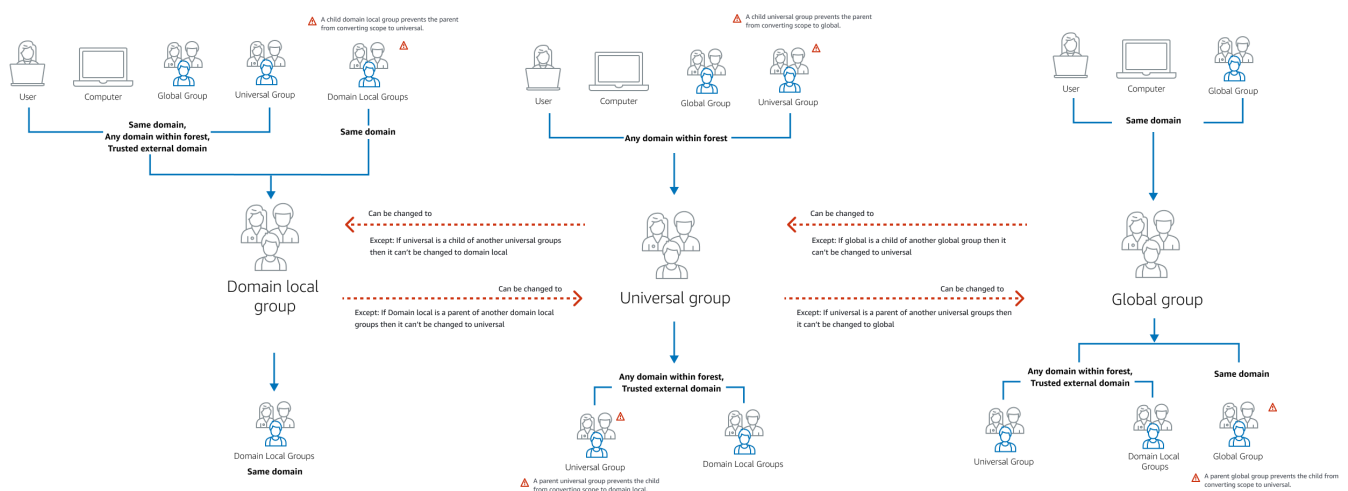
グループスコープは、ドメインツリーまたはフォレストでグループメンバーを定義する方法を決定します。3つのグループスコープがあります：

- ドメインローカル – 同じドメインにあるグループメンバーにアクセス権を割り当てます。
- ユニバーサル – 任意のドメイン内にあるグループメンバーにアクセス権を割り当てます。
- グローバル – 任意のドメインまたはフォレスト内にあるグループメンバーにアクセス権を割り当てます。

グループスコープの変更には制限があります。次のリストと図は、これらの制限の概要を示しています。

- グループスコープを [ドメインローカル] から [ユニバーサル] に変更する – はい
 - ドメインローカルグループが別のドメインローカルグループの親でない限り。
- グループスコープを [ユニバーサル] から [ドメインローカル] に変更する – はい
 - ユニバーサルグループが別のユニバーサルグループの子グループでない限り。
- グループスコープを [ユニバーサル] から [グローバル] に変更する – はい
 - ユニバーサルグループが別のユニバーサルグループの親でない限り。
- グループスコープを [グローバル] から [ユニバーサル] に変更する – はい
 - グローバルグループが別のグローバルグループの子でない限り。

グループスコープの詳細については、「[Microsoft ドキュメント](#)」を参照してください。



AWS Managed Microsoft AD を に接続する Microsoft Entra Connect Sync

このチュートリアルでは、 を AWS Managed Microsoft AD [Microsoft Entra ID](#)に同期[Microsoft Entra Connect Sync](#)するために をインストールするために必要な手順について説明します。

このチュートリアルでは、以下の作業を行います。

1. AWS Managed Microsoft AD ドメインユーザーを作成します。
2. Entra Connect Sync をダウンロードします。
3. PowerShell を使用してスクリプトを実行して、新しく作成したユーザーに適切なアクセス権限をプロビジョニングします。
4. Entra Connect Sync をインストールします。

前提条件

このチュートリアルを完了するために必要なものは以下のとおりです。

- AWS Managed Microsoft AD。詳細については、「[the section called “AWS Managed Microsoft AD の作成”](#)」を参照してください。
- AWS Managed Microsoft AD に結合された Amazon EC2 Windows Server インスタンス。詳細については、「[Windows インスタンスへの結合](#)」を参照してください。
- AWS Managed Microsoft AD を管理するためにActive DirectoryAdministration Toolsインストールされている EC2 Windowsサーバー。詳細については、「[the section called “AD 管理ツールのインストール”](#)」を参照してください。

Active Directory のドメインユーザーを作成する

このチュートリアルでは、AWS Managed Microsoft AD と がインストールされている EC2 Windows Server インスタンスが既にActive DirectoryAdministration Toolsあることを前提としています。詳細については、「[the section called “AD 管理ツールのインストール”](#)」を参照してください。

1. Active Directory Administration Tools インストールしたインスタンスに接続します。
2. AWS Managed Microsoft AD ドメインユーザーを作成します。このユーザーは Entra Connect Sync の Active Directory Directory Service (AD DS) Connector account になります。このプロセスの詳細なステップについては、「[the section called “ユーザーの作成”](#)」を参照してください。

Entra Connect Sync のダウンロード

- [Microsoft ウェブサイト](#) Entra Connect Sync から AWS Managed Microsoft AD 管理者である EC2 インスタンスにダウンロードします。

Warning

この時点では Entra Connect Sync を開いたり実行したりしないでください。次のステップでは、ステップ 1 で作成したドメインユーザーに必要なアクセス権限をプロビジョニングします。

スクリプト PowerShell を実行

- [管理者として PowerShell を開き](#)、次のスクリプトを実行します。

スクリプトの実行中に、ステップ 1 から新しく作成したドメインユーザーの [sAMAccountName](#) を入力するように求められます。

Note

スクリプトの実行の詳細については、以下を参照してください:

- ps1 拡張子を持つスクリプトは、**temp** のようなフォルダに保存できます。スクリプトを読み込むには、次の PowerShell コマンドを実行できます。

```
import-module "c:\temp\entra.ps1"
```

- スクリプトをロードしたら、次のコマンドを使用してスクリプトを実行するための必要なアクセス権限を設定し、**Entra_Service_Account_Name** を Entra サービスアカウント名に置き換えます:

```
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'

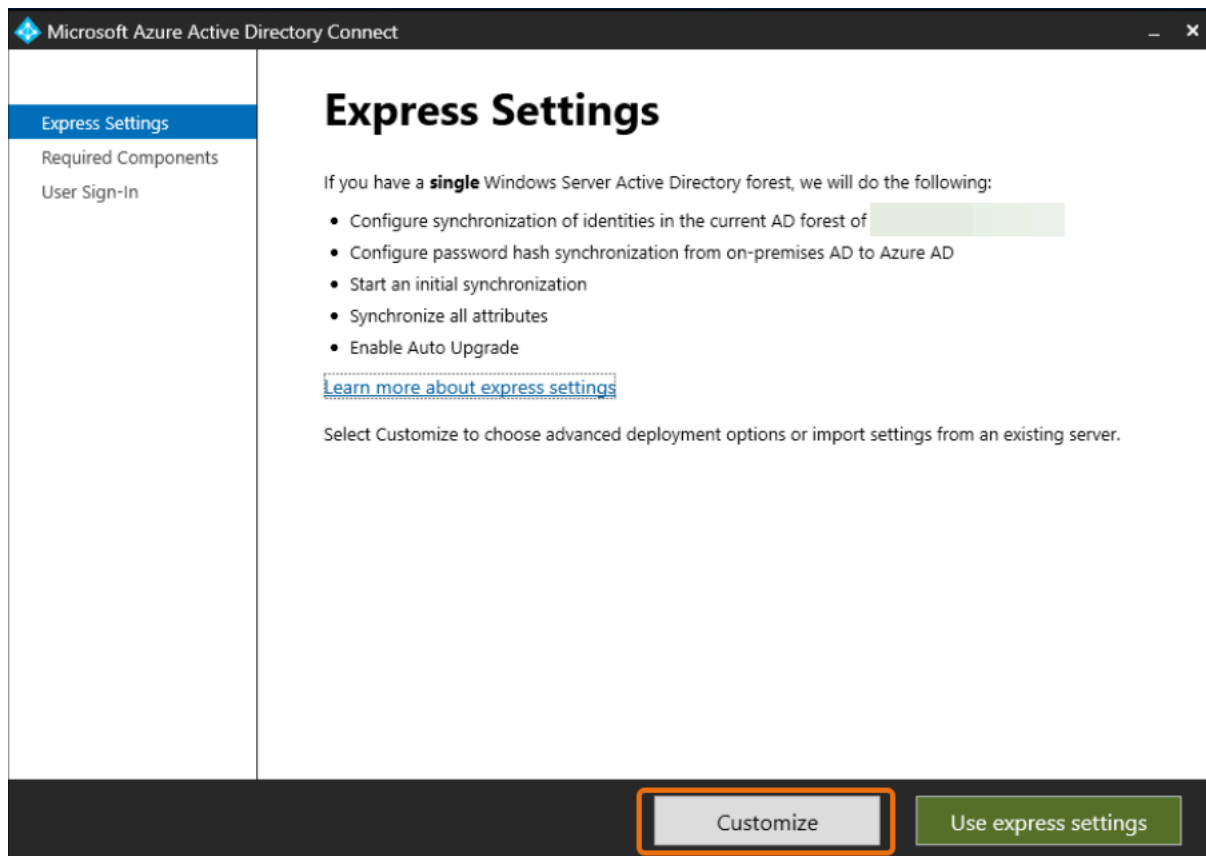
    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    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 : $_"  
    }  
}  
}
```

Entra Connect Sync をインストールする

1. スクリプトが完了したら、ダウンロードした Microsoft Entra Connect (以前は Azure Active Directory Connect と呼ばれていた) 設定ファイルを実行できます。
2. 前のステップの設定ファイルを実行した後、Microsoft Azure Active Directory Connect ウィンドウが開きます。[Express の設定] ウィンドウで、[カスタマイズ] を選択します。



3. [必要なコンポーネントのインストール] ウィンドウで、[既存のサービスアカウントを使用する] チェックボックスを選択します。[サービスアカウント名] と [サービスアカウントパスワード] で、ステップ 1 で作成したユーザーの AD DS Connector account 名とパスワードを入力します。例えば、AD DS Connector account 名が entra とすると、アカウント名は corp\entra となります。次に、[インストール] を選択します。

Microsoft Azure Active Directory Connect

Welcome
Express Settings
Required Components
User Sign-In

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed. ?

☐ Specify a custom installation location

☐ Use an existing SQL Server

☒ Use an existing service account

☐ Managed Service Account

☒ Domain Account

SERVICE ACCOUNT NAME

corp\entra

SERVICE ACCOUNT PASSWORD

.....

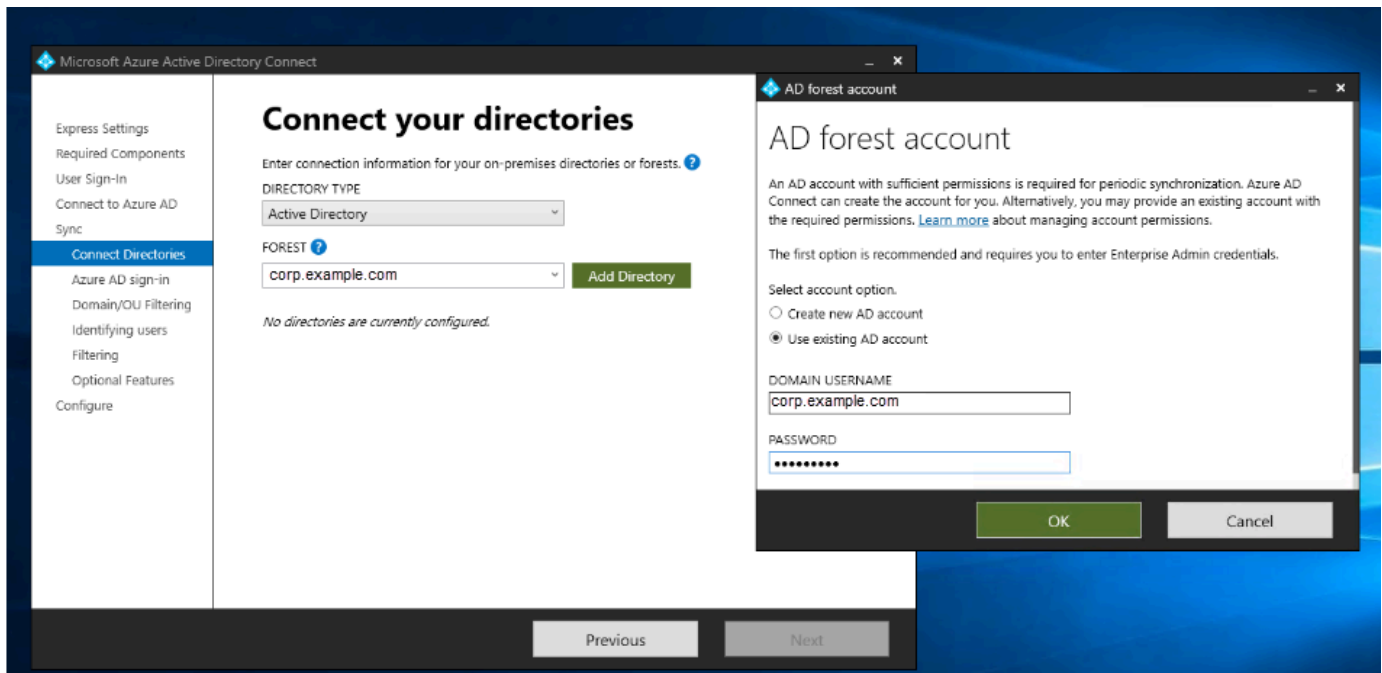
☐ Specify custom sync groups

☐ Import synchronization settings ?

Previous Install

4. [ユーザーサインイン] ウィンドウで、次のいずれかのオプションを選択します:
 - a. 「[パススルー認証](#)」 – このオプションを使用すると、ユーザー名とパスワードを使用して Active Directory にサインインできます。
 - b. 「設定しない」 – これにより Microsoft Entra、(以前は Azure Active Directory (Azure AD) と呼ばれた) または Office 365 でフェデレーションサインインを利用できます。
- [次へ] を選択します。
5. [Azure に接続する] ウィンドウで、Entra ID の [グローバル管理者](#) のユーザー名とパスワードを入力し、[次へ] を選択します。
6. [ディレクトリを接続する] ウィンドウで、Active Directory を [ディレクトリタイプ] に選択します。FOREST 用の AWS Managed Microsoft AD のフォレストを選択します。次に、[ディレクトリの追加] を選択します。

7. アカウントオプションをリクエストするポップアップボックスが表示されます。[既存の AD アカウントを使用する] を選択します。ステップ 1 で作成した AD DS Connector account のユーザー名とパスワードを入力し、[確認] を選択します。[次へ] を選択します。



8. [Azure AD サインイン] ウィンドウで、検証済みのバニティドメインが Entra ID に追加されていない場合にのみ、[すべての UPN サフィックスを検証済みのドメインと一致せずに続行] を選択します。[次へ] を選択します。
9. [ドメイン/OU フィルタリング] ウィンドウで、必要に応じてオプションを選択します。詳細については、Microsoft ドキュメントの「[Entra Connect Sync 設定ファイル](#)」を参照してください。[次へ] を選択します。
10. [ユーザーの特定、フィルタリング、およびオプションの機能] ウィンドウで、デフォルト値を維持し、[次へ] を選択します。
11. [設定] ウィンドウで、設定を確認し、[設定] を選択します。Entra Connect Sync のインストールが確定され、ユーザーは Microsoft Entra ID との同期を開始します。

AWS Managed Microsoft AD テストラボのチュートリアル

このセクションでは、AWS Managed Microsoft AD を試すことができるテストラボ環境をで確立するのに役立つ一連のガイド付きチュートリアルを提供します。

トピック

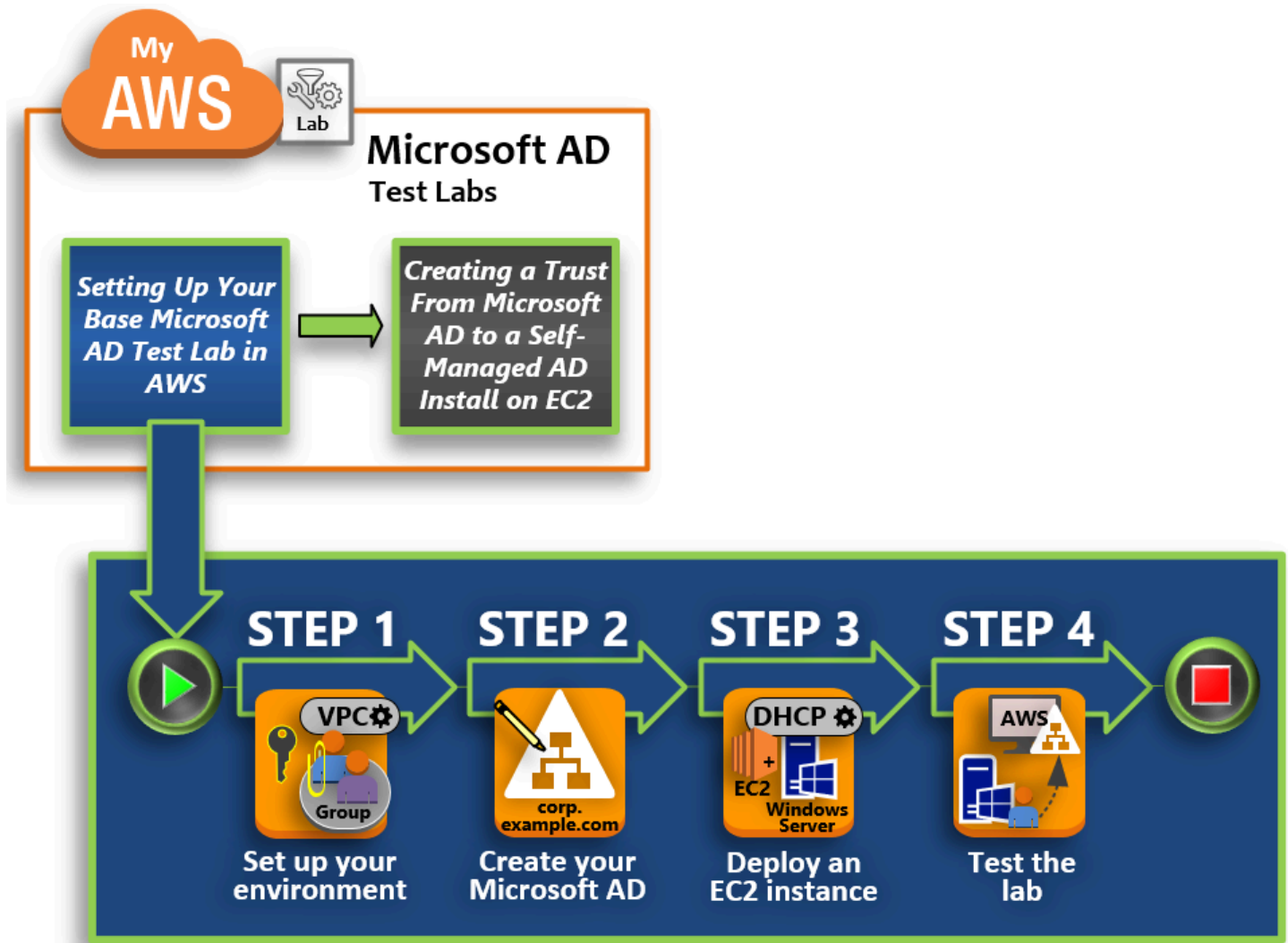
- [チュートリアル: で基本的な AWS Managed Microsoft AD テストラボをセットアップする AWS](#)

- [チュートリアル: AWS Managed Microsoft AD から Amazon EC2 へのセルフマネージド Active Directory インストールへの信頼の作成](#)

チュートリアル: で基本的な AWS Managed Microsoft AD テストラボをセットアップする AWS

このチュートリアルでは、Windows Server 2019 を実行する新しい Amazon EC2 インスタンスを使用する新しい AWS Managed Microsoft AD インストールを準備するように AWS 環境を設定する方法について説明します。次に、一般的な Active Directory 管理ツールを使用して EC2 Windows インスタンスから AWS Managed Microsoft AD 環境を管理する方法について説明します。チュートリアルを完了するまでに、ネットワークの前提条件を設定し、新しい AWS Managed Microsoft AD フォレストを設定します。

次の図に示すように、このチュートリアルで作成したラボは、AWS Managed Microsoft AD に関する実践的な学習の基盤となるコンポーネントです。後に、この土台を他のチュートリアルでも使用することで、実践的な経験をさらに積むことができます。このチュートリアルシリーズは、AWS Managed Microsoft AD の使用を始めたばかりで、評価目的のためにテストラボを試したいと考えているユーザーに最適です。チュートリアルの所要時間は約 1 時間です。



ステップ 1: AWS Managed Microsoft AD Active Directory の AWS 環境を設定する

前提条件タスクを完了した後、EC2 インスタンス内で Amazon VPC を作成および構成します。

ステップ 2: AWS Managed Microsoft AD Active Directory を作成する

このステップでは、AWS で初めて AWS Managed Microsoft AD を設定します。

ステップ 3: Amazon EC2 インスタンスをデプロイして AWS Managed Microsoft AD Active Directory を管理する

ここでは、クライアントコンピュータから新しいドメインに接続し、EC2 で Windows Server システムをセットアップするために必要なデプロイ後の各種タスクを実行していきます。

ステップ 4: 基本テストラボが正常に機能することを確認する

最後に、管理者として、EC2 の Windows Server システムから AWS Managed Microsoft AD にログインして接続できることを確認します。テストにより、このラボが正常に機能することが確認できれば、さらに他のテストラボのガイドモジュールを追加していくことができます。

前提条件

このチュートリアルでの UI 手順のみを使用してテストラボを作成する場合は、この前提条件のセクションをスキップしてステップ 1 に進むことができます。ただし、AWS CLI コマンドまたは AWS Tools for Windows PowerShell モジュールを使用してテストラボ環境を作成する場合は、まず以下を設定する必要があります。

- アクセスキーとシークレットアクセスキーを持つ IAM ユーザー – AWS CLI または AWS Tools for Windows PowerShell モジュールを使用する場合は、アクセスキーを持つ IAM ユーザーが必要です。アクセスキーがない場合は、「[アクセスキーの管理 \(AWS Management Console\)](#)」を参照してください。
- AWS Command Line Interface (オプション) – [Windows AWS CLI をダウンロードしてインストール](#)します。インストールが完了したら、コマンドプロンプトまたは PowerShell ウィンドウを開き、そして `aws configure` を入力します。このセットアップを完了するには、アクセスキーとシークレットキーが必要なことにご注意ください。この作業に必要な手順については最初の前提条件を参照してください。以下を指定することを求められます。
 - AWS アクセスキー ID [None]: AKIAIOSFODNN7EXAMPLE
 - AWS シークレットアクセスキー [なし]: wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
 - デフォルトのリージョン名 [None]: us-west-2
 - デフォルトの出力形式 [None]: json
- AWS Tools for Windows PowerShell (オプション) – 最新バージョンの AWS Tools for Windows PowerShell を <https://aws.amazon.com/powershell/> からダウンロードしてインストールした上で、以下のコマンドを実行します。このセットアップを完了するには、アクセスキーとシークレットキーが必要なことにご注意ください。この作業に必要な手順については最初の前提条件を参照してください。

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey  
{wJalrXUtnFEMI/K7MDENG/ bPxrFiCYEXAMPLEKEY} -StoreAs {default}
```

ステップ 1: AWS Managed Microsoft AD Active Directory の AWS 環境を設定する

AWS テストラボで AWS Managed Microsoft AD を作成する前に、まずすべてのログインデータが暗号化されるように Amazon EC2 キーペアを設定する必要があります。

キーペアを作成する

既存のキーペアがある場合は、このステップを省略できます。Amazon EC2 キーペアの詳細については、「[キーペアの作成](#)」を参照してください。

キーペアを作成するには

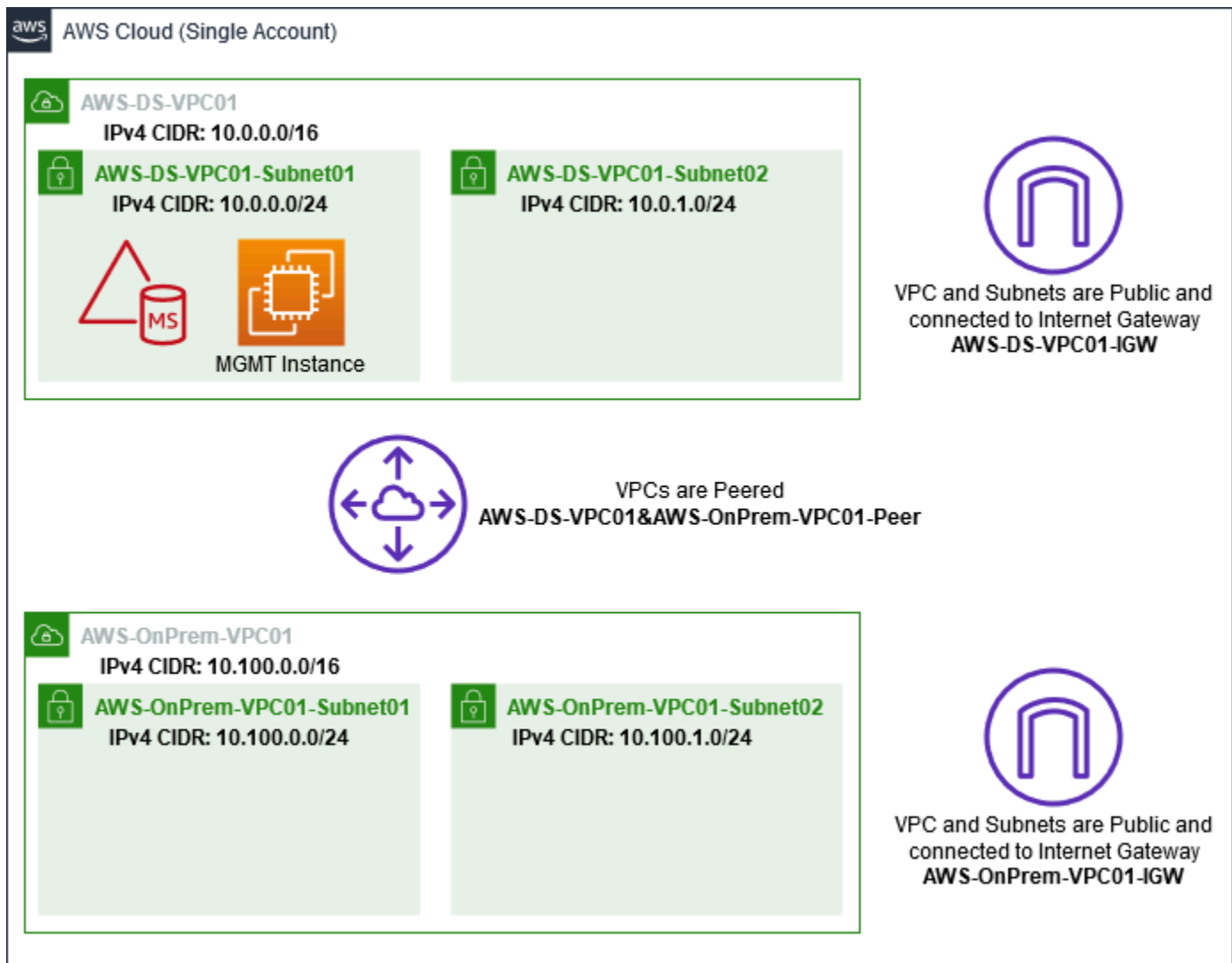
1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
2. ナビゲーションペインの [Network & Security] (ネットワークとセキュリティ) で、[Key Pairs] (キーペア)、[Create Key Pair] (キーペアを作成) の順に選択します。
3. [Key Pair Name] (キーペア名) に「**AWS-DS-KP**」と入力します。[Key pair file format] (キーペアのファイル形式) で、[pem] を選択した上で、[Create] (作成) をクリックします。
4. ブラウザによって秘密キーファイルが自動的にダウンロードされます。このファイル名は、キーペアを作成した際に指定した名前で、拡張子は .pem となります。ダウンロードしたプライベートキーのファイルを安全な場所に保存します。

Important

プライベートキーのファイルを保存できるのは、このタイミングだけです。インスタンスの起動時にはキーペア名を指定する必要があり、インスタンスのパスワードを復号する際には、対応するプライベートキーを毎回指定する必要があります。

2 つの Amazon VPC を作成、設定、およびピアリングします。

次の図に示すように、複数ステップによるこのプロセスを完了すると、2 つのパブリック VPC、VPC ごとに 2 つのパブリックサブネット、VPC ごとに 1 つのインターネットゲートウェイ、および VPC の間に 1 つの VPC ピアリング接続が作成および設定されます。ここでは、シンプルさとコストを考慮し、パブリック VPC およびサブネットを使用します。本番向けのワークロードの場合は、プライベート VPC を使用することをお勧めします。VPC セキュリティの強化の詳細については、「[Amazon Virtual Private Cloud でのセキュリティ](#)」を参照してください。



AWS CLI および PowerShell の例はすべて、以下の VPC 情報を使用し、us-west-2 で構築されています。自分用の環境を構築する際には、[サポートされているリージョン](#)のいずれかを選択します。詳細については、「[Amazon VPC とは?](#)」を参照してください。

ステップ 1: 2 つの VPC を作成する

このステップでは、次の表で指定されたパラメータを使用して、同じアカウントに 2 つの VPCs を作成する必要があります。AWS マネージド Microsoft AD は、[AWS Managed Microsoft AD を共有する](#)機能で個別のアカウントの使用をサポートしています。最初の VPC は AWS Managed Microsoft AD に使用されます。2 つ目の VPC はリソース用です。これらのリソースは、後に「[チュートリアル: AWS Managed Microsoft AD から Amazon EC2 へのセルフマネージド Active Directory インストールへの信頼の作成](#)」で使

マネージド Active DirecVPC 情報	オンプレミス VPC 情報
名前タグ : AWS-DS-VPC01	名前タグ : AWS-OnPrem-VPC01
IPv4 CIDR ブロック: 10.0.0.0/16	IPv4 CIDR ブロック: 10.100.0.0/16
IPv6 CIDR ブロック: IPv6 CIDR ブロックなし	IPv6 CIDR ブロック: IPv6 CIDR ブロックなし
テナンシー: デフォルト	テナンシー: デフォルト

詳細な手順については、「[VPC を作成する](#)」を参照してください。

ステップ 2: VPC ごとに 2 つのサブネットを作成する

VPC を作成したら、次の表に指定されているパラメータを使用して、VPC ごとに 2 つのサブネットを作成する必要があります。このテストラボでは、各サブネットは /24 になります。これにより、サブネットごとに最大 256 個のアドレスを発行できます。各サブネットは、それぞれ個別の AZ に配置する必要があります。各サブネットを個別の AZ に配置することは [AWS Managed Microsoft AD を作成するための前提条件](#) の 1 つです。

AWS-DS-VPC01 サブネット情報:	AWS-OnPrem-VPC01 サブネット情報
名前タグ : AWS-DS-VPC01-Subnet01	名前タグ : AWS-OnPrem-VPC01-Subnet01
VPC: vpc-xxxxxxxxxxxxxxxxxxxxx AWS-DS-VPC01	VPC: vpc-xxxxxxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01
アベイラビリティーゾーン: us-west-2a	アベイラビリティーゾーン: us-west-2a
IPv4 CIDR ブロック: 10.0.0.0/24	IPv4 CIDR ブロック: 10.100.0.0/24
名前タグ : AWS-DS-VPC01-Subnet02	名前タグ : AWS-OnPrem-VPC01-Subnet02
VPC: vpc-xxxxxxxxxxxxxxxxxxxxx AWS-DS-VPC01	VPC: vpc-xxxxxxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01
アベイラビリティーゾーン: us-west-2b	アベイラビリティーゾーン: us-west-2b
IPv4 CIDR ブロック: 10.0.1.0/24	IPv4 CIDR ブロック: 10.100.1.0/24

詳細な手順については、「[Creating a subnet in your VPC](#)」(VPC でのサブネットの作成) を参照してください。

ステップ 3: インターネットゲートウェイを作成して VPC にアタッチする

ここではパブリック VPC を使用しているため、次の表に指定されているパラメータを使用し、インターネットゲートウェイを作成して VPC にアタッチする必要があります。これにより、EC2 インスタンスに接続し、それを管理できるようになります。

AWS-DS-VPC01 インターネットゲートウェイ情報	AWS-OnPrem-VPC01 インターネットゲートウェイ情報
名前タグ: AWS-DS-VPC01-IGW	名前タグ: AWS-OnPrem-VPC01-IGW
VPC: vpc-xxxxxxxxxxxxxxxxxxxxx AWS-DS-VPC01	VPC: vpc-xxxxxxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01

詳細な手順については、「[インターネットゲートウェイを使用してインターネットに接続する](#)」を参照してください。

ステップ 4: AWS-DS-VPC01と - AWS-OnPrem-VPC01 間の VPC ピアリング接続を設定する

既に 2 つの VPC を作成しているので、次の表に指定されているパラメータを使用して、これらの VPC を VPC ピアリングでネットワーク接続する必要があります。VPC を接続する方法は多数ありますが、このチュートリアルでは VPC ピアリングを使用します。AWS マネージド Microsoft AD は VPCs を接続するための多くのソリューションをサポートしています。これには、VPC [ピアリング](#)、[Transit Gateway](#)、[VPN](#) などがあります。

ピアリング接続名タグ: AWS-DS-VPC01&AWS-OnPrem-VPC01-Peer

VPC (リクエスタ): vpc-xxxxxxxxxxxxxxxxxxxxx AWS-DS-VPC01

アカウント: My Account

リージョン: 使用しているリージョン

VPC (アクセプタ): vpc-xxxxxxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01

アカウント内で別の VPC と VPC ピアリング接続を作成する手順については、「[アカウント内の別の VPC との VPC ピアリング接続を作成する](#)」を参照してください。

ステップ 5: 各 VPC のメインルートテーブルに 2 つのルートを追加する

前の手順で作成したインターネットゲートウェイと VPC ピアリング接続が機能するには、次の表に指定されているパラメータを使用して、両方の VPC のメインルートテーブルを更新する必要があります。ここでは、以下の 2 つのルートを追加します。ルートテーブルに明示的に認識されていないすべての送信先にルーティングする 0.0.0.0/0 と、これまでのステップで確立した VPC ピアリング接続を介して各 VPC にルーティングする 10.0.0.0/16 または 10.100.0.0/16 です。

VPC 名タグ (AWS-DS-VPC01 または AWS-OnPrem-VPC01) でフィルタリングすることで、各 VPC の正しいルートテーブルを簡単に見つけることができます。

AWS-DS-VPC01 ルート 1 情報	AWS-DS-VPC01 ルート 2 情報	AWS-OnPrem-VPC01 ルート 1 情報	AWS-OnPrem-VPC01 ルート 2 情報
送信先: 0.0.0.0/0	送信先: 10.100.0.0/16	送信先: 0.0.0.0/0	送信先: 10.0.0.0/16
ターゲット: igw-xxxxx- xxxxxxxxxxxxx AWS- DS-VPC01-IGW	ターゲット: pcx- AWS xxxxxxxxx xxxxxxxxxxxxx-DS-VP C01&AWS-OnPrem- VPC01-Peer	ターゲット: igw-xxxxx- xxxxxxxxxxxxx AWS- Onprem-VPC01	ターゲット: pcx- AWS xxxxxxxxx xxxxxxxxxxxxx-DS-VP C01&AWS-OnPrem- VPC01-Peer

VPC ルートテーブルにルートを追加する手順については、「[ルートテーブルのルートの追加と削除](#)」を参照してください。

Amazon EC2 インスタンスのセキュリティグループを作成する

デフォルトでは、AWS マネージド Microsoft AD はドメインコントローラー間のトラフィックを管理するセキュリティグループを作成します。このセクションでは、次の表に指定されているパラメータを使用して、EC2 インスタンスの VPC 内でトラフィックを管理するための、2 つのセキュリティグループ (VPC ごとに 1 つ) を作成する必要があります。また、任意の場所からの RDP (3389) インバウンドを許可するためと、ローカル VPC からのすべてのインバウンドトラフィックタイプに適用するためのルールも追加します。詳細については、「[Amazon EC2 security groups for Windows instances](#)」(Windows インスタンス用の Amazon EC2 セキュリティグループ) を参照してください。

AWS-DS-VPC01 セキュリティグループ情報:

セキュリティグループ名 : AWS DS Test Lab セキュリティグループ

説明 : AWS DS Test Lab セキュリティグループ

VPC: vpc-xxxxxxxxxxxxxxxxxxx AWS-DS-VPC01

AWS-DS-VPC01のセキュリティグループのインバウンドルール

タイプ	プロトコル	ポート範囲	ソース	トラフィックの種類
カスタム TCP ルール	TCP	3389	マイ IP	リモートデスクトップ
すべてのトラフィック	すべて	すべて	10.0.0.0/16	すべてのローカル VPC トラフィック

AWS-DS-VPC01のセキュリティグループアウトバウンドルール

タイプ	プロトコル	ポート範囲	送信先	トラフィックの種類
すべてのトラフィック	すべて	すべて	0.0.0.0/0	すべてのトラフィック

AWS-OnPrem-VPC01 セキュリティグループ情報:

セキュリティグループ名 : AWS OnPrem Test Lab セキュリティグループ。

説明: AWS OnPrem Test Lab セキュリティグループ。

VPC: vpc-xxxxxxxxxxxxxxxxxxx AWS-OnPrem-VPC01

AWS-OnPrem-VPC01 用のセキュリティグループのインバウンドルール

タイプ	プロトコル	ポート範囲	ソース	トラフィックの種類
カスタム TCP ルール	TCP	3389	マイ IP	リモートデスクトップ
カスタム TCP ルール	TCP	53	10.0.0.0/16	DNS
カスタム TCP ルール	TCP	88	10.0.0.0/16	Kerberos
カスタム TCP ルール	TCP	389	10.0.0.0/16	LDAP
カスタム TCP ルール	TCP	464	10.0.0.0/16	Kerberos パスワードの変更 / 設定
カスタム TCP ルール	TCP	445	10.0.0.0/16	SMB / CIFS
カスタム TCP ルール	TCP	135	10.0.0.0/16	レプリケーション
カスタム TCP ルール	TCP	636	10.0.0.0/16	LDAP SSL
カスタム TCP ルール	TCP	49152 - 65535	10.0.0.0/16	RPC
カスタム TCP ルール	TCP	3268 - 3269	10.0.0.0/16	LDAP GC および LDAP GC SSL
カスタム UDP ルール	UDP	53	10.0.0.0/16	DNS

タイプ	プロトコル	ポート範囲	ソース	トラフィックの種類
カスタム UDP ルール	UDP	88	10.0.0.0/16	Kerberos
カスタム UDP ルール	UDP	123	10.0.0.0/16	Windows タイム
カスタム UDP ルール	UDP	389	10.0.0.0/16	LDAP
カスタム UDP ルール	UDP	464	10.0.0.0/16	Kerberos パスワードの変更 / 設定
すべてのトラフィック	すべて	すべて	10.100.0.0/16	すべてのローカル VPC トラフィック

AWS-OnPrem-VPC01 用のセキュリティグループのアウトバウンドルール

タイプ	プロトコル	ポート範囲	送信先	トラフィックの種類
すべてのトラフィック	すべて	すべて	0.0.0.0/0	すべてのトラフィック

ルールを作成してセキュリティグループに追加する詳細な手順については、「[Working with security groups](#)」(セキュリティグループを操作する)を参照してください。

ステップ 2: AWS Managed Microsoft AD Active Directory を作成する

このディレクトリの作成には、異なる 3 つの方法があります。プロシージャ (このチュートリアルでは推奨) を使用する AWS Management Console か、AWS CLI または AWS Tools for Windows PowerShell プロシージャを使用してディレクトリを作成できます。

方法 1: AWS Managed Microsoft AD ディレクトリを作成するには (AWS Management Console)

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ)、[Set up directory] (ディレクトリの設定) の順に選択します。
2. [Select directory type] (ディレクトリタイプの選択) ページで [AWS Managed Microsoft AD] を選択してから、[Next] (次へ) をクリックします。
3. [Enter directory information] (ディレクトリ情報の入力) ページで、以下の情報を指定した後に [Next] (次へ) をクリックします。
 - [Edition] (エディション) で、[Standard Edition] または [Enterprise Edition] を選択します。エディションの詳細については、「[AWS Directory Service for Microsoft Active Directory](#)」を参照してください。
 - [Directory DNS name] (ディレクトリの DNS 名) に「**corp.example.com**」と入力します。
 - [Directory NetBIOS name] (ディレクトリの NetBIOS 名) に「**corp**」と入力します。
 - [Directory description] (ディレクトリの説明) に「**AWS DS Managed**」と入力します。
 - [Admin password] (管理者パスワード) に、このアカウントに使用するパスワードを入力し、[Confirm password] (パスワードの確認) に同じパスワードを再度入力します。この [Admin] (管理者) アカウントは、ディレクトリの作成プロセス中に自動的に作成されます。パスワードに、「admin」という単語を含めることはできません。ディレクトリ管理者のパスワードは大文字と小文字が区別され、8～64 文字以内の長さにする必要があります。また、次の 4 つのカテゴリうち 3 つから少なくとも 1 文字を含める必要があります。
 - 小文字 (a～z)
 - 大文字 A～Z
 - 数字 (0～9)
 - 英数字以外の文字 (~!@#\$%^&* _-+=`|(){}[];:'"<>,.?/)
4. [Choose VPC and subnets] (VPC とサブネットの選択) ページで、次の情報を指定して [Next] (次へ) をクリックします。
 - [VPC] で、AWS-DS-VPC01 で始まり、(10.0.0.0/16) で終わるオプションを選択します。
 - [Subnets] (サブネット) で、パブリックサブネットとして 10.0.0.0/24 と 10.0.1.0/24 を選択します。
5. [Review & create] (確認と作成) ページでディレクトリ情報を確認し、必要に応じて変更を加えます。情報が正しい場合は、[Create directory] (ディレクトリの作成) を選択します。ディレクトリの作成所要時間は 20～40 分です。作成が完了すると、[Status] (ステータス) 値が [Active] (アクティブ) に変わります。

方法 2: AWS Managed Microsoft AD を作成するには (PowerShell) (オプション)

1. PowerShell を開きます。
2. 次のコマンドを入力します。前の AWS Management Console 手順のステップ 4 で指定した値を使用してください。

```
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
```

方法 3: AWS Managed Microsoft AD を作成するには (AWS CLI) (オプション)

1. を開きます AWS CLI。
2. 次のコマンドを入力します。前の AWS Management Console 手順のステップ 4 で指定した値を使用してください。

```
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
```

ステップ 3: Amazon EC2 インスタンスをデプロイして AWS Managed Microsoft AD Active Directory を管理する

このラボでは、管理インスタンスにどこからでも簡単にアクセスできるように、パブリック IP アドレスを持つ Amazon EC2 インスタンスを使用します。本番環境では、VPN や AWS Direct Connect リンクを介してのみアクセス可能なプライベート VPC 内のインスタンスを使用できます。インスタンスでパブリック IP アドレスを使用することは必須条件ではありません。

このセクションでは、デプロイ後の新しい EC2 インスタンスで Windows Server を使用し、クライアントコンピュータからドメインに接続するために必要となる、各種のタスクを実行していきます。次のステップでは、Windows Server を使用し、ラボが正常に機能することを確認します。

オプション: ディレクトリの AWS-DS-VPC01 で DHCP オプションセットを作成する

このオプションの手順では、VPC 内の EC2 インスタンスが DNS 解決に AWS Managed Microsoft AD を自動的に使用するように DHCP オプションスコープを設定します。詳細については、「[DHCP options sets](#)」(DHCP オプションセット)を参照してください。

ディレクトリの DHCP オプションセットを作成するには

1. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
2. ナビゲーションペインで [DHCP Options Sets] (DHCP オプションセット) を選択し、[Create DHCP options set] (DHCP オプションセットの作成) を選択します。
3. [Create DHCP options set] (DHCP オプションセットの作成) ページで、ディレクトリ用に以下の値を指定します。
 - [Name] (名前) に、「**AWS_DS_DHCP**」と入力します。
 - [Domain Name] (ドメイン名) に、「**corp.example.com**」と入力します。
 - [Domain name servers] (ドメインネームサーバー) には、AWS が提供するディレクトリの DNS サーバーの IP アドレスを入力します。

 Note

これらのアドレスを検索するには、AWS Directory Service ディレクトリページに移動し、該当するディレクトリ ID を選択します。[Details] (詳細) ページで、[DNS address] (DNS アドレス) に表示されている IP から、使用するものを選択します。または、AWS Directory Service の [Directories] (ディレクトリ) ページで、該当するディレクトリ ID を選択することで、これらのアドレスを検索できます。次に、[Scale & share] (スケール & 共有) をクリックします。[Domain controllers] (ドメインコントローラ) で、[IP address] (IP アドレス) に表示されている中から、使用する IP を選択します。

- [NTP servers] (NTP サーバー)、[NetBIOS name servers] (NetBIOS ネームサーバー)、[NetBIOS node type] (NetBIOS ノードタイプ) は空白のままにします。
4. [Create DHCP options set] (DHCP オプションセットを作成) をクリックし、次に [Close] (閉じる) をクリックします。新しい DHCP オプションのセットが DHCP オプションの一覧に表示されます。
 5. 新しい DHCP オプションセットの ID (dopt-**xxxxxxxx**) を書き留めておきます。この ID は、この手順の最後で新しいオプションセットを VPC と関連付ける際に使用します。

 Note

シームレスなドメイン参加は、DHCP オプションセットを設定しなくても機能します。

6. ナビゲーションペインで、Your VPCs (お客様の VPC) をクリックします。

7. VPC のリストから [AWS DS VPC] を選択し、[Actions] (アクション)、[Edit DHCP Options Set] (DHCP オプションセットの編集) の順に選択します。
8. [Edit DHCP options set] (DHCP オプションセットの編集) ページで、ステップ 5 で書き留めたオプションセットを選択し、[Save] (保存) をクリックします。

Windows インスタンスを AWS Managed Microsoft AD ドメインに結合するロールを作成する

この手順を使用して、Amazon EC2 Windows インスタンスをドメインに結合するためのロールを設定します。詳細については、「[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)」を参照してください。

Windows インスタンスをドメインに結合するように EC2 を設定するには

1. IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. IAM コンソールのナビゲーションペインで、[Roles] (ロール)、[Create role] (ロールを作成) の順に選択します。
3. [Select type of trusted entity] (信頼されたエンティティの種類を選択) で、[AWS service] (AWS のサービス) を選択します。
4. [Choose the service that will use this role] (このロールを使用するサービスを選択) のすぐ下で、[EC2] を選択し、次に [Next: Permissions] (次へ: アクセス許可) を選択します。
5. [Attached permissions policy] (アタッチされているアクセス許可ポリシー) ページで、以下の操作を行います。
 - 管理ポリシー [AmazonSSMMManagedInstanceCore] の横にあるボックスをオンにします。このポリシーは、Systems Manager サービスを使用するために必要な最小限のアクセス許可を付与します。
 - 管理ポリシー [AmazonSSMDirectoryServiceAccess] の横にあるボックスをオンにします。このポリシーでは、AWS Directory Serviceによって管理されている Active Directory にインスタンスを結合するためのアクセス許可を付与します。

これらのマネージドポリシーと、Systems Manager の IAM インスタンスプロファイルにアタッチできるその他のポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。管理ポリシーの詳細については、「IAM ユーザーガイド」の「[AWS 管理ポリシー](#)」を参照してください。

6. [Next: Tags] (次へ: タグ) を選択します。

7. (オプション) 1 つまたは複数のタグキーと値のペアを追加して、このロールのアクセスを整理、追跡、または制御し、[Next: Review] (次へ: 確認) を選択します。
8. [Role name] (ロール名) には、「EC2DomainJoin」など、インスタンスをドメインに結合させるために使用されることがわかるような名前を入力します。
9. (オプション) [Role description] (ロールの説明) に、説明を入力します。
10. [Create role] (ロールの作成) を選択します。ロールページが再度表示されます。

Amazon EC2 インスタンスを作成し、ディレクトリを自動的に結合する

この手順では、EC2 インスタンス内に Windows Server システムをセットアップし、後に Active Directory でユーザー、グループ、およびポリシーを管理するために使用できるようにします。

EC2 インスタンスを作成しディレクトリを自動的に結合するには

1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2/>) を開きます。
2. [Launch Instance] (インスタンスの起動) を選択します。
3. [Step 1] (ステップ 1) ページで、[Microsoft Windows Server 2019 Base - ami-xxxxxxxxxxxxxxxxxx] の横にある [Select] (選択) をオンにします。
4. [Step 2] (ステップ 2。 ページで、[t3.micro] を選択します (これより大きいインスタンスタイプも選択できます)。次に、[Next: Configure Instance Details] (次へ: インスタンス詳細の設定) をクリックします。
5. [Step 3] (ステップ 3) ページで、以下の操作を行います。
 - [Network] (ネットワーク) で、AWS-DS-VPC01 で終わる VPC (例: vpc-xxxxxxxxxxxxxxxx | AWS-DS-VPC01) を選択します。
 - [Subnet] (サブネット) で、該当するアベイラビリティーゾーンに事前設定されている [Public subnet 1] を選択します (例: subnet-xxxxxxxxxxxxxxxx | AWS-DS-VPC01-Subnet01 | **us-west-2a**)。
 - Auto-assign Public IP (自動割り当てパブリック IP) で、[Enable] (有効) を選択します (サブネットの設定がデフォルトで有効ではない場合)。
 - [Domain join directory] (ドメイン結合ディレクトリ) で、[corp.example.com (d-xxxxxxxxxx)] を選択します。
 - [IAM role] (IAM ロール) で、[Windows インスタンスを AWS Managed Microsoft AD ドメインに結合するロールを作成する](#) でインスタンスロールを付与した名前 (例: EC2DomainJoin) を選択します。

- 残りの設定はデフォルトのままにしておきます。
 - [Next: Add Storage] (次へ: ストレージの追加) をクリックします。
6. [Step 4] (ステップ 4) ページで、デフォルト設定をそのままにして、[Next: Add Tags] (次へ: タグの追加) をクリックします。
 7. [Step 5] (ステップ 5) ページで、[Add Tag] (タグを追加) をクリックします。[Key] (キー) に「**corp.example.com-mgmt**」と入力し、[Next: Configure Security Group] (次へ: セキュリティグループの設定) を選択します。
 8. [Step 6] (ステップ 6) ページで、[Select an existing security group] (既存のセキュリティグループを選択する) をクリックし、[AWS DS Test Lab Security Group] (DS テストラボセキュリティグループ) ([入門チュートリアル](#)でセットアップ済み) を選択します。次に [Review and Launch] (確認と作成) をクリックしてインスタンスを確認します。
 9. [Step 7] (ステップ 7) ページで内容を確認した上で、[Launch] (起動) をクリックします。
 10. [Select an existing key pair or create a new key pair] (既存のキーペアを選択するか、新しいキーペアを作成します。) ダイアログボックスで、以下の操作を行います。
 - [Choose an existing key pair] (既存のキーペアの選択) をクリックします。
 - [Select a key pair] (キーペアの選択) で、[AWS-DS-KP] を選択します。
 - [I acknowledge...] (...を認識しています) チェックボックスをオンにします。
 - [Launch Instances] (インスタンスを起動) をクリックします。
 11. [View Instances] (インスタンスの表示) をクリックして Amazon EC2 コンソールに戻り、デプロイのステータスを確認します。

EC2 インスタンスに Active Directory のツールをインストールする

Active Directory ドメイン管理ツールを EC2 インスタンスにインストールするには、2 つの方法があります。Server Manager UI (このチュートリアルでの推奨) または PowerShell を使用できます。

Active Directory のツールを EC2 インスタンスにインストールするには (Server Manager)

1. Amazon EC2 コンソールで [Instances] (インスタンス) をクリックし、先ほど作成したインスタンスを選択して、[Connect] (接続) をクリックします。
2. [Connect To Your Instance] (インスタンスに接続) ダイアログボックスで、[Get Password] (パスワードを取得) をクリックしてパスワードを取得し (まだ取得していない場合)、続いて

- [Download Remote Desktop File] (リモートデスクトップファイルのダウンロード) をクリックします。
3. [Windows Security] (Windows セキュリティ) ダイアログボックスで、Windows Server コンピュータのログインに使用する、ローカル管理者の認証情報 (「**administrator**」など) を入力します。
 4. [Start] (スタート) メニューで、[Server Manager] (サーバーマネージャー) を選択します。
 5. [Dashboard] (ダッシュボード) で、[Add Roles and Features] (ロールと機能の追加) をクリックします。
 6. [Add Roles and Features Wizard] (ロールと機能の追加ウィザード) で、[Next] (次へ) をクリックします。
 7. [Select installation type] (インストールタイプの選択) ページで、[Role-based or feature-based installation] (ロールベースもしくは機能ベースのインストール) を選択し、[Next] (次へ) をクリックします。
 8. Select destination server (送信先サーバーの選択) ページで、ローカルサーバーが選択されていることを確認し、[Next] (次へ) をクリックします。
 9. [Select server roles] (サーバーロールの選択) ページで、[Next] (次へ) をクリックします。
 10. [Select features] (機能の選択) ページで、以下の操作を行います。
 - [Group Policy Management] (グループポリシー管理) チェックボックスをオンにします。
 - [Remote Server Administration Tools] (リモートサーバー管理ツール)、[Role Administration Tools] (ロール管理ツール) の順に展開します。
 - [AD DS and AD LDS Tools] (AD DS と AD LDS ツール) チェックボックスをオンにします。
 - [DNS Server Tools] (DNS サーバーツール) チェックボックスをオンにします。
 - [Next] (次へ) をクリックします。
 11. [Confirm installation selections] (インストール設定の確認) ページで、情報を確認し、[Install] (インストール) をクリックします。機能のインストールが完了すると、[スタート] メニューの [Windows Administrative Tools] フォルダで、以下の新しいツールやスナップインが利用可能になります。
 - Active Directory 管理センター
 - Active Directory のドメインと信頼関係
 - PowerShell の Active Directory モジュール
 - Active Directory のサイトとサービス
 - Active Directory のユーザーとコンピュータ

- ADSI エディター
- DNS
- グループポリシーの管理

EC2 インスタンスに Active Directory ツールをインストールするには (PowerShell) (選択可能)

1. PowerShell を起動します。
2. 次のコマンドを入力します。

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
```

ステップ 4: 基本テストラボが正常に機能することを確認する

追加のテストラボのガイドモジュールを追加する前に、次の手順に従い、テストラボが正常にセットアップされていることを確認します。この手順では、Windows Server が適切に設定され、corp.example.com ドメインに接続でき、AWS Managed Microsoft AD フォレストの管理に使用できることを確認します。

テストラボが正常に機能することを確認するには

1. ローカル管理者としてログインした EC2 インスタンスからサインアウトします。
2. Amazon EC2 コンソールに戻り、ナビゲーションペインで [Instances] (インスタンス) をクリックします。次に、作成したインスタンスを選択します。[Connect] (接続) をクリックします。
3. [Connect To Your Instance] (インスタンスへの接続) ダイアログボックスで、[Download Remote Desktop File] (リモートデスクトップファイルのダウンロード) をクリックします。
4. [Windows Security] (Windows セキュリティ) ダイアログボックスで、CORP ドメインに管理者としてログインするための認証情報 (**corp\admin**など) を入力します。
5. ログインしたら、[Start] (スタート) メニューから [Windows Administrative Tools] (Windows 管理ツール) を選択し、[Active Directory Users and Computers] (Active Directory とコンピュータ) を選択します。
6. 新しいドメインと関連付けられたすべてのデフォルト OU およびアカウントで「corp.example.com」が表示されます。ドメインコントローラーで、このチュートリアルの手ステップ 2 で AWS Managed Microsoft AD を作成したときに自動的に作成されたドメインコントローラーの名前に注意してください。

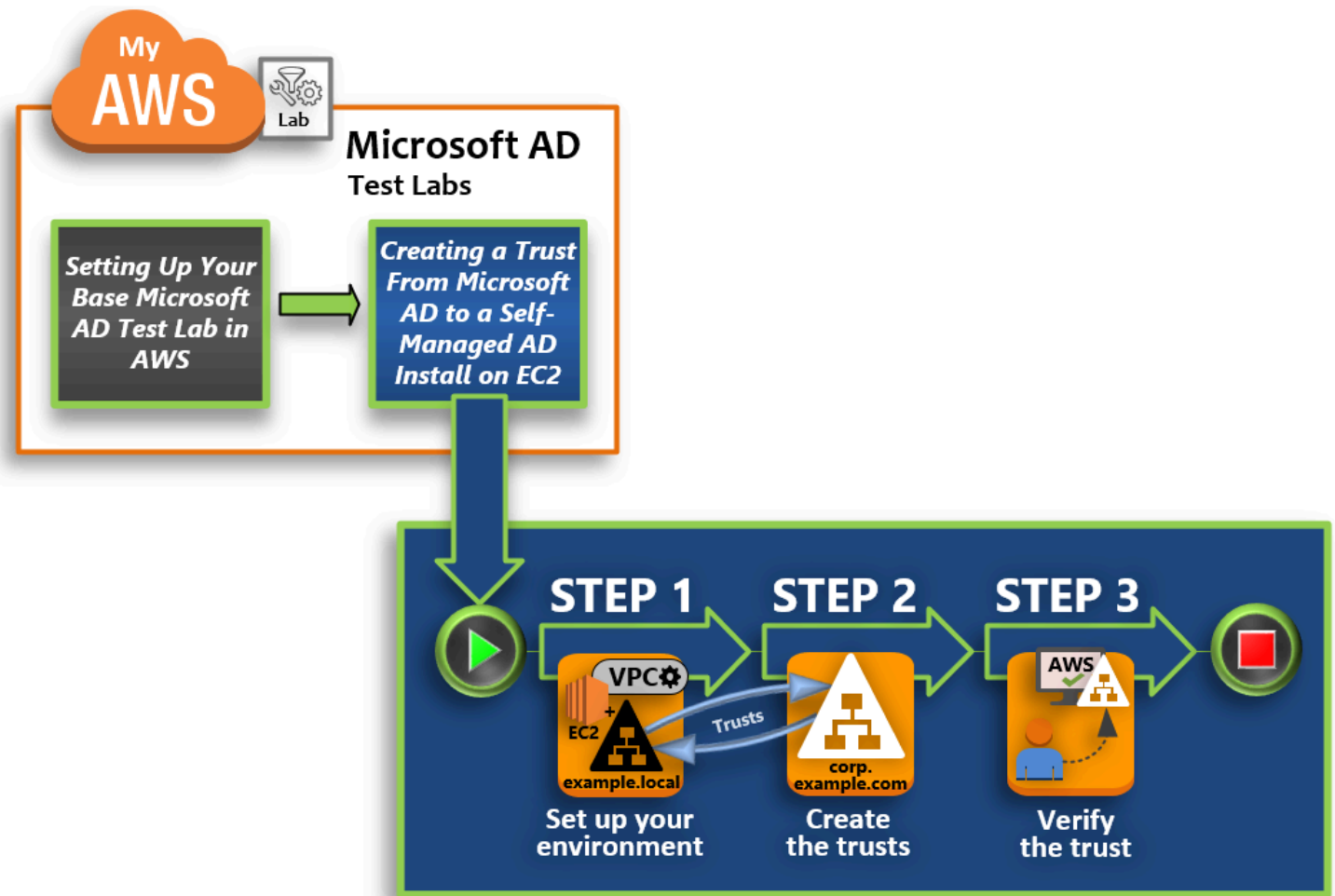
お疲れ様でした。AWS Managed Microsoft AD のベーステストラボ環境が設定されました。このシリーズの次のテストラボを追加する準備が整いました。

次のチュートリアル: [チュートリアル: AWS Managed Microsoft AD から Amazon EC2 へのセルフマネージド Active Directory インストールへの信頼の作成](#)

チュートリアル: AWS Managed Microsoft AD から Amazon EC2 へのセルフマネージド Active Directory インストールへの信頼の作成

このチュートリアルでは、[基本チュートリアル](#)で作成した AWS Directory Service for Microsoft Active Directory フォレスト間に信頼を作成する方法について説明します。また、Amazon EC2 で Windows Server 上にネイティブの新しい Active Directory フォレストを作成する方法についても説明します。次の図に示すように、このチュートリアルで作成するラボは、完全な AWS Managed Microsoft AD テストラボを設定するために必要な 2 番目の構成要素です。テストラボを使用して、純粋なクラウドまたはハイブリッドクラウドベースの AWS ソリューションをテストできます。

このチュートリアルは 1 度だけ作成する必要があります。その後は、経験に応じて必要な時にオプションのチュートリアルを追加できます。



ステップ 1: 信頼の環境セットアップ

新しい Active Directory フォレストと[基本のチュートリアル](#)で作成した AWS Managed Microsoft AD フォレストとの信頼を確立するには、Amazon EC2 環境の準備を整える必要があります。そのためには、まず Windows Server 2019 サーバーを作成して、このサーバーをドメインコントローラーに昇格し、その後 VPC を適切に設定します。

ステップ 2: 信頼の作成

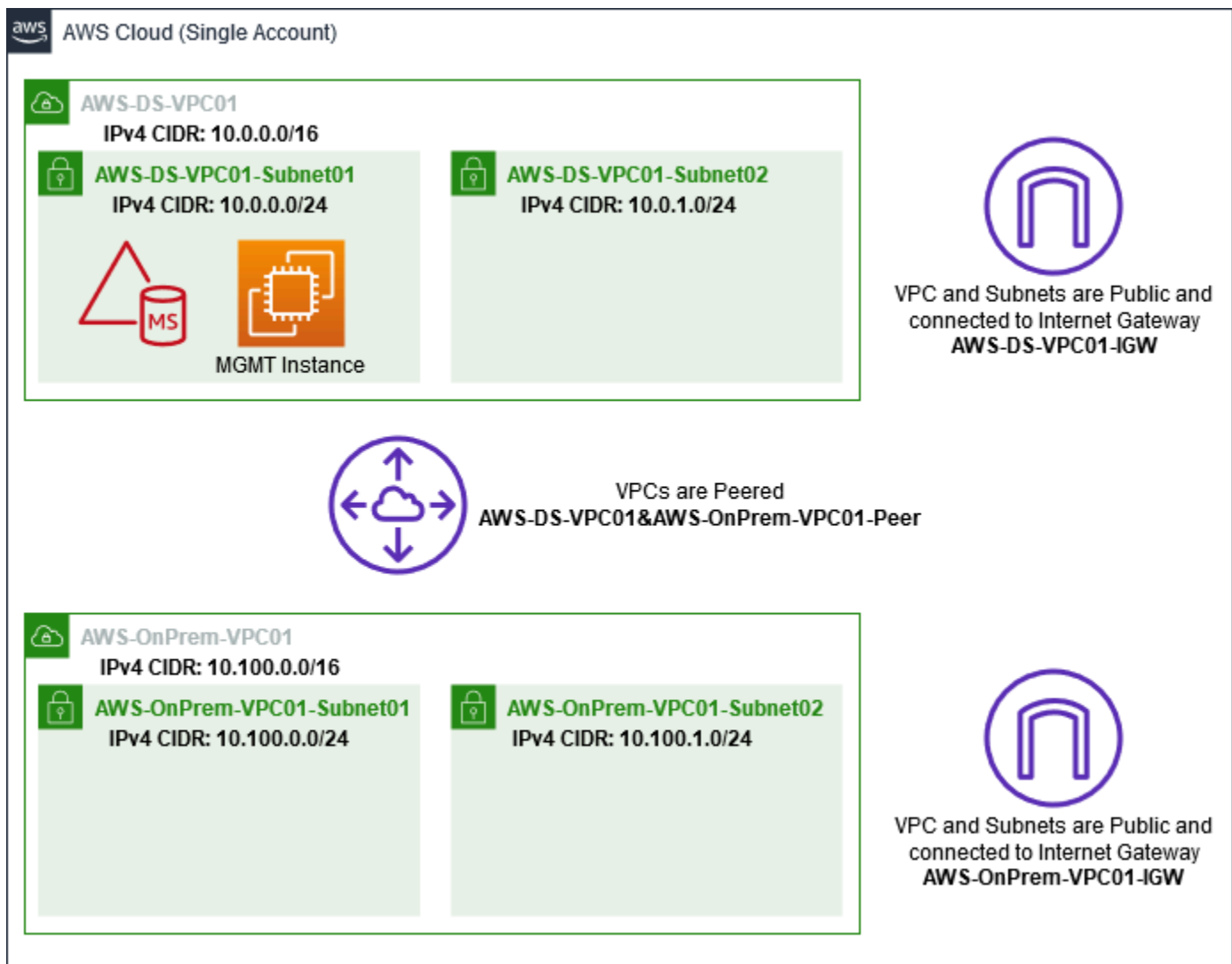
このステップでは、Amazon EC2 でホストされている新しく作成された Active Directory フォレストと、の AWS Managed Microsoft AD フォレストとの間に双方向のフォレスト信頼関係を作成します AWS。

ステップ 3: 信頼の検証

最後に、管理者として AWS Directory Service コンソールを使用して、新しい信頼が機能していることを確認します。

ステップ 1: 信頼の環境セットアップ

このセクションでは、Amazon EC2 環境をセットアップし、新しいフォレストをデプロイして、この信頼のために VPC を準備します AWS。



Windows Server 2019 の EC2 インスタンスを作成する

Amazon EC2 で Windows Server 2019 のメンバーサーバーを作成するには、次の手順に従います。

Windows Server 2019 の EC2 インスタンスを作成するには

1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2/>) を開きます。
2. Amazon EC2 コンソールで、[Launch Instance] (インスタンスを起動) を選択します。
3. [Step 1] (ステップ 1) ページのリストで、[Microsoft Windows Server 2019 Base - ami-xxxxxxxxxxxxxxxxxx] を見つけます。続いて、[Select] (選択) を選択します。

4. [Step 2] (ステップ 2。 ページで、[t2.large]、[Next: Configure Instance Details] (次へ: インスタンスの詳細の設定) の順に選択します。
5. [Step 3] (ステップ 3) ページで、以下の操作を行います。
 - [Network] (ネットワーク) で、[vpc-~~xxxxxxxxxxxxxxxxxxxx~~ AWS-OnPrem-VPC01] ([基本のチュートリアル](#)でセットアップ済み) を選択します。
 - Subnet には、subnet-~~xxxxxxxxxxxxxxxxxxxx~~ | AWS-OnPrem-VPC01-Subnet01 | AWS-OnPrem-VPC01 を選択します。
 - [Auto-assign Public IP] (自動割り当てパブリック IP) リストで、サブネットのデフォルト設定が [Enable] (有効) でない場合、[Enable] (有効) を選択します。
 - 残りの設定はデフォルトのままにしておきます。
 - [Next: Add Storage] (次へ: ストレージの追加) をクリックします。
6. [Step 4] (ステップ 4) ページで、デフォルト設定をそのままにして、[Next: Add Tags] (次へ: タグの追加) をクリックします。
7. [Step 5] (ステップ 5) ページで、[Add Tag] (タグを追加) をクリックします。[Key] (キー) に「**example.local-DC01**」と入力し、[Next: Configure Security Group] (次へ: セキュリティグループの設定) を選択します。
8. [ステップ 6] ページで、[既存のセキュリティグループを選択する] を選択し、[AWS オンプレミステストラボセキュリティグループ] ([基本のチュートリアル](#)でセットアップ済み) を選択します。次に [確認と作成] を選択してインスタンスを確認します。
9. [Step 7] (ステップ) ページで内容を確認した上で、[Launch] (起動) をクリックします。
10. [Select an existing key pair or create a new key pair] (既存のキーペアを選択するか、新しいキーペアを作成します。) ダイアログボックスで、以下の操作を行います。
 - [Choose an existing key pair] (既存のキーペアの選択) をクリックします。
 - [Select a key pair] (キーペアの選択) で、[AWS-DS-KP] ([基本のチュートリアル](#)でセットアップ済み) を選択します。
 - [I acknowledge...] (...を認識しています) チェックボックスをオンにします。
 - [Launch Instances] (インスタンスを起動) をクリックします。
11. [View Instances] (インスタンスの表示) をクリックして Amazon EC2 コンソールに戻り、デプロイのステータスを確認します。

サーバーをドメインコントローラーに昇格する

信頼を作成する前に、新しいフォレスト用に最初のドメインコントローラーを構築してデプロイする必要があります。このプロセスでは、新しい Active Directory フォレストを設定し、DNS をインストールして、名前の解決にローカル DNS サーバーを使用するようにこのサーバーを設定します。この手順の最後にサーバーを再起動する必要があります。

Note

オンプレミスネットワークでレプリケート AWS するドメインコントローラーを作成する場合は、まず EC2 インスタンスをオンプレミスドメインに手動で結合します。その後、サーバーをドメインコントローラーに昇格できます。

サーバーをドメインコントローラーに昇格するには

1. Amazon EC2 コンソールで [Instances] (インスタンス) をクリックし、先ほど作成したインスタンスを選択して、[Connect] (接続) をクリックします。
2. [Connect To Your Instance] (インスタンスへの接続) ダイアログボックスで、[Download Remote Desktop File] (リモートデスクトップファイルのダウンロード) をクリックします。
3. [Windows Security] ダイアログボックスで、Windows Server コンピュータのローカル管理者の認証情報 (「**administrator**」など) を入力してログインします。ローカル管理者のパスワードがない場合は、Amazon EC2 コンソールに戻り、インスタンスを右クリックして [Get Windows Password] (Windows パスワードを取得) を選択します。AWS_DS_KP.pem ファイルまたは個人用の .pem キーに移動して、[Decrypt Password] (パスワードの復号) を選択します。
4. [Start] (スタート) メニューで、[Server Manager] (サーバーマネージャー) を選択します。
5. [Dashboard] (ダッシュボード) で、[Add Roles and Features] (ロールと機能の追加) をクリックします。
6. [Add Roles and Features Wizard] (ロールと機能の追加ウィザード) で、[Next] (次へ) をクリックします。
7. [Select installation type] (インストールタイプの選択) ページで、[Role-based or feature-based installation] (ロールベースもしくは機能ベースのインストール) を選択し、[Next] (次へ) をクリックします。
8. Select destination server (送信先サーバーの選択) ページで、ローカルサーバーが選択されていることを確認し、[Next] (次へ) をクリックします。

9. [Select server roles] (サーバーロールの選択) ページで、[Active Directory Domain Services] (Active Directory ドメインサービス) を選択します。[Add Roles and Features Wizard] (ロールと機能の追加ウィザード) ダイアログボックスで、[Include management tools] (管理ツールを含める (該当する場合)) チェックボックスがオンになっていることを確認します。[Add Features] (機能を追加)、[Next] (次へ) の順に選択します。
10. [Select features] (機能を選択) ページで、[Next] (次へ) を選択します。
11. [Active Directory Domain Services] (Active Directory ドメインサービス) ページで、[Next] (次へ) を選択します。
12. [Confirm installation selections] (インストールの選択を確認) ページで、[Install] (インストール) を選択します。
13. Active Directory バイナリがインストールされたら、[Close] (閉じる) をクリックします。
14. Server Manager (サーバーマネージャー) が表示されたら、上部の [Manage] (管理) の横にあるフラグを確認します。このフラグが黄色に変われば、サーバーを昇格する準備は完了です。
15. 黄色のフラグを選択し、[Promote this server to a domain controller] (このサーバーをドメインコントローラーに昇格) を選択します。
16. [Deployment Configuration] (デプロイ設定) ページで、[Add a new forest] (新しいフォレストを追加) を選択します。[Root domain name] (ルートドメイン名) に「**example.local**」と入力し、[Next] (次へ) を選択します。
17. [Domain Controller Options] (ドメインコントローラーのオプション) ページで、次の操作を行います。
 - [Forest functional level] (フォレストの機能レベル) と [Domain functional level] (ドメインの機能レベル) の両方で、[Windows Server 2016] を選択します。
 - [ドメインコントローラーの機能を指定] で、[Domain Name System (DNS) サーバー] と [グローバルカタログ (GC)] の両方が選択されていることを確認します。
 - Directory Services Restore Mode (DSRM) のパスワードを入力し、確認します。続いて、[Next] (次へ) をクリックします。
18. [DNS Options] (DNS のオプション) ページで、委任に関する警告を無視し、[Next] (次へ) を選択します。
19. [Additional options] (追加のオプション) ページで、NetBios のドメイン名として [EXAMPLE] が表示されていることを確認します。
20. [Paths] (パス) ページで、デフォルト値のまま [Next] (次へ) を選択します。

21. [Review Options] (オプションの確認) ページで、[Next] (次へ) を選択します。これで、ドメインコントローラーのすべての前提条件が満たされていることがサーバーで確認できます。いくつかの警告が表示されることがありますが、無視して構いません。
22. [Install] (インストール) をクリックします。インストールが完了すると、サーバーが再起動し、ドメインコントローラーとして機能するようになります。

VPC の設定

次の 3 つの手順で、AWS と接続するように VPC を設定します。

VPC のアウトバウンドルールを設定するには

1. [AWS Directory Service コンソール](#)で、[基本チュートリアル](#)で以前に作成した corp.example.com の AWS Managed Microsoft AD ディレクトリ ID を書き留めます。
2. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
3. ナビゲーションペインで、[Security Groups] を選択します。
4. AWS Managed Microsoft AD ディレクトリ ID を検索します。検索結果で、[AWS created security group for d-xxxxxx directory controllers] (AWS が d-xxxxxx ディレクトリコントローラーのセキュリティグループを作成しました) という説明が表示されている項目を選択します。

Note

このセキュリティグループは、ディレクトリを最初に作成するときに自動的に作成されます。

5. そのセキュリティグループの下にある [Outbound Rules] (アウトバウンドルール) タブを選択します。[Edit] (編集)、[Add another rule] (別のルールの追加) の順に選択し、次の値を追加します。
 - [Type] (タイプ) で、[All Traffic] (すべてのトラフィック) を選択します。
 - [Destination] (送信先) に「0.0.0.0/0」と入力します。
 - 残りの設定はデフォルトのままにしておきます。
 - [Save] (保存) をクリックします。

Kerberos の事前認証が有効になっていることを確認するには

1. example.local ドメインコントローラーで、[Server Manager] (サーバーマネージャー) を開きます。
2. [Tools] (ツール) メニューで、[Active Directory Users and Computers] (Active Directory ユーザーとコンピュータ) を選択します。
3. [Users] (ユーザー) ディレクトリに移動してユーザーを右クリックし、[Properties] (プロパティ) を選択して [Account] (アカウント) タブを選択します。[Account options] (アカウントオプション) リストを下にスクロールし、[Do not require Kerberos preauthentication] (Kerberos の事前認証を要求しない) が選択されていないことを確認します。
4. corp.example.com-mgmt インスタンスの corp.example.com ドメインに対しても同じ手順を実行します。

DNS の条件付きフォワーダーを設定するには

 Note

条件付きフォワーダーは、クエリ内の DNS ドメイン名に従って DNS クエリを転送するためのネットワーク上の DNS サーバーです。例えば、widgets.example.com で終わる名前に関して受信したすべてのクエリを、特定の DNS サーバーや複数の DNS サーバーの IP アドレスに転送するように DNS サーバーを設定できます。

1. [AWS Directory Service コンソール](#)を開きます。
2. ナビゲーションペインで [ディレクトリ] を選択します。
3. AWS Managed Microsoft AD のディレクトリ ID を選択します。
4. 完全修飾ドメイン名 (FQDN) であるディレクトリの DNS アドレスと corp.example.com を書き留めます。
5. ここで、example.local ドメインコントローラーに戻り、[Server Manager] (サーバーマネージャー) を開きます。
6. [Tools] (ツール) メニューで、[DNS] を選択します。
7. コンソールツリーで、信頼を設定するドメインの DNS サーバーを展開し、[Conditional Forwarders] (条件付きフォワーダー) に移動します。
8. [Conditional Forwarders] (条件付きフォワーダー) を右クリックし、[New Conditional Forwarder] (新しい条件付きフォワーダー) を選択します。

9. DNS ドメインに、「**corp.example.com**」と入力します。
10. プライマリサーバーの IP アドレスで、<ここをクリック>を選択して...>を追加し、AWS Managed Microsoft AD ディレクトリの最初の DNS アドレス (前の手順で書き留めたもの) を入力し、Enter キーを押します。2 目の DNS アドレスにも同じ操作を行います。DNS アドレスを入力すると、「タイムアウト」または「解決できません」というエラーが表示される場合があります。通常、このエラーは無視できます。
11. [Store this conditional forwarder in Active Directory, and replicate as follows] (Active Directory で条件付きフォワーダーを保存して、次の通りにレプリケートする) チェックボックスをオンにします。ドロップダウンメニューで [All DNS servers in this Forest] (このフォレストのすべての DNS サーバー) を選択し、[OK] を選択します。

ステップ 2: 信頼の作成

このセクションでは、2 つのフォレストの信頼を別々に作成します。1 つの信頼は EC2 インスタンスの Active Directory ドメインから作成され、もう 1 つの信頼は の AWS Managed Microsoft AD から作成されます AWS。



EC2 ドメインから AWS Managed Microsoft AD への信頼を作成するには

1. **example.local** にログインします。
2. [Server Manager] (サーバーマネージャー) を開き、コンソールツリーで [DNS] を選択します。表示されたサーバーの IPv4 アドレスを書き留めます。このアドレスは、次の手順で **corp.example.com** から **example.local** ディレクトリへの条件付きフォワーダーを作成する際に必要になります。
3. [Tools] (ツール) メニューで、[Active Directory Domains and Trusts] (Active Directory のドメインと信頼) を選択します。
4. コンソールツリーで、[example.local] を右クリックし、[Properties] (プロパティ) を選択します。
5. [Trusts] (信頼) タブで、[New Trust] (新しい信頼) を選択し、[Next] (次へ) を選択します。

6. [Trust Name] (信頼の名前) ページで、「**corp.example.com**」と入力し、[Next] (次へ) を選択します。
7. [Trust Type] (信頼のタイプ) ページで、[Forest trust] (フォレストの信頼) を選択し、[Next] (次へ) を選択します。

 Note

AWS Managed Microsoft AD は、外部信頼もサポートしています。ただし、このチュートリアルは、双方向フォレストの信頼を作成することを目的とします。

8. [Direction of Trust] (信頼の方向) ページで、[Two-way] (双方向) を選択し、[Next] (次へ) を選択します。

 Note

後で一方向の信頼でこれを試す場合、信頼の方向が正しく設定されていることを確認します (信頼するドメインでの送信、信頼されたドメインでの受信)。一般的な情報については、Microsoft のウェブサイトでの「[Understanding Trust Direction](#)」を参照してください。

9. [Sides of Trust] (信頼のサイド) ページで、[This domain only] (このドメインのみ) を選択し、[Next] (次へ) を選択します。
10. [Outgoing Trust Authentication Level] (送信する信頼の認証レベル) ページで、[Forest-wide authentication] (フォレスト全体の認証) を選択し、[Next] (次へ) を選択します。

 Note

[Selective authentication] (選択的な認証) はオプションですが、このチュートリアルをシンプルにするため、ここでは有効にしないことをお勧めします。これを設定すると、外部またはフォレストの信頼を介したアクセスが、信頼されたドメインやフォレスト内のユーザーのみに制限されます。これらには、信頼するドメインやフォレストに存在するコンピュータオブジェクト (リソースコンピュータ) に対する認証のアクセス許可が明示的に付与されています。詳細については、「[Configuring Selective Authentication Settings](#)」を参照してください。

11. [Trust Password] (信頼のパスワード) ページで、信頼のパスワードを 2 回入力し、[Next] (次へ) を選択します。この同じパスワードを次の手順でも使用します。

12. [Trust Selections Complete] (信頼の選択の完了) ページで結果を確認し、[Next] (次へ) を選択します。
13. [Trust Creation Complete] (信頼の作成の完了) ページで結果を確認し、[Next] (次へ) を選択します。
14. [Confirm Outgoing Trust] (送信する信頼の確認) ページで、[No, do not confirm the outgoing trust] (いいえ、送信の信頼を承認しません) を選択します。その後、[Next] (次へ) を選択します。
15. [Confirm Incoming Trust] (受信の信頼の確認) ページで、[No, do not confirm the incoming trust] (いいえ、受信の信頼を承認しません) を選択します。その後、[Next] (次へ) を選択します。
16. [Completing the New Trust Wizard] (新しい信頼ウィザードの完了) ページで、[Finish] (完了) を選択します。

Note

信頼関係は AWS Managed Microsoft AD のグローバル機能です。[AWS Managed Microsoft AD のマルチリージョンレプリケーションを設定する](#) を使用している場合、[プライマリリージョン](#) で次の手順を実行する必要があります。変更した内容は、レプリケートされたすべてのリージョンで自動的に適用されます。詳細については、「[グローバル機能とリージョン機能](#)」を参照してください。

AWS Managed Microsoft AD から EC2 ドメインへの信頼を作成するには

1. [AWS Directory Service コンソール](#)を開きます。
2. [corp.example.com] ディレクトリを選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、[Actions] (アクション)、[Add trust relationship] (信頼関係の追加) の順に選択します。
5. [Add a trust relationship] (信頼関係の追加) ダイアログボックスで、次の操作を行います。

- [Trust type] (信頼のタイプ) で、[Forest trust] (フォレストの信頼) を選択します。

 Note

ここで選択する信頼タイプが、前の手順で設定したものと同じ信頼タイプ (EC2 ドメインから AWS Managed Microsoft AD への信頼を作成するには) と一致することを確認します。

- [Existing or new remote domain name] (既存または新しいリモートのドメイン名) に、「example.local」と入力します。
- [Trust password] (信頼のパスワード) に、前の手順で指定したものと同一パスワードを入力します。
- [Trust direction] (信頼の方向) で、[Two-way] (双方向) を選択します。

 Note

- 後で一方向の信頼でこれを試す場合、信頼の方向が正しく設定されていることを確認します (信頼するドメインでの送信、信頼されたドメインでの受信)。一般的な情報については、Microsoft のウェブサイトでの「[Understanding Trust Direction](#)」を参照してください。
- [Selective authentication] (選択的な認証) はオプションですが、このチュートリアルをシンプルにするため、ここでは有効にしないことをお勧めします。これを設定すると、外部またはフォレストの信頼を介したアクセスが、信頼されたドメインやフォレスト内のユーザーのみに制限されます。これらには、信頼するドメインやフォレストに存在するコンピュータオブジェクト (リソースコンピュータ) に対する認証のアクセス許可が明示的に付与されています。詳細については、「[Configuring Selective Authentication Settings](#)」を参照してください。

- [Conditional forwarder] (条件付きフォワーダー) に、example.local フォレストでの DNS サーバーの IP アドレス (前の手順で書き留めたもの) を入力します。

 Note

条件付きフォワーダーは、クエリ内の DNS ドメイン名に従って DNS クエリを転送するためのネットワーク上の DNS サーバーです。例えば、widgets.example.com で

終わる名前に関して受信したすべてのクエリを、特定の DNS サーバーや複数の DNS サーバーの IP アドレスに転送するように DNS サーバーを設定できます。

6. [Add] (追加) を選択します。

ステップ 3: 信頼の検証

このセクションでは、AWS と Amazon EC2 上の Active Directory の間で信頼が正常に設定されたかどうかをテストします。

信頼を検証するには

1. [AWS Directory Service コンソール](#)を開きます。
2. [corp.example.com] デイレクトリを選択します。
3. [Directory details] (ディレクトリ詳細) ページで、以下のいずれかの操作を行います。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下に複数のリージョンが表示されている場合は、プライマリリージョンを選択した上で、[Networking & security] (ネットワークとセキュリティ) タブを開きます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。
 - [Multi-Region replication] (マルチリージョンレプリケーション) の下にリージョンが表示されない場合は、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Trust relationships] (信頼関係) セクションで、作成したばかりの信頼関係を選択します。
5. [Actions] (アクション) を選択し、[Verify trust relationship] (信頼関係の検証) を選択します。

検証が完了すると、[Status] (ステータス) の列に [Verified] (検証済み) と表示されます。

以上でこのチュートリアルは完了です。これで、マルチフォレストの Active Directory 環境が完全に機能するようになりました。この環境で、さまざまなシナリオのテストを開始できます。テストラボの追加のチュートリアルは、2018 年に予定されています。定期的に最新情報を確認してください。

AWS Managed Microsoft AD のクォータ

AWS Managed Microsoft AD のデフォルトのクォータは次のとおりです。特に明記されていない限り、各クォータはリージョンごとに適用されます。

AWS Managed Microsoft AD のクォータ

リソース	デフォルトのクォータ
AWS Managed Microsoft AD ディレクトリ	20
手動スナップショット *	AWS Managed Microsoft AD あたり 5
手動スナップショットの保持期間 **	180 日間
ディレクトリあたりのドメインコントローラーの最大数	20
Microsoft AD (Standard) あたりの共有ドメイン数 ***	5
Microsoft AD (Enterprise) あたりの共有ドメイン数 ***	125
ディレクトリあたりの登録済み認証機関 (CA) 証明書の最大数	5
1 つの AWS Managed Microsoft AD (Enterprise Edition) ディレクトリ内の AWS リージョンの最大合計数 ****	5

* 手動スナップショットのクォータは変更できません。

** 手動スナップショットでサポートされる最大保持期間は 180 日で、これを変更することはできません。これは、削除済みオブジェクトの Tombstone-Lifetime 属性により決定されています。この属性では、Active Directory のシステム状態のバックアップの有効な保存期間を定義します。180 日より古いスナップショットから復元することはできません。詳細については、Microsoft ウェブサイトの「[Active Directory のシステム状態バックアップの有効な保存期間](#)」を参照してください。

*** 共有ドメインのデフォルトのクォータとは、個々のディレクトリを共有できるアカウントの数を指します。

**** これには 1 つのプライマリリージョンと最大 4 つの追加リージョンが含まれます。詳細については、「[プライマリリージョンと追加のリージョン](#)」を参照してください。

Note

AWS Elastic Network Interface (ENI) にパブリック IP アドレスをアタッチすることはできません。

アプリケーションの設計と負荷の分散については、「[AWS Managed Microsoft AD 用にアプリケーションをプログラミングする際のベストプラクティス](#)」を参照してください。

ストレージとオブジェクトのクォータについては、「[AWS Directory Service の料金](#)」ページの「比較表」を参照してください。

AWS Managed Microsoft AD のトラブルシューティング

以下は、AWS Managed Microsoft AD の作成時または使用時に発生する可能性がある一般的な問題のトラブルシューティングに役立ちますActive Directory。

AWS Managed Microsoft AD の問題

一部のトラブルシューティングタスクは、サポートのみで完了する必要があります。以下は、タスクの一部です：

- AWS Directory Serviceが提供するドメインコントローラーを再起動します。
- [AWS Managed Microsoft AD のアップグレード](#)。

サポートケースの作成については、「[サポートケースの作成とケース管理](#)」を参照してください。

Netlogon とセキュリティでセキュリティで保護されたチャネルでの通信に関する問題

[CVE-2020-1472](#) に対する緩和策として、Microsoft は、Netlogon のセキュリティで保護されたチャネルでの通信をドメインコントローラーが処理する方法を変更するパッチをリリースしました。これらの安全な Netlogon の導入により、一部の Netlogon 接続 (サーバー、ワークステーション、信頼検証) が AWS Managed Microsoft AD で受け入れられない場合があります。

Netlogon もしくはセキュリティで保護されたチャネルでの通信に、問題との関連があるかどうかを確認するには、Amazon CloudWatch Logs でイベント ID 5827 (デバイス認証関連の問題) または 5828 (AD の信頼検証に関連する問題) を検索します。AWS Managed Microsoft AD の CloudWatch

に関する詳細については、「[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#)」を参照してください。

CVE-2020-1472 に対する緩和策の詳細については、Microsoft のウェブサイトの[CVE-2020-1472 に関連付けられた Netlogon セキュアチャネル接続の変更を管理する方法](#)」を参照してください。

ユーザーのパスワードをリセットしようとする、「応答ステータス: 400 リクエストの失敗」エラーが表示されます。

ユーザーのパスワードをリセットしようとする、次のようなエラーメッセージが表示されます。

Response Status: 400 Bad Request

この問題は、同じユーザー名の AWS Managed Microsoft AD Organizational Unit (OU) に重複するオブジェクトがある場合に発生する可能性があります。ユーザーログオン名は一意である必要があります。詳細については、Microsoft ドキュメントの「[ディレクトリデータの問題のトラブルシューティング](#)」を参照してください。

パスワードの復旧

ユーザーがパスワードを忘れた場合や AWS Managed Microsoft AD ディレクトリへのサインインに問題がある場合は、AWS Management Console、PowerShell、または AWS CLIを使用してパスワードをリセットできます。

詳細については、「[AWS Managed Microsoft AD ユーザーパスワードのリセット](#)」を参照してください。

追加リソース

以下のリソースは、作業中のトラブルシューティングに役立ちます AWS。

- [AWS ナレッジセンター](#) – 問題のトラブルシューティングに役立つFAQsと他のリソースへのリンクを見つけてみます。
- [AWS サポートセンター](#) – テクニカルサポートを受ける。
- [AWS プレミアムサポートセンター](#) – プレミアムテクニカルサポートを利用できます。

以下のリソースは、一般的な Active Directory 問題のトラブルシューティングに役立ちます。

- [Active Directory ドキュメント](#)
- [AD DSトラブルシューティング](#)

トピック

- [Amazon EC2 Linux インスタンスドメインの結合エラー](#)
- [AWS Managed Microsoft AD の使用可能なストレージ容量が少ない](#)
- [スキーマ拡張のエラー](#)
- [信頼作成ステータスの理由](#)

Amazon EC2 Linux インスタンスドメインの結合エラー

以下は、Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD ディレクトリに結合するときに発生する可能性のあるエラーメッセージのトラブルシューティングに役立ちます。

Linux インスタンスはドメインに結合したり、認証を行ったりすることができません

Ubuntu の領域を Microsoft Active Directory で使用する際は、その Ubuntu の (14.04、16.04、および 18.04 の) インスタンスでは、DNS での逆引き解決ができる必要があります。それ以外の場合は、以下の 2 つのシナリオのいずれかが発生する可能性があります。

シナリオ 1: まだ領域に結合されていない Ubuntu インスタンス

領域への結合を試行中の Ubuntu インスタンスの場合、ドメインに結合するために必要なアクセス許可が `sudo realm join` コマンドにより提供されず、次のようなエラーが表示されることがあります。

```
! Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) adcli: couldn't connect to EXAMPLE.COM domain: Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) !
(! Active Directory への認証に失敗しました: SASL(-1): 一般エラー: GSSAPI エラー: 無効な名前が入力されました (成功) adcli: EXAMPLE.COM ドメインに接続できませんでした: Active Directory への認証に失敗しました: SASL(-1): 一般エラー: GSSAPI エラー: 無効な名前が入力されました (成功) !)
Insufficient permissions to join the domain realm: Couldn't join realm: Insufficient permissions to join the domain (ドメイン領域に結合するための権限が不十分です: 領域に結合できませんでした: ドメインに結合するための権限が不十分です)
```

シナリオ 2: 領域に結合済みの Ubuntu インスタンス

既に Microsoft Active Directory ドメインに結合されている Ubuntu インスタンスの場合、ドメイン認証情報を使用してインスタンスに SSH 接続を試みると、次のエラーで失敗することがあります。

```
$ ssh admin@EXAMPLE.COM@198.51.100
```

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

```
admin@EXAMPLE.COM@198.51.100's password: (admin@EXAMPLE.COM@198.51.100 のパスワード:)
```

```
Permission denied, please try again.
```

```
admin@EXAMPLE.COM@198.51.100's password: (admin@EXAMPLE.COM@198.51.100 のパスワード:)
```

公開キーを使用してインスタンスにログインし `/var/log/auth.log` を参照すると、次のような、ユーザーが見つからないことを知らせるエラーが表示されることがあります。

```
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]
```

ただし、このユーザーの `kinit` は引き続き使用可能です。以下に例を示します。

```
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
```

回避方法

これらの両方のシナリオで現在推奨されている回避策は、次に示すように `[libdefaults]` セクションの `/etc/krb5.conf` でリバース DNS を無効にすることです。

```
[libdefaults]
```

```
default_realm = EXAMPLE.COM
rdns = false
```

シームレスなドメイン結合での一方向の信頼認証の問題

AWS Managed Microsoft AD とオンプレミス Active Directory の間で一方向の送信信頼が確立されている場合、Winbind で信頼された Active Directory 認証情報を使用してドメインに参加している Linux インスタンスに対して認証を試みると、認証の問題が発生する可能性があります。

エラー

```
Jul 31 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Failed password for user@corp.example.com
from xxx.xxx.xxx.xxx port 18309 ssh2 (7月31日 00:00:00 EC2AMAZ-LSMWqT sshd[23832]:
xxx.xxx.xxx.xxx ポート 18309 ssh2 からの user@corp.example.com のパスワードが失敗しました)
```

```
Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): getting password
(0x00000390) (7月31日 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): パス
ワードの取得 (0x00000390))
```

```
Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item returned
a password (7月31日 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth):
pam_get_item がパスワードを返しました)
```

```
7月31日 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): リクエスト
wbcLogonUser が失敗しました: WBC_ERR_AUTH_ERROR: PAM エラー: PAM_SYSTEM_ERR
(4)、NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_FOUND**、エラーメッセージ: オブジェク
ト名が見つかりません。
```

```
Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): internal module error
(retval = PAM_SYSTEM_ERR(4), user = 'CORP\user') (7月31日 00:05:00 EC2AMAZ-LSMWqT
sshd[23832]: pam_winbind(sshd:auth): 内部モジュールエラー (retval = PAM_SYSTEM_ERR (4)、
ユーザー = 'CORP\user'))
```

回避方法

この問題を解決するには、次の手順に従って、PAM モジュール設定ファイル (/etc/security/pam_winbind.conf) 内のディレクティブをコメントアウトするか、それを削除する必要があります。

1. テキストエディタで /etc/security/pam_winbind.conf ファイルを開きます。

```
sudo vim /etc/security/pam_winbind.conf
```

2. ディレクティブ「krb5_auth = yes」をコメントアウトするか、削除してください。

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. Winbind サービスを停止した後に再起動します。

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

AWS Managed Microsoft AD の使用可能なストレージ容量が少ない

AWS Managed Microsoft AD Active Directoryのストレージ容量が少ないために障害が発生した場合は、ディレクトリをアクティブ状態に戻すための即時のアクションが必要です。この障害に関する最も一般的な 2 つの原因について、以下のセクションで説明します。

1. [\[SYSVOL\] フォルダにグループポリシーの必須オブジェクト以外のオブジェクトが保存されている](#)
2. [Active Directory のデータベースがボリュームを使い切っている](#)

AWS Managed Microsoft AD ストレージの料金については、[AWS Directory Service 「の料金」](#)を参照してください。

[SYSVOL] フォルダにグループポリシーの必須オブジェクト以外のオブジェクトが保存されている

この障害の一般的な原因の 1 つとして、グループポリシーによる処理に必須ではないファイルが [SYSVOL] フォルダに保存されていることが挙げられます。これらの必須ではないファイルには、グループポリシーが処理する際に必須ではない、EXE、MSI、などのファイルも含まれます。グループポリシーによる処理に必須であるオブジェクトは、グループポリシーオブジェクト、ログオン/オフスクリプト、および [グループポリシーオブジェクト用のセントラルストア](#)です。重要でないファイ

ルは、AWS Managed Microsoft AD ドメインコントローラー以外のファイルサーバー (複数可) に保存する必要があります。

[グループポリシーソフトウェアのインストール](#)用のファイルが必要な場合は、ファイルサーバーを使用してこれらのインストールファイルを保存する必要があります。ファイルサーバーを自己管理しない場合、はマネージドファイルサーバーオプションである [Amazon FSx](#) AWS を提供します。

不要なファイルを削除するには、ユニバーサル命名規則 (UNC) パスを介して SYSVOL 共有にアクセスできます。たとえば、ドメインの完全修飾ドメイン名 (FQDN) が example.com の場合、SYSVOL の UNC パスは「\\example.local\\SYSVOL\\example.local」になります。グループポリシーによるディレクトリの処理に必須ではないオブジェクトを特定し削除すると、そのディレクトリは 30 分以内にアクティブな状態に戻ります。30 分経過してもディレクトリがアクティブでない場合は、AWS サポートにお問い合わせください。

グループポリシーの必須ファイルのみを SYSVOL 共有に保存することで、SYSVOL の肥大化によるディレクトリの障害を回避しています。

Active Directory のデータベースがボリュームを使い切っている

この障害の一般的な原因の 1 つに、Active Directory データベースがボリュームを使い切っている場合があります。これが該当するかどうかを調べるには、ディレクトリ内のオブジェクト数の [total] (合計) を確認します。削除済み オブジェクトもディレクトリ内のオブジェクトの合計数にカウントされるため、それを明記するために、ここでは合計 を太字で強調しています。

デフォルトでは、AWS Managed Microsoft AD は、リサイクルオブジェクトになる前に 180 日間 AD ごみ箱に項目を保持します。オブジェクトがリサイクルされた (捨てられた) オブジェクトになると、そのオブジェクトは、さらに 180 日間保持された後で最終的にディレクトリから除去されます。つまり、削除されたオブジェクトは、完全に除去されるまで 360 日間ディレクトリデータベースに存在し続けます。この理由により、オブジェクトの合計数の評価が必要になります。

AWS Managed Microsoft AD がサポートするオブジェクト数の詳細については、[AWS Directory Service](#) 「[料金表](#)」を参照してください。

ディレクトリ内のオブジェクトについて、削除済みオブジェクトも含んだ合計数を取得するには、ドメインに参加している Windows インスタンスから次の PowerShell コマンドを実行します。管理インスタンスをセットアップする手順については、「[AWS Managed Microsoft AD でのユーザーとグループの管理](#)」を参照してください。

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' |  
Select-Object -Property 'Count'
```

上記のコマンドからの出力例を次に示します。

```
Count
10000
```

合計数が、上に示したディレクトリサイズでサポートされるオブジェクト数を上回っている場合は、ディレクトリの容量を超えています。

この障害を解決するためのオプションを以下に示します。

1. AD のクリーンアップ

- a. 不要な AD オブジェクトを削除します。
- b. AD のごみ箱から不要なオブジェクトを削除します。これによりオブジェクトは破壊されるので、ディレクトリの復元を実行することが、削除されたオブジェクトを回復する唯一の方法となります。
- c. 次のコマンドは、AD のごみ箱からすべての削除済みオブジェクトを除去します。

Important

これはオブジェクトを破壊するコマンドであり、削除したオブジェクトを回復するにはディレクトリの復元を実行する以外にないため、このコマンドの使用には細心の注意を払ってください。

```
$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. AWS Support でケースを開き、 が空き容量 AWS Directory Service を再利用するようにリクエストします。
- ## 2. ディレクトリタイプが Standard Edition の場合は、AWS サポートでケースを開き、ディレクトリを Enterprise Edition にアップグレードするようリクエストします。このアップグレードを行う

と、ディレクトリのコストも増加します。料金に関する情報については、[\[AWS Directory Service の料金\]](#)を参照してください。

AWS Managed Microsoft AD では、AWS 委任削除オブジェクトのライフタイム管理者グループのメンバーは、削除されたオブジェクトがリサイクルオブジェクトになる前に AD ごみ箱に保持される日数を設定する msDS-DeletedObjectLifetime 属性を変更することができます。

 Note

これは進んだ内容のトピックです。設定が不適切であると、データが失われる可能性があります。最初に「[The AD Recycle Bin: Understanding, Implementing, Best Practices, and Troubleshooting](#)」(AD のごみ箱について: その理解と実装、ベストプラクティス、ならびにトラブルシューティング) をお読みになり、これらのプロセスをよく理解することを強くお勧めします。

msDS-DeletedObjectLifetime 属性値は、より低い数値に変更でき、これによりオブジェクト数がサポートされているレベルを超えないようにできます。この属性に設定できる有効な最低値は 2 日です。この設定日数を超えた削除済みオブジェクトは、AD のごみ箱を使用しての復元が不可能になります。オブジェクトを回復するには、スナップショットからディレクトリを復元する必要があります。詳細については、「[スナップショットを使用した AWS Managed Microsoft AD の復元](#)」を参照してください。スナップショットから復元した結果、現時点でのデータが失われる場合があります。

ディレクトリの削除済みオブジェクトの保持期間を変更するには、次のコマンドを実行します。

 Note

このコマンドを変更せずに実行すると、Deleted Object Lifetime (削除済みオブジェクトの保持期間) 属性値が 30 日に設定されます。長くしたり短くしたりする場合は、「30」を任意の数に置き換えます。ただし、デフォルト値の 180 を超えないようにすることをお勧めします。

```
$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 }
```

スキーマ拡張のエラー

以下は、AWS Managed Microsoft AD ディレクトリのスキーマを拡張するときに発生する可能性のあるエラーメッセージのトラブルシューティングに役立ちます。

照会

エラー

Add error on entry starting on line 1: Referral The server side error is: 0x202b A referral was returned from the server. (1 行目で開始するエントリへのエラー追加: 照会 サーバー側エラー: 0x202b サーバーから照会が返されました。) The extended server error is: 0000202B: RefErr: DSID-0310082F, data 0, 1 access points \tref 1: 'example.com' Number of Objects Modified: 0 (拡張サーバーエラー: 0000202B: RefErr: DSID-0310082F、データ 0、1 アクセスポイント \tref 1: 「example.com」変更されたオブジェクト数: 0)

トラブルシューティング

すべての個別名前フィールドに正しいドメイン名が設定されていることを確認します。上記の例では、DC=example,dc=com はコマンドレット Get-ADDomain に示される DistinguishedName に置換される必要があります。

インポートファイルを読み取れない

エラー

インポートファイルを読み取れない。変更されたオブジェクト数: 0

トラブルシューティング

インポートされた LDIF ファイルは空 (0 バイト) です。適切なファイルをアップロードしてください。

構文エラー

エラー

There is a syntax error in the input file Failed on line 21. (21 行目で失敗した入力ファイルに構文エラーがあります) 最後のトークンは「q」で始まります。変更されたオブジェクト数: 0

トラブルシューティング

21 行目のテキスト が正しい形式で記述されていません。この無効なテキストの最初の文字は、A です。有効な LDIF 構文で行 21 を更新してください。LDIF ファイルで使用する形式の詳細については、「[ステップ 1: LDIF ファイルを作成する](#)」を参照してください。

属性または値が存在する

エラー

Add error on entry starting on line 1: Attribute Or Value Exists The server side error is: 0x2083 The specified value already exists. (1 行目で開始する エントリへのエラー追加: 属性または値が存在するサーバー側のエラー: 0x2083 指定された値はすでに存在しています。) The extended server error is: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0 (拡張サーバーエラー: 00002083: AtrErr:DSID-03151830、#1: \t0:00002083: DSID-03151830、問題 1006 (ATT_OR_VALUE_EXISTS)、データ 0、Att 20019 (mayContain):len 4 変更されたオブジェクト数: 0)

トラブルシューティング

スキーマに行った変更は既に適用されます。

該当する属性なし

エラー

Add error on entry starting on line 1: No Such Attribute The server side error is: 0x2085 The attribute value cannot be removed because it is not present on the object. (1 行目で開始する エントリへのエラー追加: 該当する属性がないサーバー側エラー: 0x2085 属性値はオブジェクトに存在しないため削除できません。) The extended server error is: 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problem 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0 (拡張サーバーエ

ラー: 00002085: AttrErr:DSID-03152367、#1: \t0:00002085: DSID-03152367、問題 1001 (NO_ATTRIBUTE_OR_VAL)、データ 0、Att 20019 (mayContain):len 4 変更されたオブジェクト数: 0)

トラブルシューティング

LDIF ファイルはクラスから属性を削除しようとしたが、その属性は現在、対象のクラスに関連付けられていません。スキーマの変更がすでに適用されている可能性があります。

エラー

Add error on entry starting on line 41: No Such Attribute 0x57 The parameter is incorrect. (41 行目で開始するエントリへのエラー追加: 属性 0x57が存在しません パラメータが正しくありません。) The extended server error is: 0x208d Directory object not found. (拡張サーバーエラー: 0x208d ディレクトリオブジェクトが見つかりません。) The extended server error is: "00000057: LdapErr: DSID-0C090D8A, comment: Error in attribute conversion operation, data 0, v2580" Number of Objects Modified: 0 (拡張サーバーエラー: "00000057: LdapErr:DSID-0C090D8A、コメント: 属性変換操作エラー、データ 0、v2580" 変更されたオブジェクト数: 0)

トラブルシューティング

41 行目に記載されている属性が正しくありません。スペルを再確認してください。

該当するオブジェクトなし

エラー

Add error on entry starting on line 1: No Such Object The server side error is: 0x208d Directory object not found. (1 行目で開始するエントリへのエラー追加: 該当するオブジェクトなし サーバー側エラー: 0x208d ディレクトリオブジェクトが見つかりません。) The extended server error is: 0000208D: NameErr: DSID-03100238, problem 2001 (NO_OBJECT), data 0, best match of: 'CN=Schema,CN=Configuration,DC=example,DC=com' Number of Objects Modified: 0 (拡張サーバーエラー: 0000208D: NameErr: DSID-03100238、問題 2001 (NO_OBJECT)、データ 0、ベストマッチ: 'CN=Schema,CN=Configuration,DC=example,DC=com' 変更されたオブジェクト数: 0)

トラブルシューティング

この識別名 (DN) によって参照されるオブジェクトは存在しません。

信頼作成ステータスの理由

AWS Managed Microsoft AD の信頼の作成に失敗すると、ステータスメッセージに追加情報が含まれます。以下は、これらのメッセージが何を意味するかを理解するのに役立ちます。

アクセスが拒否されました

信頼の作成を試みた際にアクセスが拒否されました。信頼パスワードが正しくないか、リモートドメインのセキュリティ設定で信頼を設定できません。信頼の詳細については、「」を参照してください [サイト名と DCLocator による信頼効率の向上](#)。この問題を解決するには、以下の手順を実行します。

- リモートドメインで対応する信頼を作成する際に使用したものと、同じ信頼パスワードを使用していることを確認します。
- ドメインのセキュリティ設定で、信頼の作成を許可していることを確認します。
- ローカルセキュリティポリシーが正しく設定されていることを確認します。特に Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously をチェックして、少なくとも以下の 3 つの名前付きパイプが含まれていることを確認してください
 - netlogon
 - samr
 - lsarpc
- 上記の名前付きパイプが、レジストリパス [HKLM\SYSTEM\CurrentControlSet\services\LanmanServer\Parameters] にある [NullSessionPipes] レジストリキーの値として存在することを確認します。これらの値は、別々の行に挿入する必要があります。

Note

デフォルトで Network access: Named Pipes that can be accessed anonymously は設定されていないので、Not Defined が表示されます。これは正常な動作であり、Network access: Named Pipes that can be accessed anonymously に対するドメインコントローラの有効なデフォルト設定は netlogon、samr、lsarpc です。

- デフォルトのドメインコントローラーポリシーで、次のサーバーメッセージブロック (SMB) 署名設定を確認します。これらの設定は、[コンピュータ設定] > [Windows 設定] > [セキュリティ設定]

> [ローカルポリシー/セキュリティオプション] で見つけることができます。次の設定と一致する必要があります:

- Microsoft ネットワーククライアント: 通信にデジタル署名 (常に): デフォルト: 有効
- Microsoft ネットワーククライアント: 通信にデジタル署名 (サーバーが同意する場合): デフォルト: 有効
- Microsoft ネットワークサーバー: 通信にデジタル署名 (常に): 有効
- Microsoft ネットワークサーバー: デジタル署名通信 (クライアントが同意した場合): デフォルト: 有効

サイト名と DCLocator による信頼効率の向上

Default-First-Site-Name のような最初のサイト名は、ドメイン間の信頼関係を確立するための要件ではありません。ただし、ドメイン間でサイト名を調整すると、ドメインコントローラーロケーター (DCLocator) プロセスの効率が大幅に向上する可能性があります。この調整により、フォレストの信頼全体でのドメインコントローラーの選択の予測と制御が向上します。

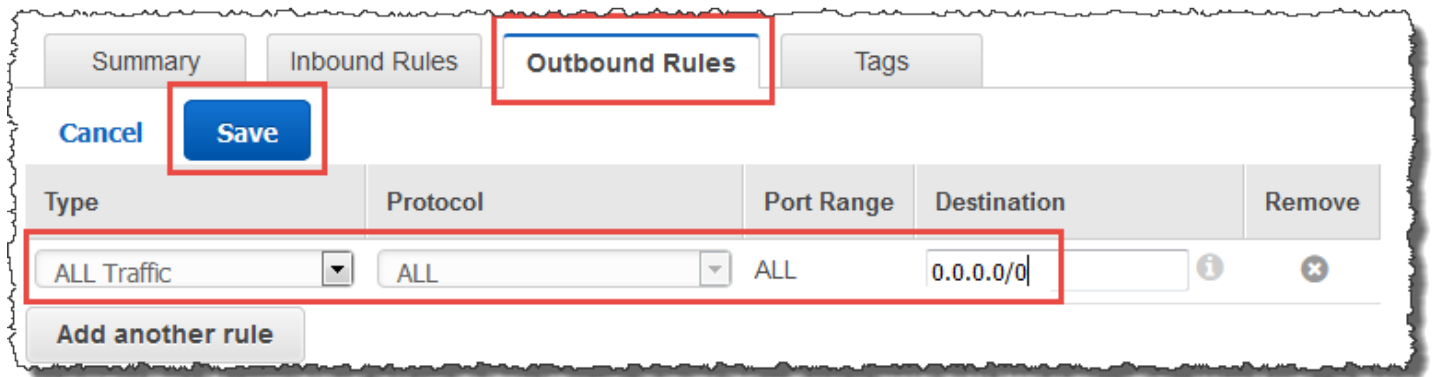
DCLocator プロセスは、さまざまなドメインとフォレストのドメインコントローラーを見つけるために不可欠です。DCLocator プロセスの詳細については、「[Microsoft ドキュメント](#)」を参照してください。効率的なサイト設定により、より迅速かつ正確なドメインコントローラーの場所が可能になり、クロスフォレストオペレーションのパフォーマンスと信頼性が向上します。

サイト名と DCLocator プロセスのやり取りの詳細については、以下の Microsoft 記事を参照してください。

- [信頼間のドメインコントローラーの配置方法](#)
- [フォレスト間のドメインロケーター](#)

指定されたドメイン名が存在しない、または接続できませんでした。

この問題を解決するには、ドメインおよび VPC のアクセスコントロールリスト (ACL) でのセキュリティグループ設定が正しいこと、ならびに条件付きフォワーダーの情報が正確に入力されていることを確認します。AWS は、Active Directory の通信に必要なポートのみを開くようにセキュリティグループを設定します。セキュリティグループのデフォルト設定では、これらのポートに対する任意の IP アドレスからのトラフィックを受け入れます。アウトバウンドトラフィックは、セキュリティグループに制限されます。オンプレミスネットワークへのトラフィックを許可するには、セキュリティグループのアウトバウンドルールを更新する必要があります。セキュリティ要件の詳細については、「[ステップ 2: AWS Managed Microsoft AD を準備する](#)」を参照してください。



他のディレクトリのネットワークの DNS サーバーで、(RFC 1918 ではない) パブリックIP アドレスを使用している場合、Directory Service コンソールから、ディレクトリの IP ルートを DNS サーバーに追加する必要があります。詳細については、「[信頼関係を作成、検証、または削除する](#)」および「[前提条件](#)」を参照してください。

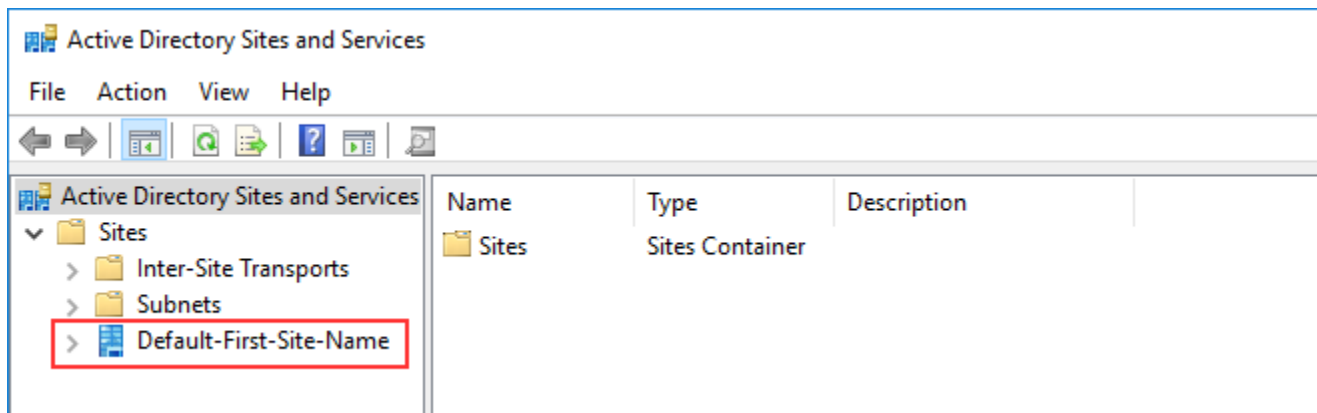
The Internet Assigned Numbers Authority (IANA) は、プライベートインターネット用に次の 3 つの IP アドレス空間ブロックを予約しています。

- 10.0.0.0 – 10.255.255.255 (10/8 プレフィックス)
- 172.16.0.0 – 172.31.255.255 (172.16/12 プレフィックス)
- 192.168.0.0 – 192.168.255.255 (192.168/16 プレフィックス)

詳細については、<https://tools.ietf.org/html/rfc1918> を参照してください。

AWS Managed Microsoft AD のデフォルトの AD サイト名が、オンプレミスインフラストラクチャのデフォルトの AD サイト名と一致していることを確認します。コンピュータは、ユーザーのドメインではなく、コンピュータがメンバーであるドメインを使用してサイト名を決定します。最も近いオンプレミスと一致するようにサイトの名前を変更すると、最も近いサイトにあるドメインコントローラーを、DC ロケーターに選択させることができます。これで問題が解決しない場合は、先に作成してある条件付きフォワーダーからの情報がキャッシュされたことで、新しい信頼の作成が妨げられている可能性があります。数分待ってから、信頼と条件付きフォワーダーの作成を再試行してください。

この機能に関する情報については、Microsoft のウェブサイトの「[Domain フォレスト信頼関係間でのドメインロケーター](#)」を参照してください。



このドメインでオペレーションを実行できませんでした

この問題を解決するには、ドメイン / ディレクトリの両方で NETBIOS 名が重複していないことを確認します。ドメイン / ディレクトリで NETBIOS 名の重複がある場合は、別の NETBIOS 名を使用してそれらのいずれかを再作成した上で、もう一度試してください。

「Required and valid domain name (必須かつ有効なドメイン名)」というエラーが原因で、信頼の作成に失敗しました

DNS 名に使用できるのは、アルファベット文字 (A~Z)、数字 (0~9)、マイナス記号 (-)、ピリオド (.) のみです。ピリオド文字を使用できるのは、ドメインスタイル名のコンポーネントを区切るために使用する場合があります。また、以下の点を考慮してください。

- AWS Managed Microsoft AD は、単一ラベルドメインでの信頼をサポートしていません。詳細については、「[シングルラベルドメインの Microsoft サポート](#)」を参照してください。
- RFC 1123 (<https://tools.ietf.org/html/rfc1123>) の規定では、DNSラベルで利用できる文字は「A」から「Z」、「a」から「z」、「0」から「9」、およびハイフン (「-」) のみです。ピリオド [.] は DNS 名でも使用されますが、DNS ラベルの間と FQDN の末尾にのみ配置できます。
- RFC 952 (<https://tools.ietf.org/html/rfc952>) の規定では、「名前」(ネット、ホスト、ゲートウェイ、ドメイン名) は、アルファベット (A~Z)、数字 (0~9)、マイナス記号 (-)、ピリオド (.) を使用した最大 24 文字のテキスト文字列となります。ピリオド文字を使用できるのは、「ドメインスタイル名」のコンポーネントを区切るために使用する場合があります。

詳細については、Microsoft ウェブサイトの「[ホストとドメインの名前制限に準拠する](#)」を参照してください

信頼テスト用の一般的なツール

以下は、信頼に関連するさまざまな問題をトラブルシューティングするために使用できるツールです。

AWS Systems Manager Automation のトラブルシューティングツール

[サポート自動化ワークフロー \(SAW\)](#) は AWS Systems Manager Automation を活用して、事前定義されたランブックを提供します AWS Directory Service。 [AWSSupport-TroubleshootDirectoryTrust](#) ランブックツールは、AWS Managed Microsoft AD とオンプレミス Microsoft の間の一般的な信頼作成問題を診断するのに役立ちますActive Directory。

DirectoryServicePortTest ツール

[DirectoryServicePortTest](#) テストツールは、AWS Managed Microsoft AD とオンプレミス Active Directory 間の信頼作成に関する問題のトラブルシューティングに役立ちます。ツール使用方法の例については、「[AD Connector をテストする](#)」を参照してください。

NETDOM および NLTEST ツール

管理者は、Netdom および Nltest のコマンドラインツールを使用して、信頼の検索、表示、作成、削除、および管理を行うことができます。これらのツールは、ドメインコントローラー上の LSA 権限と直接通信します。これらのツールの使用方法例については、Microsoft ウェブサイトの「[Netdom](#)」および「[NLTEST](#)」を参照してください。

パケットキャプチャツール

組み込みの Windows パッケージキャプチャユーティリティを使用して、ネットワークの問題の可能性を調査し、トラブルシューティングを行うことができます。詳細については、「[Capture a Network Trace without installing anything](#)」(インストールを一切行わずにネットワークトレースをキャプチャする) を参照してください。

AD Connector

AD Connector は、クラウド内の情報をキャッシュせずにディレクトリリクエストをオンプレミスの Microsoft Active Directory にリダイレクトするために使用できるディレクトリゲートウェイです。AD Connector には、スモールとラージの 2 つのサイズがあります。小さな AD Connector は、小規模な組織向けに設計されており、1 秒あたり少数のオペレーション数进行处理することを目的としています。大きな AD Connector は、大規模な組織向けに設計されており、1 秒あたり中程度から多数のオペレーション数进行处理することを目的としています。パフォーマンスのニーズに合わせてスケーリングし、複数の AD Connector 間でアプリケーションの負荷を分散させることができます。適用されるユーザー制限や接続制限はありません。

AD Connector は Active Directory 推移的信頼をサポートしていません。AD Connector とオンプレミスの Active Directory ドメインには 1 対 1 の関係があります。つまり、オンプレミスのドメインごとに (認証対象の Active Directory フォレスト内の子ドメインを含む)、一意の AD Connector を作成する必要があります。

Note

AD Connector を他の AWS アカウントと共有することはできません。これが要件である場合は、AWS Managed Microsoft AD を使用することを検討してください[AWS Managed Microsoft AD を共有する](#)。AD Connector もマルチ VPC 対応ではないため、[WorkSpaces](#) などの AWS アプリケーションは AD Connector と同じ VPC にプロビジョニングする必要があります。

セットアップすると、AD Connector には次のような利点があります。

- エンドユーザーと IT 管理者は、既存の企業認証情報を使用して WorkSpaces、WorkDocs、Amazon WorkMail などの AWS アプリケーションにログオンできます。
- への IAM ロールベースのアクセスを通じて Amazon EC2 インスタンスや Amazon S3 バケットなどの AWS リソースを管理できます AWS Management Console。
- ユーザーまたは IT 管理者がオンプレミスインフラストラクチャまたは AWS クラウドのリソースにアクセスするかどうかにかかわらず、既存のセキュリティポリシー (パスワードの有効期限、パスワード履歴、アカウントのロックアウトなど) を一貫して適用できます。

- AD Connector を使用して、既存の RADIUS ベースの MFA インフラストラクチャと統合することで多要素認証を有効にし、ユーザーが AWS アプリケーションにアクセスするときに追加のセキュリティレイヤーを提供できます。

このセクションの残りのトピックでは、ディレクトリに接続する方法および AD Connector の機能を最大限に利用する方法について説明しています。

トピック

- [AD Connector の開始](#)
- [AD Connector のベストプラクティス](#)
- [AD Connector ディレクトリを維持する](#)
- [AD Connector ディレクトリをセキュリティで保護する](#)
- [AD Connector ディレクトリをモニタリングする](#)
- [AD Connector から AWS アプリケーションとサービスへのアクセス](#)
- [Amazon EC2 インスタンスを Active Directory に結合する方法](#)
- [AD Connector クォータ](#)
- [AD Connector のトラブルシューティング](#)

AD Connector の開始

AD Connector を使用すると、既存のエンタープライズ AWS Directory Service に接続できます Active Directory。既存のディレクトリに接続されている場合、ドメインコントローラーにすべてのディレクトリデータが留まります。AWS Directory Service では、ディレクトリデータはレプリケートされません。

トピック

- [AD Connector の前提条件](#)
- [AD Connector を作成する](#)
- [AD Connector で作成されるもの](#)

AD Connector の前提条件

AD Connector を使用して既存のディレクトリに接続するには、以下が必要です。

Amazon VPC

次のように VPC を設定します。

- 少なくとも 2 つのサブネット。各サブネットはそれぞれ異なるアベイラビリティーゾーンにある必要があります。
- VPC は、バーチャルプライベートネットワーク (VPN) 接続または AWS Direct Connectを通じて既存のネットワークに接続されている必要があります。
- VPC にはデフォルトのハードウェアテナンシーが必要です。

AWS Directory Service は 2 つの VPC 構造を使用します。ディレクトリを構成する EC2 インスタンスは、AWS アカウント外で実行され、によって管理されます AWS。これらには、2 つのネットワークアダプタ (ETH0 および ETH1) があります。ETH0 は管理アダプタで、アカウント外部に存在します。ETH1 はアカウント内で作成されます。

ディレクトリの ETH0 ネットワークの管理 IP 範囲は、ディレクトリがデプロイされている VPC と競合しないようにするため、プログラムによって選択されます。この IP 範囲は、(ディレクトリが 2 つのサブネットで実行されるため) 次のいずれかのペアになります。

- 10.0.1.0/24 と 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 と 192.168.2.0/24

ETH1 CIDR の最初のオクテットをチェックすることで、競合を回避します。10 で始まる場合は、192.168.1.0/24 と 192.168.2.0/24 のサブネットを持つ 192.168.0.0/16 VPC を選択します。最初のオクテットが 10 以外である場合は、10.0.1.0/24 と 10.0.2.0/24 のサブネットを持つ 10.0.0.0/16 VPC を選択します。

選択アルゴリズムには、VPC 上のルートは含まれません。そのため、このシナリオから IP ルーティングの競合が発生する可能性があります。

詳細については、「Amazon VPC ユーザーガイド」の次のトピックを参照してください。

- [Amazon VPC とは？](#)
- [VPC のサブネット](#)
- [VPC へのハードウェア仮想プライベートゲートウェイの追加](#)

詳細については AWS Direct Connect、[AWS Direct Connect 「ユーザーガイド」](#) を参照してください。

既存の Active Directory

Active Directory ドメインを持つ既存のネットワークに接続する必要があります。

Note

AD Connector は、[単一ラベルのドメイン](#)をサポートしていません。

この Active Directory ドメインの機能レベルは Windows Server 2003 以上である必要があります。AD Connector は、Amazon EC2 インスタンスでホストされているドメインへの接続もサポートしています。

Note

AD Connector は、Amazon EC2 のドメイン結合機能と併用する場合の読み取り専用ドメインコントローラー (RODC) をサポートしていません。

サービスアカウント

次の権限が委任されている既存のディレクトリのサービスアカウントの認証情報が必要です。

- ユーザーおよびグループの読み取り - 必須
- コンピュータのドメインへの結合 - シームレスなドメイン結合と WorkSpaces を使用する場合にのみ必要
- コンピュータオブジェクトの作成 - シームレスなドメイン結合と WorkSpaces を使用する場合にのみ必要
- サービスアカウントのパスワードは、パスワード要件に準拠 AWS している必要があります。AWS パスワードは次のようになります。
 - 長さは 8～128 文字以内。
 - 次の 4 つのカテゴリのうち、3 つからの少なくとも 1 文字を含めます。
 - 小文字 a～z
 - 大文字 A～Z
 - 数字 (0～9)
 - 英数字以外の文字 (~!@#\$%^&* _-+=`|(){}[];:'"<>,.?/)

詳細については、「[権限をサービスアカウントに委任する](#)」を参照してください。

 Note

AD Connector は、AWS アプリケーションの認証および認可に Kerberos を使用します。LDAP は、ユーザーおよびグループオブジェクトの検索 (読み取りオペレーション) にのみ使用されます。LDAP トランザクションでは、変更可能なものはなく、認証情報はクリアテキストで渡されません。認証は、Kerberos チケットを使用して LDAP オペレーションをユーザーとして実行する AWS 内部サービスによって処理されます。

ユーザーアクセス許可

すべての Active Directory ユーザーは、各ユーザー独自の属性を読み取るアクセス許可を持っている必要があります。具体的には次の属性があります。

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

デフォルトでは、Active Directory ユーザーには、これらの属性に対する読み取りアクセス許可があります。ただし、時間の経過に伴い管理者がこれらのアクセス許可を変更する可能性があるため、AD Connector を初めて設定する前に、ユーザーがこれらの読み取りアクセス許可を持っているかどうか確認することをお勧めします。

IP アドレス

既存のディレクトリの 2 つの DNS サーバーまたはドメインコントローラーの IP アドレスを取得します。

AD Connector は、ディレクトリに接続するときに `_ldap._tcp.<DnsDomainName>` および `_kerberos._tcp.<DnsDomainName>` SRV レコードをこれらのサーバーから取得します。そのため、これらのサーバーにはこれらの SRV レコードが含まれている必要があります。AD Connector は、LDAP と Kerberos サービスの両方を提供する共通ドメインコントローラーを見つけようとします。そのため、これらの SRV レコードには、少なくとも 1 つの共通ドメインコントローラーが含まれている必要があります。SRV レコードの詳細については、Microsoft TechNet の「[SRV Resource Records](#)」(SRV リソースレコード) を参照してください。

サブネット用のポート

AD Connector で既存の Active Directory のドメインコントローラーにディレクトリリクエストをリダイレクトするには、既存のネットワークのファイアウォールで、Amazon VPC の両方のサブネットの CIDR に対して次のポートを開く必要があります。

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 認証
- TCP/UDP 389 - LDAP

これらは、AD Connector をディレクトリに接続する前に必要な最小限のポートです。固有の設定によっては、追加ポートが開かれていることが必要です。

AD Connector と Amazon WorkSpaces を使用する場合は、ドメインコントローラーの DisableVLVSupportLDAP 属性を 0 に設定する必要があります。これはドメインコントローラーのデフォルト設定です。DisableVLVSupportLDAP 属性が有効になっている場合、AD Connector はディレクトリ内のユーザーをクエリできません。これにより、AD Connector が Amazon WorkSpaces と連携することを防止します。

Note

既存の Active Directory ドメインの DNS サーバーまたはドメインコントローラーサーバーが VPC 内にある場合、これらのサーバーに関連付けられたセキュリティグループでは、VPC の両方のサブネットで、CIDR に対して上記のポートが開かれている必要があります。

追加のポート要件については、Microsoft ドキュメントの「[AD と AD DS ポートの要件](#)」を参照してください。

Kerberos 事前認証

ユーザーアカウントの Kerberos 事前認証を有効にしておく必要があります。この設定を有効にする方法の詳細については、「[Kerberos の事前認証が有効化されていることを確認する](#)」を参照してください。この設定に関する一般的な情報については、Microsoft TechNet の「[事前認証](#)」を参照してください。

暗号化タイプ

AD Connector は、Active Directory ドメインコントローラーへの Kerberos を介した認証時に、次のタイプの暗号化をサポートしています。

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

AWS IAM Identity Center 前提条件

IAM Identity Center を AD Connector で使用する場合は、次の条件が満たされていることを確認する必要があります。

- AD Connector は AWS 、組織の管理アカウントで設定されます。
- IAM Identity Center のインスタンスが AD Connector の設定先と同じリージョンにある。

詳細については、「AWS IAM Identity Center ユーザーガイド」の [「IAM Identity Center の前提条件」](#) を参照してください。

Multi-Factor Authentication の前提条件

AD Connector ディレクトリで Multi-Factor Authentication をサポートするには、以下が必要です。

- 2 つのクライアントエンドポイントを持つ、既存のネットワーク内の [Remote Authentication Dial-In User Service](#) (RADIUS) サーバー。RADIUS クライアントエンドポイントには次の要件があります。
 - エンドポイントを作成するには、AWS Directory Service サーバーの IP アドレスが必要です。これらの IP アドレスは、ディレクトリの詳細の [Directory IP Address] (ディレクトリの IP アドレス) フィールドから取得できます。
 - 2 つの RADIUS エンドポイントが同じ共有シークレットコードを使用する必要があります。
- 既存のネットワークでは、AWS Directory Service サーバーからのデフォルトの RADIUS サーバーポート (1812) 経由のインバウンドトラフィックを許可する必要があります。
- RADIUS サーバーと既存のディレクトリの間でユーザー名が同じである必要があります。

AD Connector で MFA を使用する場合の詳細については、「[AD Connector の多要素認証を有効にする](#)」を参照してください。

権限をサービスアカウントに委任する

既存のディレクトリに接続するには、特定の権限が委任されている既存のディレクトリの AD Connector サービスアカウントの認証情報が必要です。[Domain Admins] (ドメインの管理者) グループ

プのメンバーにはディレクトリに接続するために十分な権限がありますが、ベストプラクティスとして、そのディレクトリへの接続に必要な最小限の権限が付与されたサービスアカウントを使用することをお勧めします。次の手順では、という新しいグループを作成しConnectors、このグループへの接続に必要な権限 AWS Directory Service を委任してから、このグループに新しいサービスアカウントを追加する方法を示します。

この手順は、ディレクトリに結合され、[Active Directory User and Computers] (Active Directory ユーザーとコンピュータ) MMC スナップインがインストールされたマシンで実行する必要があります。また、ドメイン管理者としてログインする必要があります。

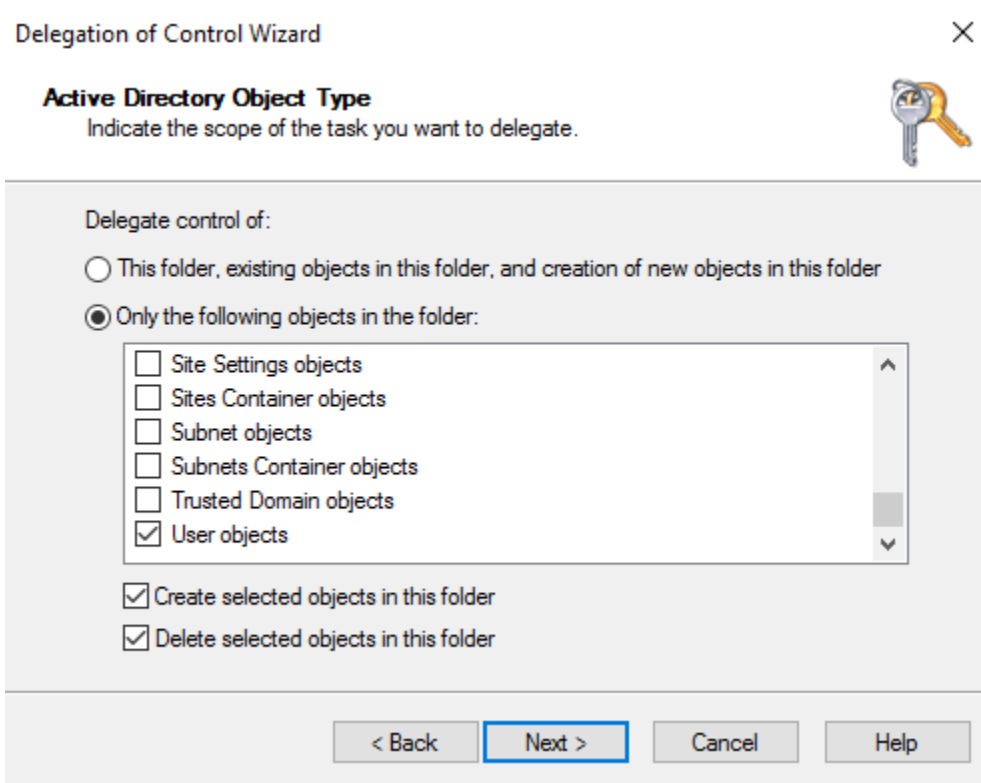
権限をサービスアカウントに委任するには

1. [Active Directory User and Computers] (Active Directory ユーザーとコンピュータ) を開き、ナビゲーションツリーのドメインルートを選択します。
2. 左のペインのリストで、[Users] (ユーザー) を右クリックし、[New] (新規) を選択して、[Group] (グループ) を選択します。
3. [New Object - Group] (新しいオブジェクト - グループ) ダイアログボックスで次のように入力し、[OK] をクリックします。

フィールド	値/選択
グループ名	Connectors
グループのスコープ	グローバル
グループのタイプ	セキュリティ

4. [Active Directory ユーザーとコンピュータ] のナビゲーションツリーで、コンピュータアカウントが作成される組織単位 (OU) を指定します。メニューで [Action] (アクション) を選択し、[Delegate Control] (制御を委任する) を選択します。子 OU に伝達されるアクセス権限として、ドメインまでの親 OU を選択できます。AD Connector が AWS Managed Microsoft AD に接続されている場合、ドメインルートレベルで制御を委任することはできません。この場合、制御を委任するには、コンピュータオブジェクトが作成されるディレクトリ OU で OU を選択します。
5. [Delegation of Control Wizard] (制御の委任ウィザード) ページで [Next] (次へ) をクリックし、[Add] (追加) をクリックします。
6. [Select Users, Computers, or Groups] (ユーザー、コンピュータ、またはグループの選択) ダイアログボックスで「Connectors」と入力し、[OK] をクリックします。複数のオブジェクトがあ

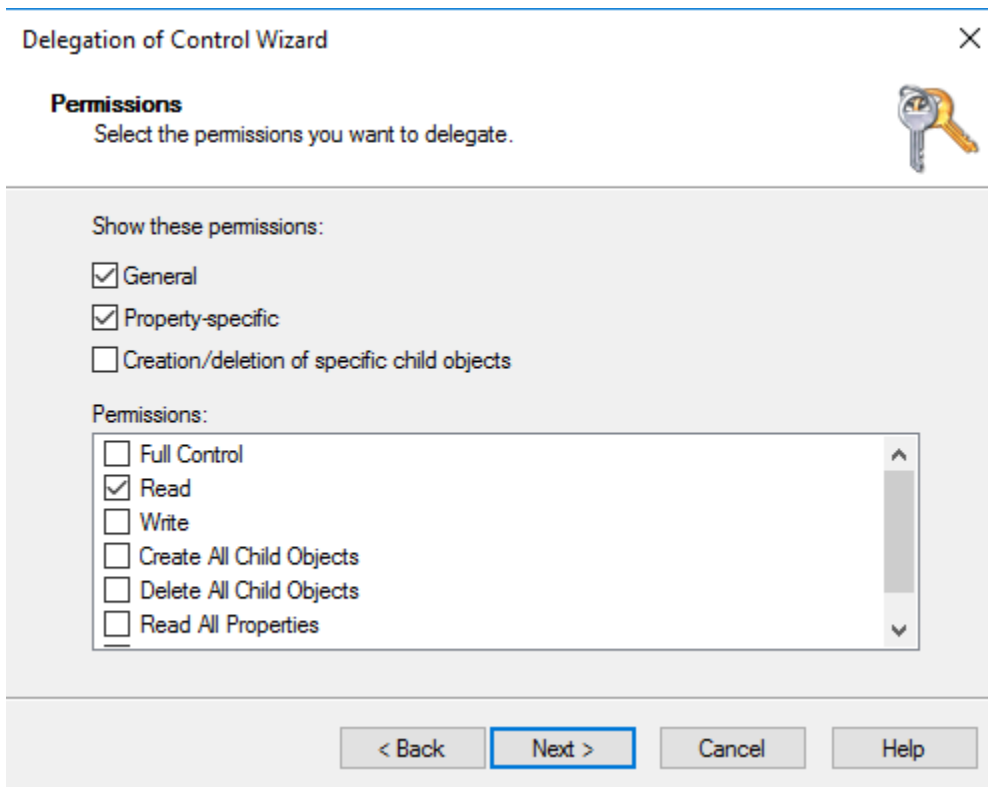
- る場合は、上記で作成した Connectors グループを選択します。[Next] (次へ) をクリックします。
7. [Tasks to Delegate] (委任するためのタスク) ページで、[Create a custom task to delegate] (委任するためのカスタムタスクを作成) を選択し、[Next] (次へ) をクリックします。
 8. [Only the following objects in the folder] (フォルダ内の次のオブジェクトのみ) を選択してから、[Computer objects] (コンピュータオブジェクト) と [User objects] (ユーザーオブジェクト) を選択します。
 9. [Create selected objects in this folder] (選択したオブジェクトをこのフォルダに作成) を選択し、[Delete selected objects in this folder] (このフォルダ内の選択したオブジェクトを削除) を選択します。続いて、[Next] (次へ) をクリックします。



10. [Read] (読み取り) を選択し、[Next] (次へ) をクリックします。

Note

シームレスなドメイン結合または WorkSpaces を使用する場合は、Active Directory がコンピュータオブジェクトを作成できるように、[Write] (書き込み) アクセス許可も有効にする必要があります。



11. [Completing the Delegation of Control Wizard] (制御の委任の完了ウィザード) ページの情報を確認し、[Finish] (完了) をクリックします。
12. 強力なパスワードでユーザーアカウントを作成し、そのユーザーを Connectors グループに追加します。このユーザーは AD Connector サービスアカウントと呼ばれ、グループのメンバーになったため、ディレクトリ AWS Directory Service に接続するための十分な権限が付与される Connectors ようになりました。

AD Connector をテストする

AD Connector で既存のディレクトリに接続するには、既存のネットワークのファイアウォールで VPC の両方のサブネットの CIDR に対して特定のポートが開かれている必要があります。これらの要件が満たされるかどうかをテストするには、次の手順に従います。

接続をテストするには

1. VPC で Windows インスタンスを起動し、RDP 経由でインスタンスに接続します。インスタンスは、既存のドメインのメンバーである必要があります。残りの手順は、この VPC インスタンスで実行します。

2. [DirectoryServicePortTest](#) テストアプリケーションをダウンロードして解凍します。ソースコードと Visual Studio プロジェクトファイルが含まれており、必要に応じてテストアプリケーションを変更できます。

 Note

このスクリプトは Windows Server 2003 以前のオペレーティングシステムではサポートされていません。

3. Windows のコマンドプロンプトで、次のオプションを指定して DirectoryServicePortTest テストアプリケーションを実行します。

 Note

DirectoryServicePortTest テストアプリケーションは、ドメインおよびフォレストの機能レベルが Windows Server 2012 R2 以下に設定されている場合にのみ使用できます。

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp  
"53,88,389" -udp "53,88,389"
```

<domain_name>

完全修飾ドメイン名。これは、フォレストとドメインの機能レベルをテストするために使用されます。ドメイン名を除外した場合、機能レベルはテストされません。

<server_IP_address>

既存のドメインのドメインコントローラーの IP アドレス。ポートはこの IP アドレスに対してテストされます。IP アドレスを除外した場合、ポートはテストされません。

このテストアプリケーションは、VPC からドメインに必要なポートが開いているかどうかを判断し、最小のフォレストとドメインの機能レベルも検証します。

出力は次のようになります。

```
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
```

DirectoryServicePortTest アプリケーションのソースコードは次のとおりです。

```
using System;  
using System.Collections.Generic;  
using System.IO;  
using System.Linq;  
using System.Net;  
using System.Net.Sockets;  
using System.Text;  
using System.Threading.Tasks;  
using System.DirectoryServices.ActiveDirectory;  
using System.Threading;  
using System.DirectoryServices.AccountManagement;  
using System.DirectoryServices;  
using System.Security.Authentication;  
using System.Security.AccessControl;  
using System.Security.Principal;  
  
namespace DirectoryServicePortTest  
{  
    class Program  
    {  
        private static List<int> _tcpPorts;  
        private static List<int> _udpPorts;  
  
        private static string _domain = "";  
        private static IPAddress _ipAddr = null;  
  
        static void Main(string[] args)
```

```
{
    if (ParseArgs(args))
    {
        try
        {
            if (_domain.Length > 0)
            {
                try
                {
                    TestForestFunctionalLevel();

                    TestDomainFunctionalLevel();
                }
                catch (ActiveDirectoryObjectNotFoundException)
                {
                    Console.WriteLine("The domain {0} could not be found.\n",
                        _domain);
                }
            }

            if (null != _ipAddr)
            {
                if (_tcpPorts.Count > 0)
                {
                    TestTcpPorts(_tcpPorts);
                }

                if (_udpPorts.Count > 0)
                {
                    TestUdpPorts(_udpPorts);
                }
            }
        }
        catch (AuthenticationException ex)
        {
            Console.WriteLine(ex.Message);
        }
    }
    else
    {
        PrintUsage();
    }

    Console.Write("Press <enter> to continue.");
}
```

```
        Console.ReadLine();
    }

    static void PrintUsage()
    {
        string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
        Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
    }

    static bool ParseArgs(string[] args)
    {
        bool fReturn = false;
        string ipAddress = "";

        try
        {
            _tcpPorts = new List<int>();
            _udpPorts = new List<int>();

            for (int i = 0; i < args.Length; i++)
            {
                string arg = args[i];

                if ("-tcp" == arg | "/tcp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _tcpPorts = ParsePortList(portList);
                }

                if ("-udp" == arg | "/udp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _udpPorts = ParsePortList(portList);
                }

                if ("-d" == arg | "/d" == arg)
                {
                    i++;
                    _domain = args[i];
                }
            }
        }
    }
}
```

```
        }

        if ("-ip" == arg | "/ip" == arg)
        {
            i++;
            ipAddress = args[i];
        }
    }
}
catch (ArgumentOutOfRangeException)
{
    return false;
}

if (_domain.Length > 0 || ipAddress.Length > 0)
{
    fReturn = true;
}

if (ipAddress.Length > 0)
{
    _ipAddr = IPAddress.Parse(ipAddress);
}

return fReturn;
}

static List<int> ParsePortList(string portList)
{
    List<int> ports = new List<int>();

    char[] separators = {',', ';', ':'};

    string[] portStrings = portList.Split(separators);
    foreach (string portString in portStrings)
    {
        try
        {
            ports.Add(Convert.ToInt32(portString));
        }
        catch (FormatException)
        {
        }
    }
}
```

```
        return ports;
    }

    static void TestForestFunctionalLevel()
    {
        Console.WriteLine("Testing forest functional level.");

        DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Forest, _domain, null, null);
        Forest forestContext = Forest.GetForest(dirContext);

        Console.Write("Forest Functional Level = {0} : ",
forestContext.ForestMode);

        if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
        {
            Console.WriteLine("PASSED");
        }
        else
        {
            Console.WriteLine("FAILED");
        }

        Console.WriteLine();
    }

    static void TestDomainFunctionalLevel()
    {
        Console.WriteLine("Testing domain functional level.");

        DirectoryContext dirContext = new
DirectoryContext(DirectoryContextType.Domain, _domain, null, null);
        Domain domainObject = Domain.GetDomain(dirContext);

        Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);

        if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
        {
            Console.WriteLine("PASSED");
        }
        else
        {
            Console.WriteLine("FAILED");
        }
    }
}
```

```
    }

    Console.WriteLine();
}

static List<int> TestTcpPorts(List<int> portList)
{
    Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

    List<int> failedPorts = new List<int>();

    foreach (int port in portList)
    {
        Console.Write("Checking TCP port {0}: ", port);

        TcpClient tcpClient = new TcpClient();

        try
        {
            tcpClient.Connect(_ipAddr, port);

            tcpClient.Close();
            Console.WriteLine("PASSED");
        }
        catch (SocketException)
        {
            failedPorts.Add(port);
            Console.WriteLine("FAILED");
        }
    }

    Console.WriteLine();

    return failedPorts;
}

static List<int> TestUdpPorts(List<int> portList)
{
    Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

    List<int> failedPorts = new List<int>();

    foreach (int port in portList)
    {
```



```
        Console.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;
}
}
```

AD Connector を作成する

既存のディレクトリを AD Connector に接続するには、次の手順を実行します。この手順を開始する前に、[AD Connector の前提条件](#) で定義されている前提条件を満たしていることを確認します。

Note

Cloud Formation テンプレートを使用して AD Connector を作成することはできません。

AD Connector に接続するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ)、[Set up directory] (ディレクトリの設定) の順に選択します。
2. [Select directory type] (ディレクトリタイプの選択) ページで [AD Connector] を選択してから、[Next] (次へ) をクリックします。

3. [Enter AD Connector information] (AD Connector 情報の入力) ページで、次の情報を指定します。

[Directory size] (ディレクトリのサイズ)

[Small] (スモール) または [Large] (ラージ) サイズオプションのどちらかを選択します。サイズの詳細については、「[AD Connector](#)」を参照してください。

[Directory description] (ディレクトリの説明)

必要に応じて、ディレクトリの説明。

4. [Choose VPC and subnets] (VPC とサブネットの選択) ページで、次の情報を指定して [Next] (次へ) をクリックします。

[VPC]

ディレクトリ用の VPC。

[Subnets] (サブネット)

ドメインコントローラーのサブネットを選択します。2 つのサブネットは、異なるアベイラビリティゾーンに存在している必要があります。

5. [Connect to AD] (AD への接続) ページで、次の情報を指定します。

[Directory DNS name] (ディレクトリの DNS 名)

既存のディレクトリの完全修飾名 (例: corp.example.com)。

[Directory NetBIOS name] (ディレクトリの NetBIOS 名)

既存のディレクトリの短縮名 (例: CORP)。

[DNS IP addresses] (DNS IP アドレス)

既存のディレクトリ内の少なくとも 1 つの DNS サーバーの IP アドレス。これらのサーバーは、ステップ 4 で指定する各サブネットからアクセスできる必要があります。これらのサーバーは AWS、指定されたサブネットと DNS サーバーの IP アドレスの間にネットワーク接続がある限り、の外部に配置できます。

[Service account username] (サービスアカウントのユーザー名)

既存のディレクトリのユーザーのユーザー名。このアカウントの詳細については、「[AD Connector の前提条件](#)」を参照してください。

[Service account password] (サービスアカウントのパスワード)

既存のユーザーアカウントのパスワード。このパスワードは大文字と小文字が区別され、8文字以上 128 文字以下の長さにする必要があります。また、次の 4 つのカテゴリうち 3 つから少なくとも 1 文字を含める必要があります。

- 小文字 (a～z)
- 大文字 A～Z
- 数字 (0～9)
- アルファベットと数字以外の文字 (~!@#\$%^&* _+=`|\(){}[];:'"<>.,?/)

[Confirm password] (パスワードを確認)

既存のユーザーアカウントのパスワードを再入力します。

6. [Review & create] (確認と作成) ページでディレクトリ情報を確認し、必要に応じて変更を加えます。情報が正しい場合は、[Create directory] (ディレクトリの作成) を選択します。ディレクトリが作成されるまで、数分かかります。作成が完了すると、[Status] (ステータス) 値が [Active] (アクティブ) に変わります。

AD Connector で作成される内容の詳細については、「[AD Connector で作成されるもの](#)」を参照してください。

AD Connector で作成されるもの

AD Connector を作成すると、は Elastic Network Interface (ENI) AWS Directory Service を自動的に作成し、各 AD Connector インスタンスに関連付けます。これらの各 ENIs は VPC と AWS Directory Service AD Connector 間の接続に不可欠であり、削除しないでください。で使用するために予約されているすべてのネットワークインターフェイスは、「ディレクトリ directory-id 用にAWS 作成されたネットワークインターフェイス」という説明 AWS Directory Service で識別できます。詳細については、Amazon EC2 ユーザーガイドの「[Elastic Network Interface](#)」を参照してください。

Note

AD Connector インスタンスは、デフォルトでリージョン内の 2 つのアベイラビリティゾーンにデプロイされ、Amazon Virtual Private Cloud (VPC) に接続されます。失敗した AD Connector インスタンスは、同じ IP アドレスを使用して同じアベイラビリティゾーンで自動的に置き換えられます。

AD Connector (AWS IAM Identity Center 付属) と統合された AWS アプリケーションまたはサービスにサインインすると、アプリケーションまたはサービスは認証リクエストを AD Connector に転送し、AD Connector はセルフマネージド Active Directory のドメインコントローラーに認証のためにリクエストを転送します。自己管理型 AD への認証が成功すると、Active Directory AD Connector はアプリケーションまたはサービスに認証トークンを返します (Kerberos トークンと同様)。この時点で、AWS アプリまたはサービスにアクセスできるようになりました。

AD Connector のベストプラクティス

問題を回避し、AD Connector を最大限に活用するために考慮すべき推奨事項とガイドラインを次に示します。

セットアップ: 前提条件

ディレクトリを作成する前に、これらのガイドラインを考慮してください。

ディレクトリタイプが正しいことを確認する

AWS Directory Service には、他の AWS のサービス Microsoft Active Directory で使用する複数の方法があります。予算に合わせたコストで必要な機能を備えた、ディレクトリサービスを次のように選択できます。

- AWS Directory Service for Microsoft Active Directory は、AWS クラウド上で Microsoft Active Directory ホストされる機能豊富なマネージド型です。AWS マネージド Microsoft AD は、5,000 人を超えるユーザーがあり、ホストディレクトリとオンプレミスディレクトリのために AWS 信頼関係を設定する必要がある場合に最適です。
- AD Connector は、既存のオンプレミスをに接続するだけです Active Directory AWS。AD Connector は、AWS のサービスで既存のオンプレミスのディレクトリを使用する場合に最適な選択です。
- Simple AD は、基本的な Active Directory 互換性を持つ低スケール、低コストのディレクトリです。5,000 人以下のユーザー、Samba 4 互換アプリケーション、LDAP 対応アプリケーションの LDAP 互換性をサポートします。

AWS Directory Service オプションの詳細については、「」を参照してください [オプションの選択](#)。

VPC とインスタンスが正しく設定されていることを確認する

ディレクトリに接続して、管理および使用するためには、ディレクトリが関連付けられている VPC を適切に設定する必要があります。VPC セキュリティおよびネットワーク要件の詳細については、「[AWS Managed Microsoft AD を作成するための前提条件](#)」、「[AD Connector の前提条件](#)」、「[Simple AD の前提条件](#)」のいずれかを参照してください。

ドメインにインスタンスを追加する場合は、「[Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法](#)」に説明されているように、インスタンスへの接続およびリモートアクセスがあることを確認します。

制限を理解する

特定のディレクトリタイプのさまざまな制限について説明します。ディレクトリに保存できるオブジェクトの数については、使用可能なストレージとオブジェクトの集約サイズのみに制限があります。選択したディレクトリに関する詳細については、「[AWS Managed Microsoft AD のクォータ](#)」、「[AD Connector クォータ](#)」、「[Simple AD のクォータ](#)」のいずれかを参照してください。

ディレクトリ AWS のセキュリティグループ設定を理解し、 を使用する

AWS は[セキュリティグループ](#)を作成し、ピア接続またはサイズ変更された VPC 内からアクセスできるディレクトリの [Elastic Network Interface](#) にアタッチします。は、ディレクトリへの不要なトラフィックをブロックし、必要なトラフィックを許可するようにセキュリティグループ AWS を設定します。 [VPCs](#)

ディレクトリのセキュリティグループを変更する

ディレクトリのセキュリティグループのセキュリティは、必要に応じて変更することができます。このような変更を行うのは、セキュリティグループのフィルタリング機能を完全に理解している場合に限りです。詳細については、「Amazon EC2 ユーザーガイド」の「[Amazon EC2 security groups for Linux instances](#)」(Linux インスタンス用の Amazon EC2 セキュリティグループ) を参照してください。不適切な変更を行うと、目的のコンピュータやインスタンスとの通信が失われる可能性があります。ディレクトリのセキュリティが低下するため、ディレクトリへの追加のポートを開こうとしない AWS ことをお勧めします。「[AWS 責任共有モデル](#)」をよくお読みください。

Warning

技術的には、ディレクトリのセキュリティグループを作成した他の EC2 インスタンスに関連付けることができます。ただし、はこのプラクティスに反対 AWS することをお勧めします。AWS には、マネージドディレクトリの機能またはセキュリティのニーズに対応するた

めに、予告なしにセキュリティグループを変更する理由がある場合があります。このような変更は、ディレクトリのセキュリティグループを関連付けるすべてのインスタンスに影響を及ぼすため、関連付けられたインスタンスのオペレーションが中断する場合があります。さらに、ディレクトリのセキュリティグループを EC2 インスタンスに関連付けると、EC2 インスタンスのセキュリティリスクが生じる可能性があります。

AD Connector を使用するときのオンプレミスのサイトとサブネットを正しく設定する

オンプレミスのネットワークに Active Directory のサイトが定義されている場合、AD Connector が存在する VPC 内のサブネットが Active Directory のサイトで定義されていること、および VPC 内のサブネットとその他のサイトのサブネットの間に競合が存在しないことを確認する必要があります。

ドメインコントローラーを検出するために、AD Connector はサブネット IP アドレス範囲が AD Connector を含む VPC 内の IP アドレス範囲に近い Active Directory のサイトを使用します。VPC 内の IP アドレス範囲と同じ IP アドレス範囲のサブネットを持つサイトがある場合、AD Connector はそのサイトのドメインコントローラーを検出します。これは物理的にユーザーのリージョンに近くない可能性があります。

AWS アプリケーションのユーザー名制限を理解する

AWS Directory Service では、ユーザー名の構築に使用できるほとんどの文字形式がサポートされています。ただし、WorkSpaces、WorkDocs、Amazon WorkMail、QuickSight などの AWS アプリケーションへのサインインに使用されるユーザー名には、文字制限が適用されます。これらの制限により、以下の文字は使用できません。

- スペース
- マルチバイト文字
- !"#\$%&'()*+,-./:;<=>?@[^\`{}~

Note

@ 記号は、UPN サフィックスが後に続く場合に限り、使用できます。

アプリケーションをプログラミングする

アプリケーションをプログラミングする前に、以下の点を考慮してください。

本番稼働用環境にロールアウトする前の負荷テスト

本番稼働用環境のワークロードを表すアプリケーションとリクエストを使用してラボテストを行い、ディレクトリがアプリケーションの負荷に合わせてスケーリングされることを確認します。追加のキャパシティーが必要な場合は、複数の AD Connector ディレクトリに負荷を分散します。

ディレクトリを使用する

ここでは、ディレクトリを使用する場合に、留意すべき推奨事項をいくつか示します。

管理者の認証情報を定期的にローテーションする

AD Connector サービスアカウントの管理者パスワードは定期的に変更し、パスワードが既存の Active Directory パスワードポリシーに準拠していることを確認します。サービスアカウントのパスワードを変更する手順については、「[での AD Connector サービスアカウントの認証情報の更新 AWS Management Console](#)」を参照してください。

各ドメインの一意の AD Connector を使用する

AD Connector とオンプレミスの AD ドメインには 1 対 1 の関係があります。つまり、オンプレミスのドメインごとに (認証対象の AD フォレスト内の子ドメインを含む)、一意の AD Connector を作成する必要があります。作成する各 AD Connector は、同じディレクトリに接続されていても、別のサービスアカウントを使用する必要があります。

互換性を確認する

AD Connector を使用する場合は、オンプレミスディレクトリが AWS Directory Service と互換性があり、引き続き互換性があることを確認する必要があります。お客様の責任の詳細については、「[責任共有モデル](#)」を参照してください。

AD Connector ディレクトリを維持する

を使用して AD Connector AWS Management Console を維持し、day-to-day 管理タスクを完了できます。ディレクトリを維持する方法は次のとおりです:

- 「[AD Connector に関する詳細情報を表示する](#)」。
- 「[AD Connector の DNS アドレスを更新する](#)」(その指定先)。
- 不要になる場合に、「[AD Connector を削除する](#)」。

AD Connector ディレクトリ情報の表示

で詳細なディレクトリ情報を表示するには AWS Management Console

1. 「[AWS Directory Service コンソール](#)」のナビゲーションペインで、[Active Directory] の下の [ディレクトリ] を選択します。
2. ディレクトリのディレクトリ ID リンクを選択します。ディレクトリに関する情報は、[Directory details] (ディレクトリの詳細) ページに表示されます。

[Status] (ステータス) フィールドの詳細については、「[ディレクトリのステータスを把握する](#)」を参照してください。

AD Connector の DNS アドレスを更新する

AD Connector が指している DNS アドレスを更新するには、次の手順を実行します。

Note

更新が進行中の場合は、この更新が完了してから別の更新を行う必要があります。
AD Connector で WorkSpaces を使用している場合は、WorkSpace の DNS アドレスも更新されていることを確認してください。詳細については、「[Amazon WorkSpaces の DNS サーバーの更新](#)」を参照してください。

AD Connector の DNS 設定を更新するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインの [Active Directory] で、[Directories] を選択します。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [ディレクトリの詳細] ページで、[ネットワークとセキュリティ] タブを選択します。
4. [既存の DNS 設定] セクションで [更新] をクリックします。
5. [Update existing DNS addresses] (既存の DNS アドレスの更新) ダイアログで、更新された DNS IP アドレスを入力し、[Update] (更新) をクリックします。

AD Connector のトラブルシューティングの詳細については、「[AD Connector のトラブルシューティング](#)」を参照してください。

AD Connector を削除する

AD Connector を削除してもオンプレミスのディレクトリはそのまま残ります。ディレクトリに結合されているインスタンスもすべてそのまま残り、オンプレミスのディレクトリに結合された状態のまま変わりません。引き続き、ディレクトリの認証情報を使用して、このインスタンスにログインできます。

AD Connector を削除するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。AD Connector がデプロイ AWS リージョン されている いることを確認します。詳細については、「[リージョンの選択](#)」を参照してください。
2. 削除する AD Connector に対して AWS アプリケーションが有効になっていないことを確認します。AWS アプリケーションを有効にすると、AD Connector を削除できなくなります。
 - a. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
 - b. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。AWS アプリケーションとサービスセクションには、AD Connector で有効になっている AWS アプリケーションが表示されます。
 - AWS Management Console アクセスを無効にします。詳細については、「[AWS Management Console アクセスの無効化](#)」を参照してください。
 - Amazon WorkSpaces を無効にするには、WorkSpaces コンソールでディレクトリからサービスを登録解除する必要があります。詳細については、Amazon WorkSpaces 管理ガイドの「[ディレクトリの削除](#)」を参照してください。
 - WorkDocs を無効にするには、WorkDocs コンソールで WorkDocs サイトを削除する必要があります。詳細については、「Amazon WorkDocs Administration Guide」(Amazon WorkDocs 管理ガイド) の「[Delete a site](#)」(サイトを削除する) を参照してください。
 - Amazon WorkMail を無効にするには、Amazon WorkMail コンソールで Amazon WorkMail 組織を削除する必要があります。詳細については、「Amazon WorkMail Administrator Guide」(Amazon WorkMail 管理者ガイド) の「[Remove an organization](#)」(組織を削除する) を参照してください。
 - Amazon FSx for Windows File Server を無効にするには、ドメインから Amazon FSx ファイルシステムを削除する必要があります。詳細については、「Amazon FSx for Windows File Server User Guide」の「[Working with Active Directory in FSx for Windows File Server](#)」を参照してください。

- Amazon Relational Database Service を無効にするには、ドメインから Amazon RDS インスタンスを削除する必要があります。詳細については、「[Amazon RDS ユーザーガイド](#)」の「ドメインの DB インスタンスの管理」を参照してください。
- AWS Client VPN サービスを無効にするには、クライアント VPN エンドポイントからディレクトリサービスを削除する必要があります。詳細については、「AWS Client VPN 管理者ガイド」の「[Work with Client VPN](#)」を参照してください。
- Amazon Connect を無効にするには、Amazon Connect インスタンスを削除する必要があります。詳細については、「Amazon Connect 管理者ガイド」の「[Delete your Amazon Connect instance](#)」を参照してください。
- Amazon QuickSight を無効にするには、Amazon QuickSight のサブスクリプションを解除する必要があります。詳細については、Amazon QuickSight ユーザーガイド」の[Amazon QuickSight 「アカウントの閉鎖」](#)を参照してください。

 Note

を使用して AWS IAM Identity Center、以前に削除予定の AWS Managed Microsoft AD ディレクトリに接続したことがある場合は、削除する前に ID ソースを変更する必要があります。詳細については、「IAM Identity Center ユーザーガイド」の「[ID ソースを変更する](#)」を参照してください。

3. ナビゲーションペインで [ディレクトリ] を選択します。
4. 削除するディレクトリを選択し、[削除] をクリックします。AD Connector が削除されるまでに数分かかります。AD Connector を削除すると、ディレクトリリストからも削除されます。

AD Connector ディレクトリをセキュリティで保護する

多要素認証 (MFA)、Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) を介したクライアント側の Lightweight Directory Access Protocol、AD Connector AWS Private Certificate Authority のセキュリティ保護などの機能を使用できます。AD Connector を保護する方法は次のとおりです:

- MFA を有効にすると、AD Connector のセキュリティが向上します。
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS) (LDAPS) でクライアント側の Lightweight ディレクトリアクセスプロトコルを有効にすると、LDAP 経由の通信が暗号化され、セキュリティが向上します。

- スマートカードを使用して証明書に基づく相互トランスポートレイヤーセキュリティ (mTLS) 認証を有効にします。これにより、ユーザーは Active Directory と AD Connector を使用して Amazon Web Services に認証できます。
- AD Connector サービスアカウントの認証情報を更新します。
- AWS Private CA AD Connector for AD をセットアップして、AD Connector の証明書を発行および管理できるようにします。

AD Connector を保護するタスク

- [AD Connector の多要素認証を有効にする](#)
- [AD Connector を使用してクライアント側の LDAPS を有効にする](#)
- [認証にスマートカードを使用できるように、AD Connector で mTLS 認証を有効化する](#)
- [での AD Connector サービスアカウントの認証情報の更新 AWS Management Console](#)
- [AWS Private CA Connector for AD をセットアップする](#)

AD Connector の多要素認証を有効にする

オンプレミスまたは Amazon EC2 インスタンスで Active Directory を実行している場合は、AD Connector の多要素認証を有効にすることができます。での多要素認証の使用の詳細については AWS Directory Service、「」を参照してください[AD Connector の前提条件](#)。

Note

Multi-Factor Authentication は、Simple AD では使用できません。ただし、AWS Managed Microsoft AD ディレクトリに対して MFA を有効にすることができます。詳細については、「[AWS Managed Microsoft AD の多要素認証の有効化](#)」を参照してください。

AD Connector の Multi-Factor Authentication を有効にするには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. AD Connector ディレクトリのディレクトリ ID リンクをクリックします。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。

4. [Multi-factor authentication] セクションで、[Actions] (アクション)、[Enable] (有効化) の順に選択します。
5. [Enable multi-factor authentication (MFA)] (Multi-Factor-Authentication (MFA) の有効化) ページで、次の値を指定します。

[Display label] (表示ラベル)

ラベル名を指定します。

[RADIUS server DNS name or IP addresses] (RADIUS サーバーの DNS 名または IP アドレス)

RADIUS サーバーエンドポイントの IP アドレス、または、RADIUS サーバーロードバランサーの IP アドレス。カンマで区切って、複数の IP アドレスを入力できます (例えば、192.0.0.0,192.0.0.12)。

 Note

RADIUS MFA は、へのアクセス、または WorkSpaces AWS Management Console、Amazon QuickSight、Amazon Chime などの Amazon Enterprise アプリケーションやサービスへのアクセスを認証する場合にのみ適用できます。EC2 インスタンスで実行されている Windows ワークロード、または EC2 インスタンスにサインインするための MFA は提供されません。AWS Directory Service は RADIUS チャレンジ/レスポンス認証をサポートしていません。

ユーザーは、ユーザー名とパスワードを入力するときに、MFA コードを持っている必要があります。または、ユーザーの SMS テキストの検証など、MFA 帯域外を実行するソリューションを使用する必要があります。帯域外 MFA ソリューションでは、ソリューションに合わせて RADIUS タイムアウト値を適切に設定する必要があります。帯域外 MFA ソリューションを使用している場合、ユーザーはサインインページで MFA コードの入力を求められます。この場合は、ベストプラクティスとして、ユーザーはパスワードフィールドと MFA フィールドの両方に自分のパスワードを入力することをお勧めします。

[Port] (ポート)

RADIUS サーバーが通信のために使用しているポート。オンプレミスネットワークでは、AWS Directory Service サーバーからのデフォルトの RADIUS サーバーポート (UDP:1812) 経由のインバウンドトラフィックを許可する必要があります。

[Shared secret code] (共有シークレットコード)

RADIUS エンドポイントの作成時に指定された共有シークレットコード。

[Confirm shared secret code] (共有シークレットコードの確認)

RADIUS エンドポイントの共有シークレットコードを確認します。

[Protocol] (プロトコル)

RADIUS エンドポイントの作成時に指定されたプロトコルを選択します。

[Server timeout (in seconds)] (サーバータイムアウト (秒単位))

RADIUS サーバーのレスポンスを待つ時間 (秒)。これは 1～50 の範囲の値にする必要があります。

[Max RADIUS request retries] (RADIUS リクエストの最大再試行数)

RADIUS サーバーとの通信を試みる回数。これは 0～10 の範囲の値にする必要があります。

Multi-Factor Authentication は、[RADIUS Status] (RADIUS 状態) が [Enabled] (有効) に変わると使用できます。

6. [Enable] (有効化) を選択します。

AD Connector を使用してクライアント側の LDAPS を有効にする

AD Connector でのクライアント側の LDAPS サポートは、Microsoft Active Directory (AD) と AWS アプリケーション間の通信を暗号化します。このようなアプリケーションの例には、WorkSpaces、AWS IAM Identity Center、QuickSight、Amazon Chime などがあります。この暗号化は、組織の ID データをより適切に保護し、セキュリティ要件を満たすのに役立ちます。

クライアント側の LDAPS の登録を解除したり、無効にしたりすることもできます。

トピック

- [前提条件](#)
- [クライアント側の LDAPS の有効化](#)
- [クライアント側の LDAPS を管理する](#)

前提条件

クライアント側 LDAPS を有効にする前に、次の要件を満たす必要があります。

前提条件:

- [Active Directory にサーバー証明書をデプロイする](#)
- [CA 証明書の要件](#)
- [ネットワーク要件](#)

Active Directory にサーバー証明書をデプロイする

クライアント側の LDAPS を有効にするには、Active Directory 内のドメインコントローラーごとに、サーバー証明書を取得しインストールする必要があります。これらの証明書は、LDAP サービスが LDAP クライアントからの SSL 接続をリッスンして自動的に承認するために使用されます。SSL 証明書は、社内の Active Directory 証明書サービス (ADCS) のデプロイから発行されたもの、または商用発行者から購入したものを使用できます。Active Directory サーバー証明書の要件の詳細については、Microsoft のウェブサイト「[LDAP over SSL \(LDAPS\) Certificate](#)」(LDAP over SSL (LDAPS) 証明書) を参照してください。

CA 証明書の要件

クライアント側 LDAPS のオペレーションには、サーバー証明書の発行元を表す認証機関 (CA) 証明書が必要です。LDAP 通信を暗号化するために、CA 証明書は、Active Directory のドメインコントローラーから提示されるサーバー証明書と照合されます。次の CA 証明書の要件に注意してください。

- 証明書を登録するには、有効期限までに 90 日超の期間があることが必要です。
- 証明書は、プライバシー強化メール (PEM) 形式である必要があります。Active Directory 内から CA 証明書をエクスポートする場合は、そのファイル形式として Base64 でエンコードされた X.509 (.CER) を選択します。
- AD Connector ディレクトリごとに最大 5 個の CA 証明書を保存できます。
- RSASSA-PSS 署名アルゴリズムを使用する証明書はサポートされていません。

ネットワーク要件

AWS アプリケーション LDAP トラフィックは TCP ポート 636 でのみ実行され、LDAP ポート 389 へのフォールバックはありません。ただし、レプリケーション、信頼などをサポートする Windows

LDAP 通信は、Windows ネイティブセキュリティを備えた LDAP ポート 389 を引き続き使用します。AD Connector (アウトバウンド) とセルフマネージド Active Directory (インバウンド) のポート 636 で TCP 通信を許可するように AWS セキュリティグループとネットワークファイアウォールを設定します。

クライアント側の LDAPS の有効化

クライアント側 LDAPS を有効にするには、認証機関 (CA) 証明書を AD Connector にインポートし、ディレクトリで LDAPS を有効にします。有効にすると、AWS アプリケーションとセルフマネージド Active Directory 間のすべての LDAP トラフィックが Secure Sockets Layer (SSL) チャンネル暗号化で流れます。

2 つの異なる方法を使用して、ディレクトリのクライアント側 LDAPS を有効にできます。AWS Management Console メソッドまたは AWS CLI メソッドを使用できます。

AWS Directory Serviceで証明書を登録する

証明書を登録するには、次のいずれかの方法を使用します AWS Directory Service。

方法 1: 証明書を AWS Directory Service (AWS Management Console) に登録するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションで、[Actions] (アクション) メニューを選択してから、[Register certificate] (証明書の登録) を選択します。
5. [Register a CA certificate] (CA 証明書を登録する) ダイアログボックスで [Browse] (参照) をクリックしてから、証明書を選択し、[Open] (開く) をクリックします。
6. [Register certificate] (証明書の登録) を選択します。

方法 2: 証明書を AWS Directory Service (AWS CLI) に登録するには

- 以下のコマンドを実行してください。証明書データについては、CA 証明書ファイルの場所を指定します。証明書 ID がレスポンスとして提供されます。

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

登録のステータスを確認する

証明書登録のステータスまたは登録済み証明書のリストを表示するには、次のいずれかの方法を使用します。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の登録ステータスを確認するには

1. [Directory details] (ディレクトリの詳細) ページの [Client-side LDAPS] (クライアント側 LDAPS) セクションに移動します。
2. [Registration status] (登録ステータス) 列に表示される現在の証明書登録状態を確認します。登録ステータスの値が [Registered] (登録済み) に変わると、証明書は正常に登録されています。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の登録ステータスを確認するには

- 次のコマンドを実行します。ステータス値として Registered が返される場合、証明書は正常に登録されています。

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

クライアント側の LDAPS を有効にする

でクライアント側の LDAPS を有効にするには、次のいずれかの方法を使用します AWS Directory Service。

Note

クライアント側 LDAPS を有効にするには、1 つ以上の証明書が正常に登録されている必要があります。

方法 1: AWS Directory Service (AWS Management Console) でクライアント側の LDAPS を有効にするには

1. [Directory details] (ディレクトリの詳細) ページの [Client-side LDAPS] (クライアント側 LDAPS) セクションに移動します。
2. [Enable] (有効化) を選択します。このオプションを使用できない場合は、有効な証明書が正常に登録されていることを確認してから、もう一度やり直してください。
3. [Enable client-side LDAPS] (クライアント側 LDAPS を有効にする) ダイアログボックスで、[Enable] (有効化) を選択します。

方法 2: AWS Directory Service (AWS CLI) でクライアント側の LDAPS を有効にするには

- 以下のコマンドを実行してください。

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

LDAPS ステータスを確認する

LDAPS ステータスを確認するには、次のいずれかの方法を使用します AWS Directory Service。

方法 1: LDAPS ステータスを確認するには AWS Directory Service (AWS Management Console)

1. [Directory details] (ディレクトリの詳細) ページの [Client-side LDAPS] (クライアント側 LDAPS) セクションに移動します。
2. ステータス値が [Enabled] (有効) と表示されている場合、LDAPS は正常に設定されています。

方法 2: LDAPS ステータスを確認するには AWS Directory Service (AWS CLI)

- 以下のコマンドを実行してください。ステータス値として Enabled が返される場合、LDAPS は正常に設定されています。

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

クライアント側の LDAPS 証明書の表示、LDAPS 証明書の登録解除または無効化の詳細については、「[クライアント側の LDAPS を管理する](#)」を参照してください。

クライアント側の LDAPS を管理する

LDAPS 設定を管理するには、以下のコマンドを使用します。

2 つの異なる方法を使用して、クライアント側 LDAPS 設定を管理できます。AWS Management Console メソッドまたは AWS CLI メソッドを使用できます。

証明書の詳細を表示する

以下のいずれかの方法を使用して、証明書の有効期限を確認します。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の詳細を表示するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションの [CA certificates] (CA 証明書) に、証明書に関する情報が表示されます。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の詳細を表示するには

- 以下のコマンドを実行してください。証明書 ID として、register-certificate または list-certificates から返される識別子を使用します。

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

証明書の登録解除

以下のいずれかの方法を使用して、証明書を登録解除します。

Note

登録されている証明書が 1 つのみの場合は、証明書を登録解除する前に、まず LDAPS を無効にする必要があります。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の登録を解除するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションで、[Actions] (アクション) を選択してから、[Deregister certificate] (証明書の登録解除) を選択します。
5. [Deregister a CA certificate] (CA 証明書を登録解除する) ダイアログボックスで、[Deregister] (登録解除) をクリックします。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の登録を解除するには

- 以下のコマンドを実行してください。証明書 ID として、register-certificate または list-certificates から返される識別子を使用します。

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

クライアント側 LDAPS の無効化

以下のいずれかの方法を使用して、クライアント側 LDAPS を無効にします。

方法 1: AWS Directory Service (AWS Management Console) でクライアント側の LDAPS を無効にするには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Client-side LDAPS] (クライアント側 LDAPS) セクションで、[Disable] (無効化) を選択します。
5. [Disable client-side LDAPS] (クライアント側 LDAPS を無効にする) ダイアログボックスで、[Disable] (無効化) をクリックします。

方法 2: AWS Directory Service (AWS CLI) でクライアント側の LDAPS を無効にするには

- 以下のコマンドを実行してください。

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

認証にスマートカードを使用できるように、AD Connector で mTLS 認証を有効化する

証明書ベースの相互 Transport Layer Security (mTLS) 認証にスマートカードを使用して、自己管理型 Active Directory (AD) および AD Connector を介して Amazon WorkSpaces へのユーザー認証を行います。有効にすると、ユーザーは WorkSpaces ログイン画面でスマートカードを選択し、ユーザーネームとパスワードを使用する代わりに PIN を入力して認証します。そこから、Windows または Linux 仮想デスクトップがスマートカードを使用して、ネイティブデスクトップ OS から AD への認証を行います。

Note

AD Connector のスマートカード認証は、次の AWS リージョンの WorkSpaces でのみ使用できます。現時点では、他の AWS アプリケーションはサポートされていません。

- 米国東部 (バージニア北部)
- 米国西部 (オレゴン)
- アジアパシフィック (シドニー)
- アジアパシフィック (東京)
- 欧州 (アイルランド)
- AWS GovCloud (米国西部)
- AWS GovCloud (米国東部)

証明書の登録を解除したり、無効にしたりすることもできます。

トピック

- [前提条件](#)
- [スマートカード認証を有効にしている](#)

- [スマートカード認証の設定を管理する](#)

前提条件

Amazon WorkSpaces クライアントでスマートカードを使用した相互トランスポートレイヤーセキュリティ (mTLS) 認証を有効にするには、自己管理型 Active Directory と統合された運用上のスマートカードインフラストラクチャが必要です。Amazon WorkSpaces と Active Directory でスマートカード認証を設定する方法の詳細については、「[Amazon WorkSpaces 管理ガイド](#)」を参照してください。

WorkSpaces でスマートカード認証を有効にする前に、次の前提条件を確認してください:

- [CA 証明書の要件](#)
- [ユーザー証明書の要件](#)
- [証明書失効チェックのプロセス](#)
- [考慮事項](#)

CA 証明書の要件

AD Connector では、スマートカード認証にユーザー証明書の発行者を表す認証機関 (CA) 証明書が必要です。AD Connector は、CA 証明書をユーザーがスマートカードで提示した証明書と照合します。次の CA 証明書の要件に注意してください。

- CA 証明書を登録するには、有効期限までに 90 日超の期間があることが必要です。
- CA 証明書は、プライバシー強化メール (PEM) 形式である必要があります。Active Directory 内から CA 証明書をエクスポートする場合は、エクスポートファイル形式として Base64 でエンコードされた X.509 (.CER) を選択します。
- スマートカード認証を成功させるには、発行元 CA からユーザー証明書まで繋がるすべてのルートおよび中間 CA 証明書をアップロードする必要があります。
- AD Connector ディレクトリごとに最大 100 個の CA 証明書を保存できます。
- AD Connector は、CA 証明書の RSASSA-PSS 署名アルゴリズムをサポートしていません。
- Certificate Propagation サービスが自動的に設定され、実行されていることを確認します。

ユーザー証明書の要件

ユーザー証明書の要件の一部が以下に示されます:

- ユーザーのスマートカード証明書には、ユーザーの userPrincipalName (UPN) のサブジェクト代替名 (SAN) があります。
- ユーザーのスマートカード証明書には、スマートカードログオン (1.3.6.1.4.1.311.20.2.2) クライアント認証 (1.3.6.1.5.5.7.3.2) として拡張キーの使用法があります。
- ユーザーのスマートカード証明書のオンライン証明書ステータスプロトコル (OCSP) 情報は、Authority Information Access の Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) である必要があります。

AD Connector とスマートカード認証要件の詳細については、「Amazon WorkSpaces 管理ガイド」の「[要件](#)」を参照してください。WorkSpaces への登録、パスワードのリセット、または WorkSpaces への接続などの Amazon WorkSpaces 問題のトラブルシューティングへのサポートについては、「Amazon WorkSpaces ユーザーガイド」の「[Troubleshoot WorkSpaces client issues](#)」を参照してください。

証明書失効チェックのプロセス

スマートカード認証を実行するには、AD Connector がオンライン証明書ステータスプロトコル (OCSP) を使用してユーザー証明書の失効ステータスをチェックする必要があります。証明書失効チェックを実行するには、OCSP レスポンダー URL がインターネットでアクセス可能である必要があります。DNS 名を使用する場合、OCSP レスポンダー URL は、「[Internet Assigned Numbers Authority \(IANA\) Root Zone Database](#)」(Internet Assigned Numbers Authority (IANA) のルートゾーンデータベース) にある最上位ドメインである必要があります。

AD Connector 証明書失効チェックでは、次のプロセスが使用されます。

- AD Connector は、OCSP レスポンダー URL のユーザー証明書の機関情報アクセス (AIA) の拡張機能を確認する必要があります。その後、AD Connector は URL を使用して失効をチェックします。
- AD Connector がユーザー証明書の AIA 拡張機能で見つかった URL を解決できない場合、またはユーザー証明書で OCSP レスポンダー URL が見つからない場合、AD Connector は、ルート CA 証明書の登録時に提供されるオプションの OCSP URL を使用します。

ユーザー証明書の AIA 拡張機能の URL が解決しても応答しない場合、ユーザー認証は失敗します。

- ルート CA 証明書の登録中に提供された OCSP レスポンダー URL が解決できない、応答しない、または OCSP レスポンダー URL が指定されていない場合、ユーザー認証は失敗します。

- OCSP サーバーは [RFC 6960](#) に準拠する必要があります。さらに、OCSP サーバーは、合計 255 バイト以下のリクエストに対して GET 方法を使用したリクエストをサポートする必要があります。

 Note

AD Connector には OCSP レスポンダー URL の HTTP URL が必要です。

考慮事項

AD Connector でスマートカード認証を有効にする前に、次の項目を考慮してください。

- AD Connector は、証明書ベースの相互 Transport Layer Security 認証 (相互 TLS) を使用して、ハードウェアまたはソフトウェアベースのスマートカード証明書を使用した Active Directory へのユーザー認証を行います。現在、共通アクセスカード (CAC) および個人識別検証 (PIV) カードのみがサポートされています。他のタイプのハードウェアベースまたはソフトウェアベースのスマートカードも機能する可能性があります。WorkSpaces Streaming Protocol での使用はテストされていません。
- スマートカード認証は、WorkSpaces へのユーザーネームとパスワードによる認証に代わるものです。

スマートカード認証が有効になっている他の AWS アプリケーションが AD Connector ディレクトリに設定されている場合でも、それらのアプリケーションにはユーザー名とパスワードの入力画面が表示されます。

- スマートカード認証を有効にすると、ユーザーセッション期間が Kerberos サービスチケットの最大有効期間に制限されます。この設定はグループポリシーを使用して設定でき、デフォルトで 10 時間に設定されています。この設定の詳細については、[Microsoft のドキュメント](#)を参照してください。
- AD Connector サービスアカウントでサポートされる Kerberos 暗号化タイプは、各ドメインコントローラーでサポートされる Kerberos 暗号化タイプと一致する必要があります。

スマートカード認証を有効にしている

AD Connector で WorkSpaces のスマートカード認証を有効にするには、まず認証局 (CA) 証明書を AD Connector にインポートする必要があります。CA 証明書は、AWS Directory Service コンソー

ル、[API](#)、または [CLI](#) を使用して AD Connector にインポートできます。以下の手順を使用して CA 証明書をインポートし、その後スマートカード認証を有効にします。

ステップ

- [AD Connector サービスアカウントの Kerberos 制約付き委任を有効にします](#)
- [AD Connector に CA 証明書を登録します](#)
- [サポートされている AWS アプリケーションとサービスのスマートカード認証を有効にします](#)

AD Connector サービスアカウントの Kerberos 制約付き委任を有効にします

AD Connector でスマートカード認証を使用するには、AD Connector サービスアカウントの Kerberos の制約付き委任 (KCD) を自己管理型 AD ディレクトリ内の LDAP サービスに対して有効にする必要があります。

Kerberos の制約付き委任は、Windows Server の機能の 1 つです。この機能を使用すると、管理者は、アプリケーションサービスがユーザーに代わって動作できる範囲を制限することで、アプリケーションの信頼境界を指定して適用できます。詳細については、「[Kerberos の制約付き委任](#)」を参照してください。

Note

Kerberos の制約付き委任 (KCD) では、AD Connector サービスアカウントのユーザー名部分が、同じユーザーの sAMAccountName と一致している必要があります。sAMAccountName は 20 文字に制限されています。sAMAccountName は Microsoft Active Directory 属性で、以前のバージョンの Windows クライアントおよびサーバーのサインイン名として使用されてきました。

1. SetSpn コマンドを使用して、自己管理型 AD の AD Connector サービスアカウントのサービスプリンシパル名 (SPN) を設定します。これにより、サービスアカウントを委任設定に使用できるようになります。

SPN には、任意のサービスまたは名前の組み合わせを指定できますが、既存の SPN と重複しているものは指定できません。-s で、重複がないかチェックされます。

```
setspn -s my/spn service_account
```

2. [AD Users and Computers] で、コンテキスト (右クリック) メニューを開き、AD Connector サービスアカウントを選択して、[Properties] を選択します。
3. [Delegation] (委任) タブを選択します。
4. [Trust this user for delegation to specified service only] と [Use any authentication protocol] オプションを選択します。
5. [Add] (追加) を選択し、[Users or Computers] (ユーザーまたはコンピュータ) を選択して、ドメインコントローラーを見つけます。
6. [OK] をクリックして、委任に使用できるサービスのリストを表示します。
7. ldap サービスタイプを選択して、[OK] を選択します。
8. もう一度 OK を選択して、設定を保存します。
9. Active Directory 内の他のドメインコントローラーでこのプロセスを繰り返します。または、PowerShell を使用してこのプロセスを自動化することもできます。

AD Connector に CA 証明書を登録します

以下のいずれかの方法を使用して、AD Connector ディレクトリの CA 証明書を登録します。

方法 1: AD Connector で CA 証明書を登録するには (AWS Management Console)

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Smart card authentication] セクションで、[Actions] メニューをクリックし、[Register certificate] を選択します。
5. [Register a certificate] ダイアログボックスで [Choose file] をクリックして、証明書を選択し、[Open] をクリックします。オプションで、オンライン証明書ステータスプロトコル (OCSP) レスポンダー URL を指定して、この証明書の失効チェックを実行することもできます。OCSP の詳細については、「[証明書失効チェックのプロセス](#)」を参照してください。
6. [Register certificate] (証明書の登録) を選択します。証明書のステータスが [Registered] (登録済み) に変わったら、登録プロセスは正常に完了しています。

方法 2: AD Connector で CA 証明書を登録するには (AWS CLI)

- 次のコマンドを実行します。証明書データについては、CA 証明書ファイルの場所を指定します。セカンダリ OCSP レスポンダーアドレスを指定するには、オプションの ClientCertAuthSettings オブジェクトを使用します。

```
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
```

成功すると、証明書 ID が返されます。次の CLI コマンドを実行して、CA 証明書が正常に登録されていることを検証することもできます。

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

ステータス値として Registered が返される場合、証明書は正常に登録されています。

サポートされている AWS アプリケーションとサービスのスマートカード認証を有効にします

以下のいずれかの方法を使用して、AD Connector ディレクトリの CA 証明書を登録します。

方法 1: AD Connector でスマートカード認証を有効にするには (AWS Management Console)

- [Directory details] ページの [Smart card authentication] セクションで、[Enable] をクリックします。このオプションを使用できない場合は、有効な証明書が正常に登録されていることを確認してから、もう一度やり直してください。
- [Enable smart card authentication] (スマートカード認証を有効にする) ダイアログボックスで、[Enable] (有効化) をクリックします。

方法 2: AD Connector でスマートカード認証を有効にするには (AWS CLI)

- 次のコマンドを実行します。

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

成功すると、AD Connector は HTTP 本文が空の HTTP 200 レスポンスを返します。

証明書の表示、証明書の登録解除または証明書の無効化の詳細については、「[スマートカード認証の設定を管理する](#)」を参照してください。

スマートカード認証の設定を管理する

2つの異なる方法を使用して、スマートカード認証の設定を管理できます。AWS Management Console メソッドまたは AWS CLI メソッドを使用できます。

トピック

- [証明書の詳細を表示する](#)
- [証明書の登録解除](#)
- [スマートカード認証を無効にする](#)

証明書の詳細を表示する

以下のいずれかの方法を使用して、証明書の有効期限を確認します。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の詳細を表示するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. AD Connector ディレクトリのディレクトリ ID リンクをクリックします。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Smart card authentication] (スマートカード認証) セクションの [CA certificates] (CA 証明書) で、証明書 ID を選択し、その証明書に関する詳細を表示します。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の詳細を表示するには

- 以下のコマンドを実行してください。証明書 ID として、register-certificate または list-certificates から返される識別子を使用します。

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

証明書登録解除

以下のいずれかの方法を使用して、証明書を登録解除します。

Note

登録されている証明書が 1 つのみの場合は、証明書を登録解除する前に、まずスマートカード認証を無効にする必要があります。

方法 1: (AWS Directory ServiceAWS Management Console) で証明書の登録を解除するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. AD Connector ディレクトリのディレクトリ ID リンクをクリックします。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Smart card authentication] (スマートカード認証) セクションの [CA certificates] (CA 証明書) で、登録解除する証明書を選択して [Actions] (アクション) をクリックし、[Deregister certificate] (証明書の登録解除) をクリックします。

Important

登録解除しようとしている証明書がアクティブではなく、スマートカード認証の CA 証明書チェーンの一部として現在使用されていないことを確認してください。

5. [Deregister a CA certificate] (CA 証明書を登録解除する) ダイアログボックスで、[Deregister] (登録解除) をクリックします。

方法 2: (AWS Directory ServiceAWS CLI) で証明書の登録を解除するには

- 以下のコマンドを実行してください。証明書 ID として、register-certificate または list-certificates から返される識別子を使用します。

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

スマートカード認証を無効にする

スマートカード認証を無効にするには、以下のいずれかの方法を使用します。

方法 1: AWS Directory Service (AWS Management Console) でスマートカード認証を無効にするには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. AD Connector ディレクトリのディレクトリ ID リンクをクリックします。
3. [Directory details] (ディレクトリの詳細) ページで、[Networking & security] (ネットワークとセキュリティ) タブを選択します。
4. [Smart card authentication] (スマートカード認証) セクションで、[Disable] (無効化) をクリックします。
5. [Disable smart card authentication] (スマートカード認証を無効にする) ダイアログボックスで、[Disable] (無効化) をクリックします。

方法 2: AWS Directory Service (AWS CLI) でスマートカード認証を無効にするには

- 以下のコマンドを実行してください。

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

での AD Connector サービスアカウントの認証情報の更新 AWS Management Console

で指定する AD Connector 認証情報は、既存のオンプレミスディレクトリへのアクセスに使用されるサービスアカウント AWS Directory Service を表します。でサービスアカウントの認証情報を変更するには AWS Directory Service、次の手順を実行します。

Note

ディレクトリに対して が有効になっている場合 AWS IAM Identity Center は、サービスプリンシパル名 (SPN) を現在のサービスアカウントから新しいサービスアカウントに転送 AWS Directory Service する必要があります。現在のサービスアカウントに SPN を削除するアクセ

ス許可がない場合、または新しいサービスアカウントに SPN を追加するアクセス許可がない場合は、両方のアクションを実行するアクセス許可が付与されたディレクトリアカウントの認証情報の入力を求められます。これらの認証情報は、SPN を転送する目的でのみ使用され、サービスで保存されることはありません。

で AD Connector サービスアカウントの認証情報を更新するには AWS Directory Service

1. [AWS Directory Service コンソール](#) のナビゲーションペインの [Active Directory] で、[Directories] を選択します。
2. ディレクトリのディレクトリ ID リンクを選択します。
3. [ディレクトリの詳細] ページで [サービスアカウント認証情報] セクションまでスクロールします。
4. [Service account credentials] (サービスアカウントの認証情報) セクションで、[Update] (更新) を選択します。
5. [サービスアカウント認証情報の更新] ダイアログボックスでサービスアカウントのユーザー名とパスワードを入力します。パスワードを再入力して確認し、[更新] を選択します。

AWS Private CA Connector for AD をセットアップする

AD Connector AWS Private Certificate Authority を使用してセルフマネージド Active Directoryをと統合し、AD ドメインに参加しているユーザー、グループ、マシンの証明書を発行および管理できます。AWS Private CA Connector for AD は、ローカルエージェントまたはプロキシサーバーのデプロイ、パッチ適用、更新を必要とせずに、セルフマネージド型エンタープライズ CAs のドロップイン代替 AWS Private CA としてフルマネージド型を提供します。

この統合 AWS Directory Service は、コンソール、AWS Private CA Connector for AD コンソール、または [CreateTemplate](#) API を呼び出すことで設定できます。AWS Private CA Connector for Active Directoryコンソールを使用するには、[AWS Private CA 「Connector for Active Directory」](#) を参照してください。以下のセクションでは、コンソールから AWS Directory Service この統合を設定する方法について説明します。

前提条件

セットアップ手順については、[「Connector for AD ユーザーガイド」の「Set up AWS Private CA Connector for AD」](#) を参照してください。

AWS Private CA Connector for AD を設定する

1. にサインイン AWS Management Console し、 で AWS Directory Service コンソールを開きます <https://console.aws.amazon.com/directoryservicev2/>。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. 「アプリケーション管理」タブとAWS 「アプリケーションとサービス」セクションで、「AWS Private CA Connector for AD」を選択します。[Active Directory 用のプライベート CA 証明書の作成] ページが表示されます。コンソールの手順に従って Active Directory Connector 用のプライベート CA を作成し、ご使用のプライベート CA に登録します。詳細については、「[コネクタの作成](#)」を参照してください。
4. コネクタを作成したら、コネクタのステータスと関連するプライベート CA のステータスなど、AWS Private CA Connector for AD の詳細を表示する方法について説明します。

AWS Private CA Connector for AD を表示する

1. にサインイン AWS Management Console し、 で AWS Directory Service コンソールを開きます <https://console.aws.amazon.com/directoryservicev2/>。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. アプリケーション管理タブとAWS アプリケーションとサービスセクションで、プライベート CA コネクタと関連するプライベート CA を表示できます。デフォルトでは、以下のフィールドが表示されます。
 - a. AWS Private CA コネクタ ID — AWS Private CA コネクタの一意の識別子。これを選択すると、その AWS Private CA コネクタの詳細ページが表示されます。
 - b. AWS Private CA subject — CA の識別名に関する情報。こちらをクリックすると、その AWS Private CAの詳細ページが表示されます。
 - c. ステータス — AWS Private CA Connector と のステータスチェックに基づきます AWS Private CA。両方のチェックに合格すると、[アクティブ] と表示されます。いずれかのチェックが失敗すると、[1/2 チェック失敗] と表示されます。両方のチェックが失敗すると、[失敗] と表示されます。失敗ステータスの詳細については、ハイパーリンクにカーソルを合わせると、どのチェックが失敗したか確認できます。コンソール内の指示に従い、修正します。
 - d. 作成日 — AWS Private CA Connector が作成された日。

詳細については、「[コネクタの詳細表示](#)」を参照してください。

AD ユーザーへの証明書の発行を検証する

AWS Private CA がセルフマネージドに証明書を発行していることを確認するには、次の手順を実行しますActive Directory。

- オンプレミスドメインコントローラーを再起動します。
- Microsoft Management Console で証明書を表示します。詳細については、「[Microsoft ドキュメント](#)」を参照してください。

AD Connector ディレクトリをモニタリングする

AD Connector のさまざまなステータスと、AD Connector に対する意味について詳しく知ること
で、AD Connector を最大限に活用できます。Amazon Simple Notification Service を使用して、AD
Connector のステータスに関する通知を受信することもできます。

AD Connector をモニタリングするタスク:

- [ディレクトリのステータスを把握する](#)
- [Amazon SNS で AD Connector ディレクトリステータス通知を有効にする](#)

ディレクトリのステータスを把握する

ディレクトリのステータスには以下の種類があります。

[Active] (アクティブ)

ディレクトリは正常に動作しています。ディレクトリには AWS Directory Service が検出した問題はありません。

[Creating] (作成中)

ディレクトリは現在作成中です。ディレクトリの作成には通常 20〜45 分かかりますが、システムの負荷によって異なる場合があります。

[Deleted] (削除済み)

ディレクトリは削除されています。ディレクトリのリソースはすべて解放されています。ディレクトリがこの状態になったら、復元できません。

[Deleting] (削除中)

ディレクトリは削除中です。ディレクトリが完全に削除されるまでは、この状態です。ディレクトリがこの状態になると、削除操作を取り消すことができず、ディレクトリを回復できません。

[Failed] (失敗)

ディレクトリを作成できませんでした。このディレクトリを削除してください。問題が解決しない場合は、[AWS サポート センター](#)までお問い合わせください。

[Impaired] (障害)

ディレクトリがパフォーマンスが低下した状態で実行されています。1 つまたは複数の問題が検出され、すべてのディレクトリのオペレーションが最適に動作しているとは限りません。ディレクトリがこのステータスになるのは、さまざまな原因があり得ます。パッチ適用や EC2 インスタンスのローテーションなど通常の運用メンテナンス、いずれかのドメインコントローラーにおけるアプリケーションの一時的なホットスポットティング、あるいは、ネットワークに行った変更が意図せずディレクトリの通信を妨害するなどです。詳細については、「[AWS Managed Microsoft AD のトラブルシューティング](#)」、「[AD Connector のトラブルシューティング](#)」、「[Simple AD のトラブルシューティング](#)」のいずれかを参照してください。通常のメンテナンス関連の問題の場合、AWS は 40 分以内にこれらの問題を解決します。トラブルシューティングのトピックを確認した後も、ディレクトリの障害の状態が 40 分以上続く場合は、[AWS サポート センター](#)までお問い合わせください。

Important

ディレクトリが障害の状態あるときは、スナップショットを復元しないでください。障害の解消にスナップショットの復元が必要になることはほとんどありません。詳細については、「[スナップショットを使用した AWS Managed Microsoft AD の復元](#)」を参照してください。

[Inoperable] (操作不能)

ディレクトリが動作しません。すべてのディレクトリエンドポイントが問題を報告しています。

[Requested] (リクエスト済み)

ディレクトリの作成リクエストは現在保留中です。

Amazon SNS で AD Connector ディレクトリステータス通知を有効にする

Amazon Simple Notification Service (Amazon SNS) を使用して、ディレクトリのステータスが変更されたときに E メールまたはテキストメッセージ (SMS) を受け取ることができます。ディレクトリが Active ステータスから [Impaired \(障害\)](#) または [Inoperable \(操作不能\)](#) ステータスに変わると通知されます。ディレクトリが Active ステータスに戻ったときも通知を受け取ります。

仕組み

Amazon SNS では「トピック」を使用してメッセージを収集し、配信します。各トピックには、そのトピックに発行されたメッセージを受け取る 1 人または複数の受信者が存在します。以下のステップを使用して、Amazon SNS トピックにパブリッシャー AWS Directory Service としてを追加できます。はディレクトリのステータスの変更 AWS Directory Service を検出すると、そのトピックにメッセージを発行し、トピックのサブスクライバーに送信します。

発行者として、複数のディレクトリを単一のトピックに関連付けることができます。以前に Amazon SNS で作成したトピックに、ディレクトリステータスのメッセージを追加することもできます。トピックの発行者と受信者は詳細に管理できます。Amazon SNS の詳細については、「[Amazon SNS とは](#)」を参照してください。

ディレクトリの SNS メッセージングを有効にするには

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Maintenance] (メンテナンス) タブを選択します。
4. [Directory monitoring] (ディレクトリのモニタリング) セクションで [Actions] (アクション) をクリックし、[Create notification] (通知の作成) をクリックします。
5. [Create notification] (通知の作成) ページで、[Choose a notification type] (通知タイプを選択) をクリックしてから、[Create a new notification] (新しい通知の作成) を選択します。または、既存の SNS トピックがある場合は、[Associate with existing SNS topic] (既存の SNS トピックに関連付ける) を選択し、このディレクトリからそのトピックにステータスメッセージを送信できます。

Note

[Create a new notification] (新しい通知の作成) を選択した場合でも、既存の SNS トピックと同じトピック名を使用すると、Amazon SNS は新しいトピックを作成せずに、既存のトピックに新しいサブスクリプション情報を追加するだけです。

[Associate with existing SNS topic] (既存の SNS トピックに関連付ける) を選択した場合は、ディレクトリと同じリージョンにある SNS トピックのみを選択できます。

6. [Recipient type] (受信タイプ) を選択し、[Recipient] (受信者) の連絡先情報を入力します。SMS の電話番号を入力する場合は、数字のみを入力します。ハイフン、スペース、括弧を含めないでください。
7. (オプション) トピックの名前と SNS 表示名を入力します。表示名は、このトピックから送信されるすべての SMS メッセージに含まれる短縮名 (最大 10 文字) です。SMS オプションを使用する場合、表示名は必須です。

 Note

IAM ユーザーまたは [DirectoryServiceFullAccess](#) 管理ポリシーのみを持つロールを使用してログインしている場合、トピック名は「DirectoryMonitoring」で始まる必要があります。トピック名をさらにカスタマイズするには、SNS の権限が追加が必要です。

8. [Create] (作成) を選択します。

追加の E メールアドレス、Amazon SQS キュー、など、追加の SNS サブスクライバーを指定する場合は AWS Lambda、[Amazon SNS コンソール](#) から指定できます。

トピックからディレクトリステータスメッセージを削除するには

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Maintenance] (メンテナンス) タブを選択します。
4. [Directory monitoring] (ディレクトリのモニタリング) セクションでリストから SNS トピック名を選択し、[Actions] (アクション) をクリックして、[Remove] (削除) を選択します。
5. [Remove] (削除) をクリックします。

これで、選択した SNS トピックへの発行者であるディレクトリが削除されます。トピック全体を削除する場合は、「[Amazon SNS コンソール](#)」から削除できます。

 Note

SNS コンソールを使用して Amazon SNS トピックを削除する前に、ディレクトリがそのトピックにステータスメッセージを送信していないことを確認する必要があります。

SNS コンソールを使用して Amazon SNS トピックを削除した場合、この変更は Directory Services コンソール内にはすぐに反映されません。この削除済みトピックに対して、次回、ディレクトリから通知が発行されたときに初めて変更が反映され、トピックが見つからないという最新のステータスがディレクトリの [Monitoring] (モニタリング) タブに表示されます。

したがって、重要なディレクトリステータスメッセージが欠落しないようにするには、メッセージを受信するトピックを削除する前に AWS Directory Service、ディレクトリを別の Amazon SNS トピックに関連付けます。

AD Connector から AWS アプリケーションとサービスへのアクセス

接続された の AWS アプリケーションとサービスへの AD Connector アクセスを許可できますActive Directory。サポートされている AWS アプリケーションとサービスには、次のようなものがあります。

- Amazon Chime
- Amazon WorkSpaces
- IAM アイデンティティセンター
- AWS Management Console

AD Connector で動作するサードパーティー製アプリケーションはありません。

AD Connector から AWS アプリケーションとサービスにアクセスするタスク

- [AD Connector のアプリケーションの互換性ポリシー](#)
- [AD Connector から AWS アプリケーションとサービスへのアクセスを有効にする](#)

AD Connector のアプリケーションの互換性ポリシー

AWS Directory Service for Microsoft Active Directory ([AWS Managed Microsoft AD](#)) の代わりに、AD Connector は AWS 作成されたアプリケーションとサービス専用の Active Directory プロキシです。指定した Active Directory ドメインを使用するように、このプロキシを設定します。アプリケーションが Active Directory のユーザーまたはグループを検索する必要があるとき、AD Connector はそのリクエストをディレクトリにプロキシとして送信します。同様に、ユーザーがアプリケーションに口

グインするとき、AD Connector は認証リクエストをディレクトリにプロキシとして送信します。AD Connector で動作するサードパーティー製アプリケーションはありません。

以下は、互換性のある AWS アプリケーションとサービスのリストです。

- Amazon Chime - 詳細な手順については、「[Active Directory への接続](#)」を参照してください。
- Amazon Connect - 詳細については、「[Amazon Connect とは](#)」を参照してください。
- Windows 用または Linux 用 Amazon EC2 – Amazon EC2 Windows または Linux のシームレスな Active Directory ドメイン結合機能を使用して、インスタンスを自己管理型 Active Directory (オンプレミス) に結合できます。結合すると、インスタンスは Active Directory と直接通信し、AD Connector をバイパスします。詳細については、「[Amazon EC2 インスタンスを Active Directory に結合する方法](#)」を参照してください。
- AWS Management Console – AD Connector を使用して、SAML インフラストラクチャを設定せずに Active Directory 認証情報で AWS Management Console ユーザーを認証できます。詳細については、「[AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化](#)」を参照してください。
- QuickSight - 詳細については、[QuickSight Enterprise Edition でのユーザーアカウントの管理](#)」を参照してください。
- AWS IAM Identity Center - 詳細な手順については、「[IAM アイデンティティセンターをオンプレミスの Active Directory に接続する](#)」を参照してください。
- AWS Transfer Family - 詳細な手順については、「[Microsoft Active Directory での の使用 AWS Directory Service](#)」を参照してください。
- AWS クライアント VPN - 詳細な手順については、「[クライアント認証と認可](#)」を参照してください。
- WorkDocs - 詳細な手順については、「[AD Connector を使用したオンプレミスディレクトリへの接続](#)」を参照してください。
- Amazon WorkMail - 詳細な手順については、「[Integrate Amazon WorkMail with an existing directory \(standard setup\)](#)」(Amazon WorkMail を既存のディレクトリに統合する (標準セットアップ)) を参照してください。
- WorkSpaces - 詳細な手順については、「[AD Connector を使用して WorkSpace を起動する](#)」を参照してください。

Note

Amazon RDS は AWS Managed Microsoft AD とのみ互換性があり、AD Connector と互換性がありません。詳細については、よくある質問ページの AWS Managed Microsoft AD セクションを参照してください。 [AWS Directory Service FAQs](#)

AD Connector から AWS アプリケーションとサービスへのアクセスを有効にする

ユーザーは、AD Connector が Amazon WorkSpaces などの AWS アプリケーションやサービスへのアクセスを許可することを承認できますActive Directory。AD Connector を操作するには、次の AWS アプリケーションとサービスを有効または無効にできます。

AWS アプリケーション/サービス	詳細情報
Amazon Chime	詳細については、「 Active Directory への接続 」を参照してください。
Amazon Connect	詳細については、「 Amazon Connect 管理者ガイド 」を参照してください。
Amazon WorkDocs	詳細については、「 Getting started with Amazon WorkDocs 」を参照してください。
Amazon WorkMail	詳細については、「 Creating an organization 」を参照してください。
Amazon WorkSpaces	WorkSpaces から、Simple AD、AWS Microsoft AD、または AD Connector を直接作成することが可能です。このためには単純に、Workspace の作成時に [Advanced Setup] (高度なセットアップ) を起動します。 詳細については、「Amazon WorkSpaces 管理ガイド」を参照してください。

AWS アプリケーション/サービス	詳細情報
AWS Client VPN	詳細については、 AWS Client VPN ユーザーガイド をご参照ください。
AWS IAM Identity Center	詳細については、 AWS IAM Identity Center ユーザーガイド をご参照ください。
AWS Management Console	詳細については、「 AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化 」を参照してください。
AWS Transfer Family	詳細については、 AWS Transfer Family ユーザーガイド をご参照ください。

有効化の完了後は、ディレクトリへのアクセス権限を付与したアプリケーションまたはサービスのコンソールから、そのディレクトリへのアクセスを管理します。AWS Directory Service コンソールで上記の AWS アプリケーションとサービスのリンクを見つけるには、次の手順を実行します。

ディレクトリにアクセスしているアプリケーションおよびサービスを表示するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. [AWS apps & services] (AWS アプリおよびサービス) セクションでリストを確認します。

を使用して AWS アプリケーションとサービスを認可または認可解除する方法の詳細については AWS Directory Service、「」を参照してください [を使用した AWS アプリケーションとサービスの認可 AWS Directory Service](#)。

Amazon EC2 インスタンスを Active Directory に結合する方法

AD Connector は、クラウド内の情報をキャッシュせずにディレクトリリクエストをオンプレミスの Microsoft Active Directory にリダイレクトするために使用できるディレクトリゲートウェイです。Amazon EC2 を Active Directory ドメインに結合する方法の詳細について:

- インスタンスを起動したときに Amazon EC2 インスタンスを Active Directory ドメインにシームレスに結合できます。EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する方法の詳細については、「」を参照してください[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)。
- EC2 インスタンスを Active Directory ドメインに手動で結合する必要がある場合は、適切な AWS リージョン セキュリティグループまたはサブネットでインスタンスを起動し、そのインスタンスを Active Directory ドメインに結合する必要があります。
- これらのインスタンスにリモート接続できるようにするには、接続元のネットワークからインスタンスへの IP 接続が必要です。ほとんどの場合、これには、インターネットゲートウェイが Amazon VPC にアタッチされていることと、インスタンスにパブリック IP アドレスがあることが必要です。インターネットゲートウェイを使用したインターネットへの接続の詳細については、「Amazon VPC ユーザーガイド」の「[インターネットゲートウェイを使用してインターネットに接続する](#)」を参照してください。

Note

インスタンスを自己管理型 Active Directory (オンプレミス) に結合すると、インスタンスは Active Directory と直接通信し、AD Connector をバイパスします。

AD Connector クォータ

以下に示しているのは、AD Connector のデフォルトのクォータです。特に明記されていない限り、各クォータはリージョンごとに適用されます。

AD Connector クォータ

リソース	デフォルトのクォータ
AD Connector ディレクトリ	10

リソース	デフォルトのクォータ
ディレクトリあたりの登録済み認証機関 (CA) 証明書の最大数	5

AD Connector のトラブルシューティング

以下のセクションは、AD Connector 作成時および使用時に直面する可能性のある一般的な問題をトラブルシューティングするのに役立ちます。

トピック

- [作成に関する問題](#)
- [接続の問題](#)
- [認証問題](#)
- [メンテナンスの問題](#)
- [AD Connector を削除できない](#)
- [AD Connector 発行者を調査するための一般的なツール](#)

作成に関する問題

AD Connector の作成に関する一般的な問題は次のとおりです

- [ディレクトリを作成すると、「AZ Constrained」\(AZ 制約\) エラーが表示される](#)
- [AD Connector を作成しようとする、「Connectivity issues detected」というエラーが表示される](#)

ディレクトリを作成すると、「AZ Constrained」(AZ 制約) エラーが表示される

2012 年以前に作成された一部の AWS アカウントでは、AWS Directory Service ディレクトリをサポートしていない米国東部 (バージニア北部)、米国西部 (北カリフォルニア)、またはアジアパシフィック (東京) リージョンのアベイラビリティゾーンにアクセスできる場合があります。Active Directory 作成時にこのようなエラーが表示される場合は、別のアベイラビリティゾーンのサブネットを選択して、ディレクトリを再度作成してください。

AD Connector を作成しようとする、「Connectivity issues detected」というエラーが表示される

AD Connector の作成時に「接続の問題が検出されました」というエラーが表示された場合は、ポートの可用性または AD Connector パスワードの複雑さが原因である可能性があります。AD Connector の接続をテストして、次のポートが使用可能かどうかを確認できます。

- 53 (DNS)
- 88 (Kerberos)
- 389 (LDAP)

接続をテストするには、「[AD Connector をテストする](#)」を参照してください。接続テストは、AD Connector の IP アドレスが関連付けられている両方のサブネットに結合されたインスタンスで実行する必要があります。

接続テストが成功し、インスタンスがドメインに参加する場合は、AD Connector のパスワードを確認します。AD Connector は AWS パスワードの複雑さの要件を満たしている必要があります。詳細については、「[AD Connector の前提条件](#) のサービスアカウント」を参照してください。

AD Connector がこれらの要件を満たしていない場合は、これらの要件を満たすパスワードを使用する AD Connector を再作成してください。

ディレクトリの接続中に内部サービスエラーが発生しました。オペレーションを再試行してください。」 AD Connector の作成時の エラー

このエラーは通常、AD Connector が作成に失敗し、セルフマネージドドメインの有効な Active Directory ドメインコントローラーに接続できない場合に発生します。

Note

[ベストプラクティス](#)として、セルフマネージドネットワークに Active Directory サイトが定義されている場合は、以下を確認する必要があります。

- AD Connector が存在する VPC サブネットは、Active Directory サイトで定義されます。
- VPC サブネットと他のサイトのサブネットの間に競合はありません。

AD Connector は、サブネット IP アドレス範囲が AD Connector を含む VPC 内の範囲に近い Active Directory サイトを使用して、AD ドメインコントローラーを検出します。サブネットの IP アドレス範囲が VPC と同じサイトがある場合、AD Connector はそのサイトのドメインコントローラーを検出します。ドメインコントローラーは、AD Connector が存在するリージョンに物理的に近くない場合があります。

- カスタマーマネージド Active Directory ドメインで作成された DNS SRV レコード (これらのレコードは `_ldap._tcp.<DnsDomainName>` および `_kerberos._tcp.<DnsDomainName>`) の不整合。これは、AD Connector がこれらの SRV レコードに基づいて有効なドメインコントローラーを見つけて接続できなかった場合に発生する可能性があります。
- AD Connector とファイアウォールデバイスなどのカスタマーマネージド AD 間のネットワークの問題。

ディレクトリ [ネットワークインターフェイスのドメインコントローラー、DNS サーバー、VPC フローログでネットワークパケットキャプチャ](#) を使用して、この問題を調査できます。追加のサポートが必要な場合は、[AWS サポート](#) にお問い合わせください。

接続の問題

AD Connector の接続に関する一般的な問題は次のとおりです

- [オンプレミスのディレクトリに接続しようとする、 「Connectivity issues detected」 \(接続の問題が検出されました\) というエラーが表示される](#)
- [オンプレミスのディレクトリに接続しようとする、 「DNS unavailable」 \(DNS が使用できません\) というエラーが表示される](#)
- [オンプレミスのディレクトリに接続しようとする、 「SRV record」 \(SRV レコード\) というエラーが表示される](#)

オンプレミスのディレクトリに接続しようとする、 「Connectivity issues detected」 (接続の問題が検出されました) というエラーが表示される

オンプレミスディレクトリに接続すると、次のようなエラーメッセージが表示されます。接続の問題が検出されました。IP の場合は LDAP が使用不可 (TCP ポート 389)、IP の場合は **<IP ##### Kerberos/認証が使用不可 (TCP ポート 88)、<IP #####** リストされているポートが使用可能であることを確認し、オペレーションを再試行してください。

AD Connector は、以下のポート上で TCP および UDP によってオンプレミスのドメインコントローラーと通信できる必要があります。セキュリティグループおよびオンプレミスのファイアウォールが、これらのポート上の TCP および UDP 通信を許可していることを確認します。詳細については、「[AD Connector の前提条件](#)」を参照してください。

- 88 (Kerberos)
- 389 (LDAP)

必要に応じて、追加の TCP/UDP ポートが必要になる場合があります。これらのポートの一部については、次のリストを参照してください。Active Directory で使用されるポートの詳細については、Microsoft ドキュメントの「[Active Directory ドメインと信頼のファイアウォールを構成する方法](#)」を参照してください。

- 135 (RPC エンドポイントマッパー)
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

オンプレミスのディレクトリに接続しようとする、「DNS unavailable」(DNS が使用できません) というエラーが表示される

オンプレミスのディレクトリに接続するときに、次のようなエラーメッセージが表示されます。

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector は、ポート 53 上で TCP および UDP によってオンプレミスの DNS サーバーと通信できる必要があります。セキュリティグループおよびオンプレミスのファイアウォールが、このポート上の TCP および UDP 通信を許可していることを確認します。詳細については、「[AD Connector の前提条件](#)」を参照してください。

オンプレミスのディレクトリに接続しようとする、「SRV record」(SRV レコード) というエラーが表示される

オンプレミスのディレクトリに接続するときに、次のいずれかまたは複数のエラーメッセージが表示されます。

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 は、ディレクトリに接続するときに、`_ldap._tcp.<DnsDomainName>` および `_kerberos._tcp.<DnsDomainName>` SRV レコードを取得する必要があります。ディレクトリに接続するときに、サービスが指定された DNS サーバーからこれらのレコードを取得できない場合、このエラーが表示されます。これらの SRV レコードの詳細については、「[SRV record requirements](#)」を参照してください。

認証問題

AD Connector の一般的な認証問題は次のとおりです。

- [スマートカード Amazon WorkSpaces でサインインしようとする](#)と、「[証明書](#)の検証に失敗しました」というエラーが表示される
- [AD Connector で使用されるサービスアカウントで認証を試みる](#)と、「Invalid Credentials」(無効な認証情報) というエラーが表示される
- [AWS アプリケーションを使用してユーザーまたはグループを検索する](#)と、「認証できない」というエラーが表示される
- [AD Connector サービスアカウントを更新しようとする](#)と、ディレクトリ認証情報に関するエラーが表示される
- [一部のユーザーがディレクトリで認証されない](#)

スマートカード Amazon WorkSpaces でサインインしようとする、「[証明書](#)の検証に失敗しました」というエラーが表示される

スマートカードを使用して WorkSpaces にサインインしようとする、次のようなエラーメッセージが表示されます。ERROR: Certificate Validation failed。ブラウザまたはアプリケーションを再起動してもう一度試し、正しい証明書を選択していることを確認してください。このエラーは、スマートカードの証明書が証明書を使用するクライアントに正しく保存されていない場合に発生します。AD Connector とスマートカードの要件の詳細については、「[前提条件](#)」を参照してください。

ユーザーの証明書ストアに証明書を保存するスマートカードの機能をトラブルシューティングするには、次の手順に従います。

1. 証明書へのアクセスに問題があるデバイスで、Microsoft Management Console (MMC) にアクセスします。

⚠ Important

先に進む前に、スマートカードの証明書のコピーを作成します。

- MMC の証明書ストアに移動します。証明書ストアからユーザーのスマートカード証明書を削除します。MMC で証明書ストアを表示する方法の詳細については、Microsoft ドキュメントの「[方法: MMC スナップインを使用して証明書を参照する](#)」を参照してください。
- スマートカードを削除します。
- スマートカードを再挿入して、ユーザーの証明書ストアにスマートカード証明書を再入力できるようにします。

⚠ Warning

スマートカードが証明書を User Store に再入力していない場合、WorkSpaces スマートカード認証には使用できません。

AD Connector のサービスアカウントには、次のものがが必要です:

- my/spn がサービスプリンシパル名に追加される
- LDAP サービスに委任

証明書がスマートカードに再入力されると、オンプレミスドメインコントローラーをチェックして、サブジェクト代替名のユーザープリンシパルネーム (UPN) マッピングからブロックされているかどうかを判断する必要があります。この変更の詳細については、Microsoft ドキュメントの「[UPN マッピングのサブジェクトの別名を無効にする方法](#)」を参照してください。

ドメインコントローラーのレジストリキーを確認するには、次の手順に従います:

- 「レジストリエディター」で、次のレジストリエントリに移動します

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc\UseSubjectAltName

- UseSubjectAltName の値を検査します。
 - i. 値が 0 に設定されている場合、サブジェクト代替名のマッピングは無効になり、特定の証明書を 1 人のユーザーにのみ明示的にマッピングする必要があります。証明書が

複数のユーザーにマッピングされ、この値が 0 の場合、その証明書を使用したログインは失敗します。

- ii. 値が設定または 1 に設定されていない場合は、特定の証明書を 1 ユーザーのみに明示的にマッピングするか、ログインにサブジェクト代替名フィールドを使用する必要があります。
 - A. 証明書にサブジェクト代替名フィールドが存在する場合、優先順位が付けられます。
 - B. サブジェクト代替名フィールドが証明書に存在しず、証明書が複数のユーザーに明示的にマッピングされている場合、その証明書を使用したログインは失敗します。

 Note

レジストリキーがオンプレミスのドメインコントローラーで設定されている場合、AD Connector は Active Directory でユーザーを見つけることができず、上記のエラーメッセージが表示されます。

認証機関 (CA) 証明書は、AD Connector スマートカード証明書にアップロードする必要があります。証明書には OCSP 情報が含まれている必要があります。CA の追加要件を以下の通りです:

- 証明書は、ドメインコントローラー、認証機関サーバー、WorkSpaces の信頼されたルート権限にある必要があります。
- オフライン CA 証明書とルート CA 証明書には OSCP 情報は含まれません。これらの証明書には、取り消しに関する情報が含まれています。
- スマートカード認証にサードパーティーの CA 証明書を使用している場合は、CA 証明書と中間証明書を Active Directory NTAAuth ストアに発行する必要があります。これらは、すべてのドメインコントローラー、認証機関サーバー、WorkSpaces の信頼できるルート権限にインストールされる必要があります。
- 次のコマンドを使用して、Active Directory NTAAuth ストアに証明書を発行できます:

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

NTAuth ストアへの証明書の発行の詳細については、一般的なアクセスカードのインストールで Amazon WorkSpaces をアクセスするガイドの「[Enterprise NTAuth ストアに発行済み CA 証明書をインポートする](#)」を参照してください。

ユーザー証明書または CA チェーン証明書が OCSP によって検証されているかどうかを確認するには、次の手順に従います:

1. スマートカード証明書を C: ドライブなどのローカルマシン上の場所にエクスポートします。
2. コマンドラインプロンプトを開き、エクスポートされたスマートカード証明書が保存されている場所に移動します。
3. 次のコマンドを入力します。

```
certutil -URL Certificate_name.cer
```

4. コマンドを使用すると、ポップアップウィンドウが表示されます。右隅の [OCSP オプション] を選択し、[取得] を選択します。「検証済み」のステータスで返されるはずです。

certutil コマンドの詳細については、Microsoft ドキュメントの「[certutil](#)」を参照してください

AD Connector で使用されるサービスアカウントで認証を試みると、「Invalid Credentials」(無効な認証情報) というエラーが表示される

このエラーは、ドメインコントローラーのハードドライブ容量が不足している場合に発生する場合があります。ドメインコントローラーのハードドライブがいっぱいでないことを確認します。

AD Connector サービスアカウントを更新しようとする、「エラーが発生した」または「予期しないエラー」が表示されます

[Amazon WorkSpaces Console Launch Wizard](#) などの AWS エンタープライズアプリケーションでユーザーを検索するときに、次のエラーまたは症状が発生します。

- エラーが発生しました。問題が引き続き発生する場合は、コミュニティフォーラムの AWS サポート チームに連絡して、AWS プレミアムサポート経由でお問い合わせください。
- エラーが発生しました。ディレクトリには認証情報の更新が必要です。ディレクトリ認証情報を更新してください。

AD Connector で AD Connector サービスアカウントの認証情報を更新しようとする、次のエラーメッセージが表示されます。

- 予期しないエラー。予期しないエラーが発生しました。
- エラーが発生しました。サービスアカウントとパスワードの組み合わせでエラーが発生しました。もう一度試してください。

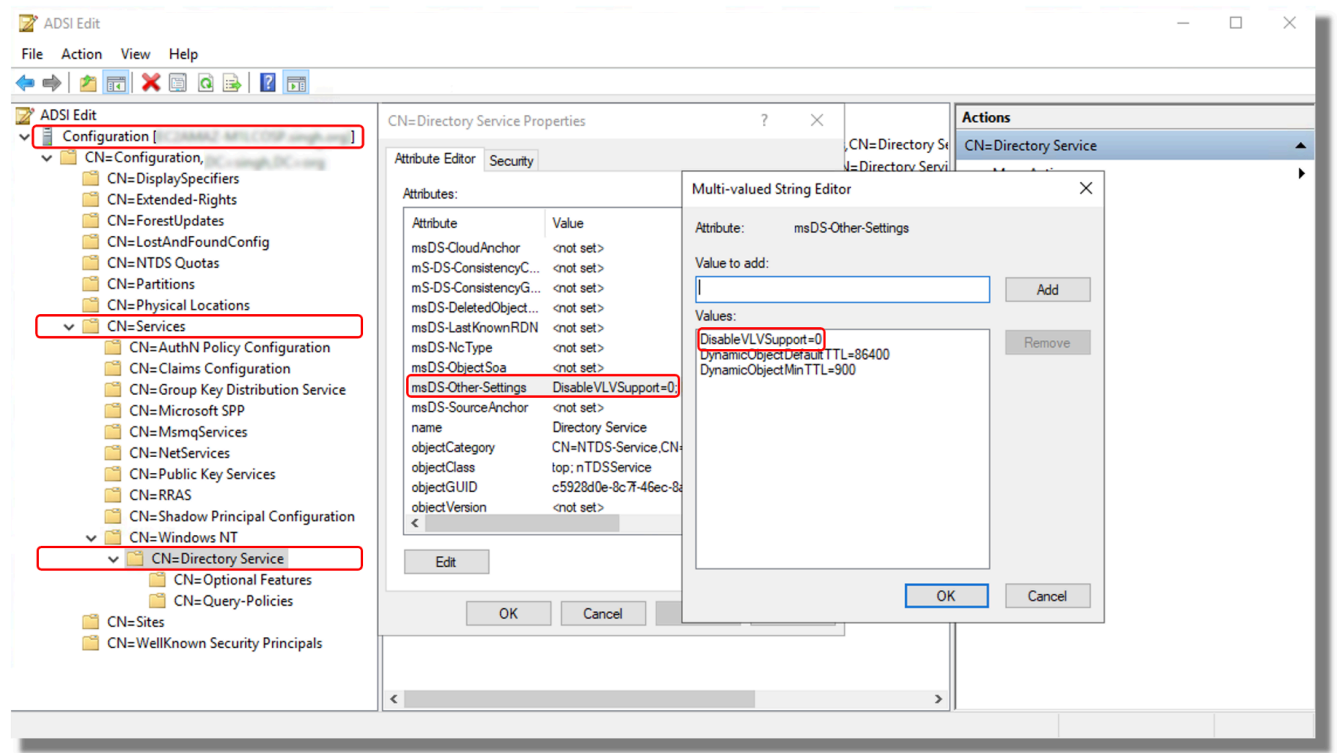
AD Connector ディレクトリのサービスアカウントは、カスタマー管理の にありますActive Directory。アカウントは、エンタープライズアプリケーションに代わって AWS AD Connector を介してカスターマネージドActive Directoryドメインに対してクエリとオペレーションを実行するための ID として使用されます。AD Connector は、Kerberos と LDAP を使用してこれらのオペレーションを実行します。

次のリストでは、これらのエラーメッセージの意味について説明します。

- 時刻の同期と Kerberos に問題がある可能性があります。AD Connector は Kerberos 認証リクエストを Active Directory に送信します。これらのリクエストには時間的制約があり、遅延すると失敗します。カスターマネージドドメインコントローラー間にタイム同期の問題がないことを確認します。この問題を解決するには、Microsoftドキュメントの [「レコメンデーション - 信頼できるタイムソースを使用してルート PDC を設定し、広範なタイムスキューを回避する」](#) を参照してください。タイムサービスと同期の詳細については、以下を参照してください。
 - [Windows タイムサービスの仕組み](#)
 - [コンピュータクロック同期の最大許容値](#)
 - [Windows タイムサービスツールと設定](#)
- AD Connector とカスターマネージドドメインコントローラーの間にファイアウォールや VPN ハードウェア設定などのネットワーク [MTU](#) 制限がある中間ネットワークデバイスは、[ネットワークの断片化](#)によりこのエラーを引き起こす可能性があります。
 - MTU 制限を確認するには、カスターマネージドドメインコントローラーと、AD Connector を介して接続されているディレクトリサブネットの 1 つで起動される Amazon EC2 インスタンスとの間で [Ping テスト](#) を実行できます。フレームサイズは、デフォルトのサイズである 1500 バイト以下にする必要があります
 - ping テストは、フレームサイズが 1500 バイト (ジャンボフレームとも呼ばれます) を超えており、断片化を必要とせずに AD Connector VPC とサブネットに到達できるかどうかを理解するのに役立ちます。さらに、ネットワークチームに確認し、ジャンボフレームが中間ネットワークデバイスで許可されていることを確認します。
- AD Connector で [クライアント側の LDAPS](#) が有効になっており、証明書の有効期限が切れている場合、この問題が発生する可能性があります。サーバー側の証明書と CA 証明書の両方が有効で、有効期限が切れておらず、[LDAPsドキュメント](#)の要件を満たしていることを確認します。

- カスタマーマネージドActive Directoryドメインで[仮想リストビューのサポート](#)が無効になっている場合、AD Connector AWS は LDAP クエリで VLV 検索を使用するため、アプリケーションはユーザーを検索できません。DisableVLVSupport がゼロ以外の値に設定されている場合、仮想リストビューのサポートは無効になります。次の手順Active Directoryを使用して、で[仮想リストビュー \(VLV\) サポート](#)が有効になっていることを確認します。

1. Schema Admin 認証情報を持つアカウントを使用して、スキーママスターロール所有者としてドメインコントローラーにログインします。
2. Start and then Run を選択し、 と入力します**Adsiedit.msc**。
3. ADSI Edit ツールで、Configuration Partition に接続し、Configuration[DomainController] ノードを展開します。
4. CN=Configuration、DC=DomainName コンテナを展開します。
5. CN=Services オブジェクトを展開します。
6. CN=Windows NT オブジェクトを展開します。
7. CN=Directory Service オブジェクトを選択します。プロパティを選択します。
8. 属性リストで、msds-Other-Settings を選択します。[Edit] (編集) を選択します。
9. 値リストで、x が 0 と等しくない DisableVLVSupport=x のインスタンスを選択し、削除を選択します。
10. 削除したら、 と入力します**DisableVLVSupport=0**。[追加] を選択します。
11. [OK] を選択します。ADSI 編集ツールを閉じることができます。次の図は、ADSI 編集ウィンドウの複数値文字列エディタダイアログボックスを示しています。



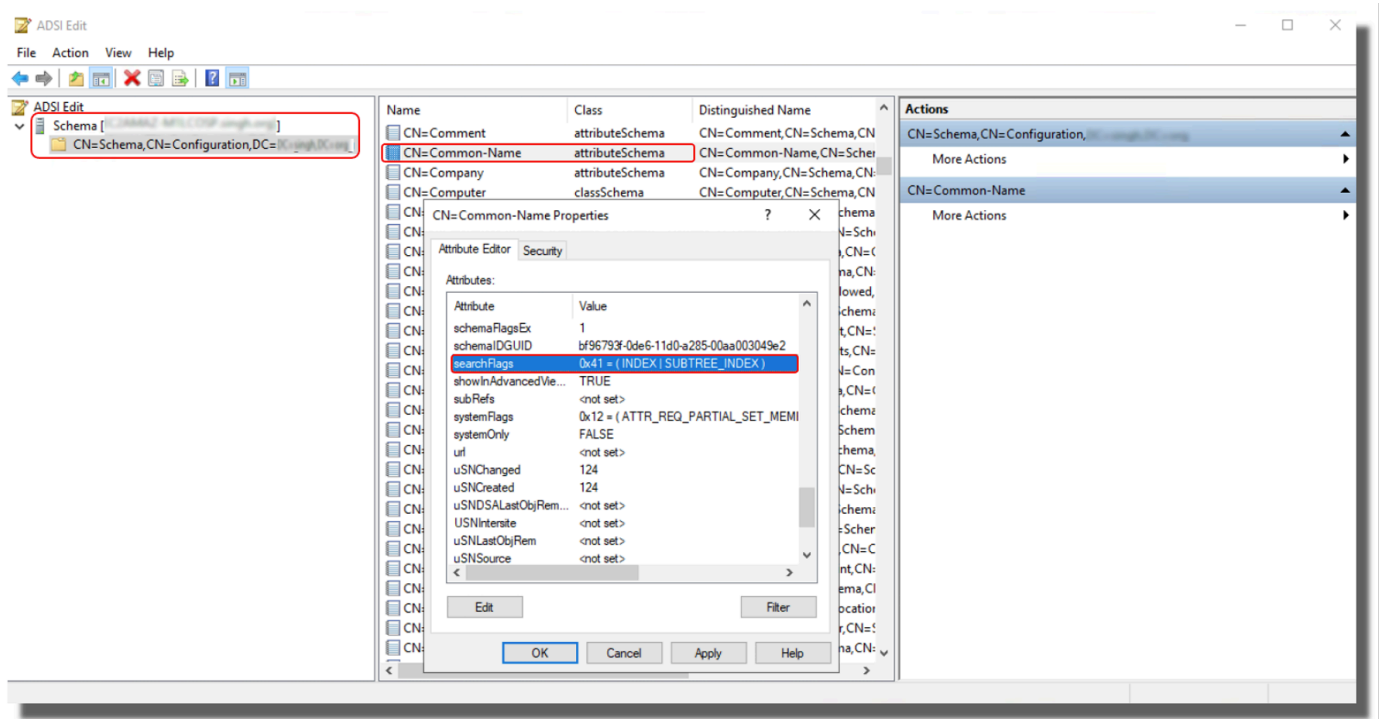
Note

ユーザー数が 100,000 人を超える大規模な Active Directory インフラストラクチャでは、特定のユーザーのみを検索できる場合があります。ただし、すべてのユーザーを一度に一覧表示しようとする (WorkSpaces Launch Wizard ですべてのユーザーを表示など)、VLV サポートが有効になっていても同じエラーが発生する可能性があります。AD Connector では、Subtree Index を使用して属性「CN」の結果をソートする必要があります。Subtree Index は、AD Connector がソートされた検索を完了できるようにする仮想リストビュー (LDAP) 検索オペレーションを実行するためにドメインコントローラーを準備するインデックスのタイプです。このインデックスは VLV 検索を改善し、[MaxTempTableSize](#) と呼ばれる一時データベーステーブルの使用を防止します。このテーブルのサイズは異なる場合がありますが、デフォルトではエントリの最大数は 10,000 (デフォルトのクエリポリシーの MaxTempTableSize 設定) です。MaxTempTableSize を増やすことは、Subtree Indexing を使用するよりも効率的ではありません。大規模な AD 環境でこれらのエラーを回避するには、Subtree Indexing を使用することをお勧めします。

Subtree インデックスを有効にするには、次のステップに従って ADSEdit を使用して、Active Directory スキーマ内の属性定義 [検索フラグ](#) 属性を 65 (0x41) の値に変更します。

1. Schema Admin 認証情報を持つアカウントを使用して、スキーママスターロール所有者としてドメインコントローラーにログインします。
2. Start and Run を選択し、と入力します **Adsiedit.msc**。
3. ADSI 編集ツールで、スキーマパーティションに接続します。
4. CN=Schema、CN=Configuration、DC=DomainName コンテナを展開します。
5. 「Common-Name」属性を見つけ、右クリックしてプロパティを選択します。
6. searchFlags 属性を見つけ、その値を に変更**65 (0x41)**して、通常のインデックスとともに SubTree インデックスを有効にします。

次の図は、ADSI 編集ウィンドウの CN=Common-Name プロパティダイアログボックスを示しています。



7. [OK] を選択します。ADSI 編集ツールを閉じることができます。
8. 確認のために、AD が指定された属性の新しいインデックスを正常に作成したことを示すイベント ID 1137 (ソース: Active Directory_DomainServices) が表示されるはずです。

詳細については、「[Microsoft ドキュメント](#)」を参照してください。

AWS アプリケーションを使用してユーザーまたはグループを検索すると、「認証できない」というエラーが表示される

AD Connector のステータスがアクティブであっても、ユーザーを検索したり、WorkSpaces や QuickSight などのアプリケーションにログイン AWS したりすると、エラーが発生することがあります。AD Connector のサービスアカウントのパスワードが変更されているか、有効期限が切れている場合、AD Connector は Active Directory ドメインをクエリできなくなります。AD 管理者に連絡して、以下を確認してください。

- AD Connector サービスアカウントのパスワードの有効期限が切れていないことを確認します。
- AD Connector サービスアカウントに オプションがないことを確認しました。次回のログオン時にパスワードを変更する必要があります。
- AD Connector サービスアカウントがロックされていないことを確認します。
- パスワードの有効期限が切れているか変更されているかわからない場合は、サービスアカウントのパスワードをリセットし、AD Connector で同じパスワード [を更新](#)することもできます。

AD Connector サービスアカウントを更新しようとすると、ディレクトリ認証情報に関するエラーが表示される

AD Connector サービスアカウントを更新しようとすると、次のようなエラーメッセージが表示されます:

メッセージ: エラーが発生した ディレクトリには認証情報の更新が必要です。ディレクトリ認証情報を更新してください。エラー発生 ディレクトリには認証情報の更新が必要です。ディレクトリ認証情報を更新してください。「AD Connector サービスアカウントの認証情報の更新」メッセージ: エラー発生 リクエストに問題があります。以下の詳細を参照してください。サービスアカウントとパスワードの組み合わせでエラーが発生しました

時刻の同期と Kerberos に問題がある可能性があります。AD Connector は Kerberos 認証リクエストを Active Directory に送信します。これらのリクエストには時間的制約があり、遅延すると失敗します。この問題を解決するには、Microsoft ドキュメントの「[推奨 - 権限のあるタイム ソースを使用してルート PDC を構成し、広範囲に及ぶ時刻のずれを回避する](#)」を参照してください。タイムサービスと同期の詳細については、以下を参照してください:

- [Windows タイムサービスの仕組み](#)
- [コンピュータクロック同期の最大許容値](#)
- [Windows タイムサービスツールと設定](#)

一部のユーザーがディレクトリで認証されない

ユーザーアカウントの Kerberos 事前認証を有効にしておく必要があります。これは、新しいユーザーアカウントのデフォルト設定ですが、変更しないでください。この設定の詳細については、Microsoft TechNet の「[事前認証](#)」を参照してください。

メンテナンスの問題

AD Connector の一般的なメンテナンス問題は次のとおりです

- ディレクトリが「Requested」(リクエスト済み)の状態から変化しない
- Amazon EC2 インスタンスのシームレスなドメイン結合の動作が停止した

ディレクトリが「Requested」(リクエスト済み)の状態から変化しない

5 分を経過しても、ディレクトリのステータスが「Requested」(リクエスト済み)の状態から変わらない場合は、ディレクトリを削除して、作成し直してください。If this problem persists, contact [AWS サポート](#). (この問題が解決しない場合は、お問い合わせください。)

Amazon EC2 インスタンスのシームレスなドメイン結合の動作が停止した

EC2 インスタンスのシームレスなドメイン結合が動作していたものの、その後、AD Connector がアクティブになっている時に停止した場合は、AD Connector サービスアカウントの認証情報が期限切れになっている可能性があります。認証情報が期限切れになると、AD Connector が Active Directory 内にコンピュータオブジェクトを作成できなくなる可能性があります。

この問題を解消するには、パスワードが一致するように、次の順序でサービスアカウントのパスワードを更新します。

1. Active Directory でのサービスアカウントのパスワードを更新します。
2. AWS Directory Serviceでの AD Connector のサービスアカウントのパスワードを更新します。詳細については、「[での AD Connector サービスアカウントの認証情報の更新 AWS Management Console](#)」を参照してください。

⚠ Important

でのみパスワードを更新 AWS Directory Service しても、パスワードの変更は既存のオンプレミスにプッシュされないActive Directoryため、前の手順で示した順序で実行することが重要です。

AD Connector を削除できない

AD Connector が動作不能な状態に切り替わると、ドメインコントローラーにアクセスできなくなります。AD Connector にリンクされているアプリケーションがまだ存在する場合は、それらのアプリケーションの 1 つが引き続きディレクトリを使用している可能性があるため、AD Connector の削除をブロックします。AD Connector を削除するには、無効にする必要があるアプリケーションのリストについては、「[AD Connector を削除する](#)」を参照してください。AD Connector を削除できない場合は、[AWS サポート](#) を通じてサポートをリクエストできます。

AD Connector 発行者を調査するための一般的なツール

次のツールを使用して、作成、認証、接続に関連するさまざまな AD Connector の問題をトラブルシューティングできます。

DirectoryServicePortTest ツール

[DirectoryServicePortTest](#) テストツールは、AD Connector とカスターマネージドサーバー Active Directoryまたは DNS サーバー間の接続に関する問題のトラブルシューティングに役立ちます。ツールの使用方法の詳細については、「」を参照してください[AD Connector をテストする](#)。

パケットキャプチャツール

組み込みWindowsパッケージキャプチャユーティリティ ([netsh](#)) を使用して、潜在的なネットワークまたはActive Directory通信 (ldap および kerberos) の問題を調査およびトラブルシューティングできます。詳細については、「[Capture a Network Trace without installing anything](#)」(インストールを一切行わずにネットワークトレースをキャプチャする) を参照してください。

VPC フローログ

AD Connector から受信および送信されるリクエストをよりよく理解するために、ディレクトリネットワークインターフェイスの [VPC フローログ](#)を設定できます。で使用するために予約されているすべてのネットワークインターフェイスは、の説明 AWS Directory Service で識別できますAWS created network interface for directory *your-directory-id*。

シンプルなユースケースは、多数のActive Directoryドメインコントローラーを持つカスタマーマネージドドメインを使用した AD Connector の作成時です。VPC フローログを使用し、Kerberos ポート (88) でフィルタリングして、カスタマーマネージドのどのドメインコントローラーが認証のために問い合わせられているActive Directoryかを調べることができます。

Simple AD

Simple AD は、Samba 4 Active Directory Compatible Server を使用するスタンドアロンのマネージドディレクトリです。2 つのサイズから選択できます。

- スモール – 最大 500 ユーザー (ユーザー、グループ、コンピュータを含めて約 2,000 オブジェクト) をサポートします。
- ラージ – 最大 5,000 ユーザー (ユーザー、グループ、コンピュータを含めて約 20,000 オブジェクト) をサポートします。

Simple AD は、ユーザーアカウントとグループメンバーシップの管理、グループポリシーの作成と適用、Amazon EC2 インスタンスへの安全な接続、Kerberos ベースのシングルサインオン (SSO) の提供など、AWS Managed Microsoft AD が提供する機能のサブセットを提供します。ただし、Simple AD では、Multi-Factor Authentication (MFA)、他のドメインとの信頼関係、Active Directory 管理センター、PowerShell サポート、Active Directory のごみ箱、グループ管理サービスアカウント、POSIX および Microsoft アプリケーションのスキーマ拡張などの機能はサポートされていません。

Simple AD には、次のような多くの利点があります。

- Simple AD を使用すると、[Linux と Windows を実行している Amazon EC2 インスタンスを管理し](#)、Windows アプリケーションを AWS クラウドにデプロイしやすくなります。
- 現在使用している Microsoft Active Directory のサポートを必要とするアプリケーションやツールの多くは、Simple AD で使用することができます。
- Simple AD のユーザーアカウントは、WorkSpaces、WorkDocs、Amazon WorkMail などの AWS アプリケーションへのアクセスを許可します。
- AWS への IAM ロールベースのアクセスを通じてリソースを管理できます AWS Management Console。
- 毎日の自動スナップショットで、ポイントインタイムリカバリを行うことができます。

Simple AD では、以下はサポートされていません。

- Amazon AppStream 2.0
- Amazon Chime
- Amazon FSx
- Amazon RDS for SQL Server

- Amazon RDS for Oracle
- AWS IAM Identity Center
- 他のドメインとの信頼関係
- Active Directory 管理センター
- PowerShell
- Active Directory のごみ箱
- グループ管理サービスアカウント
- POSIX および Microsoft アプリケーションのスキーマ拡張

独自の Simple AD を作成する方法については、このセクションの後半のトピックを参照してください。

トピック

- [Simple AD の開始](#)
- [Simple AD のベストプラクティス](#)
- [Simple AD ディレクトリの維持](#)
- [Simple AD ディレクトリを保護する](#)
- [Simple AD ディレクトリのモニタリング](#)
- [Simple AD から AWS アプリケーションとサービスへのアクセス](#)
- [Amazon EC2 インスタンスを Simple AD に結合する方法](#)
- [Simple AD におけるユーザーとグループの管理](#)
- [Simple AD のクォータ](#)
- [Simple AD のトラブルシューティング](#)

Simple AD の開始

Simple AD は、AWS クラウドにフルマネージドの Samba ベースのディレクトリを作成します。Simple AD を使用してディレクトリを作成すると、はユーザーに代わって 2 つのドメインコントローラーと DNS サーバー AWS Directory Service を作成します。ドメインコントローラーは、1 つの Amazon VPC の異なるサブネットに作成されます。この冗長性により、障害が発生してもディレクトリに確実にアクセスできます。

トピック

- [Simple AD の前提条件](#)
- [Simple AD を作成する](#)
- [Simple AD で作成されるもの](#)

Simple AD の前提条件

Simple AD Active Directory を作成するには、次の条件を満たす Amazon VPC が必要です:

- VPC にはデフォルトのハードウェアテナンシーが必要です。
- 少なくとも 2 つのサブネットが異なるアベイラビリティゾーンに存在している。サブネットは同じ Classless Inter-Domain Routing (CIDR) の範囲に存在する必要があります。ディレクトリの VPC を拡張またはサイズ変更する場合は、拡張する VPC CIDR の範囲における両方のドメインコントローラーのサブネットを選択してください。Simple AD を作成すると、はユーザーに代わって 2 つのドメインコントローラーと DNS サーバー AWS Directory Service を作成します。
- 詳細については、「Amazon VPC ユーザーガイド」の「[VPC とサブネットの IP アドレス設定](#)」を参照してください。
- Simple AD による LDAPS のサポートが必要な場合は、ポート 389 に接続された Network Load Balancer を使用して設定することをお勧めします。このモデルを使用することで、LDAPS 接続に強力な証明書を使用して、単一の NLB IP アドレスを通じて LDAPS へのアクセスを簡素化できます。また、NLB を通じて自動フェイルオーバーを実現できます。Simple AD では、ポート 636 での自己署名証明書の使用はサポートされていません。Simple AD を使用した LDAPS の設定方法の詳細については、「AWS Security Blog」の「[How to configure an LDAPS endpoint for Simple AD](#)」を参照してください。
- 次の暗号化タイプは、ディレクトリで有効にする必要があります。
 - RC4_HMAC_MD5
 - AES128_HMAC_SHA1
 - AES256_HMAC_SHA1
 - 今後の暗号化タイプ

Note

これらの暗号化タイプを無効にすると、RSAT (Remote Server Administration Tools) との通信に問題が発生し、可用性またはディレクトリに影響を与える可能性があります。

- 詳細については、「Amazon VPC ユーザーガイド」の「[Amazon VPC とは](#)」を参照してください。

AWS Directory Service は 2 つの VPC 構造を使用します。ディレクトリを構成する EC2 インスタンスは、AWS アカウント外で実行され、によって管理されます AWS。これらには、2 つのネットワークアダプタ (ETH0 および ETH1) があります。ETH0 は管理アダプタで、アカウント外部に存在します。ETH1 はアカウント内で作成されます。

ディレクトリの ETH0 ネットワークの管理 IP 範囲は、ディレクトリがデプロイされている VPC と競合しないようにするため、プログラムによって選択されます。この IP 範囲は、(ディレクトリが 2 つのサブネットで行われるため) 次のいずれかのペアになります。

- 10.0.1.0/24 と 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 と 192.168.2.0/24

ETH1 CIDR の最初のオクテットをチェックすることで、競合を回避します。10 で始まる場合は、192.168.1.0/24 と 192.168.2.0/24 のサブネットを持つ 192.168.0.0/16 VPC を選択します。最初のオクテットが 10 以外である場合は、10.0.1.0/24 と 10.0.2.0/24 のサブネットを持つ 10.0.0.0/16 VPC を選択します。

選択アルゴリズムには、VPC 上のルートは含まれません。そのため、このシナリオから IP ルーティングの競合が発生する可能性があります。

Important

Simple AD の作成後に前提条件が変更された場合、Simple AD が [障害] ステータスになる可能性があります。Simple AD の [障害] ステータスを解決するには、「[AWS サポート](#)」に連絡する必要があります。

Simple AD を作成する

この手順では、Simple AD を作成するために必要なすべてのステップについて説明します。これは Simple AD を迅速かつ簡単に使い始めるためのものであり、大規模な本番環境での使用を目的としたものではありません。

ステップ

- [前提条件](#)
- [Simple AD の Amazon VPC の作成と設定](#)
- [Simple AD の作成](#)

前提条件

この手順では、以下を前提とします。

- アクティブな AWS アカウントがあります。
- お使いのアカウントは、Simple AD を使用するリージョンにおける Amazon VPC の上限に達していません。Amazon VPC の詳細については、「VPC ユーザーガイド」の「[Amazon VPC とは?](#)」および「[VPC のサブネット](#)」を参照してください。
- CIDR が 10.0.0.0/16 のリージョンに VPC が存在しない。
- Simple AD が利用可能なリージョンにいます。詳細については、「[のリージョンの可用性 AWS Directory Service](#)」を参照してください。

詳細については、「[Simple AD の前提条件](#)」を参照してください。

Simple AD の Amazon VPC の作成と設定

まず、Simple AD で使用するために Amazon VPC を作成および設定します。この手順を開始する前に、[前提条件](#) を満たしていることを確認します。

作成する VPC には 2 つのパブリックサブネットがあります。AWS Directory Service VPC には 2 つのサブネットが必要であり、各サブネットは異なるアベイラビリティゾーンにある必要があります。

「VPC を作成する」

1. Amazon VPC コンソールの <https://console.aws.amazon.com/vpc/> を開いてください。
2. VPC ダッシュボードで、[VPC の作成] を選択します。
3. [VPC 設定] で、[VPC など] を選択します。
4. フィールドに以下のように入力します。
 - [名前タグの自動生成] で [自動生成] を選択したままにします。[プロジェクト] を ADS VPC に変更します。
 - [IPv4 CIDR ブロック] は 10.0.0.0/16 である必要があります。

- [IPv6 CIDR ブロックなし] オプションを選択したままにします。
- [テナンシー] は [デフォルト] のままにする必要があります。
- [アベイラビリティーゾーン (AZ) 数] として [2] を選択します。
- [パブリックサブネットの数] で [2] を選択します。[プライベートサブネットの数] は 0 に変更できます。
- [サブネット CIDR ブロックをカスタマイズ] を選択して、パブリックサブネット IP アドレス範囲を設定します。パブリックサブネット CIDR ブロックは 10.0.0.0/20 と 10.0.16.0/20 である必要があります。

5. [Create VPC (VPC の作成)] を選択します。VPC の作成には数分かかります。

Simple AD の作成

新しい Simple AD を作成するには、以下の手順を実行します。この手順を開始する前に、次の [前提条件](#) と [Simple AD の Amazon VPC の作成と設定](#) 内の手順を完了したことを確認します。

Simple AD を作成する

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ)、[Set up directory] (ディレクトリの設定) の順に選択します。
2. [Select directory type] (ディレクトリタイプの選択) ページで、[Simple AD] を選択し、[Next] (次へ) を選択します。
3. [Enter directory information] (ディレクトリ情報の入力) ページに、以下の情報を指定します。

[Directory size] (ディレクトリのサイズ)

[Small] (スモール) または [Large] (ラージ) サイズオプションのどちらかを選択します。サイズの詳細については、「[Simple AD](#)」を参照してください。

[Organization name] (組織名)

クライアントデバイスの登録に使用するディレクトリの一意の組織名です。

このフィールドは、WorkSpaces の起動の一環としてディレクトリを作成する場合にのみ使用できます。

[Directory DNS name] (ディレクトリの DNS 名)

ディレクトリの完全修飾名 (例: corp.example.com)。

[Directory NetBIOS name] (ディレクトリの NetBIOS 名)

ディレクトリの短縮名 (例: CORP)。

[Administrator password] (管理者パスワード)

ディレクトリ管理者のパスワードです。ディレクトリの作成プロセスでは、ユーザー名 Administrator とこのパスワードを使用して管理者アカウントが作成されます。

ディレクトリ管理者のパスワードは大文字と小文字が区別され、8 文字以上 64 文字以下の長さにする必要があります。また、次の 4 つのカテゴリうち 3 つから少なくとも 1 文字を含める必要があります。

- 小文字 (a～z)
- 大文字 A～Z
- 数字 (0～9)
- アルファベットと数字以外の文字 (~!@#\$%^&*_-+=`|\\(){}[];:'"<>.,?/)

[Confirm password] (パスワードを確認)

管理者のパスワードをもう一度入力します。

 Important

このパスワードは必ず保存してください。このパスワードは保存 AWS Directory Service されず、取得できません。ただし、コンソールから、AWS Directory Service または [ResetUserPassword](#) API を使用してパスワードをリセットできます。

[Directory description] (ディレクトリの説明)

必要に応じて、ディレクトリの説明。

4. [Choose VPC and subnets] (VPC とサブネットの選択) ページで、次の情報を指定して [Next] (次へ) をクリックします。

[VPC]

ディレクトリ用の VPC。

[Subnets] (サブネット)

ドメインコントローラーのサブネットを選択します。2つのサブネットは、異なるアベイラビリティゾーンに存在している必要があります。

5. [Review & create] (確認と作成) ページでディレクトリ情報を確認し、必要に応じて変更を加えます。情報が正しい場合は、[Create directory] (ディレクトリの作成) を選択します。ディレクトリが作成されるまで、数分かかります。作成が完了すると、[Status] (ステータス) 値が [Active] (アクティブ) に変わります。

Simple AD で作成される内容の詳細については、[Simple AD で作成されるもの](#) を参照してください。

Simple AD で作成されるもの

Simple AD Active Directoryで を作成すると、 はユーザーに代わって次のタスク AWS Directory Service を実行します。

- VPC 内に Samba ベースのディレクトリを設定します。
- ユーザー名 Administrator と指定されたパスワードで、ディレクトリの管理者アカウントを作成する。このアカウントはディレクトリの管理に使用します。

Important

このパスワードは必ず保存してください。このパスワードは保存 AWS Directory Service されず、取得できません。ただし、コンソールから、AWS Directory Service または [ResetUserPassword](#) API を使用してパスワードをリセットできます。

- ディレクトリコントローラー用のセキュリティグループを作成する。
- ドメイン管理者の権限を持つ名前 AWSAdminD-**xxxxxxxxxx** で、アカウントを作成する。このアカウントは、ディレクトリスナップショットの作成や FSMO ロールの転送など、ディレクトリメンテナンスオペレーションの自動オペレーションを実行する AWS Directory Service ために によって使用されます。このアカウントの認証情報は、AWS Directory Serviceにより安全に保存されます。
- Elastic Network Interface (ENI) を自動作成し、各ドメインコントローラーと関連付けます。これらの各 ENIs は VPC と AWS Directory Service ドメインコントローラー間の接続に不可欠であり、削除しないでください。で使用するために予約されているすべてのネットワークインターフェイスは、「ディレクトリ directory-id 用にAWS 作成されたネットワークインターフェイス」という

説明 AWS Directory Service で識別できます。詳細については、「Amazon EC2 ユーザーガイド」の「[Elastic Network Interface](#)」を参照してください。AWS Managed Microsoft AD のデフォルトの DNS サーバー Active Directory は、Classless Inter-Domain Routing (CIDR)+2 の VPC DNS サーバーです。詳細については、「Amazon VPC ユーザーガイド」の「[Amazon DNS サーバー](#)」を参照してください。

 Note

ドメインコントローラーは、デフォルトでリージョン内の 2 つのアベイラビリティーゾーンにまたがってデプロイされ、Amazon Virtual Private Cloud (VPC) に接続されます。バックアップは 1 日に 1 回自動的に実行され、Amazon Elastic Block Store (EBS) ボリュームは保管中のデータを保護するために暗号化されます。障害が発生したドメインコントローラーは、同じ IP アドレスを使用して同じアベイラビリティーゾーン内で自動的に置き換えられ、最新のバックアップを使用して完全な災害対策を実行できます。

Simple AD のベストプラクティス

Simple AD を最大限に活用し、問題を避けるために考慮すべき提案とガイドラインをいくつか紹介します。

セットアップ: 前提条件

ディレクトリを作成する前に、これらのガイドラインを考慮してください。

ディレクトリタイプが正しいことを確認する

AWS Directory Service には、他の AWS のサービス Microsoft Active Directory で使用する複数の方法があります。予算に合わせたコストで必要な機能を備えた、ディレクトリサービスを次のように選択できます。

- AWS Directory Service for Microsoft Active Directory は、AWS クラウド上で Microsoft Active Directory ホストされる機能豊富なマネージド型です。AWS マネージド Microsoft AD は、5,000 人を超えるユーザーがあり、ホストディレクトリとオンプレミスディレクトリの間に AWS 信頼関係を設定する必要がある場合に最適です。
- AD Connector は、既存のオンプレミスをに接続するだけです Active Directory AWS。AD Connector は、AWS のサービスで既存のオンプレミスのディレクトリを使用する場合に最適な選択です。

- Simple AD は、基本的な Active Directory 互換性を持つ低スケール、低コストのディレクトリです。5,000 人以下のユーザー、Samba 4 互換アプリケーション、LDAP 対応アプリケーションの LDAP 互換性をサポートします。

AWS Directory Service オプションの詳細については、「」を参照してください[オプションの選択](#)。

VPC とインスタンスが正しく設定されていることを確認する

ディレクトリに接続して、管理および使用するためには、ディレクトリが関連付けられている VPC を適切に設定する必要があります。VPC セキュリティおよびネットワーク要件の詳細については、「[AWS Managed Microsoft AD を作成するための前提条件](#)」、「[AD Connector の前提条件](#)」、「[Simple AD の前提条件](#)」のいずれかを参照してください。

ドメインにインスタンスを追加する場合は、「[Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する方法](#)」に説明されているように、インスタンスへの接続およびリモートアクセスがあることを確認します。

制限を理解する

特定のディレクトリタイプのさまざまな制限について説明します。ディレクトリに保存できるオブジェクトの数については、使用可能なストレージとオブジェクトの集約サイズのみに制限があります。選択したディレクトリに関する詳細については、「[AWS Managed Microsoft AD のクォータ](#)」、「[AD Connector クォータ](#)」、「[Simple AD のクォータ](#)」のいずれかを参照してください。

ディレクトリ AWS のセキュリティグループ設定を理解し、を使用する

AWS は[セキュリティグループ](#)を作成し、ディレクトリのドメインコントローラーの [Elastic Network Interface](#) にアタッチします。は、ディレクトリへの不要なトラフィックをブロックし、必要なトラフィックを許可するようにセキュリティグループ AWS を設定します。

ディレクトリのセキュリティグループを変更する

ディレクトリのセキュリティグループのセキュリティは、必要に応じて変更することができます。このような変更を行うのは、セキュリティグループのフィルタリング機能を完全に理解している場合に限りです。詳細については、「Amazon EC2 ユーザーガイド」の「[Amazon EC2 security groups for Linux instances](#)」(Linux インスタンス用の Amazon EC2 セキュリティグループ) を参照してください。不適切な変更を行うと、目的のコンピュータやインスタンスとの通信が失われる可能性があります。ディレクトリのセキュリティが低下するため、ディレクトリへの追加のポートを開こうとしない AWS ことをお勧めします。「[AWS 責任共有モデル](#)」をよくお読みください。

⚠ Warning

技術的には、ディレクトリのセキュリティグループを作成した他の EC2 インスタンスに関連付けることができます。ただし、はこのプラクティスに反対 AWS することをお勧めします。AWS には、マネージドディレクトリの機能またはセキュリティのニーズに対応するために、予告なしにセキュリティグループを変更する理由がある場合があります。このような変更は、ディレクトリのセキュリティグループを関連付けるすべてのインスタンスに影響を及ぼすため、関連付けられたインスタンスのオペレーションが中断する場合があります。さらに、ディレクトリのセキュリティグループを EC2 インスタンスに関連付けると、EC2 インスタンスのセキュリティリスクが生じる可能性があります。

信頼が必要な場合は AWS Managed Microsoft AD を使用する

Simple AD では信頼関係はサポートされていません。AWS Directory Service ディレクトリと別のディレクトリの上に信頼を確立する必要がある場合は、AWS Directory Service for Microsoft Active Directory を使用する必要があります。

セットアップ: ディレクトリを作成する

ディレクトリを作成する際に考慮すべき推奨事項をいくつか示します。

管理者 ID とパスワードを記憶する

ディレクトリを設定するときに、管理者アカウントのパスワードを指定します。Simple AD のアカウント ID は Administrator です。このアカウント用に作成したパスワードを忘れないでください。そうでないと、ディレクトリにオブジェクトを追加できません。

AWS アプリケーションのユーザー名制限を理解する

AWS Directory Service では、ユーザー名の構築に使用できるほとんどの文字形式がサポートされています。ただし、WorkSpaces、WorkDocs、Amazon WorkMail、QuickSight などの AWS アプリケーションへのサインインに使用されるユーザー名には、文字制限が適用されます。これらの制限により、以下の文字は使用できません。

- スペース
- マルチバイト文字
- !"#\$%&'()*+,-./:;<=>?@[\\]^_{|}~

Note

@ 記号は、UPN サフィックスが後に続く場合に限り、使用できます。

アプリケーションをプログラミングする

アプリケーションをプログラミングする前に、以下の点を考慮してください。

Windows DC Locator Service を使用する

アプリケーションを開発するときは、Windows DC ロケータサービスを使用するか、AWS Managed Microsoft AD の動的 DNS (DDNS) サービスを使用してドメインコントローラー (DCs)。アプリケーションを DC のアドレスでハードコーディングしないでください。DC Locator Service では、ディレクトリの負荷を分散できるだけでなく、デプロイにドメインコントローラーを追加することにより水平スケーリングを活用できます。アプリケーションを固定 DC にバインドした場合、その DC がパッチ適用または復旧を行うと、アプリケーションは残りのいずれかの DC を使用することなく、DC へのアクセスを失います。さらに、DC をハードコーディングすると、1 つの DC にホットスポットが発生する可能性があります。極端な場合、ホットスポットが原因で DC が応答しなくなる可能性があります。このような場合、AWS ディレクトリの自動化によってディレクトリに障害があるとフラグが立てられ、応答しない DC を置き換える復旧プロセスがトリガーされる可能性があります。

本番稼働用環境にロールアウトする前の負荷テスト

本番稼働用環境のワークロードを表すオブジェクトとリクエストを使用してラボテストを行い、ディレクトリがアプリケーションの負荷に合わせてスケーリングされることを確認します。追加の容量が必要な場合は、for AWS Directory Service Microsoft Active Directory を使用する必要があります。これにより、高性能なドメインコントローラーを追加できます。詳細については、「[AWS Managed Microsoft AD に追加するドメインコントローラーのデプロイ](#)」を参照してください。

効率的な LDAP クエリを使用する

何千個ものオブジェクトにまたがるドメインコントローラーの広範な LDAP クエリにより、単一の DC で大量の CPU サイクルが消費され、ホットスポットが発生することがあります。これは、クエリ中に同じ DC を共有するアプリケーションに影響を与える可能性があります。

Simple AD ディレクトリの維持

を使用して Simple AD AWS Management Console を維持し、day-to-day管理タスクを完了できます。Simple AD を維持する方法は次のとおりです：

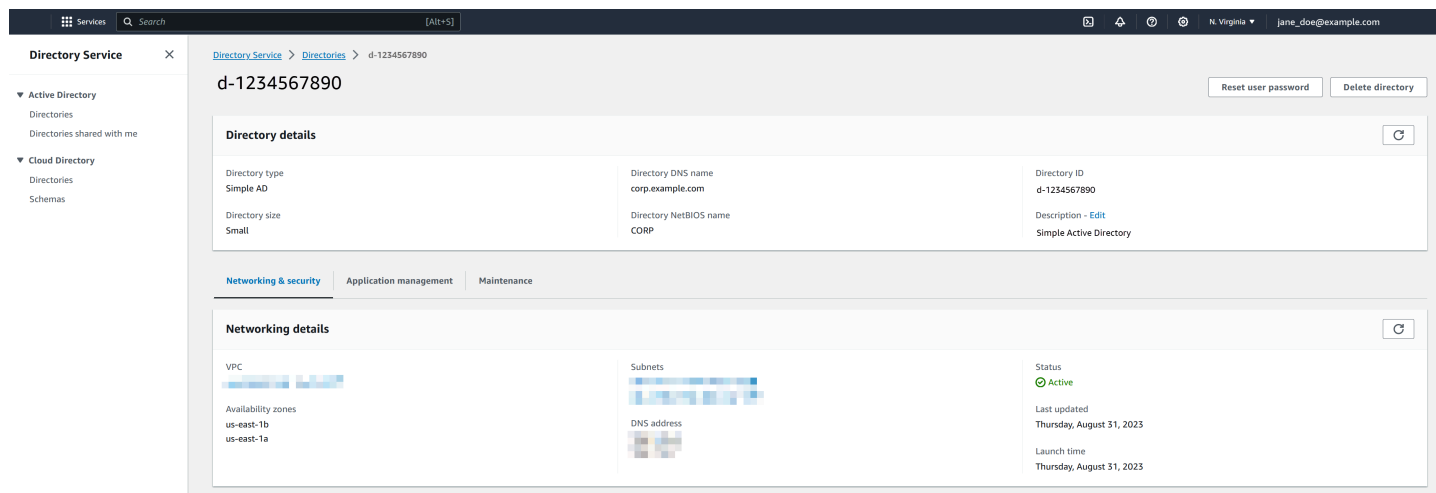
- DNS 名、ディレクトリ ID、ディレクトリステータスなど、[Simple AD に関する詳細を表示する](#)。
- [Simple AD の DNS アドレスを更新する](#)。
- [スナップショットを使用して Simple AD を復元する](#)。スナップショットの作成と削除もできます。
- 不要になった [Simple AD を削除します](#)。

Simple AD ディレクトリ情報の表示

で詳細なディレクトリ情報を表示するには AWS Management Console

1. 「[AWS Directory Service コンソール](#)」のナビゲーションペインで、[Active Directory] の下の [ディレクトリ] を選択します。
2. ディレクトリのディレクトリ ID リンクを選択します。ディレクトリに関する情報は、[Directory details] (ディレクトリの詳細) ページに表示されます。

[Status] (ステータス) フィールドの詳細については、「[Simple AD ディレクトリのステータスについて](#)」を参照してください。



Simple AD の DNS サーバーの設定

Simple AD が、Amazon VPC 用に Amazon が提供する DNS サーバーの IP アドレスに DNS リクエストを転送します。これらの DNS サーバーは、Amazon Route 53 プライベートホストゾーンに設定されている名前を解決します。オンプレミスのコンピュータを Simple AD に指定することで、プライベートホストゾーンへの DNS リクエストを解決できるようになりました。Route 53 の詳細については、「[What is Route 53](#)」(Amazon Route 53 とは?) を参照してください。

Simple AD が外部の DNS クエリに応答できるようにするには、Simple AD を含む VPC のネットワークアクセスコントロールリスト (ACL) を、VPC 外からのトラフィックを許可するように設定する必要があります。

- Route 53 プライベートホストゾーンを使用していない場合、DNS リクエストはパブリック DNS サーバーに転送されます。
- VPC の外部にあるカスタム DNS サーバーを使用しており、プライベート DNS を使用する場合は、VPC 内の EC2 インスタンスのカスタム DNS サーバーを使用するように再設定する必要があります。詳細については、「[プライベートホストゾーンの使用](#)」を参照してください。
- Simple AD が VPC 内の DNS サーバーと VPC 外のプライベート DNS サーバーの両方を使用して名前を解決するには、DHCP オプションセットを使用できます。詳細な例については、[この記事](#)を参照してください。
- [Directory Service'DNS 解決と の統合 Amazon Route 53 Resolver](#)。

Note

DNS の動的な更新は、Simple AD ドメインでサポートされていません。ドメインに結合されているインスタンスで DNS Manager を使用してディレクトリに接続し、直接変更を行うこともできます。

スナップショットで Simple AD の復元

AWS Directory Service では、Simple AD ディレクトリのデータの手動スナップショットを作成できます。このスナップショットは、ディレクトリのポイントインタイムの復元に使用できます。AD Connector ディレクトリのスナップショットを作成することはできません。

トピック

- [ディレクトリのスナップショットの作成](#)

- [スナップショットからのディレクトリの復元](#)
- [スナップショットの削除](#)

ディレクトリのスナップショットの作成

ディレクトリのスナップショットを使用することで、それが作成された時点の状態に、対象のディレクトリを復元することができます。ディレクトリのスナップショットを手動で作成するには、以下の手順を実行します。

Note

各ディレクトリに作成できる手動スナップショット数は、5 つまでに制限されています。既にこの制限に達している場合は、新しく作成する前に既存の手動スナップショットのいずれかを削除する必要があります。

スナップショットを手動で作成するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [ディレクトリの詳細] ページで、[メンテナンス] タブを選択します。
4. [Snapshots] (スナップショット) セクションで、[Actions] (アクション)、[Create snapshot] (スナップショットの作成) の順に選択します。
5. [Create directory snapshot] (ディレクトリスナップショットの作成) ダイアログボックスで、必要に応じてスナップショットの名前を入力します。準備が整ったら、[Create] (作成) を選択します。

ディレクトリのサイズによっては、スナップショットの作成に数分かかる場合があります。スナップショットの準備が整うと、[Status] (ステータス) の値が「Completed」に変わります。

スナップショットからのディレクトリの復元

スナップショットからディレクトリを復元することは、ディレクトリを過去の状態に戻すことを意味します。ディレクトリスナップショットは、元となったディレクトリごとに固有です。スナップショットは、元のディレクトリにのみ復元できます。また、手動スナップショットでサポートされる

最大保持期間は 180 日です。詳細については、Microsoft ウェブサイトの「[Active Directory のシステム状態バックアップの有効な保存期間](#)」を参照してください。

 Warning

スナップショットを復元しようとする場合は、事前に [AWS サポート センター](#) までお問合せいただくことをお勧めします。スナップショットを復元する必要性を回避できる場合があります。スナップショットから復元した結果、現時点でのデータが失われる場合があります。この復元処理が完了するまで、ディレクトリに関連付けられているすべての DC および DNS サーバーがオフラインになることを、十分に理解しておいてください。

スナップショットからディレクトリを復元するには、以下の手順を実行します。

スナップショットからディレクトリを復元するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [ディレクトリの詳細] ページで、[メンテナンス] タブを選択します。
4. [Snapshots] (スナップショット) セクションでリストからスナップショットを選択し、[Actions] (アクション)、[Restore snapshot] (スナップショットの復元) の順に選択します。
5. [Restore directory snapshot] (ディレクトリスナップショットの復元) ダイアログボックスで情報を確認した後、[Restore] (復元) をクリックします。

Simple AD ディレクトリの場合、ディレクトリの復元に数分かかる場合があります。正常に復元されると、ディレクトリの [Status] (ステータス) の値が Active に変わります。スナップショット作成後にディレクトリに対して行われた変更は、すべて上書きされます。

スナップショットの削除

スナップショットを削除するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [ディレクトリの詳細] ページで、[メンテナンス] タブを選択します。

4. [Snapshots] (スナップショット) セクションで、[Actions] (アクション)、[Delete snapshot] (スナップショットの削除) の順に選択します。
5. スナップショットを削除することを確認した上で、[Delete] (削除) をクリックします。

Simple AD を削除する

Simple AD を削除すると、ディレクトリデータおよびスナップショットはすべて削除され、元に戻せません。ディレクトリが削除されても、ディレクトリに結合されているインスタンスはすべてそのまま残ります。ただし、ディレクトリの認証情報を使用して、これらのインスタンスにログインすることはできません。これらのインスタンスにログインするには、インスタンス専用のユーザーアカウントを使用します。

AWS Managed Microsoft AD または Simple AD を削除すると、すべてのディレクトリデータとスナップショットが削除され、復元できなくなります。ディレクトリが削除されても、ディレクトリに結合されているインスタンスはすべてそのまま残ります。ただし、ディレクトリの認証情報を使用して、これらのインスタンスにログインすることはできません。これらのインスタンスにログインするには、インスタンス専用のユーザーアカウントを使用します。

AD Connector を削除してもオンプレミスのディレクトリはそのまま残ります。ディレクトリに結合されているインスタンスもすべてそのまま残り、オンプレミスのディレクトリに結合された状態のまま変わりません。引き続き、ディレクトリの認証情報を使用して、このインスタンスにログインできます。

ディレクトリを削除するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。Active Directory がデプロイ AWS リージョン されている いることを確認します。詳細については、「[リージョンの選択](#)」を参照してください。
2. 削除するディレクトリに対して AWS アプリケーションが有効になっていないことを確認します。AWS アプリケーションを有効にすると、AWS Managed Microsoft AD または Simple AD を削除できなくなります。
 - a. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
 - b. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。AWS アプリケーションとサービスセクションには、ディレクトリで有効になっている AWS アプリケーションが表示されます。

- AWS Management Console アクセスを無効にします。詳細については、「[AWS Management Console アクセスの無効化](#)」を参照してください。
- Amazon WorkSpaces を無効にするには、WorkSpaces コンソールでディレクトリからサービスを登録解除する必要があります。詳細については、Amazon WorkSpaces 管理ガイドの「[ディレクトリの削除](#)」を参照してください。
- WorkDocs を無効にするには、WorkDocs コンソールで WorkDocs サイトを削除する必要があります。詳細については、「Amazon WorkDocs Administration Guide」(Amazon WorkDocs 管理ガイド) の「[Delete a site](#)」(サイトを削除する) を参照してください。
- Amazon WorkMail を無効にするには、Amazon WorkMail コンソールで Amazon WorkMail 組織を削除する必要があります。詳細については、「Amazon WorkMail Administrator Guide」(Amazon WorkMail 管理者ガイド) の「[Remove an organization](#)」(組織を削除する) を参照してください。
- Amazon FSx for Windows File Server を無効にするには、ドメインから Amazon FSx ファイルシステムを削除する必要があります。詳細については、「Amazon FSx for Windows File Server User Guide」の「[Working with Active Directory in FSx for Windows File Server](#)」を参照してください。
- Amazon Relational Database Service を無効にするには、ドメインから Amazon RDS インスタンスを削除する必要があります。詳細については、「[Amazon RDS ユーザーガイド](#)」の「ドメインの DB インスタンスの管理」を参照してください。
- AWS Client VPN サービスを無効にするには、クライアント VPN エンドポイントからディレクトリサービスを削除する必要があります。詳細については、「AWS Client VPN 管理者ガイド」の「[Work with Client VPN](#)」を参照してください。
- Amazon Connect を無効にするには、Amazon Connect インスタンスを削除する必要があります。詳細については、「Amazon Connect 管理者ガイド」の「[Delete your Amazon Connect instance](#)」を参照してください。
- Amazon QuickSight を無効にするには、Amazon QuickSight のサブスクリプションを解除する必要があります。詳細については、Amazon QuickSight ユーザーガイドの[Amazon QuickSight 「アカウントの閉鎖」](#)を参照してください。

 Note

を使用して AWS IAM Identity Center、削除予定の AWS Managed Microsoft AD ディレクトリに以前に接続したことがある場合は、削除する前に ID ソースを変

更する必要があります。詳細については、「IAM Identity Center ユーザーガイド」の「[ID ソースを変更する](#)」を参照してください。

3. ナビゲーションペインで [Directories] (ディレクトリ) を選択します。
4. 削除するディレクトリのみを選択し、[Delete] (削除) をクリックします。ディレクトリが削除されるまでに数分かかります。ディレクトリを削除すると、ディレクトリリストからも削除されます。

Simple AD ディレクトリを保護する

このセクションでは、Simple AD 環境を保護する際の考慮事項について説明します。

トピック

- [Simple AD krbtgt アカウントのパスワードをリセットする方法](#)

Simple AD krbtgt アカウントのパスワードをリセットする方法

krbtgt アカウントは、Kerberos チケットの交換で重要な役割を果たします。krbtgt アカウントは、Kerberos チケットを付与するチケット (TGT) の暗号化に使用される特別なアカウントであり、Kerberos 認証プロトコルのセキュリティに重要な役割を果たします。Samba AD では、krbtgt は (無効化された) ユーザーアカウントとして表示されます。このアカウントのパスワードは、ドメインがプロビジョニングされた時点でランダムに生成されます。このシークレットにアクセスすると、新しい Kerberos チケットを監査なしで印刷できるため、検出不能なドメイン侵害が発生する可能性があります。詳細については、「[Samba ドキュメント](#)」を参照してください。

このパスワードは 90 日ごとに定期的に変更することをお勧めします。Simple AD に結合された Amazon EC2 Windows インスタンスから krbtgt アカウントのパスワードをリセットできます。

Note

AWS Simple AD は Samba-AD を使用しています。Samba-AD は krbtgt アカウントのために N-1 ハッシュを保存しません。したがって、krbtgt アカウントのパスワードがリセットされると、Kerberos クライアントは、次のサービスチケット (ST) リクエストの間に新しいチケットを付与するチケット (TGT) をネゴシエートする必要があります。サービスの中断を最小限に抑えるには、krbtgt アカウントのパスワードリセットを営業時間外にスケジュールす

る必要があります。このアプローチにより、進行中のオペレーションへの影響が軽減され、認証の継続性がスムーズになります。

次の手順は、Amazon EC2 Windows インスタンスから krbtgt アカウントのパスワードをリセットする方法を示しています。

前提条件

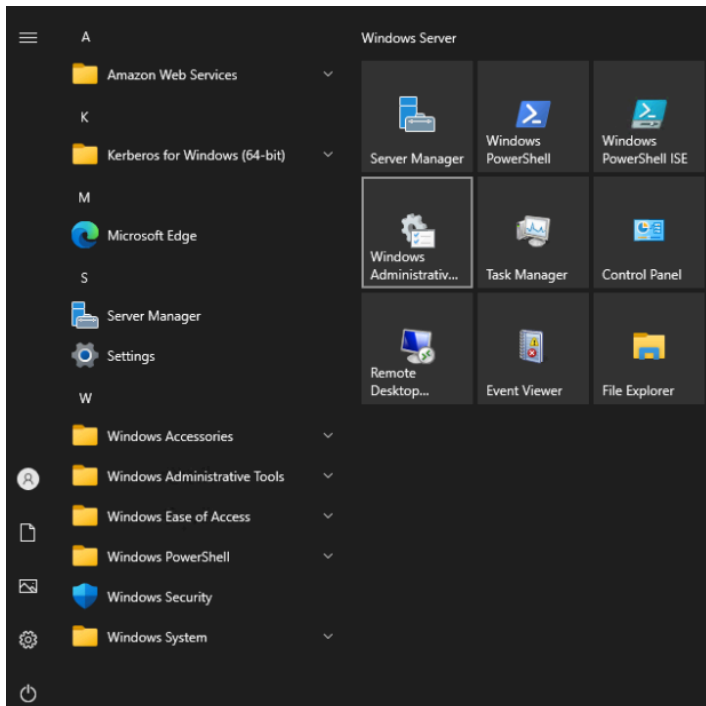
- この手順を開始する前に、以下を完了してください。
- EC2 インスタンスを Simple AD ディレクトリにドメイン結合しました。
- EC2 Windows インスタンスを Simple AD に結合する方法の詳細については、[the section called “Windows インスタンスへの結合”](#) を参照してください。
- Simple AD ディレクトリ管理者認証情報があります。この手順では、Simple AD ディレクトリ管理者としてサインインします。

Note

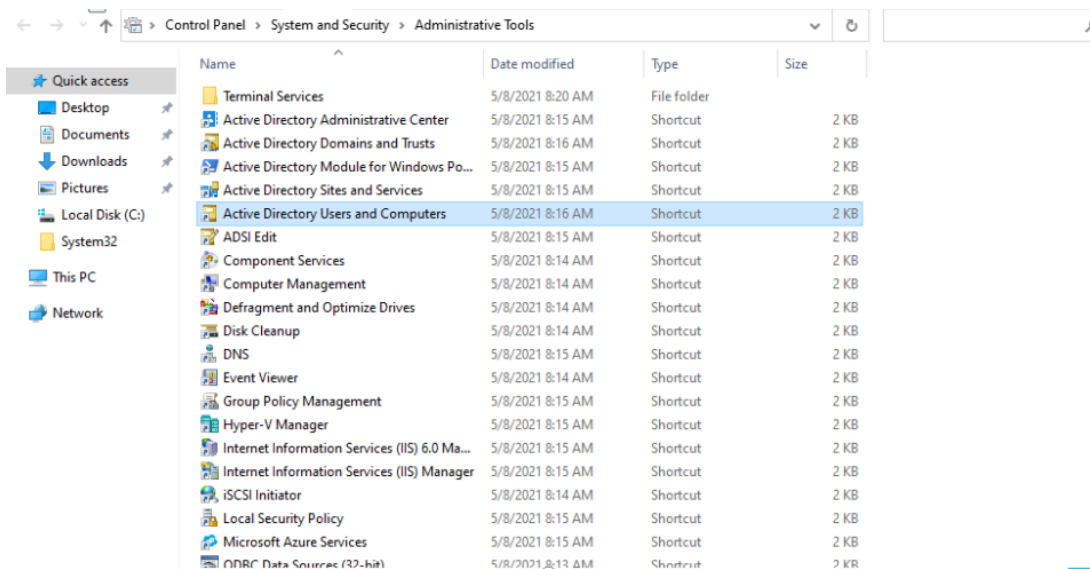
Amazon WorkDocs や Amazon WorkSpaces AWS のサービス などの一部の は、ユーザーに代わって Simple AD を作成します。

Simple AD krbtgt アカウントのパスワードをリセットする

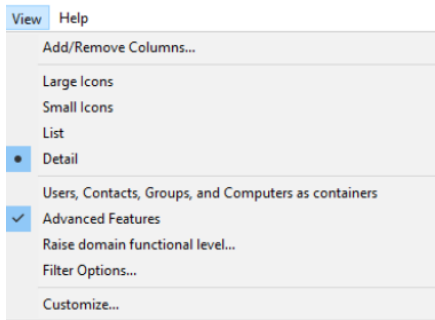
1. Amazon EC2 コンソール (<https://console.aws.amazon.com/ec2/>) を開きます。
2. Amazon EC2 コンソールで [インスタンス] を選択し、Windows Server インスタンスを選択します。次に、[接続] を選択します。
3. [インスタンスに接続] ページで [RDP クライアント] を選択します。
4. [Windows セキュリティ] ダイアログボックスで、Windows サーバーコンピュータにサインインするためのローカル管理者の認証情報をコピーします。ユーザー名を NetBIOS-Name \administrator または DNS-Name \administrator の形式にすることができます。たとえば、[the section called “Simple AD を作成する”](#) の手順に従った場合 corp\administrator はユーザー名になります。
5. Windows Server コンピュータにサインインすると、[Windows 管理ツール] フォルダを選択することで、スタートメニューから [Windows 管理ツール] を開きます。



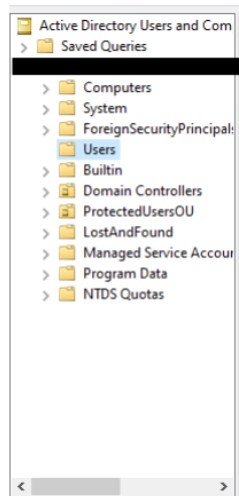
6. Windows 管理ツールダッシュボードで、[Active Directory ユーザーとコンピュータ] を選択して、[Active Directory ユーザーとコンピュータ] を開きます。



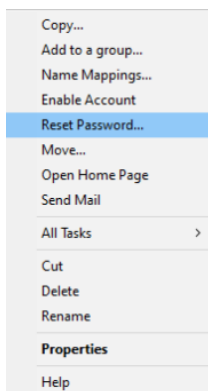
7. [Active Directory ユーザーとコンピュータ] ウィンドウで、[表示] を選択し、[高度な機能を有効にする] を選択します。



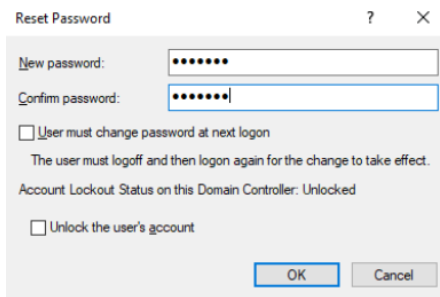
8. [Active Directory ユーザーとコンピュータ] ウィンドウで、左側のパネルから [ユーザー] を選択します。



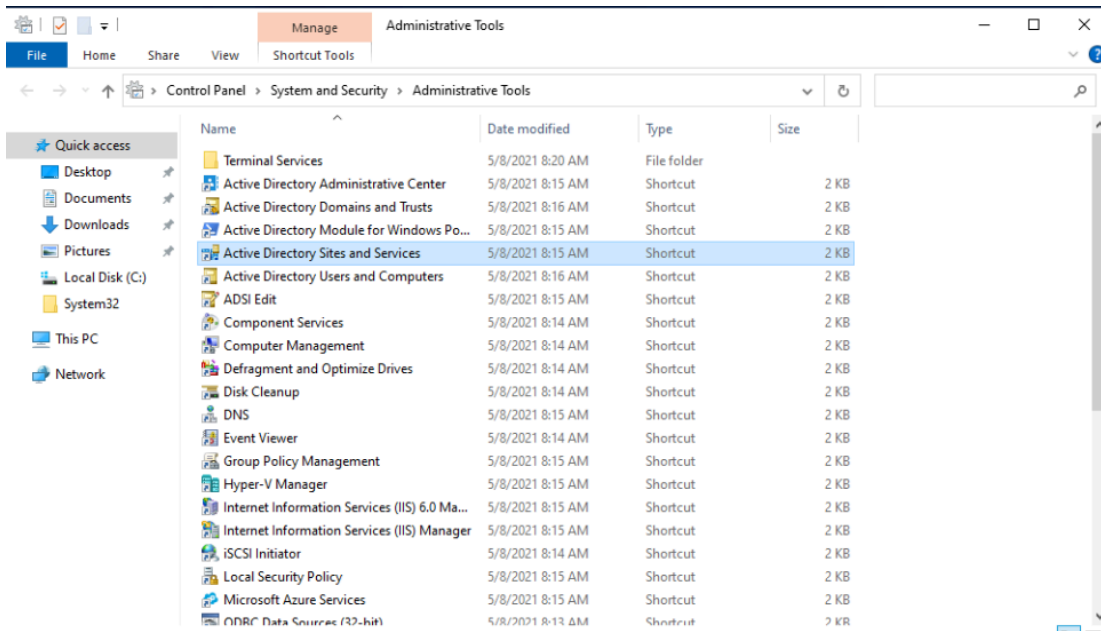
9. [krbtgt] という名前のユーザーを見つけ、右クリックして [パスワードのリセット] を選択します。



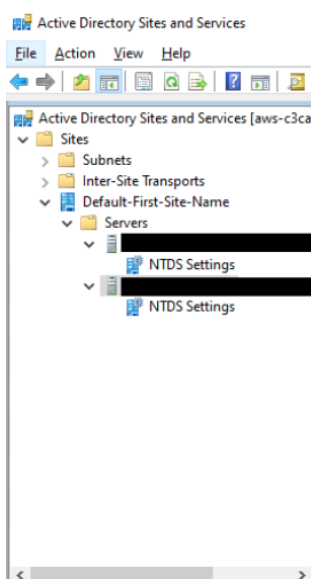
10. 新しいウィンドウで、新しいパスワードを二度入力し、[確認] を選択して krbtgt アカウントのパスワードをリセットします。



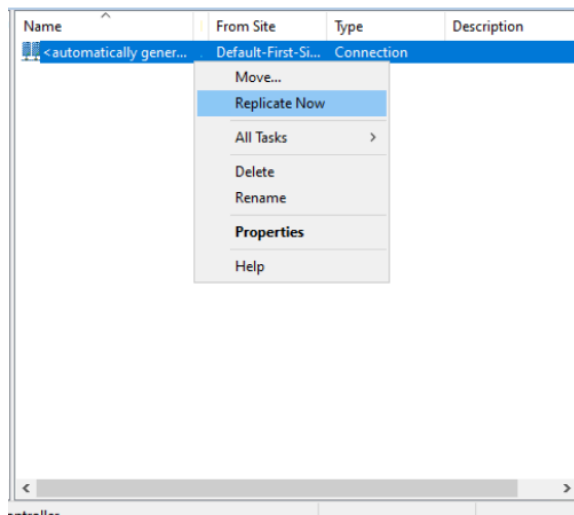
11. Windows 管理ツールダッシュボードで、[Active Directory サイトとサービス] を選択します。



12. Active Directory Sites and Services ウィンドウで、[サイト]、[Default-First-Site-Name]、および [サーバー] を展開します。



13. NTDS 設定ウィンドウで、サーバーを右クリックし、[今すぐレプリケート] を選択します。



14. 他のサーバーに対して、ステップ 13～14 を繰り返します。

Simple AD ディレクトリのモニタリング

Simple AD のさまざまなステータスと、Simple AD にとっての意味について詳しく理解することで、Simple AD を最大限に活用できます。Amazon Simple Notification Service などの AWS サービスを使用して Simple AD をモニタリングすることもできます。Amazon Simple Notification Service は、Simple AD ディレクトリのステータスの通知を送信できます。

Simple AD をモニタリングするタスク

- [Simple AD ディレクトリのステータスについて](#)
- [Amazon Simple Notification Service による Simple AD ディレクトリのステータス通知の有効化](#)

Simple AD ディレクトリのステータスについて

ディレクトリのステータスには以下の種類があります。

[Active] (アクティブ)

ディレクトリは正常に動作しています。ディレクトリには AWS Directory Service が検出した問題はありません。

[Creating] (作成中)

ディレクトリは現在作成中です。ディレクトリの作成には通常 20〜45 分かかりますが、システムの負荷によって異なる場合があります。

[Deleted] (削除済み)

ディレクトリは削除されています。ディレクトリのリソースはすべて解放されています。ディレクトリがこの状態になったら、復元できません。

[Deleting] (削除中)

ディレクトリは削除中です。ディレクトリが完全に削除されるまでは、この状態です。ディレクトリがこの状態になると、削除操作を取り消すことができず、ディレクトリを回復できません。

[Failed] (失敗)

ディレクトリを作成できませんでした。このディレクトリを削除してください。問題が解決しない場合は、[AWS サポート センター](#)までお問い合わせください。

[Impaired] (障害)

ディレクトリがパフォーマンスが低下した状態で実行されています。1 つまたは複数の問題が検出され、すべてのディレクトリのオペレーションが最適に動作しているとは限りません。ディレクトリがこのステータスになるのは、さまざまな原因があり得ます。パッチ適用や EC2 インスタンスのローテーションなど通常の運用メンテナンス、いずれかのドメインコントローラーにおけるアプリケーションの一時的なホットスポットティング、あるいは、ネットワークに行った変更が意図せずディレクトリの通信を妨害するなどです。[Simple AD の前提条件](#) で説明されている設定を変更すると、ディレクトリのステータスが「障害」になる可能性があります。詳細については、「[AWS Managed Microsoft AD のトラブルシューティング](#)」、「[AD Connector のトラブルシューティング](#)」、「[Simple AD のトラブルシューティング](#)」のいずれかを参照してください。通常のメンテナンス関連の問題の場合、AWS は 40 分以内にこれらの問題を解決します。トラブルシューティングのトピックを確認した後も、ディレクトリの障害の状態が 40 分以上続く場合は、[AWS サポート センター](#)までお問い合わせください。

Important

ディレクトリが障害の状態あるときは、スナップショットを復元しないでください。障害の解消にスナップショットの復元が必要になることはほとんどありません。詳細については、「[スナップショットを使用した AWS Managed Microsoft AD の復元](#)」を参照してください。

[Inoperable] (操作不能)

ディレクトリが動作しません。すべてのディレクトリエンドポイントが問題を報告しています。

[Requested] (リクエスト済み)

ディレクトリの作成リクエストは現在保留中です。

[RestoreFailed] (復元失敗)

スナップショットからのディレクトリの復元に失敗しました。復元操作を再試行してください。これが続く場合は、別のスナップショットを試すか、[AWS サポート センター](#)までお問い合わせください。

[Restoring] (復元中)

ディレクトリは現在、自動スナップショットまたは手動スナップショットから復元されています。スナップショットからの復元には、スナップショット内のディレクトリデータのサイズに応じて通常数分かかります。

詳細については、「[Simple AD ディレクトリのステータスメッセージのトラブルシューティング](#)」を参照してください。

Amazon Simple Notification Service による Simple AD ディレクトリのステータス通知の有効化

Amazon Simple Notification Service (Amazon SNS) を使用して、ディレクトリのステータスが変更されたときに E メールまたはテキストメッセージ (SMS) を受け取ることができます。ディレクトリが Active ステータスから [Impaired \(障害\)](#) または [Inoperable \(操作不能\)](#) ステータスに変わると通知されます。ディレクトリが Active ステータスに戻ったときも通知を受け取ります。

仕組み

Amazon SNS では「トピック」を使用してメッセージを収集し、配信します。各トピックには、そのトピックに発行されたメッセージを受け取る 1 人または複数の受信者が存在します。以下のステップを使用して、Amazon SNS トピックにパブリッシャー AWS Directory Service としてを追加できます。はディレクトリのステータスの変更 AWS Directory Service を検出すると、そのトピックにメッセージを発行し、トピックのサブスクライバーに送信します。

発行者として、複数のディレクトリを単一のトピックに関連付けることができます。以前に Amazon SNS で作成したトピックに、ディレクトリステータスのメッセージを追加することもできます。ト

ピックの発行者と受信者は詳細に管理できます。Amazon SNS の詳細については、「[Amazon SNS とは](#)」を参照してください。

ディレクトリの SNS メッセージングを有効にするには

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Maintenance] (メンテナンス) タブを選択します。
4. [Directory monitoring] (ディレクトリのモニタリング) セクションで [Actions] (アクション) をクリックし、[Create notification] (通知の作成) をクリックします。
5. [Create notification] (通知の作成) ページで、[Choose a notification type] (通知タイプを選択) をクリックしてから、[Create a new notification] (新しい通知の作成) を選択します。または、既存の SNS トピックがある場合は、[Associate with existing SNS topic] (既存の SNS トピックに関連付ける) を選択し、このディレクトリからそのトピックにステータスメッセージを送信できます。

 Note

[Create a new notification] (新しい通知の作成) を選択した場合でも、既存の SNS トピックと同じトピック名を使用すると、Amazon SNS は新しいトピックを作成せずに、既存のトピックに新しいサブスクリプション情報を追加するだけです。

[Associate with existing SNS topic] (既存の SNS トピックに関連付ける) を選択した場合は、ディレクトリと同じリージョンにある SNS トピックのみを選択できます。

6. [Recipient type] (受信タイプ) を選択し、[Recipient] (受信者) の連絡先情報を入力します。SMS の電話番号を入力する場合は、数字のみを入力します。ハイフン、スペース、括弧を含めないでください。
7. (オプション) トピックの名前と SNS 表示名を入力します。表示名は、このトピックから送信されるすべての SMS メッセージに含まれる短縮名 (最大 10 文字) です。SMS オプションを使用する場合、表示名は必須です。

 Note

IAM ユーザーまたは [DirectoryServiceFullAccess](#) 管理ポリシーのみを持つロールを使用してログインしている場合、トピック名は「DirectoryMonitoring」で始まる必要があります。トピック名をさらにカスタマイズするには、SNS の権限が追加が必要です。

8. [Create] (作成) を選択します。

追加の E メールアドレス、Amazon SQS キュー、など、追加の SNS サブスクライバーを指定する場合は AWS Lambda、[Amazon SNS コンソール](#)から指定できます。

トピックからディレクトリステータスメッセージを削除するには

1. にサインイン AWS Management Console し、[AWS Directory Service コンソール](#)を開きます。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Maintenance] (メンテナンス) タブを選択します。
4. [Directory monitoring] (ディレクトリのモニタリング) セクションでリストから SNS トピック名を選択し、[Actions] (アクション) をクリックして、[Remove] (削除) を選択します。
5. [Remove] (削除) をクリックします。

これで、選択した SNS トピックへの発行者であるディレクトリが削除されます。トピック全体を削除する場合は、「[Amazon SNS コンソール](#)」から削除できます。

Note

SNS コンソールを使用して Amazon SNS トピックを削除する前に、ディレクトリがそのトピックにステータスメッセージを送信していないことを確認する必要があります。

SNS コンソールを使用して Amazon SNS トピックを削除した場合、この変更は Directory Services コンソール内にはすぐに反映されません。この削除済みトピックに対して、次回、ディレクトリから通知が発行されたときに初めて変更が反映され、トピックが見つからないという最新のステータスがディレクトリの [Monitoring] (モニタリング) タブに表示されます。

したがって、重要なディレクトリステータスメッセージが欠落しないようにするには、メッセージを受信するトピックを削除する前に AWS Directory Service、ディレクトリを別の Amazon SNS トピックに関連付けます。

Simple AD から AWS アプリケーションとサービスへのアクセス

Simple AD ユーザーにアクセス権限を付与して、AWS アプリケーションやサービスにアクセスできます。これらの AWS アプリケーションとサービスには、次のようなものがあります。

- Amazon WorkDocs

- AWS Management Console
- Amazon WorkSpaces

Simple AD では、アクセス URL とシングルサインオンを使用することもできます。

トピック

- [Simple AD のアプリケーション互換性ポリシー](#)
- [Simple AD の AWS アプリケーションとサービスへのアクセスの有効化](#)
- [Simple AD 認証情報 AWS Management Console を使用した へのアクセスの有効化](#)
- [Simple AD のアクセス URL の作成](#)
- [シングルサインオンの有効化](#)

Simple AD のアプリケーション互換性ポリシー

Simple AD は、Active Directory の多くの基本機能を提供する Samba の実装です。Active Directory を使用するカスタムおよび商用off-the-shelfアプリケーションは多数ある AWS ため、は Simple AD とのサードパーティーアプリケーションの互換性を正式にも広範にも検証しません。は、アプリケーションのインストールで発生する可能性のある課題を克服するためにお客様と AWS 連携しますが、アプリケーションが Simple AD と互換性があること、または互換性が維持されることは保証できません。

次のサードパーティー製アプリケーションは、Simple AD と互換性があります。

- Microsoft Internet Information Services (IIS) は、次のプラットフォームで使用できます。
 - 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 および Standard エディション)
 - SQL Server 2008 R2 (Express、Web、および Standard エディション)
 - SQL Server 2012 (Express、Web、および Standard エディション)
 - SQL Server 2014 (Express、Web、および Standard エディション)

- Microsoft SharePoint:
 - SharePoint 2010 Foundation
 - SharePoint 2010 Enterprise
 - SharePoint 2013 Enterprise

お客様は、AWS 実際の Active Directory に基づいて、より高いレベルの互換性のために Directory Service for Microsoft Active Directory ([AWS Managed Microsoft AD](#)) を使用することを選択できます。

Simple AD の AWS アプリケーションとサービスへのアクセスの有効化

ユーザーは Simple AD を承認して、Amazon WorkSpaces などの AWS アプリケーションやサービスへのアクセスを許可できます。Simple AD を操作するには、次の AWS アプリケーションとサービスを有効または無効にできます。

AWS アプリケーション/サービス	詳細情報
Amazon WorkDocs	詳細については、「 Amazon WorkDocs 管理ガイド 」を参照してください。
Amazon WorkMail	詳細については、「 Amazon WorkMail 管理者ガイド 」を参照してください。
Amazon WorkSpaces	WorkSpaces から、Simple AD、AWS Microsoft AD、または AD Connector を直接作成することが可能です。このためには単純に、Workspace の作成時に [Advanced Setup] (高度なセットアップ) を起動します。 詳細については、「 Amazon WorkSpaces 管理ガイド 」を参照してください。
AWS Management Console	詳細については、「 AWS Managed Microsoft AD 認証情報を使用した AWS Management Console アクセスの有効化 」を参照してください。

有効化の完了後は、ディレクトリへのアクセス権限を付与したアプリケーションまたはサービスのコンソールから、そのディレクトリへのアクセスを管理します。AWS Directory Service コンソールで上記のアプリケーションとサービスのリンクを見つける AWS には、次の手順を実行します。

ディレクトリにアクセスしているアプリケーションおよびサービスを表示するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. [AWS apps & services] (AWS アプリおよびサービス) セクションでリストを確認します。

を使用して AWS アプリケーションとサービスを認可または認可解除する方法の詳細については [AWS Directory Service](#)、[「 」を参照してください](#) [を使用した AWS アプリケーションとサービスの認可](#) [AWS Directory Service](#)。

Simple AD 認証情報 AWS Management Console を使用した へのアクセスの有効化

AWS Directory Service では、ディレクトリのメンバーに へのアクセスを許可できます AWS Management Console。デフォルトでは、ディレクトリメンバーは AWS リソースにアクセスできません。ディレクトリメンバーに IAM ロールを割り当てて、さまざまな AWS サービスとリソースへのアクセスを許可します。IAM ロールでは、ディレクトリメンバーに付与するサービス、リソース、およびアクセス権限のレベルを定義します。

ディレクトリメンバーにコンソールへのアクセス権限を付与する際には、ディレクトリにアクセスするための URL を設定しておく必要があります。ディレクトリの詳細表示およびアクセス URL の取得に関する詳細は、「[AWS Managed Microsoft AD ディレクトリ情報の表示](#)」を参照してください。アクセス URL 作成方法の詳細については、「[AWS Managed Microsoft AD のアクセス URL の作成](#)」を参照してください。

IAM ロールを作成し、ディレクトリメンバーに割り当てる方法に関する詳細については「[AWS Managed Microsoft AD ユーザーとグループに IAM ロールを持つリソースへのアクセス権 AWS を付与する](#)」を参照してください。

トピック

- [AWS Management Console アクセスの有効化](#)
- [AWS Management Console アクセスの無効化](#)
- [ログインセッション期間の設定](#)

関連する AWS セキュリティブログ記事

- [AWS Managed Microsoft AD とオンプレミス認証情報 AWS Management Console を使用して にアクセスする方法](#)

関連 AWS re:Post 記事

- [AWS Management Console オンプレミスActive Directoryユーザーに へのアクセスを許可するにはどうすればよいですか？](#)

AWS Management Console アクセスの有効化

デフォルトでは、コンソールへのアクセスが有効化されたディレクトリはありません。ディレクトリのユーザーおよびグループによるコンソールアクセスを有効にするには、以下の手順を実行します。

コンソールアクセスを有効にするには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. AWS Management Console セクションで、[Enable] (有効) をクリックします。ディレクトリに対するコンソールアクセスが有効になりました。

Important

ユーザーがアクセス URL を使用してコンソールにサインインできるようにするには、まず、そのユーザーを IAM ロールに追加しておく必要があります。IAM ロールへのユーザーの割り当てに関する一般情報については、「[既存の IAM ロールにユーザーまたはグループを割り当てる](#)」を参照してください。IAM ロールの割り当てが完了したユーザーは、アクセス URL を使用してコンソールにアクセスできるようになります。例えば、

ディレクトリのアクセス URL が example-corp.awsapps.com である場合、コンソールへアクセスするための URL は、https://example-corp.awsapps.com/console/ となります。

AWS Management Console アクセスの無効化

ディレクトリのユーザーおよびグループによるコンソールアクセスを無効にするには、以下の手順を行います。

コンソールアクセスを無効化するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. AWS Management Console セクションで、[Disable] (無効) をクリックします。これで、ディレクトリからのコンソールアクセスが無効化されます。
5. IAM ロールがディレクトリ内のユーザーまたはグループに割り当てられている場合、[Disable] (無効) ボタンは使用できない場合があります。この場合は、先に進む前に、ディレクトリのすべての IAM ロールの割り当てを削除します。これには、ディレクトリから削除されたユーザー ([Deleted User] (削除されたユーザー) に表示) またはグループ ([Deleted Group] (削除されたグループ) に表示) への割り当ても含まれます。

すべての IAM ロールの割り当てが削除されたら、上記の手順を繰り返します。

ログインセッション期間の設定

デフォルトでは、ユーザーがコンソールにサインインしてから 1 時間経過すると、このセッションからログアウトされます。この場合、再度サインインしてセッションを開始する必要がありますが、1 時間後経過すると、再度このセッションからログオフされます。以下の手順により、使用期間をセッションごとに最大 12 時間に延長することができます。

ログインセッション期間の長さを設定するには

1. [AWS Directory Service コンソール](#)のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。

2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. [AWS apps & services] (AWS アプリおよびサービス) セクションで、[Management Console] (マネジメントコンソール) を選択します。
5. AWS リソースへのアクセスの管理ダイアログボックスで、続行を選択します。
6. [Assign users and groups to IAM roles] (ユーザーおよびグループの IAM ロールへの割り当て) ページの [Set login session length] (ログインセッション期間の設定) で数値を編集し、[Save] (保存) をクリックします。

Simple AD のアクセス URL の作成

アクセス URL は、Amazon WorkDocs などの AWS アプリケーションやサービスで使用され、ディレクトリに関連付けられたログインページにアクセスします。URL はグローバルに一意である必要があります。以下の手順を実行して、ディレクトリのアクセス URL を作成できます。

Warning

このディレクトリのアプリケーションアクセス URL は、作成した後では変更できません。アクセス URL が作成された後は、他のユーザーが使用することはできません。ディレクトリを削除すると、アクセス URL も削除され、他のアカウントで使用することができます。

アクセス URL を作成するには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) を選択します。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. [Application access URL] (アプリケーションのアクセス URL) セクションで、ディレクトリにアクセス URL が割り当てられていない場合は、[Create] (作成) ボタンが表示されます。ディレクトリのエイリアスを入力し、[Create] (作成) をクリックします。「Entity Already Exists (エンティティは既に存在しています)」というエラーが返された場合は、指定したディレクトリのエイリアスは割り当て済みです。別のエイリアスを選択して、この手順を繰り返します。

アクセス URL は、`<alias>.awsapps.com` の形式で表示されます。

シングルサインオンの有効化

AWS Directory Service は、ユーザーが認証情報を個別に入力することなく、ディレクトリに結合されたコンピュータから WorkDocs にアクセスできるようにする機能を提供します。

シングルサインオンを有効にする前に、ユーザーのウェブブラウザでシングルサインオンをサポートさせるための、追加の手順を実行する必要があります。ユーザーは、シングルサインオンを有効にするために、ウェブブラウザで設定の変更が必要な場合があります。

Note

シングルサインオンは、AWS Directory Service ディレクトリに結合されているコンピュータで使用された場合にのみ機能します。このディレクトリに結合されていないコンピュータでは使用できません。

ディレクトリに AD Connector ディレクトリを使用しており、AD Connector サービスアカウントがそのサービスプリンシパル名属性を追加または削除するためのアクセス許可を持っていない場合、下記のステップ 5 とステップ 6 では、2 つのオプションが選択できます。

1. 続行した場合、AD Connector サービスアカウントのサービスプリンシパル名属性を追加または削除するアクセス許可を持つディレクトリユーザーのユーザー名とパスワードの入力を求められます。これらの認証情報は、シングルサインオンを有効にする目的でのみ使用され、サービスで保存されることはありません。AD Connector サービスアカウントのアクセス許可は変更されません。
2. AD Connector サービスアカウントには、それ自体のサービスプリンシパル名属性を追加または削除するための権限を委任できます。AD Connector サービスアカウントのアクセス許可を変更する権限を持つアカウントを使用して、ドメインに結合済みコンピュータから次の PowerShell コマンドを実行します。次のコマンドは、AD Connector サービスアカウントに対して、それ自体のサービスプリンシパル名属性のみを追加および削除することを許可します。

```
$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"
```

WorkDocs でシングルサインオンを有効または無効にするには

1. [AWS Directory Service コンソール](#) のナビゲーションペインで、[Directories] (ディレクトリ) をクリックします。
2. [Directories] (ディレクトリ) ページで、ディレクトリ ID を選択します。
3. [Directory details] (ディレクトリの詳細) ページで、[Application management] (アプリケーション管理) タブを選択します。
4. アプリケーションアクセス URL セクションで、有効 を選択して WorkDocs のシングルサインオンを有効にします。

[Enable] (有効) ボタンが表示されていない場合は、最初にアクセス URL を作成すると、このオプションが表示されます。アクセス URL 作成方法の詳細については、「[AWS Managed Microsoft AD のアクセス URL の作成](#)」を参照してください。

5. [Enable Single Sign-On for this directory] (このディレクトリのシングルサインオンの有効化) ダイアログボックスで、[Enable] (有効) をクリックします。ディレクトリのシングルサインオンが有効に設定されます。
6. 後で WorkDocs でシングルサインオンを無効にする場合は、Disable を選択し、このディレクトリのシングルサインオンを無効にするダイアログボックスでもう一度 Disable を選択します。

トピック

- [IE および Chrome でのシングルサインオン](#)
- [Firefox でのシングルサインオン](#)

IE および Chrome でのシングルサインオン

Microsoft Internet Explorer (IE) および Google Chrome ブラウザでシングルサインオンを使用するには、クライアントコンピュータで以下のタスクを実行する必要があります。

- シングルサインオンが承認済みサイトのリストに、アクセス URL (例: `https://<alias>.awsapps.com`) を追加します。
- アクティブなスクリプト (JavaScript) を有効にします。
- 自動ログオンを許可します。
- 統合された認証を有効にします。

ユーザーは、これらのタスクを手動で実行するか、対象の設定を、グループポリシーの設定を通じて変更することができます。

トピック

- [Windows シングルサインオン用の手動アップデート](#)
- [OS X でシングルサインオンを設定するための手動アップデート](#)
- [シングルサインオンのグループポリシー設定](#)

Windows シングルサインオン用の手動アップデート

Windows コンピュータでのシングルサインオンを手動で有効にするには、クライアントコンピュータで以下の手順を行います。これらの設定の一部については、適切に事前設定が行われています。

Windows 上で Internet Explorer および Chrome のシングルサインオンを手動で有効にするには

1. [Internet Properties] (インターネットプロパティ) ダイアログボックスを開くには、[Start] (スタート) メニューを開き、検索ボックスに「Internet Options」と入力した上で、[Internet Options] (インターネットオプション) をクリックします。
2. 承認済みサイトのリストにアクセス URL を追加してシングルサインオンを設定するには、以下の手順を実行します。

- a. [Internet Properties] (インターネットプロパティ) ダイアログボックスで [Security] (セキュリティ) タブを開きます。
 - b. [Local intranet] (ローカルイントラネット)、[Sites] (サイト) の順に選択します。
 - c. [Local intranet] (ローカルイントラネット) ダイアログボックスで、[Advanced] (詳細) をクリックします。
 - d. ウェブサイトのリストにアクセス URL を追加した後、[Close] (閉じる) をクリックします。
 - e. [Local intranet] (ローカルイントラネット) ダイアログボックスで、[OK] をクリックします。
3. アクティブスクリプトを有効にするには、以下の手順を行います。
- a. [Internet Properties] (インターネットのプロパティ) ダイアログボックスの [Security] (セキュリティ) タブで、[Custom level] (カスタムレベル) をクリックします。
 - b. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、下部にある [Scripting] (スクリプト) までスクロールし、[Active scripting] (アクティブスクリプト) の下で [Enable] (有効) をクリックします。
 - c. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、[OK] をクリックします。
4. 自動ログオンを有効にするには、以下の手順を実行します。
- a. [Internet Properties] (インターネットのプロパティ) ダイアログボックスの [Security] (セキュリティ) タブで、[Custom level] (カスタムレベル) をクリックします。
 - b. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、下部の [User Authentication] (ユーザー認証) までスクロールし、[Logon] (ログオン) にある [Automatic logon only in Intranet zone] (イントラネットゾーン内のみで自動ログオンを認証する) をクリックします。
 - c. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、[OK] をクリックします。
 - d. [Security Settings - Local Intranet Zone] (セキュリティ設定 – ローカルイントラネットゾーン) ダイアログボックスで、[OK] をクリックします。
5. 統合された認証を有効にするには、以下の手順を行います。
- a. [Internet Properties] (インターネットのプロパティ) ダイアログボックスで、[Advanced] (詳細) タブを表示します。

- b. 下部にある [Security] (セキュリティ) までスクロールし、[Enable Integrated Windows Authentication] (Windows 認証の統合を有効化する) をクリックします。
 - c. [Internet Properties] (インターネットプロパティ) ダイアログボックスで、[OK] をクリックします。
6. これらの変更を適用するためにブラウザを再起動します。

OS X でシングルサインオンを設定するための手動アップデート

シングルサインオンを、OS X の Chrome 向けに手動で有効化するには、クライアントコンピュータで以下の手順を実行します。これらの手順を完了させるには、コンピュータの管理者権限が必要です。

OS X で Chrome 向けのシングルサインオンを手動で有効にするには

1. 次のコマンドを実行し、アクセス URL を [AuthServerAllowlist](#) ポリシーに追加します。

```
defaults write com.google.Chrome AuthServerAllowlist "https://<alias>.awsapps.com"
```

2. [System Preferences] (システム設定) を開き、[Profiles] (プロファイル) パネルに移動して、Chrome Kerberos Configuration プロファイルを削除します。
3. Chrome を再起動して `chrome://policy` を開き、新しい設定が適用されていることを確認します。

シングルサインオンのグループポリシー設定

ドメイン管理者は、グループポリシー設定を実装することで、ドメインに結合しているクライアントコンピュータでのシングルサインオンの設定を変更できるようになります。

Note

Chrome のポリシーを適用したドメインのコンピュータで Chrome ウェブブラウザを管理している場合は、アクセス URL を [AuthServerAllowlist](#) ポリシーに追加する必要があります。Chrome ポリシーの設定に関する詳細については、「[Policy Settings in Chrome](#)」(Chrome のポリシー設定) を参照してください。

グループポリシー設定を使用して Internet Explorer および Chrome のシングルサインオンを有効にするには

1. 以下の手順を実行し、新しいグループポリシーオブジェクトを作成します。
 - a. グループポリシー管理ツールを開き、対象のドメインに移動して [Group Policy Objects] (グループポリシーオブジェクト) をクリックします。
 - b. メインメニューで、[Action] (アクション)、[New] (新規) の順に選択します。
 - c. [New GPO] (新しい GPO) ダイアログボックスで、グループポリシーオブジェクトのために識別しやすい名前 (IAM Identity Center Policy など) を入力します。また、[Source Starter GPO] (ソース スターター GPO) は 「(none)」 のままにします。[OK] をクリックします。
2. アクセス URL を承認済みサイトのリストに追加してシングルサインオンを設定するには、以下の手順を実行します。
 - a. グループポリシー管理ツールで、使用するドメインに移動し、[Group Policy Objects] (グループポリシーオブジェクト) を選択します。次に、右クリックで IAM Identity Center ポリシーのコンテキスト メニューを開き、[Edit] (編集) を選択します。
 - b. ポリシーツリー内で、[User Configuration] (ユーザーの設定)、[Preferences] (設定)、[Windows Settings] (Windows の設定) の順に選択します。
 - c. [Windows Settings] (Windows の設定) リストから、[Registry] (レジストリ) のコンテキストメニューを右クリックで開き、[New registry item] (新規のレジストリ項目) を選択します。
 - d. [New Registry Properties] (新規レジストリ設定) ダイアログボックスで、以下の設定を入力した上で [OK] をクリックします。

[Action] (アクション)

Update

[Hive]

HKEY_CURRENT_USER

[Path] (パス)

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

`<alias>` の値は、アクセス URL から抽出します。アクセス URL が `https://examplecorp.awsapps.com` の場合、エイリアスは `examplecorp` となり、レジストリキーは `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp` になります。

[Value name] (値の名前)

`https`

[Value type] (値の型)

`REG_DWORD`

[Value data] (値のデータ)

`1`

3. アクティブスクリプトを有効にするには、以下の手順を行います。

- a. グループポリシー管理ツールで、使用するドメインに移動し、[Group Policy Objects] (グループポリシーオブジェクト) を選択します。次に、右クリックで IAM Identity Center ポリシーのコンテキスト メニューを開き、[Edit] (編集) を選択します。
- b. ポリシーツリー内で、[Computer Configuration] (コンピュータの設定)、[Policies] (ポリシー)、[Administrative Templates] (管理テンプレート)、[Windows Components] (Windows コンポーネント)、[Internet Explorer]、[Internet Control Panel] (インターネットコントロールパネル)、[Security Page] (セキュリティページ)、[Intranet Zone] (イントラネットゾーン) の順に選択します。
- c. [Intranet Zone] (イントラネットゾーン) リストで、右クリックにより [Allow active scripting] (アクティブスクリプトの許可) のコンテキストメニューを開き、[Edit] (編集) を選択します。
- d. [Allow active scripting] (アクティブスクリプトの許可) ダイアログボックスで、以下の設定を入力した上で [OK] をクリックします。
 - [Enabled] (有効) ラジオボタンをオンにします。
 - [Options] (オプション) で、[Allow active scripting] (アクティブスクリプトを許可する) を「Enable」(有効) に設定します。

4. 自動ログオンを有効にするには、以下の手順を実行します。

- a. グループポリシー管理ツールで、対象のドメインに移動しグループポリシーオブジェクトを選択します。次に、右クリックで SSO ポリシーのコンテキストメニューを開き、[Edit] (編集) を選択します。
 - b. ポリシーツリー内で、[Computer Configuration] (コンピュータの設定)、[Policies] (ポリシー)、[Administrative Templates] (管理テンプレート)、[Windows Components] (Windows コンポーネント)、[Internet Explorer]、[Internet Control Panel] (インターネットコントロールパネル)、[Security Page] (セキュリティページ)、[Intranet Zone] (イントラネットゾーン) の順に選択します。
 - c. [Intranet Zone] (イントラネットゾーン) リストで、右クリックにより [Logon options] (ログオンオプション) のコンテキストメニューを開き、[Edit] (編集) を選択します。
 - d. [Logon options] (ログオンオプション) ダイアログボックスで、以下の設定を入力した上で [OK] を選択します。
 - [Enabled] (有効) ラジオボタンをオンにします。
 - [Options] (オプション) で、[Logon options] (ログオンオプション) に [Automatic logon only in Intranet zone] (イントラネットゾーン内のみで自動ログオンを認証する) を設定します。
5. 統合された認証を有効にするには、以下の手順を行います。
- a. グループポリシー管理ツールで、使用するドメインに移動し、[Group Policy Objects] (グループポリシーオブジェクト) を選択します。次に、右クリックで IAM Identity Center ポリシーのコンテキストメニューを開き、[Edit] (編集) を選択します。
 - b. ポリシーツリー内で、[User Configuration] (ユーザーの設定)、[Preferences] (設定)、[Windows Settings] (Windows の設定) の順に選択します。
 - c. [Windows Settings] (Windows の設定) リストから、[Registry] (レジストリ) のコンテキストメニューを右クリックで開き、[New registry item] (新規のレジストリ項目) を選択します。
 - d. [New Registry Properties] (新規レジストリ設定) ダイアログボックスで、以下の設定を入力した上で [OK] をクリックします。

[Action] (アクション)

Update

[Hive]

HKEY_CURRENT_USER

[Path] (パス)

Software\Microsoft\Windows\CurrentVersion\Internet Settings

[Value name] (値の名前)

EnableNegotiate

[Value type] (値の型)

REG_DWORD

[Value data] (値のデータ)

1

6. 開いている場合は、[Group Policy Management Editor] (グループポリシー管理エディタ) ウィンドウを閉じます。
7. 次の手順を実行し、ドメインに新しいポリシーを割り当てます。
 - a. [グループポリシーの管理] ツリーで、右クリックによりドメインのコンテキストメニューを開き、[Link an Existing GPO] (既存の GPO をリンク) を選択します。
 - b. [Group Policy Objects] (グループポリシーオブジェクト) リストで、IAM Identity Center ポリシーを選択し、[OK] を選択します。

この変更は、クライアントが次にグループポリシーを更新した後、または次のユーザーログインの後に適用されます。

Firefox でのシングルサインオン

Mozilla Firefox ブラウザでシングルサインオンのサポートを許可するには、アクセス URL (例: <https://<alias>.awsapps.com>) を、シングルサインオン承認済みサイトのリストに追加します。この設定は、手動で行うことも、スクリプトを使用して自動で行うこともできます。

トピック

- [シングルサインオンのための手動による更新](#)
- [シングルサインオンのための自動によるアップデート](#)

シングルサインオンのための手動による更新

Firefox の承認済みサイトのリストに手動でアクセス URL を追加するには、クライアントコンピュータで以下の手順を実行します。

Firefox の承認済みサイトのリストに手動でアクセス URL を追加するには

1. Firefox を開いて、`about:config` ページに移動します。
2. `network.negotiate-auth.trusted-uris` の設定を開き、アクセス URL をサイトのリストに追加します。複数のエントリを設定するには、それぞれをカンマ (,) で区切ります。

シングルサインオンのための自動によるアップデート

ドメインの管理者であれば、ネットワークにあるすべてのコンピュータに対し、Firefox の `network.negotiate-auth.trusted-uris` ユーザー設定にアクセス URL を追加するためのスクリプトを使用できます。詳細については、<https://support.mozilla.org/en-US/questions/939037> にアクセスしてください。

Amazon EC2 インスタンスを Simple AD に結合する方法

インスタンスを起動したときに Amazon EC2 インスタンスを Active Directory ドメインにシームレスに結合できます。詳細については、「[Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD に結合する Active Directory](#)」を参照してください。EC2 インスタンスを起動し、[AWS Systems Manager オートメーション](#)を使用して AWS Directory Service コンソールから直接 Active Directory ドメインに参加することもできます。

手動で EC2 インスタンスを Active Directory ドメインに結合する必要がある場合は、適切なリージョン、セキュリティグループまたはサブネットでインスタンスを起動して、そのインスタンスをドメインに結合する必要があります。

これらのインスタンスにリモート接続できるようにするには、接続元のネットワークからインスタンスへの IP 接続が必要です。ほとんどの場合、これには、インターネットゲートウェイが VPC にアタッチされていることと、インスタンスにパブリック IP アドレスがあることが必要です。

トピック

- [Amazon EC2 Windows インスタンスを Simple AD Active Directory に結合する](#)
- [Amazon EC2 Linux インスタンスを Simple AD アクティブディレクトリに結合する](#)
- [Simple AD のディレクトリ結合権限を委任する](#)

- [Simple AD の DHCP オプションセットの作成](#)

Amazon EC2 Windows インスタンスを Simple AD Active Directory に結合する

Amazon EC2 Windows インスタンスを起動して Simple AD に結合できます。または、既存の EC2 Windows インスタンスを Simple AD に手動で結合することもできます。

Seamlessly join an EC2 Windows

EC2 インスタンスをシームレスにドメイン結合するには、以下を完了する必要があります。

前提条件

- シンプルな AD を使用する 詳細については、「」を参照してください[Simple AD を作成する](#)。
- EC2 Windows インスタンスをシームレスに結合するには、次の IAM アクセス許可が必要です。
 - 次の IAM アクセス許可を持つ IAM インスタンスプロファイル：
 - AmazonSSMManagedInstanceCore
 - AmazonSSMDirectoryServiceAccess
 - EC2 を Simple AD にシームレスに結合するユーザーには、次の IAM アクセス許可が必要です。
 - AWS Directory Service アクセス許可：
 - "ds:DescribeDirectories"
 - "ds:CreateComputer"
 - Amazon VPC のアクセス許可：
 - "ec2:DescribeVpcs"
 - "ec2:DescribeSubnets"
 - "ec2:DescribeNetworkInterfaces"
 - "ec2:CreateNetworkInterface"
 - "ec2:AttachNetworkInterface"
 - EC2 アクセス許可：
 - "ec2:DescribeInstances"
 - "ec2:DescribeImages"

- "ec2:DescribeInstanceTypes"
- "ec2:RunInstances"
- "ec2:CreateTags"
- AWS Systems Manager アクセス許可 :
 - "ssm:DescribeInstanceInformation"
 - "ssm:SendCommand"
 - "ssm:GetCommandInvocation"
 - "ssm:CreateBatchAssociation"

Simple AD が作成されると、インバウンドルールとアウトバウンドルールを使用してセキュリティグループが作成されます。これらのルールとポートの詳細については、「」を参照してください[Simple AD で作成されるもの](#)。EC2 Windows インスタンスをシームレスにドメイン結合するには、インスタンスを起動する VPC で、Simple AD セキュリティグループのインバウンドルールとアウトバウンドルールで許可されているのと同じポートを許可する必要があります。

- ネットワークセキュリティとファイアウォールの設定によっては、追加のアウトバウンドトラフィックを許可する必要がある場合があります。このトラフィックは、次のエンドポイントへの HTTPS (ポート 443) 用になります。

Endpoint	ロール
ec2messages. <i>region</i> .amazonaws.com	Session Manager サービスを使用してセッションチャネルを作成および削除します。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。
ssm. <i>region</i> .amazonaws.com	このエンドポイント AWS Systems Manager Session Manager。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。

Endpoint	ロール
ssmmessages. <i>region</i> .amazonaws.com	Session Manager サービスを使用してセッションチャネルを作成および削除します。詳細については、「 AWS Systems Manager エンドポイントとクォータ 」を参照してください。
ds. <i>region</i> .amazonaws.com	のエンドポイント AWS Directory Service。詳細については、「 のリージョンの可用性 AWS Directory Service 」を参照してください。

- Simple AD ドメイン名を解決する DNS サーバーを使用することをお勧めします。そのためには、DHCP オプションセットを作成できます。詳細については「[Simple AD の DHCP オプションセットの作成](#)」を参照してください。
 - DHCP オプションセットを作成しない場合、DNS サーバーは静的になり、Simple AD によって設定されます。
1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
 2. ナビゲーションバーで、既存のディレクトリ AWS リージョン と同じ を選択します。
 3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
 4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Windows EC2 インスタンスに使用する名前を入力します。
 5. (オプション) [補足タグを追加] で、タグとキーの値のペアを 1 つまたは複数追加して、この EC2 インスタンスのアクセスを整理、追跡、または制御します。
 6. [アプリケーションと OS イメージ (Amazon マシンイメージ)] セクションの [クイックスタート] ペインで [Windows] を選択します。Windows Amazon マシンイメージ (AMI) は、[Amazon マシンイメージ (AMI)] ドロップダウンリストから変更できます。
 7. [インスタンスタイプ] セクションで、[インスタンスタイプ] ドロップダウンリストから使用するインスタンスタイプを選択します。
 8. キーペア (ログイン) セクションでは、[新しいキーペアを作成する](#) か、既存のキーペアを使用するか、キーペアなしで続行するかを選択できます。

9. [インスタンスを起動する] ページの [ネットワーク設定] セクションで、[編集] を選択します。[VPC に必須の] ドロップダウンリストから、ディレクトリが作成された [VPC] を選択します。
10. [サブネット] ドロップダウンリストから VPC 内のパブリックサブネットの 1 つを選択します。選択するサブネットで、すべての外部トラフィックがインターネットゲートウェイにルーティングされるように選択する必要があります。そうでない場合は、インスタンスにリモート接続できません。

インターネットゲートウェイへの接続方法の詳細については、Amazon VPC ユーザーガイドの「[インターネットゲートウェイを使用してサブネットをインターネットに接続する](#)」を参照してください。

11. [自動割り当てパブリック IP] で、[有効化] を選択します。

公開 IP アドレス指定とプライベート IP アドレス指定の詳細については、「Amazon EC2 インスタンスユーザーガイド」の「[Amazon EC2 インスタンスの IP アドレス指定](#)」を参照してください。

12. [ファイアウォール (セキュリティグループ)] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
13. [ストレージの設定] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
14. [高度な詳細] セクションを選択し、[ドメイン結合ディレクトリ] ドロップダウンリストからドメインを選択します。

 Note

ドメイン結合ディレクトリを選択すると、次のようになります:

 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. 

このエラーは、EC2 起動ウィザードが予期しないプロパティを持つ既存の SSM ドキュメントを識別した場合に発生します。次のいずれかを試すことができます。

- 以前に SSM ドキュメントを編集し、プロパティの存在が予想される場合は、[閉じる] を選択して EC2 インスタンスを変更せずに起動します。

- ここで既存の SSM ドキュメントを削除するリンクを選択して、SSM ドキュメントを削除します。これにより、正しいプロパティを使用する SSM ドキュメントを作成できます。EC2 インスタンスを起動すると、SSM ドキュメントが自動的に作成されます。

15. [IAM インスタンスプロファイル] には既存の IAM インスタンスプロファイルを選択するか、新しいプロファイルを作成できます。管理 AWS ポリシー AmazonSSMManagedInstanceCore と AmazonSSMDirectoryServiceAccess がアタッチされている IAM インスタンスプロファイルを IAM インスタンスプロファイルのドロップダウンリストから選択します。新しい IAM プロファイルリンクを作成するには、[新しい IAM プロファイルを作成する] リンクを選択し、以下を実行します。
 1. [ロールの作成] を選択してください。
 2. [Select trusted entity] (信頼されたエンティティを選択) で、[AWS サービス] を選択します。
 3. [ユースケース] で、[EC2] を選択してください。
 4. ポリシーのリスト内の [アクセス許可を追加する] の下で、AmazonSSMManagedInstanceCore ポリシーと AmazonSSMDirectoryServiceAccess ポリシーを選択します。リストを絞り込むため、検索ボックスに **SSM** と入力します。[次へ] を選択します。

 Note

AmazonSSMDirectoryServiceAccess は、 によって Active Directory 管理される にインスタンスを結合するアクセス許可を提供します AWS Directory Service。AmazonSSMManagedInstanceCore は、 AWS Systems Manager サービスを使用するために必要な最小限のアクセス許可を提供します。これらのアクセス許可を使用してロールを作成する方法、および IAM ロールに割り当てることができるその他のアクセス許可とポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。

5. [名前、確認、作成] ページで、[ロール名] を入力します。EC2 インスタンスにアタッチするには、このロール名が必要です。
6. (オプション) IAM インスタンスプロファイルの説明を [説明] フィールドに入力できます。
7. [ロールの作成] を選択してください。

8. [インスタンスを起動する] ページに戻り、[IAM インスタンスプロファイル] の横にある更新アイコンを選択します。新しい IAM インスタンスプロファイルが [IAM インスタンスプロファイル] ドロップダウンリストに表示されるはずです。新しいプロファイルを選択し、残りの設定はデフォルト値のままにします。

16. [インスタンスを起動] を選択します。

Manually join an EC2 Windows

既存の Amazon EC2 Windows インスタンスを Simple AD Active Directory に手動で結合するには、[Amazon EC2 Windows インスタンスを Simple AD Active Directory に結合する](#) で指定したパラメータを使用して、インスタンスを起動する必要があります。

Simple AD の DNS サーバーの IP アドレスが必要です。この情報は、お使いのディレクトリ > [ディレクトリの詳細] セクションと [ネットワークとセキュリティ] セクションの、[ディレクトリサービス] > [ディレクトリ] > [ディレクトリ ID] リンクの下にあります。

The screenshot shows the AWS Directory Service console for directory d-1234567890. The left sidebar shows the navigation menu with 'Directories' highlighted. The main content area has a breadcrumb trail: Directory Service > Directories > d-1234567890. Below the breadcrumb, the directory ID 'd-1234567890' is displayed. The 'Directory details' section contains the following information:

Directory type	Directory DNS name
Microsoft AD	corp.example.com

Edition	Directory NetBIOS name
Standard	corp

Operating system version	Directory administration EC2 instance(s)
Windows Server 2019	-

Below the details, there are tabs for 'Networking & security', 'Scale & share', 'Application management', and 'Maintenance'. The 'Networking & security' tab is selected, showing 'Networking details'. This section includes a 'VPC' section and a 'Subnets' section. The 'Subnets' section contains a table of DNS addresses:

DNS address
192.0.2.1
198.51.100.1

Windows インスタンスを Simple AD Active Directory に結合するには

1. リモートデスクトッププロトコルクライアントを使用してインスタンスに接続します。
2. インスタンスの TCP / IPv4 プロパティダイアログボックスを開きます。

- a. ネットワーク接続を開きます。

 Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、[Network Connections] (ネットワーク接続) を直接開くことができます。

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

- b. 有効になっているネットワーク接続のコンテキストメニュー (右クリック) を開き、[Properties] (プロパティ) を選択します。
 - c. 接続のプロパティダイアログボックスで、[Internet Protocol Version 4] をダブルクリックして開きます。
3. [次の DNS サーバーのアドレスを使用する] を選択し、[優先 DNS サーバー] および [代替 DNS サーバー] のアドレスを Simple AD が提供した DNS サーバーの IP アドレスに変更し、[確認] をクリックします。

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. インスタンスの [System Properties] (システムプロパティ) ダイアログボックスを開き、[Computer Name] (コンピュータ名) タブを選択して、[Change] (変更) をクリックします。

 Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、[System Properties] (システムプロパティ) ダイアログボックスを直接開くことができます。

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. [所属先] フィールドで、[ドメイン] を選択し、Simple AD Active Directory の完全修飾名を入力して、[確認] をクリックします。
6. ドメイン管理者の名前とパスワードの入力を求められたら、ドメイン結合権限を持つアカウントのユーザー名とパスワードを入力します。これらの権限の委任に関する詳細については、「[Simple AD のディレクトリ結合権限を委任する](#)」を参照してください。

 Note

ドメインの完全修飾名または NetBIOS 名のいずれかを入力できます。
これに続けて、バックスラッシュ (\)、ユーザー名の順に入力します。
ユーザー名は [Administrator] になります。例えば、**corp.example.com**
\administrator、**corp\administrator** です。

7. ドメインへのアクセスを歓迎するメッセージを受け取ったら、インスタンスを再起動して変更を有効にします。

これでインスタンスは Simple AD Active Directory ドメインに結合されたので、そのインスタンスに遠隔的にログインし、ユーザーやグループの追加など、ディレクトリを管理するためのユーティリティをインストールできます。Active Directory 管理ツールを使用して、ユーザーとグループを作成できます。詳細については、「[Simple AD の Active Directory 管理ツールをインストールする](#)」を参照してください。

Amazon EC2 Linux インスタンスを Simple AD アクティブディレクトリに結合する

Amazon EC2 Linux インスタンスを起動して、AWS Management Consoleの Simple AD に結合できます。EC2 Linux インスタンスを Simple AD に手動で結合することもできます。

以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

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

Note

Ubuntu 14 および Red Hat Enterprise Linux 7 および 8 より前のディストリビューションは、シームレスなドメイン結合機能をサポートしていません。

EC2 Linux インスタンスをドメイン結合する方法：

- [Amazon EC2 Linux スタンスを Simple AD Active Directoryにシームレスに結合する](#)
- [Amazon EC2 Linux インスタンスをSimple AD アクティブディレクトリに手動で結合する](#)

Amazon EC2 Linux スタンスを Simple AD Active Directoryにシームレスに結合する

この手順では、Amazon EC2 インスタンスを Simple AD Active Directoryにシームレスに結合します。

以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 ビット x86)
- Red Hat Enterprise Linux 8 (HVM) (64 ビット x86)

- Ubuntu Server 18.04 LTS および Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

 Note

Ubuntu 14 および Red Hat Enterprise Linux 7 および 8 より前のディストリビューションは、シームレスなドメイン結合機能をサポートしていません。

前提条件

Linux インスタンスへのシームレスなドメイン結合を設定する前に、このセクションの手順を完了する必要があります。

シームレスなドメイン結合のサービスアカウントを選択する

Linux コンピュータを Simple AD ドメインにシームレスに結合できます。これを行うには、コンピュータをドメインに結合するためのコンピュータアカウントの作成アクセス許可を持つユーザーアカウントを作成する必要があります。Domain Admins または他のグループのメンバーがコンピュータをドメインに結合する十分な権限を持っていても、これらは推奨されません。ベストプラクティスとして、コンピュータをドメインに結合するために必要な最低限の権限を持つサービスアカウントを使用することをお勧めします。

コンピュータアカウントの作成のために、サービスアカウントへのアクセス許可を処理および委任する方法の詳細については、「[権限をサービスアカウントに委任する](#)」を参照してください。

ドメインサービスアカウントを保存するシークレットを作成する

AWS Secrets Manager を使用してドメインサービスアカウントを保存できます。詳細については、「[AWS Secrets Manager シークレットの作成](#)」を参照してください。

 Note

Secrets Manager には料金がかかります。詳細については、「AWS Secrets Manager ユーザーガイド」の「[料金表](#)」を参照してください。

ドメインサービスアカウントの情報を保存するシークレットを作成するには

1. にサインイン AWS Management Console し、<https://console.aws.amazon.com/secretsmanager/> で AWS Secrets Manager コンソールを開きます。
2. [Store a new secret] (新しいシークレットの保存) を選択します。
3. [Store a new secret] (新しいシークレットを保存する) のページで、次の操作を行います：
 - a. [シークレットのタイプ] で、[その他のシークレットのタイプ] を選択します。
 - b. [Key/value pairs] (キー/値ペア) で、次のように実行します。
 - i. 最初のボックスに **awsSeamlessDomainUsername** と入力します。同じ行の次のボックスに、サービスアカウントのユーザー名を入力します。例えば、以前に PowerShell コマンドを使用した場合、サービスアカウント名は **awsSeamlessDomain** になります。

 Note

awsSeamlessDomainUsername を正確に入力する必要があります。先頭または末尾にスペースがないことを確認します。スペースがあると、ドメイン結合が失敗します。

The screenshot shows the AWS Secrets Manager console interface. On the left, a sidebar lists the steps: Step 1: Choose secret type, Step 2: Configure secret, Step 3 - optional: Configure rotation, and Step 4: Review. The main area is titled 'Choose secret type'. Under 'Secret type', four options are shown: '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). Below this, the 'Key/value pairs' section shows a table with one row: 'awsSeamlessDomainUsername' (highlighted with a red box) and an empty value field. A '+ Add row' button is below the table. The 'Encryption key' section shows a dropdown menu with 'aws/secretsmanager' selected and a refresh button. At the bottom right, there are 'Cancel' and 'Next' buttons.

- ii. [Add row] (行の追加) を選択します。
- iii. 新しい行で、最初のボックスに **awsSeamlessDomainPassword** と入力します。同じ行の次のボックスに、サービスアカウントのパスワードを入力します。

Note

awsSeamlessDomainPassword を正確に入力する必要があります。先頭または末尾にスペースがないことを確認します。スペースがあると、ドメイン結合が失敗します。

- iv. 暗号化キーの下で、デフォルト値 `aws/secretsmanager` のままにしておきます。このオプションを選択すると、AWS Secrets Manager は常に秘密を暗号化します。自身で作成したキーを選択することもできます。
- v. [次へ] を選択します。

4. [Secret name]の下に、**d-xxxxxxxxxx**をディレクトリIDに置き換えて、以下のフォーマットでディレクトリIDを含むsecret nameを入力します：

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

これは、アプリケーション内のシークレットを取得するために使用されます。

 Note

aws/directory-services/d-xxxxxxxxxx**/seamless-domain-join** は正確に入力する必要がありますが、**d-xxxxxxxxxx** はディレクトリ ID に置き換えてください。先頭または末尾にスペースがないことを確認します。スペースがあると、ドメイン結合が失敗します。

Services Search [Alt+S] Ohio

AWS Secrets Manager > Secrets > Store a new secret

Step 1
[Choose secret type](#)

Step 2
Configure secret

Step 3 - optional
Configure rotation

Step 4
Review

Configure secret

Secret name and description [Info](#)

Secret name
A descriptive name that helps you find your secret later.

aws/directory-services/d-xxxxxxx/seamless-domain-join

Secret name must contain only alphanumeric characters and the characters `/_+=.@-`.

Description - optional

Access to MYSQL prod database for my AppBeta

Maximum 250 characters.

Tags - optional

No tags associated with the secret.

[Add](#)

Resource permissions - optional [Info](#)

Add or edit a resource policy to access secrets across AWS accounts.

[Edit permissions](#)

▶ Replicate secret - optional

Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

[Cancel](#) [Previous](#) [Next](#)

5. それ以外はすべてデフォルトのままにして、[Next] (次へ) をクリックします。
6. [Configure automatic rotation] (自動ローテーションを設定) で [Disable automatic rotation] (自動ローテーションを無効にする) を選択し、[Next] (次へ) をクリックします。

このシークレットの保存後にローテーションを有効にすることができます。

7. 設定を確認し、[Store] (保存) をクリックして変更を保存します。Secrets Manager コンソールがアカウントのシークレットリストに戻ります。リストには、新しいシークレットが追加されています。
8. 新しく作成したシークレット名をリストから選択し、[Secret ARN] (シークレット ARN) 値をメモします。これは次のセクションで必要になります。

ドメインサービスアカウントシークレットのローテーションを有効にする

セキュリティ体制を改善するために、シークレットを定期的にローテーションすることをお勧めします。

ドメインサービスアカウントシークレットのローテーションを有効にするには

- [「ユーザーガイド」の AWS Secrets Manager 「シークレットの自動ローテーションを設定する」](#) の手順に従います。 AWS Secrets Manager

ステップ 5 では、「AWS Secrets Manager ユーザーガイド」のローテーションテンプレート「[Microsoft Active Directory 認証情報](#)」を使用します。

ヘルプについては、「AWS Secrets Manager ユーザーガイド」の「[ロー AWS Secrets Manager テーションのトラブルシューティング](#)」を参照してください。

必要な IAM ポリシーとロールを作成する

次の前提条件の手順に従い、Secrets Manager のシームレスなドメイン結合シークレット (先ほど作成したもの) への読み取り専用アクセスを許可するカスタムポリシーを作成し、新しい LinuxEC2DomainJoin IAM ロールを作成します。

Secrets Manager の IAM 読み取りポリシーを作成する

IAM コンソールを使用して、Secrets Manager シークレットへの読み取り専用アクセスを許可するポリシーを作成します。

Secrets Manager の IAM 読み取りポリシーを作成するには

1. IAM ポリシーを作成する権限を持つユーザー AWS Management Console として にサインインします。次に、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. ナビゲーションペインの [アクセス管理] で、[ポリシー] を選択します。
3. [Create policy] (ポリシーの作成) を選択します。
4. [JSON] タブを選択し、以下の JSON ポリシードキュメントからテキストをコピーします。これを、[JSON] テキストボックスに貼り付けます。

Note

リージョンとリソース ARN を、先ほど作成したシークレットの実際のリージョンと ARN に置き換えていることを確認してください。

```
{
  "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. 完了したら、[Next] を選択します。構文エラーがある場合は、Policy Validator によってレポートされます。詳細については、「[IAM ポリシーの検証](#)」を参照してください。
6. [Review policy] (ポリシーの確認) ページで、ポリシー名を入力します (**SM-Secret-Linux-DJ-d-xxxxxxxx-Read** など)。[Summary] (概要) セクションで、ポリシーで付与されているアクセス許可を確認します。[Create Policy] (ポリシーの作成) をクリックし、変更を保存します。新しいポリシーが管理ポリシーのリストに表示されます。これで ID にアタッチする準備は完了です。

Note

シークレットごとに 1 つのポリシーを作成することをお勧めします。そうすることで、インスタンスが適切なシークレットにのみアクセスできるようになり、インスタンスが侵害された場合の影響を最小限に抑えることができます。

LinuxEC2DomainJoin ロールを作成する

IAM コンソールを使用して、Linux EC2 インスタンスへのドメイン結合に使用するロールを作成します。

LinuxEC2DomainJoin ロールを作成するには

1. IAM ポリシーを作成する権限を持つユーザー AWS Management Console として にサインインします。次に、IAM コンソール (<https://console.aws.amazon.com/iam/>) を開きます。
2. ナビゲーションペインの [Access Management] (アクセス管理) で、[Roles] (ロール) を選択します。
3. コンテンツペインで、[Create role] (ロールの作成) を選択します。
4. [Select type of trusted entity] (信頼されたエンティティの種類を選択) の下で、[AWS Service] を選択します。
5. [Use case] (ユースケース) で EC2 を選択し、[Next] (次へ) を選択します。

The screenshot shows the 'Create role' wizard in the AWS IAM console. The 'Trusted entity type' section has 'AWS service' selected. The 'Use case' section has 'EC2' selected. Red boxes highlight these selections.

6. [Filter policies] (フィルターポリシー) で、以下を実行します。
 - a. **AmazonSSManagedInstanceCore** と入力します。次に、リスト内のその項目のチェックボックスをオンにします。
 - b. **AmazonSSMDirectoryServiceAccess** と入力します。次に、リスト内のその項目のチェックボックスをオンにします。
 - c. **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read** (または前の手順で作成したポリシーの名前) を入力します。次に、リスト内のその項目のチェックボックスをオンにします。

- d. 上記の 3 つのポリシーを追加したら、[ロールを作成] を選択します。

 Note

AmazonSSMDirectoryServiceAccess は、 によってActive Directory管理されるインスタンスを結合するためのアクセス許可を提供します AWS Directory Service。AmazonSSMManagedInstanceCore は、 AWS Systems Manager サービスを使用するために必要な最小限のアクセス許可を提供します。これらのアクセス許可を使用してロールを作成する方法、および IAM ロールに割り当てることができるその他のアクセス許可とポリシーの詳細については、「AWS Systems Manager ユーザーガイド」の「[Systems Manager の IAM インスタンスプロファイルを作成する](#)」を参照してください。

7. **LinuxEC2DomainJoin**[Role name] (ロール名) 欄 に、 適宜の別の名前など 新しいロールの名前を入力します。
8. (オプション) [Role description] (ロールの説明) に、説明を入力します。
9. (オプション) [ステップ 3: タグの追加] で [新しいタグの追加] を選択してタグを追加します。タグのキーと値のペアは、このロールのアクセスを整理、追跡、または制御するために使用されます。
10. [ロールの作成] を選択してください。

Linux スタンスを Simple AD Active Directoryにシームレスに結合する

Linux インスタンスをシームレスに結合するには

1. にサインイン AWS Management Console し、 <https://console.aws.amazon.com/ec2/> で Amazon EC2 コンソールを開きます。
2. ナビゲーションバーのリージョンセレクターから、既存のディレクトリ AWS リージョン と同じ を選択します。
3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Linux EC2 インスタンスに使用する名前を入力します。
5. (選択可能) [補足タグを追加] で、タグとキーの値のペアを 1 つまたは複数追加して、この EC2 インスタンスのアクセスを整理、追跡、またはコントロールします。

6. Application and OS Image (Amazon Machine Image)セクションで、起動したいLinux AMIを選択します。

 Note

使用する AMI には AWS Systems Manager、(SSM Agent) バージョン 2.3.1644.0 以降が必要です。その AMI からインスタンスを起動して AMI にインストールされている SSM Agent のバージョンを確認するには、「[現在インストールされている SSM Agent バージョンを取得するには](#)」を参照してください。SSM Agent をアップグレードする必要がある場合は、「[Linux の EC2 インスタンスで SSM Agent をインストールして設定する](#)」を参照してください。

SSM は Linux インスタンスを Active Directory ドメインに結合する際にプラグイン aws:domainJoin を使用します。プラグインは、Linux インスタンスのホスト名を EC2AMAZ-XXXXXXX の形式に変更します。aws:domainJoinの詳細については、[AWS Systems Manager ユーザーガイド]の「[AWS Systems Manager コマンド・ドキュメント・プラグイン・リファレンス](#)」を参照してください。

7. [インスタンスタイプ] セクションで、[インスタンスタイプ] ドロップダウンリストから使用するインスタンスタイプを選択します。
8. [キーペア (ログイン)] セクションで、新しいキーペアを作成するか、既存のキーペアから選択します。新しいキーペアを作成するには、[新しいキーペアの作成] を選択します。キーペアの名前を入力し、[キーペアタイプ] と [プライベートキーファイル形式] のオプションを選択します。OpenSSH で使用できる形式でプライベートキーを保存するには、[.pem] を選択します。プライベートキーを PuTTY で使用できる形式で保存するには、[.ppk] を選択します。[キーペアの作成] を選択します。ブラウザによって秘密キーファイルが自動的にダウンロードされます。ダウンロードしたプライベートキーのファイルを安全な場所に保存します。

 Important

プライベートキーのファイルを保存できるのはこのタイミングだけです。

9. [インスタンスを起動する] ページの [ネットワーク設定] セクションで、[編集] を選択します。[VPC に必須の] ドロップダウンリストから、ディレクトリが作成された [VPC] を選択します。
10. [サブネット] ドロップダウンリストから VPC 内のパブリックサブネットの 1 つを選択します。選択するサブネットで、すべての外部トラフィックがインターネットゲートウェイにルーティングされるように選択する必要があります。そうでない場合は、インスタンスにリモート接続できません。

インターネットゲートウェイへの接続方法の詳細については、Amazon VPC ユーザーガイドの「[インターネットゲートウェイを使用してサブネットをインターネットに接続する](#)」を参照してください。

11. [自動割り当てパブリック IP] で、[有効化] を選択します。

公開 IP アドレス指定とプライベート IP アドレス指定の詳細については、「Amazon EC2 インスタンスユーザーガイド」の「[Amazon EC2 インスタンスの IP アドレス指定](#)」を参照してください。

12. [ファイアウォール (セキュリティグループ)] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
13. [ストレージの設定] 設定にはデフォルト設定を使用するか、必要に応じて変更を加えることができます。
14. [高度な詳細] セクションを選択し、[ドメイン結合ディレクトリ] ドロップダウンリストからドメインを選択します。

 Note

ドメイン結合ディレクトリを選択すると、次のようになります:

 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. 

このエラーは、EC2 起動ウィザードが予期しないプロパティを持つ既存の SSM ドキュメントを識別した場合に発生します。次のいずれかを試すことができます。

- 以前に SSM ドキュメントを編集し、プロパティの存在が予想される場合は、[閉じる] を選択して EC2 インスタンスを変更せずに起動します。
- ここで既存の SSM ドキュメントを削除するリンクを選択して、SSM ドキュメントを削除します。これにより、正しいプロパティを使用する SSM ドキュメントを作成できます。EC2 インスタンスを起動すると、SSM ドキュメントが自動的に作成されます。

15. [IAM インスタンスプロファイル] には、前提条件のセクションで以前に作成した IAM ロールを選択します ステップ 2: LinuxEC2DomainJoin ロールを作成します

16. [インスタンスを起動] を選択します。

Note

SUSE Linux でシームレスなドメイン結合を実行する場合は、認証が機能する前に再起動する必要があります。Linux ターミナルから SUSE を再起動するには、「sudo reboot」と入力します。

Amazon EC2 Linux インスタンスを Simple AD アクティブディレクトリに手動で結合する

Amazon EC2 Windows インスタンスに加え、特定の Amazon EC2 Linux インスタンスを Simple AD Active Directory に結合することもできます。以下の Linux インスタンスのディストリビューションおよびバージョンがサポートされています。

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2 (64 ビット x86)
- Amazon Linux 2023 AMI
- Red Hat Enterprise Linux 8 (HVM) (64 ビット x86)
- Ubuntu Server 18.04 LTS および Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

他の Linux ディストリビューションとバージョンも動作する可能性がありますが、まだテストされていません。

前提条件

Amazon Linux、CentOS、Red Hat、または Ubuntu インスタンスをディレクトリに結合するときは、先に、[Amazon EC2 Linux スタンスを Simple AD Active Directory にシームレスに結合する](#) で指定したとおりにインスタンスを起動する必要があります。

⚠ Important

次の手順は、正しく実行しないと、インスタンスに到達不可能になったり、インスタンスが使用できなくなったりする可能性があります。したがって、これらの手順を実行する前に、バックアップを作成するか、インスタンスのスナップショットを作成することを強くお勧めします。

Linux インスタンスをディレクトリに結合するには

個々の Linux インスタンスについて、次のいずれかのタブの手順に従います。

Amazon Linux

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. Amazon Linux - 64 bit インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な Amazon Linux パッケージを Linux インスタンスにインストールします。

i Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

Amazon Linux

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli  
krb5-workstation
```

Note

使用している Amazon Linux のバージョンを確認する方法については、「[Amazon EC2 Linux インスタンス用ユーザーガイド](#)」の「Identifying Amazon Linux images」(Amazon Linux イメージの特定)を参照してください。

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account@EXAMPLE.COM example.com --verbose
```

join_account@EXAMPLE.COM

ドメイン結合権限を持つ *example.com* ドメインのアカウント。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...  
* Successfully enrolled machine in realm
```

6. SSH サービスを設定して、パスワード認証を許可します。

- a. テキストエディタで `/etc/ssh/sshd_config` ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

7. インスタンスが再起動したら、任意の SSH クライアントを使用して接続し、次の手順を実行してドメイン管理者グループを sudoers リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

CentOS

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. CentOS 7 インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な CentOS 7 パッケージを Linux インスタンスにインストールします。

Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

ドメイン結合権限を持つ *example.com* ドメインのアカウント。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...  
* Successfully enrolled machine in realm
```

6. SSH サービスを設定して、パスワード認証を許可します。

a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

7. インスタンスが再起動したら、任意の SSH クライアントを使用して接続し、次の手順を実行してドメイン管理者グループを sudoers リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

Red hat

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. Red Hat - 64 bit インスタンスが最新であることを確認します。

```
sudo yum -y update
```

4. 必要な Red Hat パッケージを Linux インスタンスにインストールします。

 Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままで構いません。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -v -U join_account example.com --install=/  
join_account
```

join_account

ドメイン結合権限を持つ example.com ドメインのアカウントの *sAMAccountName*。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...  
* Successfully enrolled machine in realm
```

6. SSH サービスを設定して、パスワード認証を許可します。

a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

7. インスタンスが再起動したら、任意の SSH クライアントを使用して接続し、次の手順を実行してドメイン管理者グループを sudoers リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

Ubuntu

1. 任意の SSH クライアントを使用してインスタンスに接続します。
2. AWS Directory Serviceが提供する DNS サーバーの DNS サーバーの IP アドレスを使用するように Linux インスタンスを設定します。これを行うには、VPC にアタッチされている DHCP オプションセットに設定するか、または手動でインスタンスに設定します。手動で設定するには、AWS ナレッジセンターの「[プライベート Amazon EC2 インスタンスが Amazon Linux、Ubuntu、または RHEL で実行中です。再起動中も持続する EC2 インスタンスに静的 DNS サーバーを割り当てる方法を教えてください。](#)」で、特定の Linux ディストリビューションとバージョンの永続的な DNS サーバーの設定に関するガイダンスを参照してください。
3. Ubuntu - 64 bit インスタンスが最新であることを確認します。

```
sudo apt-get update  
sudo apt-get -y upgrade
```

4. 必要な Ubuntu パッケージを Linux インスタンスにインストールします。

 Note

これらのパッケージの一部が既にインストールされている可能性があります。パッケージをインストールすると、いくつかのポップアップ設定画面が表示されます。一般的に、これらの画面のフィールドは空白のままです。

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 逆引き DNS 解決を無効にし、デフォルトのレルムをドメインの FQDN に設定します。Ubuntu インスタンスは、レルムが稼働する前に DNS で逆引き解決可能になっている必要があります。なっていない場合、次のように `/etc/krb5.conf` で逆引き DNS を無効にする必要があります。

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 次のコマンドを使用してディレクトリにインスタンスを結合します。

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

ドメイン結合権限を持つ `example.com` ドメインのアカウントの *sAMAccountName*。プロンプトが表示されたら、アカウントのパスワードを入力します。これらの権限の委任に関する詳細については、「[AWS Managed Microsoft AD のディレクトリ結合権限を委任する](#)」を参照してください。

example.com

ディレクトリの完全修飾 DNS 名です。

```
...
* Successfully enrolled machine in realm
```

7. SSH サービスを設定して、パスワード認証を許可します。

- a. テキストエディタで /etc/ssh/sshd_config ファイルを開きます。

```
sudo vi /etc/ssh/sshd_config
```

- b. PasswordAuthentication 設定を「yes」に設定します。

```
PasswordAuthentication yes
```

- c. SSH サービスを再起動します。

```
sudo systemctl restart sshd.service
```

または:

```
sudo service sshd restart
```

8. インスタンスが再起動したら、任意の SSH クライアントを使用して接続し、次の手順を実行してドメイン管理者グループを sudoers リストに追加します。

- a. 次のコマンドを使用して sudoers ファイルを開きます。

```
sudo visudo
```

- b. 次の内容を sudoers ファイルの下部に追加して保存します。

```
## Add the "Domain Admins" group from the example.com domain.  
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

(上の例では「\<space>」を使用して Linux スペース文字を作成しています)。

Note

Simple AD の使用において、「最初のログイン時にユーザーにパスワードの変更を強制する」オプションを指定して Linux インスタンスのユーザーアカウントを作成する場合、そのユーザーは kpasswd を使用して初期のパスワード変更ができません。初めてパスワードを変更する場合、ドメイン管理者が Active Directory 管理ツールを使用してユーザーのパスワードを更新する必要があります。

Linux インスタンスからアカウントを管理する

Linux インスタンスから Simple AD のアカウントを管理するには、次に示すように、Linux インスタンスで特定の設定ファイルを更新する必要があります。

1. `/etc/sss/sss.conf` ファイルで、`krb5_use_kdcinfo` を「False」に設定します。例:

```
[domain/example.com]
krb5_use_kdcinfo = False
```

2. 設定を有効にするには、`sss` サービスを再起動する必要があります。

```
$ sudo systemctl restart sss.service
```

または、次のコマンドを使用できます。

```
$ sudo service sss start
```

3. CentOS Linux インスタンスからユーザーを管理する場合は、次を含めるためにファイル `/etc/smb.conf` も編集する必要があります。

```
[global]
workgroup = EXAMPLE.COM
realm = EXAMPLE.COM
netbios name = EXAMPLE
security = ads
```

アカウントのログインアクセスの制限

デフォルトでは、すべてのアカウントは Active Directory で定義されているため、ディレクトリのすべてのユーザーがインスタンスにログインできます。`sss.conf` の `ad_access_filter` を使用して、特定のユーザーのみにインスタンスへのログインを許可できます。例:

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

ユーザーは、特定のグループのメンバーである場合にのみ、インスタンスへのアクセスを許可されることを示しています。

cn

アクセス権限のあるグループの共通名。この例では、グループ名は、*admins* です。

ou

これは、上記のグループが配置される組織単位です。この例では、OU は、*Testou* です。

dc

これは、ドメインのドメインコンポーネントです。この例では、*example* です。

dc

これは、追加のドメインコンポーネントです。この例では、*com* です。

`ad_access_filter` を手動で `/etc/sss/sss.conf` に追加する必要があります。

テキストエディタで `/etc/sss/sss.conf` ファイルを開きます。

```
sudo vi /etc/sss/sss.conf
```

この操作を行った後、`sss.conf` は次のようになります。

```
[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)
```

設定を有効にするには、`sss` サービスを次のように再起動する必要があります。

```
sudo systemctl restart sssd.service
```

または、次のコマンドを使用できます。

```
sudo service sssd restart
```

ID マッピング

ID マッピングは 2 つの方法で実行でき、UNIX/Linux ユーザー識別子 (UID) とグループ識別子 (GID)、Windows ID と Active Directory セキュリティ識別子 (SID) の ID 間の統一されたエクスペリエンスを維持できます。これらのメソッドは次のとおりです。

1. 一元化
2. 分散型

Note

Active Directory での集中型ユーザーアイデンティティマッピングには、ポータブルオペレーティングシステムインターフェイス (POSIX) が必要です。

一元化されたユーザ ID マッピング

Active Directory または別の Lightweight Directory Access Protocol (LDAP) サービスは Linux ユーザーに UID と GID を提供します。では Active Directory、POSIX 拡張機能が設定されている場合、これらの識別子はユーザーの属性に保存されます。

- UID-Linux ユーザー名 (文字列)
- UID 番号-Linux ユーザー ID 番号 (整数)
- GID 番号-Linux グループ ID 番号 (整数)

Active Directory の UID と GID を使用するように Linux インスタンスを設定するには、`sssd.conf` ファイルに `ldap_id_mapping = False` を設定します。この値を設定する前に、UID、UID 番号、および GID 番号が Active Directory 内のユーザーとグループに追加されていることを確認してください。

分散型ユーザー ID マッピング

Active Directory に POSIX 拡張がない場合や、ID マッピングを集中的に管理しないことを選択した場合、Linux は UID と GID の値を計算できます。Linux はユーザー固有のセキュリティ識別子 (SID) を使用して一貫性を保ちます。

分散ユーザー ID マッピングを設定するには、`ldap_id_mapping = True` `sssd.conf` ファイルで設定します。

一般的な問題

を設定すると `ldap_id_mapping = False`、SSSD サービスの開始が失敗することがあります。この失敗の理由は、UIDs の変更がサポートされていないためです。ID マッピングから POSIX 属性、または POSIX 属性から ID マッピングに変更するたびに、SSSD キャッシュを削除することをお勧めします。ID マッピングと `ldap_id_mapping` パラメータの詳細については、Linux コマンドラインで `sssd-ldap(8) man` ページを参照してください。

Linux インスタンスへの接続

ユーザーの SSH クライアントを使用してインスタンスに接続し、ユーザー名の入力が求められます。ユーザーは、`username@example.com` または `EXAMPLE\username` のいずれかの形式でユーザー名を入力することができます。使用している Linux ディストリビューションに応じて、レスポンスは次のように表示されます。

Amazon Linux、Red Hat Enterprise Linux、および 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%
```

Simple AD のディレクトリ結合権限を委任する

コンピュータをディレクトリに結合するには、コンピュータをディレクトリに結合する権限を持つアカウントが必要です。

Simple AD では、Domain Admins グループのメンバーは、コンピュータをディレクトリに結合するのに必要な権限を持っています。

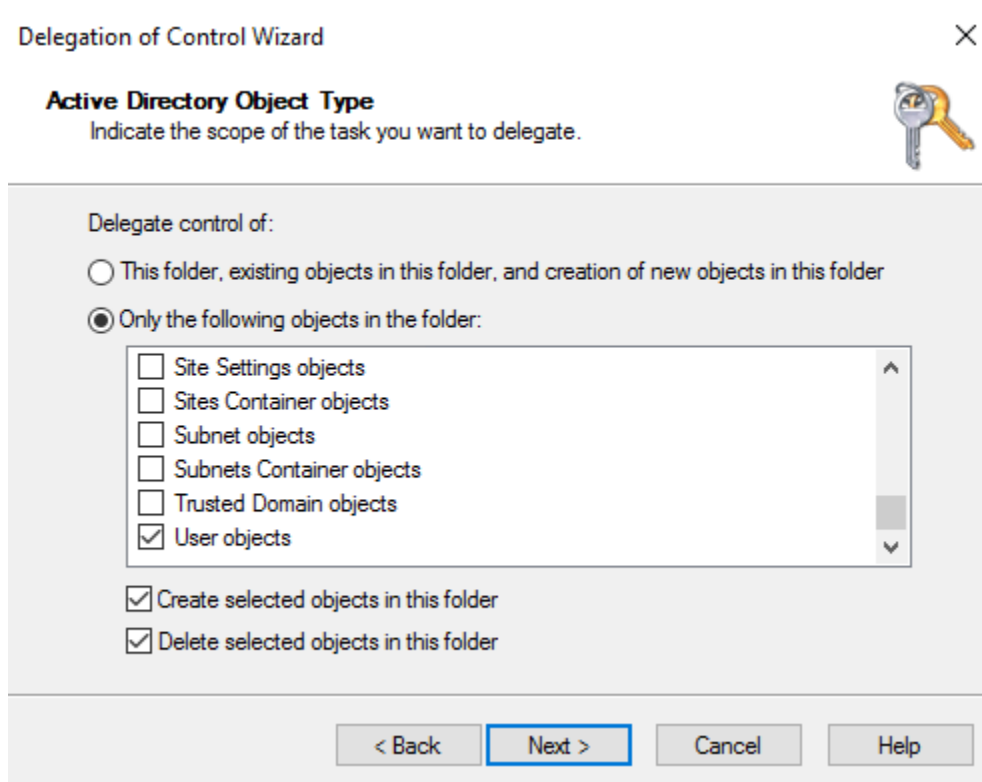
ただし、ベストプラクティスとして、必要な最小限の権限のみを持つアカウントを使用してください。次の手順は、Joiners という新しいグループを作成し、コンピュータをディレクトリに結合するために必要な権限をこのグループに委任する方法を示しています。

この手順は、ディレクトリに結合され、[Active Directory User and Computers] (Active Directory ユーザーとコンピュータ) MMC スナップインがインストールされたコンピュータで実行する必要があります。また、ドメイン管理者としてログインする必要があります。

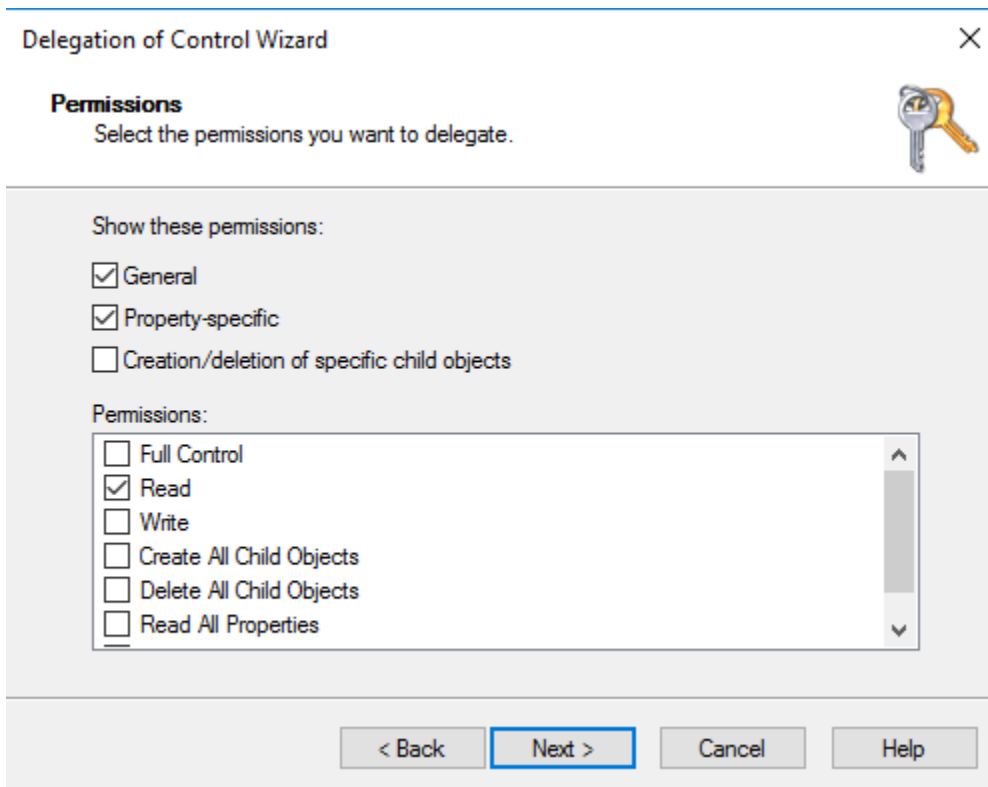
Simple AD での結合の権限を委任するには

1. [Active Directory User and Computers] (Active Directory ユーザーとコンピュータ) を開き、ナビゲーションツリーのドメインルートを選択します。
2. 左側のナビゲーションツリーで、[Users] (ユーザー) のコンテキストメニュー (右クリック) を開き、[New] (新規)、[Group] (グループ) の順に選択します。
3. [New Object - Group] (新しいオブジェクト - グループ) ボックスで、次の内容を入力し、[OK] をクリックします。

- [Group name] (グループ名) に「**Joiners**」と入力します。
 - [Group scope] (グループのスコープ) で、[Global] (グローバル) を選択します。
 - [Group type] (グループの種類) で、[Security] (セキュリティ) を選択します。
4. ナビゲーションツリーで、ドメインのルートを選択します。[Action] (アクション) メニューで、[Delegate Control] (制御の委任) を選択します。
 5. [Delegation of Control Wizard] (制御の委任ウィザード) ページで、[Next] (次へ)、[Add] (追加) の順に選択します。
 6. [Select Users, Computers, or Groups] (ユーザー、コンピュータ、またはグループの選択) ボックスで「Joiners」と入力し、[OK] をクリックします。複数のオブジェクトがある場合は、上記で作成した Joiners グループを選択します。[Next] (次へ) をクリックします。
 7. [Tasks to Delegate] (委任するためのタスク) ページで、[Create a custom task to delegate] (委任するためのカスタムタスクを作成) を選択し、[Next] (次へ) をクリックします。
 8. [Only the following objects in the folder] (フォルダ内の次のオブジェクトのみ) を選択し、[Computer objects] (コンピュータオブジェクト) を選択します。
 9. [Create selected objects in this folder] (選択したオブジェクトをこのフォルダに作成) を選択し、[Delete selected objects in this folder] (このフォルダ内の選択したオブジェクトを削除) を選択します。続いて、[Next] (次へ) をクリックします。



10. [Read] (読み取り) と [Write] (書き込み) を選択し、[Next] (次へ) をクリックします。



11. [Completing the Delegation of Control Wizard] (制御の委任の完了ウィザード) ページで情報を確認し、[Finish] (完了) を選択します。
12. 強力なパスワードでユーザーを作成し、そのユーザーを Joiners グループに追加します。その後、ユーザーは ディレクトリ AWS Directory Service に接続するための十分な権限を持ちます。

Simple AD の DHCP オプションセットの作成

AWS では、AWS Directory Service ディレクトリの DHCP オプションセットを作成し、ディレクトリがある VPC に DHCP オプションセットを割り当てることをお勧めします。これにより、VPC 内のすべてのインスタンスで指定のドメインおよび DNS サーバーを参照し、ドメイン名を解決できるようになります。

DHCP オプションセットの詳細については、「Amazon VPC ユーザーガイド」の「[DHCP options sets](#)」(DHCP オプションセット)を参照してください。

ディレクトリの DHCP オプションセットを作成するには

1. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。

2. ナビゲーションペインで [DHCP Options Sets] (DHCP オプションセット) を選択し、[Create DHCP options set] (DHCP オプションセットの作成) を選択します。
3. [Create DHCP options set] (DHCP オプションセットの作成) ページで、ディレクトリの次の値を入力します。

名前

オプションセットのオプションタグ。

ドメイン名

ディレクトリの完全修飾名 (例: corp.example.com)。

ドメインネームサーバー

AWS指定したディレクトリの DNS サーバーの IP アドレス。

 Note

この IP アドレスは、[AWS Directory Service コンソール](#)のナビゲーションペインに移動し、[Directories] (ディレクトリ) を選択して正しいディレクトリ ID を選択すると確認できます。

NTP サーバー

このフィールドは空白のままにします。

NetBIOS ネームサーバー

このフィールドは空白のままにします。

NetBIOS ノードタイプ

このフィールドは空白のままにします。

4. [Create DHCP options set] を選択します。新しい DHCP オプションのセットが DHCP オプションの一覧に表示されます。
5. 新しい DHCP オプションセットの ID (dopt-xxxxxxxx) を書き留めておきます。これは、新しいオプションセットを VPC に関連付けるときに使用します。

VPC に関連付けられた DHCP オプションセットを変更するには

DHCP オプションセットを作成後に変更することはできません。VPC で異なる DHCP オプションセットを使用するには、新しいセットを作成して VPC に関連付ける必要があります。DHCP オプションを使用しないように VPC を設定することもできます。

1. Amazon VPC コンソール (<https://console.aws.amazon.com/vpc/>) を開きます。
2. ナビゲーションペインで、[Your VPCs (お使いの VPC)] を選択します。
3. VPC を選択して、[アクション]、[DHCP オプションセットの編集] を順番に選択します。
4. [DHCP options set] (DHCP オプションセット) で、オプションセットを選択するか、[No DHCP options set] (DHCP オプションセットなし) を選択し、[Save] (保存) をクリックします。

コマンドラインを使用して、VPC に関連付けられた DHCP オプションセットを変更するには、次の内容を参照してください:

- AWS CLI: [associate-dhcp-options](#)
- AWS Tools for Windows PowerShell: [Register-EC2DhcpOption](#)

Simple AD におけるユーザーとグループの管理

ユーザーとは、ディレクトリにアクセスできる個別の人物、またはエンティティのことです。グループでは、複数のユーザーにまとめて権限を付与または拒否できるため、個別のユーザーに権限を付与する場合に比べ非常に便利になります。ユーザーが別の組織に異動した場合は、そのユーザーを別のグループに移動させます。これにより、新しい組織に必要な権限がそのユーザーに自動的に付与されます。

AWS Directory Service ディレクトリにユーザーとグループを作成するには、AWS Directory Service ディレクトリに結合されたインスタンス (オンプレミスまたは EC2 のいずれか) を使用し、ユーザーとグループを作成する権限を持つユーザーとしてログインする必要があります。また、ユーザーとコンピュータのスナップインを使用してユーザーとグループを追加できるように、EC2 Active Directory インスタンスに Active Directory ツールをインストールする必要があります。EC2 インスタンスをセットアップして必要なツールをインストールする方法の詳細については、「[Amazon EC2 インスタンスを Simple AD に結合する方法](#)」を参照してください。

 Note

ユーザーアカウントの Kerberos 事前認証を有効にしておく必要があります。これは、新しいユーザーアカウントのデフォルト設定ですが、変更しないでください。この設定の詳細については、Microsoft TechNet の「[Preauthentication](#)」(事前認証) を参照してください。

以降のトピックでは、ユーザーとグループを作成し管理する方法について取り上げます。

トピック

- [Simple AD の Active Directory 管理ツールをインストールする](#)
- [Simple AD ユーザーの作成](#)
- [Simple AD ユーザーの削除](#)
- [Simple AD ユーザーパスワードのリセット](#)
- [Simple AD グループの作成](#)
- [Simple AD ユーザーをグループに追加する](#)

Simple AD の Active Directory 管理ツールをインストールする

Amazon EC2 の Windows サーバーインスタンスから Active Directory を管理するには、そのインスタンスに Active Directory Domain Services および Active Directory Lightweight Directory Services ツールをインストールする必要があります。以下の手順を使用して、これらのツールを EC2 Windows Server インスタンスにインストールします。

前提条件

この手順を開始する前に、以下を完了してください。

1. Simple AD Active Directory を作成します。詳細については、「[Simple AD を作成する](#)」を参照してください。
2. EC2 Windows Server インスタンスを起動して Simple AD Active Directory に結合します。EC2 インスタンスでユーザーとグループを作成するには、以下のポリシーが必要です **AmazonSSMDirectoryServiceAccess** と **AmazonSSMManagedInstanceCore**。詳細については、「[Amazon EC2 Windows インスタンスを Simple AD Active Directory に結合する](#)」を参照してください。

3. アクティブディレクトリドメイン管理者の認証情報が必要になります。これらの認証情報は、管理対象の Managed Microsoft AD の作成時に作成されました。[Simple AD を作成する](#)の手順に従った場合、管理者ユーザー名には NetBIOS 名 **corp\administrator**が含まれます。

EC2 Windows Serverインスタンス に Active Directory 管理ツールをインストールするには

1. Amazon EC2 コンソールの <https://console.aws.amazon.com/ec2/> を開いてください。
2. Amazon EC2 コンソールで [インスタンス] を選択し、Windows Server インスタンスを選択して、[接続] を選択します。
3. [インスタンスに接続] ページで [RDP クライアント] を選択します。
4. [RDP クライアント] タブで [リモートデスクトップファイルのダウンロード] を選択し、[パスワードを取得] を選択してパスワードを取得します。
5. [Windows パスワードを取得] で、[プライベートキーファイルのアップロード] を選択します。Windows Server インスタンスに関連付けられている .pem プライベートキーファイルを選択します。プライベートキーファイルをアップロードしたら、[パスワードの復号化] を選択します。
6. [Windows セキュリティ] ダイアログボックスで、Windows Server コンピュータのローカル管理者の認証情報をコピーしてサインインします。ユーザー名を **NetBIOS-Name\administrator** または **DNS-Name\administrator** の形式にすることができます。たとえば、[Simple AD を作成する](#)の手順に従った場合**corp\administrator**はユーザー名になります。
7. Windows Server インスタンスにサインインしたら、[スタート] メニューから [サーバーマネージャー] を選択して [サーバーマネージャー] を開きます。
8. [サーバーマネージャー] ダッシュボードで、[役割と機能の追加] を選択します。
9. [Add Roles and Features Wizard] (ロールと機能の追加ウィザード) で、[Installation Type] (インストールのタイプ) として [Role-based or feature-based installation] (ロールベースまたは機能ベースのインストール) を選択し、[Next] (次へ) をクリックします。
10. [Server Selection] (サーバーの選択) で、ローカルサーバーが選択されていることを確認し、左のナビゲーションペインの [Features] (機能) を選択します。
11. [機能] ツリーで、[リモートサーバー管理ツール]、[ロール管理ツール] の順に開き、[AD DS および AD LDS ツール] を選択します。[AD DS および AD LDS ツール] を選択すると、[PowerShell のための Active Directory もジュール]、[AD DS ツール]、および [AD LDS スナップインとコマンドラインツール] が選択されます。下にスクロールして [DNS サーバーツール] を選択し、[次へ] を選択します。

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. 情報を確認して [Install] (インストール) を選択します。機能のインストールが終了すると、Active Directory Domain Services と Active Directory Lightweight Directory Services ツールが [スタート] 画面の [管理ツール] フォルダから利用できるようになります。

Simple AD ユーザーの作成

Simple AD ディレクトリと結合した Amazon EC2 インスタンスを使用するユーザーを作成するには、次の手順に従います。ユーザーを作成する前に、「[Active Directory 管理ツールのインストール](#)」の手順を完了する必要があります。

Note

Simple AD の使用において、「最初のログイン時にユーザーにパスワードの変更を強制する」オプションを指定して Linux インスタンスのユーザーアカウントを作成する場合、そのユーザーは kpasswd を使用して初期のパスワード変更ができません。初めてパスワードを変

更する場合、ドメイン管理者が Active Directory 管理ツールを使用してユーザーのパスワードを更新する必要があります。

ユーザーを作成するには

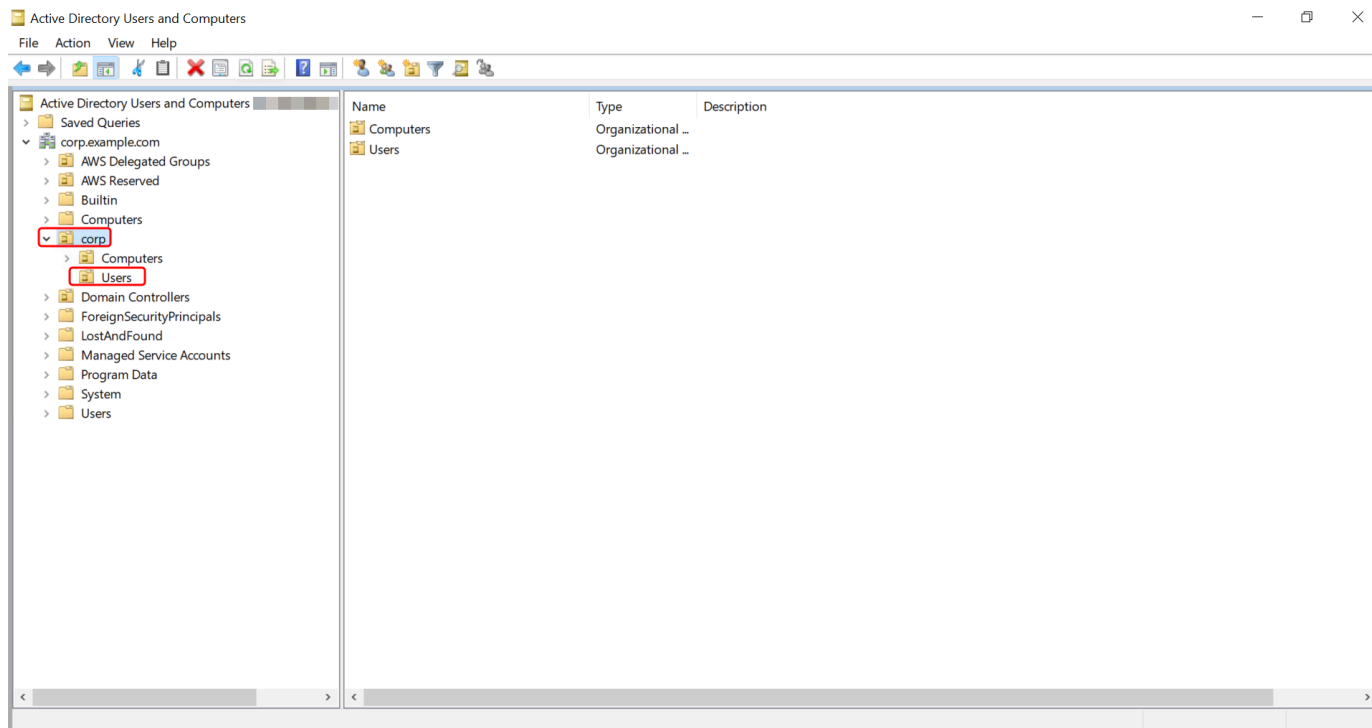
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Windows のスタートメニューから Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Windows Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリーで、ディレクトリの NetBIOS 名を持つ OU の下で、ユーザーを保存する OU (**corp\Users** など) を選択します。のディレクトリで使用する OU 構造の詳細については AWS、「」を参照してください [AWS Managed Microsoft AD で作成されるもの](#)。



4. [Action] メニューで、[New]、[User] の順に選択し、新規ユーザーのウィザードを開きます。

5. ウィザードの最初のページで、以下のフィールドに入力し、[Next] をクリックします。
 - [First name] (名)
 - [Last name] (姓)
 - [User logon name] (ユーザーのログオン名)
6. ウィザードの 2 番目のページで、[Password] と [Confirm Password] に、仮パスワードを入力します。[User must change password at next logon] (ユーザーは次回ログオン時にパスワードの変更が必要) オプションが選択されていることを確認します。その他のオプションは選択しないでください。[Next (次へ)] を選択します。
7. ウィザードの 3 番目のページで、新しいユーザーの情報が正しいことを確認し、[Finish] をクリックします。新しいユーザーが [Users] フォルダに表示されます。

Simple AD ユーザーの削除

Simple AD ディレクトリと結合した Amazon EC2 Windows インスタンスを使用するユーザーを削除するには、次の手順に従います。

ユーザーを削除するには

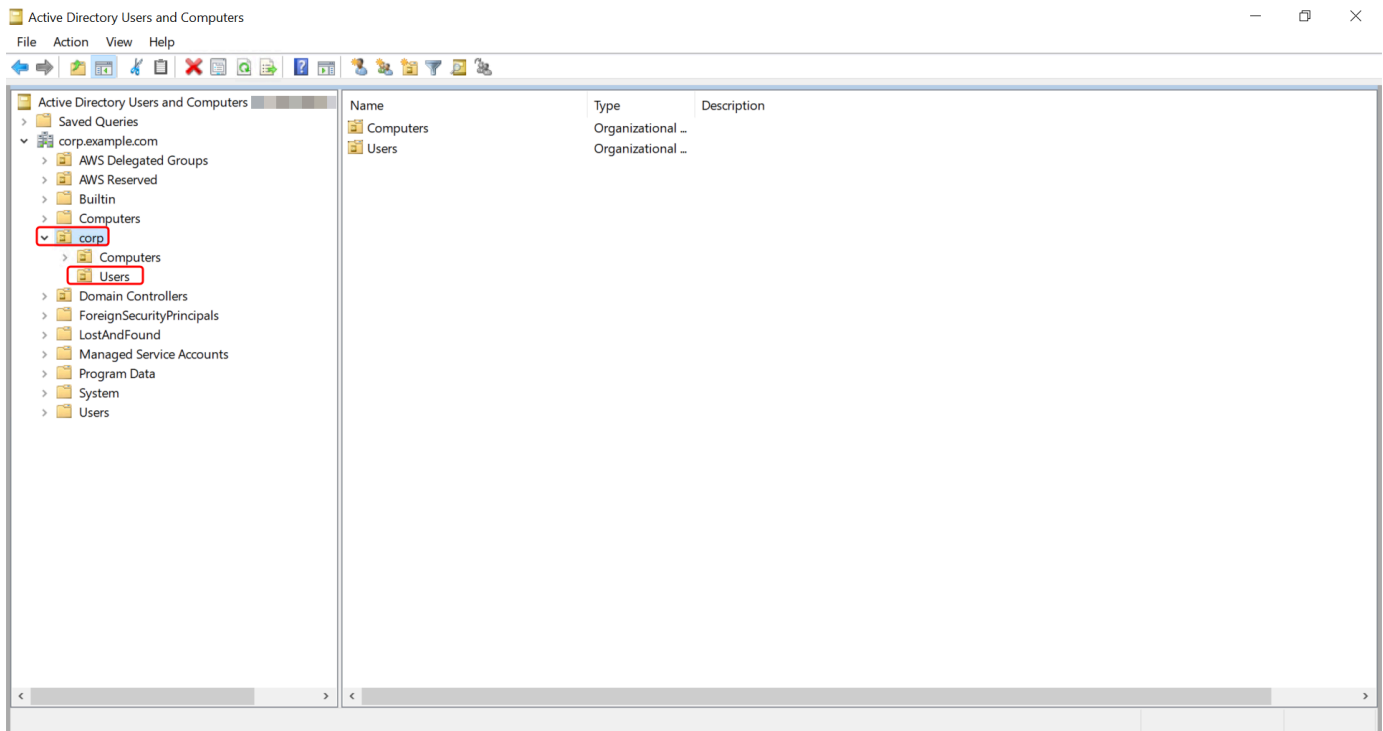
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Windows のスタートメニューから Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Windows Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリーで、削除したいユーザーを含む OU を選択します (例: **corp\Users**)。



4. 削除するユーザーを選択します。[アクション] メニューで、[削除] を選択します。
5. ユーザーを削除するかどうかを確認するダイアログボックスが表示されます。[はいs] を選択してユーザーを削除します。この操作で選択したユーザーは、完全に削除されます。

Simple AD ユーザーパスワードのリセット

ユーザーは、Active Directory で定義されているパスワードポリシーに従う必要があります。時々、Active Directory 管理者などのユーザーであってもこのルールを追えなくなり、パスワードを忘れてしまうこともあります。この場合、ユーザーが Simple AD に属 AWS Directory Service している場合は、を使用してユーザーのパスワードをすばやくリセットできます。

パスワードをリセットするには、リセットに必要な権限を持つユーザーとしてサインインする必要があります。権限の詳細については、「[AWS Directory Service リソースへのアクセス許可の管理の概要](#)」を参照してください。

Active Directory 内のユーザーのパスワードを、以下の例外を除きリセットすることが可能です：

- Active Directory の作成時に使用した NetBIOS 名に基づく組織単位 (OU) 内の任意のユーザーのパスワードをリセットできます。例えば、[Simple AD を作成する](#) の手順に従った場合、NetBIOS 名は CORP になり、リセットできるユーザーのパスワードは Corp/Users OU のメンバーになります。

- Active Directory の作成時に使用した NetBIOS 名に基づく OU 以外のユーザーのパスワードをリセットすることはできません。Simple AD の OU 構造の詳細については、[Simple AD で作成されるもの](#) を参照してください。
- 2 つのドメインのメンバーであるユーザーのパスワードをリセットすることはできません。Simple AD では、ユーザーが Domain Admins または Enterprise Admins グループのメンバーである場合、管理者ユーザー以外のどのユーザーのパスワードをリセットすることはできません。
- ユーザーが Domain Admins または Enterprise Admins グループのメンバーである場合、管理者ユーザー以外のどのユーザーのパスワードをリセットすることはできません。

以下のいずれかの方法でユーザーのパスワードをリセットできます:

- AWS Management Console
- AWS CLI

AWS Management Console

1. 「[AWS Directory Service コンソール](#)」のナビゲーションペインの [Active Directory] で、[ディレクトリ] を選択し、リスト内でユーザーのパスワードをリセットしたい Active Directory を選択します。
2. [ディレクトリの詳細] ページで、[アクション] を選択して [ユーザーパスワードのリセット] をクリックします。
3. [Reset user password] ダイアログで、[Username] に、パスワードの変更が必要なユーザーの名前を入力します。
4. [New password] (新しいパスワード) と [Confirm Password] (パスワードの確認) にパスワードを入力した上で、[Reset password] (パスワードをリセットする) をクリックします。

AWS CLI

1. をインストールするには AWS CLI、[「の最新バージョンをインストールまたは更新する AWS CLI」](#) を参照してください。
2. を開きます AWS CLI。
3. 次のコマンドを入力し、ディレクトリ ID、ユーザー名 `jane.doe`、パスワード `P@ssw0rd` を自分の Active Directory ディレクトリ ID と必要な認証情報に置き換えます。詳細については、「AWS CLI コマンドリファレンス」の [「reset-user-password」](#) を参照してください。

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

Simple AD グループの作成

以下の手順を使用して、Simple AD ディレクトリに参加している Amazon EC2 インスタンスを含むセキュリティグループを作成します。セキュリティグループを作成する前に、「Active Directory 管理ツールのインストール」の手順を完了する必要があります。

グループを作成するには

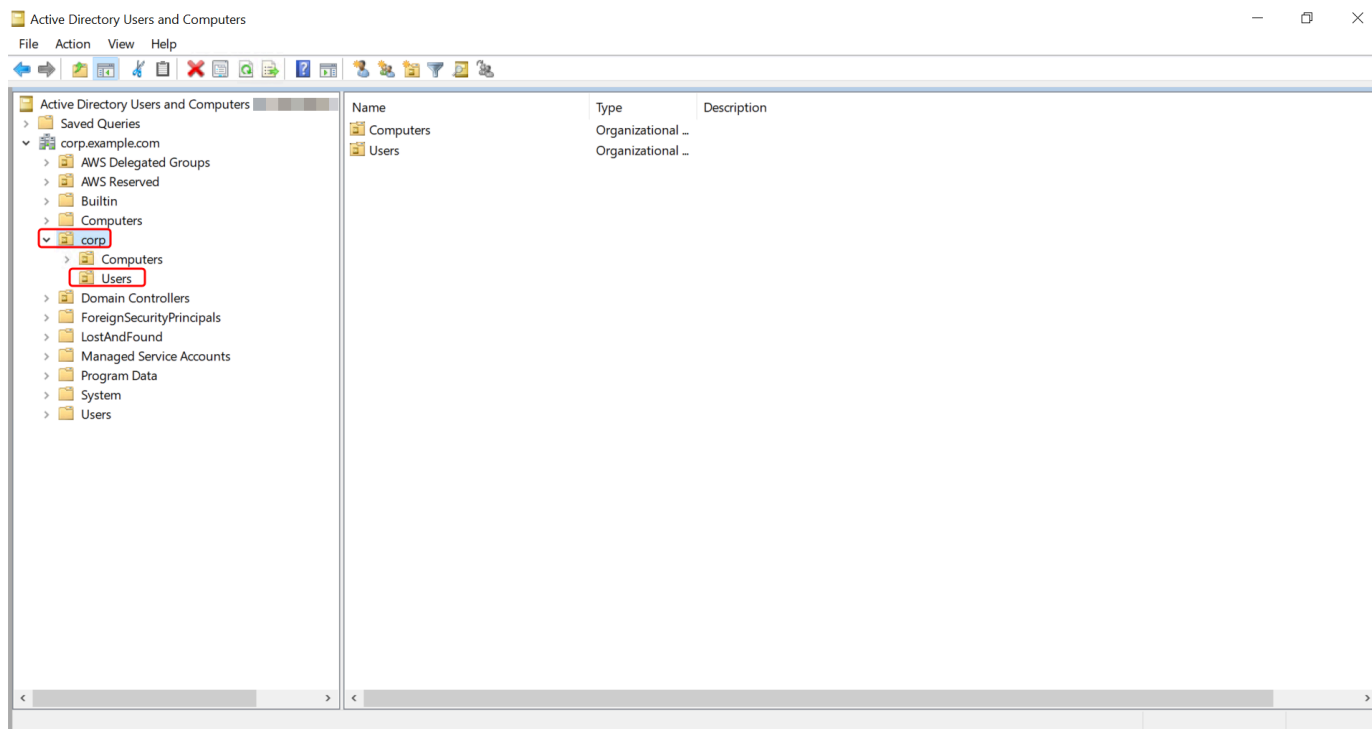
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリー内で、ディレクトリの NetBIOS 名を持つ OU の下から、グループを保存する OU (Corp\ Users など) を選択します。のディレクトリで使用される OU 構造の詳細については AWS、「」を参照してください [AWS Managed Microsoft AD で作成されるもの](#)。



4. [Action] (アクション) メニューで、[New] (新規)、[Group] (グループ) の順に選択し、新規グループのウィザードを開きます。
5. [グループ名] にグループの名前を入力し、[グループのスコープ] を選択します。[グループの種類] から [セキュリティ] を選択します。Active Directory グループのスコープとセキュリティグループの詳細については、Microsoft Windows Server ドキュメントの「[Active Directory セキュリティグループ](#)」を参照してください。
6. [OK] をクリックします。新しいセキュリティグループが [Users] フォルダに表示されます。

Simple AD ユーザーをグループに追加する

Simple AD ディレクトリに結合された EC2 インスタンスを持つセキュリティグループにユーザーを追加するには、次の手順に従います。

ユーザーをグループに追加するには

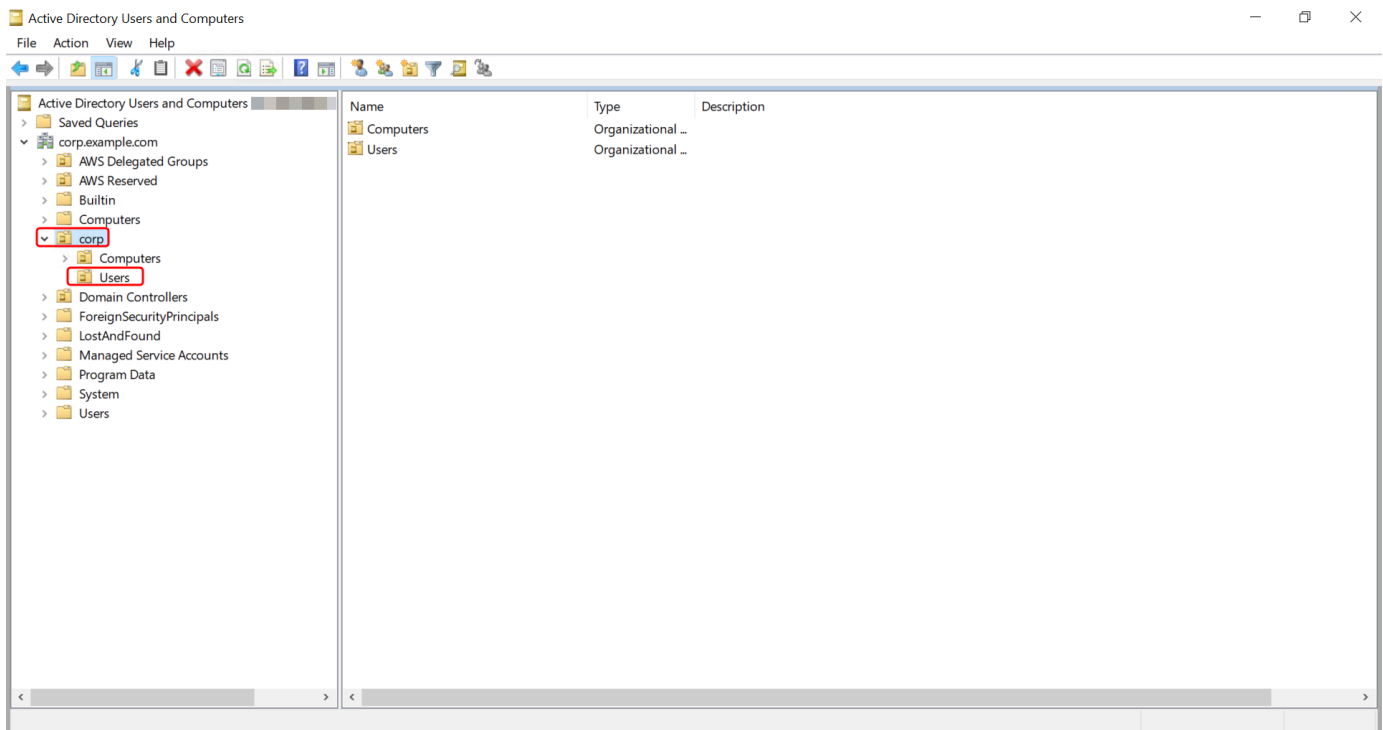
1. Active Directory 管理ツールがインストールされているインスタンスに接続します。
2. Active Directory ユーザーとコンピュータツールを開きます。このツールへのショートカットは [Administrative Tools] フォルダにあります。

Tip

インスタンスのコマンドプロンプトから以下のコマンドを実行すると、Active Directory ユーザーとコンピュータのツールボックスを直接開くことができます。

```
%SystemRoot%\system32\dsa.msc
```

3. ディレクトリツリーで、グループを保存したディレクトリの NetBIOS 名を持つ OU の下にある OU を選択し、ユーザーをメンバーとして追加するグループを選択します。



4. [Action] (アクション) メニューで、[Properties] (プロパティ) をクリックしてグループのプロパティダイアログボックスを開きます。
5. [Members] (メンバー) タブを開き、[Add] (追加) をクリックします。
6. [Enter the object names to select] で、追加するユーザー名を入力した後、[OK] をクリックします。対象の名前が [Members] (メンバー) リストに表示されます。もう一度 [OK] をクリックしてグループのメンバーシップを更新します。
7. [Users] フォルダでこのユーザーを選択し、[Action] (操作) メニューの [Properties] (プロパティ) をクリックしてプロパティダイアログボックスを開いて、ユーザーがグループのメンバーになっていることを確認します。[Member Of] (所属するグループ) タブを開きます。ユーザーが所属するグループのリストに、グループの名前が表示されます。

Simple AD のクォータ

一般的に、Small Simple AD ディレクトリには 500 人を超えるユーザーを追加できません。また、Large Simple AD ディレクトリには 5,000 人を超えるユーザーを追加できません。より柔軟なスケーリングオプションと追加の Active Directory 機能については、代わりに AWS Directory Service for Microsoft Active Directory (Standard Edition または Enterprise Edition) の使用を検討してください。

次に示すのは、Simple AD のデフォルトのクォータです。特に明記されていない限り、各クォータはリージョンごとに適用されます。

Simple AD のクォータ

リソース	デフォルトのクォータ
Simple AD ディレクトリ	10
手動スナップショット *	Simple AD ごとに 5

* 手動スナップショットのクォータは変更できません。

Note

AWS Elastic Network Interface (ENI) にパブリック IP アドレスをアタッチすることはできません。

Simple AD のトラブルシューティング

以下の内容は、Simple AD Active Directory の作成や使用時に発生する一般的な問題のトラブルシューティングに役立ちます。

トピック

- [パスワードの復旧](#)
- [Simple AD にユーザーを追加したとき、「KDC can't fulfill requested option」というエラーが表示される](#)
- [ドメインに結合したインスタンスの、DNS 名または IP アドレスの更新 \(DNS の動的更新\) ができない](#)

- [SQL Server のアカウントを使用して SQL Server にログインできない](#)
- [Simple AD が「リクエスト済み」状態で止まっている](#)
- [Simple AD を作成すると、「AZ constrained」エラーが表示される](#)
- [一部のユーザーが Simple AD で認証できない](#)
- [追加リソース](#)
- [Simple AD ディレクトリのステータスメッセージのトラブルシューティング](#)

パスワードの復旧

ユーザーがパスワードを忘れた場合や Simple AD ディレクトリへのサインインに問題がある場合は、AWS Management Console、PowerShell、または AWS CLIを使用してパスワードをリセットできます。

詳細については、「[Simple AD ユーザーパスワードのリセット](#)」を参照してください。

Simple AD にユーザーを追加したとき、「KDC can't fulfill requested option」というエラーが表示される

これは、Samba CLI クライアントがすべてのドメインコントローラーに対して「net」コマンドを正しく送信しなかった場合に発生することがあります。「net ads」コマンドを使用して Simple AD ディレクトリにユーザーを追加するときに、このエラーメッセージが表示される場合には、-S 引数を使用して、ドメインコントローラーの IP アドレスのうち 1 つを指定します。それでもこのエラーが表示される場合は、別のドメインコントローラーを試してください。また、Active Directory 管理ツールを使用して、ディレクトリにユーザーを追加することもできます。詳細については、「[Simple AD の Active Directory 管理ツールをインストールする](#)」を参照してください。

ドメインに結合したインスタンスの、DNS 名または IP アドレスの更新 (DNS の動的更新) ができない

DNS の動的な更新は、Simple AD ドメインでサポートされていません。ドメインに結合されているインスタンスで DNS Manager を使用してディレクトリに接続し、直接変更を行うこともできます。

SQL Server のアカウントを使用して SQL Server にログインできない

SQL Server アカウントで SQL Server Management Studio (SSMS) を使用して、Windows 2012 R2 Amazon EC2 インスタンス上で実行されている SQL Server にログインしようとする、エラーが表示される場合があります。この問題は、ドメインユーザーとして SSMS を実行した場合に発生しま

す。有効な認証情報を入力していても Login failed for user エラーが表示される場合があります。これは既知の問題であり AWS、積極的に解決に取り組んでいます。

この問題を回避するには、SQL 認証ではなく、Windows 認証を使用して SQL Server にログインします。または、Simple AD のドメインユーザーではなく、ローカルユーザーとして SSMS を起動します。

Simple AD が「リクエスト済み」状態で止まっている

5 分を経過しても、Simple AD が Requested の状態で止まっていて変わらない場合は、ディレクトリを削除して、作成し直してください。この問題が解決しない場合は、[AWS サポート センター](#)までお問い合わせください。

Simple AD を作成すると、「AZ constrained」エラーが表示される

2012 年より前に作成された一部の AWS アカウントでは、AWS Directory Service ディレクトリをサポートしていない米国東部 (バージニア北部)、米国西部 (北カリフォルニア)、またはアジアパシフィック (東京) リージョンのアベイラビリティゾーンにアクセスできる場合があります。ディレクトリ作成時にこのようなエラーが表示される場合は、別のアベイラビリティゾーンのサブネットを選択して、ディレクトリを再度作成してください。

一部のユーザーが Simple AD で認証できない

ユーザーアカウントの Kerberos 事前認証を有効にしておく必要があります。新しいユーザーアカウントでは、これがデフォルトの設定なので、変更しないでください。この設定の詳細については、Simple AD TechNet の「[事前認証](#)」を参照してください。

追加リソース

以下のリソースは、作業中のトラブルシューティングに役立ちます AWS。

- [AWS ナレッジセンター](#) - 問題のトラブルシューティングに役立つFAQsと他のリソースへのリンクを見つけます。
- [AWS サポートセンター](#) - テクニカルサポートを受ける。
- [AWS プレミアムサポートセンター](#) - プレミアムテクニカルサポートを利用できます。

トピック

- [Simple AD ディレクトリのステータスメッセージのトラブルシューティング](#)

Simple AD ディレクトリのステータスメッセージのトラブルシューティング

ディレクトリには障害が発生したり、動作しなかったりした場合、ディレクトリのステータスメッセージに追加情報が含まれます。ステータスメッセージは AWS Directory Service コンソールに表示されるか、[DescribeDirectories](#) API によって [DirectoryDescription.StageReason](#) メンバーに返されます。ディレクトリのステータスについての詳細は、「[AWS Managed Microsoft AD ディレクトリのステータスについて](#)」を参照してください。

次に、Simple AD ディレクトリのステータスメッセージを示します。

トピック

- [The directory service's elastic network interface is not attached \(Directory Service の Elastic Network Interface がアタッチされていません\)](#)
- [Issue\(s\) detected by instance \(インスタンスで問題が検出されました\)](#)
- [重要な AWS Directory Service 予約済みユーザーが ディレクトリにありません](#)
- [重要な AWS Directory Service 予約済みユーザーはドメイン管理者グループに属している必要があります](#)
- [重要な AWS Directory Service 予約済みユーザーは無効になっています](#)
- [The main domain controller does not have all FSMO roles \(メインのドメインコントローラーにすべての FSMO ロールがありません\)](#)
- [Domain controller replication failures \(ドメインコントローラーのレプリケーション障害\)](#)

The directory service's elastic network interface is not attached (Directory Service の Elastic Network Interface がアタッチされていません)

説明

VPC とのネットワーク接続を確立するためにディレクトリの作成時にユーザーに代わって作成された重要な Elastic Network Interface (ENI) は、ディレクトリ instance. AWS applications backed by this directory にはアタッチされません。ディレクトリをオンプレミスネットワークに接続することはできません。

トラブルシューティング

ENI がデタッチされているにもかかわらずまだ存在する場合は、サポートへお問い合わせください。ENI を削除すると、問題を解決する方法がなくなり、ディレクトリは完全に使用できなくなります。この場合、ディレクトリを削除して新しいディレクトリを作成する必要があります。

Issue(s) detected by instance (インスタンスで問題が検出されました)

説明

インスタンスにより内部エラーが検出されました。これは通常、問題のあるインスタンスの復旧をモニタリングサービスが積極的に試みていることを示します。

トラブルシューティング

ほとんどの場合、これは一時的な問題であり、ディレクトリは最終的にアクティブ状態に戻ります。問題が解決しない場合は、サポート にお問い合わせください。

重要な AWS Directory Service 予約済みユーザーが ディレクトリにありません

説明

Simple AD が作成されると、は ディレクトリに という名前のサービスアカウント AWS Directory Service を作成しますAWSAdminD-xxxxxxx。このサービスアカウントが見つからないとき、このエラーが発生します。AWS Directory Service では、このアカウントなしでディレクトリの管理機能を実行できず、ディレクトリを使用できません。

トラブルシューティング

この問題を修正するには、サービスアカウントが削除される前に作成された、以前のスナップショットにディレクトリを復元します。Simple AD ディレクトリの自動スナップショットは、1 日に 1 回作成されます。アカウントが削除された日から 5 日以上経過している場合は、このアカウントが存在する状態にディレクトリを復元できない可能性があります。このアカウントが存在するスナップショットからディレクトリを復元できない場合、ディレクトリが完全に使用できなくなる可能性があります。そのような場合、ディレクトリを削除して新しいディレクトリを作成する必要があります。

重要な AWS Directory Service 予約済みユーザーはドメイン管理者グループに属している必要があります

説明

Simple AD が作成されると、は ディレクトリに という名前のサービスアカウント AWS Directory Service を作成しますAWSAdminD-xxxxxxxxxx。このサービスアカウントが Domain Admins グループのメンバーでない場合、このエラーが発生します。このグループのメンバーシップは、FSMO ロール AWS Directory Service の移管、新しいディレクトリコントローラーのドメイン結合、スナップショットからの復元など、メンテナンスおよびリカバリオペレーションの実行に必要な権限を付与するために必要です。

トラブルシューティング

Active Directory Users and Computers ツールを使用して、サービスアカウントを Domain Admins グループに再度追加します。

重要な AWS Directory Service 予約済みユーザーは無効になっています

説明

Simple AD が作成されると、は ディレクトリに という名前のサービスアカウント AWS Directory Service を作成しますAWSAdminD-xxxxxxxxxx。このサービスアカウントが無効である場合、このエラーが発生します。が ディレクトリでメンテナンスおよびリカバリオペレーションを実行できるようにするには AWS Directory Service 、このアカウントを有効にする必要があります。

トラブルシューティング

Active Directory Users and Computers ツールを使用して、サービスアカウントを再度有効にします。

The main domain controller does not have all FSMO roles (メインのドメインコントローラーにすべての FSMO ロールがありません)

説明

すべての FSMO ロールが Simple AD のディレクトリコントローラーで所有されていません。AWS Directory Service では FSMO ロールが正しい Simple AD のディレクトリコントローラーに属していない場合、動作や機能を確実に保証することはできません。

トラブルシューティング

Active Directory ツールを使用して、元の機能するディレクトリコントローラーに FSMO ロールを戻します。FSMO ロールの転送に関する詳細は、<https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds> を参照してください。それでも問題が解決しない場合は、[お問い合わせ](#) してください サポート。

Domain controller replication failures (ドメインコントローラーのレプリケーション障害)

説明

Simple AD のディレクトリコントローラーを相互にレプリケートできません。次のいずれかの問題が原因で、このエラーが発生します。

- ディレクトリコントローラーのセキュリティグループで、正しいポートが開かれていない。
- ネットワーク ACL の制限が厳しすぎる。
- VPC ルートテーブルにより、ディレクトリコントローラー間のネットワークトラフィックが正しくルーティングされていない。
- ディレクトリで、別のインスタンスがドメインコントローラーに昇格した。

トラブルシューティング

VPC のネットワーク要件についての詳細は、AWS Managed Microsoft AD 「[AWS Managed Microsoft AD を作成するための前提条件](#)」、AD Connector 「[AD Connector の前提条件](#)」または Simple AD 「[Simple AD の前提条件](#)」のいずれかを参照してください。ディレクトリに不明なドメインコントローラーがある場合は、それを降格する必要があります。VPC のネットワーク設定が正しいにもかかわらずエラーが解決しない場合は、[サポート](#) までお問い合わせください。

のセキュリティ AWS Directory Service

でのクラウドセキュリティが最優先事項 AWS です。お客様は AWS、セキュリティを最も重視する組織の要件を満たすように構築されたデータセンターとネットワークアーキテクチャを活用できます。

セキュリティは、AWS お客様とお客様の間の責任共有です。[責任共有モデル](#)では、これをクラウドのセキュリティおよびクラウド内のセキュリティとして説明しています。

- クラウドのセキュリティ – AWS クラウドで AWS サービスを実行するインフラストラクチャを保護する AWS 責任があります。AWS また、では、安全に使用できるサービスも提供しています。[「AWS」コンプライアンスプログラム](#)の一環として、サードパーティーの監査が定期的にセキュリティの有効性をテストおよび検証しています。が適用されるコンプライアンスプログラムの詳細については AWS Directory Service、[AWS「コンプライアンスプログラムによる対象範囲内のサービス」](#)を参照してください。
- クラウド内のセキュリティ – お客様の責任は、使用する AWS サービスによって決まります。また、お客様は、お客様のデータの機密性、企業の要件、および適用可能な法律および規制などの他の要因についても責任を担います。

このドキュメントは、を使用する際の責任共有モデルの適用方法を理解するのに役立ちます AWS Directory Service。以下のトピックでは、セキュリティおよびコンプライアンスの目的を達成する AWS Directory Service ように を設定する方法を示します。また、AWS Directory Service リソースのモニタリングや保護に役立つ他の AWS サービスの使用方法についても説明します。

セキュリティに関するトピック

このセクションには、以下のセキュリティに関するトピックがあります。

- [の ID とアクセスの管理 AWS Directory Service](#)
- [でのログ記録とモニタリング AWS Directory Service](#)
- [のコンプライアンス検証 AWS Directory Service](#)
- [の耐障害性 AWS Directory Service](#)
- [のインフラストラクチャセキュリティ AWS Directory Service](#)

セキュリティに関する追加のトピック

このガイドには、以下のセキュリティに関する追加のトピックがあります。

アカウント、信頼、AWS リソースアクセス

- [AWS Managed Microsoft AD Administrator アカウントとグループのアクセス許可](#)
- [グループ管理サービスアカウント](#)
- [AWS Managed Microsoft AD とセルフマネージド AD 間の信頼関係の作成](#)
- [Kerberos の制約付き委任](#)
- [AWS Managed Microsoft AD ユーザーとグループに IAM ロールを持つリソースへのアクセス権 AWS を付与する](#)
- [を使用した AWS アプリケーションとサービスの認可 AWS Directory Service](#)

ディレクトリをセキュリティで保護する

- [AWS Managed Microsoft AD を保護する](#)
- [AD Connector ディレクトリをセキュリティで保護する](#)

ログ記録とモニタリング

- [AWS Managed Microsoft AD のモニタリング](#)
- [AD Connector ディレクトリをモニタリングする](#)

耐障害性

- [AWS Managed Microsoft AD のパッチ適用とメンテナンス](#)

の ID とアクセスの管理 AWS Directory Service

にアクセスするには、ガリクエストの認証 AWS に使用できる認証情報 AWS Directory Service が必要です。これらの認証情報には、ディレクトリなどの AWS Directory Service AWS リソースにアクセスするためのアクセス許可が必要です。以下のセクションでは、[AWS Identity and Access Management \(IAM\)](#) と AWS Directory Service を使用して、リソースにアクセスできるユーザーを制御することでリソースを保護する方法について詳しく説明します。

- [認証](#)
- [アクセスコントロール](#)

認証

[IAM ID](#) AWS を使用して にアクセスする方法について説明します。

アクセスコントロール

リクエストを認証するための有効な認証情報を持つことができますが、アクセス許可がない限り、AWS Directory Service リソースを作成またはアクセスすることはできません。たとえば、AWS Directory Service ディレクトリを作成したり、ディレクトリスナップショットを作成したりするには、アクセス許可が必要です。

以下のセクションでは、 のアクセス許可を管理する方法について説明します AWS Directory Service。最初に概要のセクションを読むことをお勧めします。

- [AWS Directory Service リソースへのアクセス許可の管理の概要](#)
- [でのアイデンティティベースのポリシー \(IAM ポリシー\) の使用 AWS Directory Service](#)
- [AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)

AWS Directory Service リソースへのアクセス許可の管理の概要

すべての AWS リソースは AWS アカウントによって所有されます。結果として、リソースを作成またはアクセスするためのアクセス権限は、アクセス許可ポリシーで管理されます。ただし、管理者権限を持つユーザーであるアカウント管理者は、リソースにアクセス権限を付加できます。には、ユーザー、グループ、ロールなどの IAM ID にアクセス許可ポリシーをアタッチする機能もあります。また、 などの一部のサービスでは、リソースへのアクセス許可ポリシーのアタッチ AWS Lambda もサポートされています。

Note

アカウント管理者ロールの詳細については、「IAM ユーザーガイド」の「[IAM ベストプラクティス](#)」を参照してください。

トピック

- [AWS Directory Service リソースとオペレーション](#)
- [リソース所有権についての理解](#)

- [リソースへのアクセスの管理](#)
- [ポリシー要素の指定: アクション、効果、リソース、プリンシパル](#)
- [ポリシーでの条件を指定する](#)

AWS Directory Service リソースとオペレーション

では AWS Directory Service、プライマリリソースは ディレクトリです。AWS Directory Service はディレクトリスナップショットリソースをサポートしているため、スナップショットは既存のディレクトリのコンテキストのみで作成できます。このスナップショットは、サブリソースと呼ばれます。

これらのリソースには、次の表に示すとおり、一意の Amazon リソースネーム (ARN) が関連付けられています。

リソースタイプ	ARN 形式
ディレクトリ	arn:aws:ds: <i>region</i> : <i>account-id</i> :directory/ <i>external-directory-id</i>
スナップショット	arn:aws:ds: <i>region</i> : <i>account-id</i> :snapshot/ <i>external-snapshot-id</i>

AWS Directory Service には、実行するオペレーションのタイプに基づいて 2 つのサービス名前空間が含まれています。

- ds サービス名前空間には、適切なリソースを操作するための一連のオペレーションが用意されています。使用可能なオペレーションのリストについては、「[Directory Service のアクション](#)」を参照してください。
- ds-data サービス名前空間は、Active Directory オブジェクトに一連のオペレーションを提供します。使用可能なオペレーションのリストについては、「[Directory Service Data API Reference](#)」を参照してください。

リソース所有権についての理解

リソース所有者は、リソースを作成した AWS アカウントです。つまり、リソース所有者は、リソースを作成するリクエストを認証するプリンシパルエンティティ (ルートアカウント、IAM ユーザー、または IAM ロール) の AWS アカウントです。次の例は、この仕組みを示しています。

- AWS アカウントのルートアカウントの認証情報を使用してディレクトリなどの AWS Directory Service リソースを作成する場合、AWS アカウントはそのリソースの所有者です。
- AWS アカウントに IAM ユーザーを作成し、そのユーザーに AWS Directory Service リソースを作成するアクセス許可を付与する場合、そのユーザーはリソースを作成 AWS Directory Service することもできます。ただし、ユーザーが属する AWS アカウントがリソースを所有します。
- AWS Directory Service リソースを作成するアクセス許可を持つ IAM ロールを AWS アカウントに作成する場合、ロールを引き受けることができるすべてのユーザーがリソースを作成できます AWS Directory Service 。ロールが属する AWS アカウントがリソースを所有します AWS Directory Service 。

リソースへのアクセスの管理

アクセス権限ポリシー では、誰が何にアクセスできるかを記述します。以下のセクションで、アクセス許可ポリシーを作成するために使用可能なオプションについて説明します。

Note

このセクションでは、 のコンテキストでの IAM の使用について説明します AWS Directory Service。ここでは、IAM サービスに関する詳細情報を提供しません。IAM に関する詳細なドキュメントについては、「IAM ユーザーガイド」の「[IAM とは？](#)」を参照してください。IAM ポリシー構文と記述の説明については、「[IAM ユーザーガイド](#)」の「IAM JSON ポリシーリファレンス」を参照してください。

IAM アイデンティティにアタッチされたポリシーはアイデンティティベースのポリシー (IAM ポリシー) と呼ばれ、リソースにアタッチされたポリシーはリソースベースのポリシーと呼ばれます。はアイデンティティベースのポリシー (IAM ポリシー) のみ AWS Directory Service をサポートします。

トピック

- [アイデンティティベースのポリシー \(IAM ポリシー\)](#)
- [リソースベースのポリシー](#)

アイデンティティベースのポリシー (IAM ポリシー)

ポリシーを IAM アイデンティティにアタッチできます。例えば、次のオペレーションを実行できます。

- アカウントのユーザーまたはグループにアクセス許可ポリシーをアタッチする – アカウント管理者は、特定のユーザーに関連付けられているアクセス許可ポリシーを使用して、そのユーザーに新しいディレクトリなどの AWS Directory Service リソースを作成するアクセス許可を付与できます。
- アクセス権限ポリシーをロールにアタッチする (クロスアカウントの許可を付与) - ID ベースのアクセス権限ポリシーを IAM ロールにアタッチして、クロスアカウントの権限を付与することができます。

IAM を使用したアクセス許可の委任の詳細については、「IAM ユーザーガイド」の「[アクセス管理](#)」を参照してください。

次のアクセス権限ポリシーは、Describe で始まるすべてのアクションを実行するためのアクセス権限をユーザーに付与します。これらのアクションは、ディレクトリやスナップショットなどの AWS Directory Service リソースに関する情報を表示します。Resource 要素のワイルドカード文字 (*) は、アカウントが所有するすべての AWS Directory Service リソースに対してアクションが許可されていることを示します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "*"
    }
  ]
}
```

でのアイデンティティベースのポリシーの使用の詳細については AWS Directory Service、「」を参照してください [でのアイデンティティベースのポリシー \(IAM ポリシー\) の使用 AWS Directory Service](#)。ユーザー、グループ、ロール、アクセス権限の詳細については、「IAM ユーザーガイド」の「[ID \(ユーザー、グループ、ロール\)](#)」を参照してください。

リソースベースのポリシー

Amazon S3 などの他のサービスでは、リソースベースの許可ポリシーもサポートされています。たとえば、ポリシーを S3 バケットにアタッチして、そのバケットへのアクセス許可を管理できます。AWS Directory Service はリソースベースのポリシーをサポートしていません。

ポリシー要素の指定: アクション、効果、リソース、プリンシパル

サービスは、AWS Directory Service リソースごとに一連の API オペレーションを定義します。詳細については、「[AWS Directory Service リソースとオペレーション](#)」を参照してください。使用可能な API オペレーションのリストについては、「[Directory Service のアクション](#)」を参照してください。

これらの API オペレーションのアクセス許可を付与するために、はポリシーで指定できる一連のアクション AWS Directory Service を定義します。API オペレーションを実行する場合には、複数のアクションに対するアクセス許可が必要になることがあります。

以下は、基本的なポリシーの要素です。

- リソース – ポリシーで Amazon リソースネーム (ARN) を使用して、ポリシーを適用するリソースを識別します。AWS Directory Service リソースでは、IAM ポリシーで常にワイルドカード文字 (*) を使用します。詳細については、「[AWS Directory Service リソースとオペレーション](#)」を参照してください。
- [Action] (アクション) - アクションのキーワードを使用して、許可または拒否するリソースオペレーションを識別します。たとえば、ds:DescribeDirectories 権限は、AWS Directory Service DescribeDirectories オペレーションの実行をユーザーに許可します。
- [Effect] (効果) - ユーザーが特定のアクションをリクエストする時の効果を指定します。これは許可または拒否とすることが出来ます。リソースへのアクセスを明示的に付与 (許可) していない場合、アクセスは暗黙的に拒否されます。また、明示的にリソースへのアクセスを拒否すると、別のポリシーによってアクセスが許可されている場合でも、ユーザーはそのリソースにアクセスできなくなります。
- プリンシパル – ID ベースのポリシー (IAM ポリシー) で、ポリシーがアタッチされているユーザーが黙示的なプリンシパルとなります。リソースベースのポリシーでは、アクセス許可を受け取るユーザー、アカウント、サービス、またはその他のエンティティを指定します (リソースベースのポリシーにのみ適用されます)。AWS Directory Service はリソースベースのポリシーをサポートしていません。

IAM ポリシーの構文と記述の詳細については、「IAM ユーザーガイド」の「[IAM JSON ポリシーリファレンス](#)」を参照してください。

すべての AWS Directory Service API アクションとそれらが適用されるリソースを示す表については、「」を参照してください[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)。

ポリシーでの条件を指定する

アクセス許可を付与するとき、アクセスポリシー言語を使用して、ポリシーが有効になる条件を指定できます。例えば、特定の日付の後にのみ適用されるポリシーが必要になる場合があります。ポリシー言語での条件の指定の詳細については、「IAM ユーザーガイド」の「[条件](#)」を参照してください。

条件を表すには、あらかじめ定義された条件キーを使用します。AWS Directory Serviceに固有の条件キーはありません。ただし、必要に応じて使用できる AWS 条件キーがあります。AWS キーの完全なリストについては、IAM ユーザーガイドの「[利用可能なグローバル条件キー](#)」を参照してください。

AWS の 管理ポリシー AWS Directory Service

以下のセクションでは、固有の AWS 管理ポリシーについて説明します AWS Directory Service。これらのポリシーは、アカウントのユーザーに付加できます。

詳細については「IAM ユーザーガイド」の「[AWS マネージドポリシー](#)」を参照してください。

AWSDirectoryServiceFullAccess

[AWSDirectoryServiceFullAccess](#) が、ユーザーまたはグループに以下の内容を付与します:

- へのフルアクセス AWS Directory Service
- の使用に必要な主要な Amazon EC2 サービスへのアクセス AWS Directory Service
- Amazon SNS トピックを一覧表示する機能
- DirectoryMonitoring」で始まる名前の Amazon SNS トピックを作成、管理、削除する機能

AWSDirectoryServiceReadOnlyAccess

この[AWSDirectoryServiceReadOnlyAccess](#)ポリシーは、ルート AWS アカウントのすべての AWS Directory Service リソース、EC2 サブネット、EC2 ネットワークインターフェイス、Amazon

Simple Notification Service (Amazon SNS) トピックとサブスクリプションへの読み取り専用アクセスをユーザーまたはグループに付与します。詳細については、「[での AWS マネージドポリシーの使用 AWS Directory Service](#)」を参照してください。

AWSDirectoryServiceDataFullAccess

[AWSDirectoryServiceDataFullAccess](#) ポリシーは、ユーザーまたはグループに、AD ユーザー、メンバー、グループを作成、管理、表示するための Directory Service Data を使用した組み込みオブジェクト管理へのフルアクセスを許可します。詳細については、「[AWS Directory Service Data API Reference](#)」を参照してください。

- Directory Service Data へのフルアクセス

AWSDirectoryServiceDataReadOnlyAccess

[AWSDirectoryServiceDataReadOnlyAccess](#) ポリシーは、AD ユーザー、メンバー、およびグループを表示および検索するためのアクセスをユーザーまたはグループに付与します。詳細については、「[AWS Directory Service Data API Reference](#)」を参照してください。

- Directory Service Data を一覧表示する機能
- Directory Service Data を検索する機能
- Directory Service Data の説明を取得する機能

詳細については、「[での AWS マネージドポリシーの使用 AWS Directory Service](#)」を参照してください。

さらに、他の IAM ロールでの使用に適した他の AWS 管理ポリシーもあります。これらのポリシーは、AWS Directory Service デイレクトリ内のユーザーに関連付けられているロールに割り当てられます。これらのポリシーは、それらのユーザーが Amazon EC2 などの他の AWS リソースにアクセスするために必要です。詳細については、「[AWS Managed Microsoft AD ユーザーとグループに IAM ロールを持つリソースへのアクセス権 AWS を付与する](#)」を参照してください。

また、ユーザーが必要な API アクションおよびリソースにアクセスできるようにするカスタム IAM ポリシーも作成できます。これらのカスタムポリシーは、それらのアクセス許可が必要な IAM ユーザーまたはグループにアタッチできます。

IAM と マネージドポリシー AWS Directory Service の更新 AWS

サービスがこれらの変更の追跡を開始してからの IAM および AWS マネージドポリシーの更新に関する詳細を表示します。このページの変更に関する自動アラートについては、IAM および AWS Directory Service ドキュメント履歴ページの RSS フィードにサブスクライブしてください。

変更	説明	日付
AWSDirectoryServiceDataReadOnlyAccess - 新しいポリシー	AWS Directory Service は、ユーザーまたはグループが AD ユーザー、メンバー、グループを表示および検索できるようにする新しいポリシーを追加しました。	2024 年 9 月 17 日
AWSDirectoryServiceDataFullAccess - 新しいポリシー	AWS Directory Service は、ユーザーまたはグループが Directory Service Data を使用した組み込みオブジェクト管理にアクセスして AD ユーザー、メンバー、グループを作成、管理、表示できるようにする新しいポリシーを追加しました。	2024 年 9 月 17 日
AWS Directory Service が変更の追跡を開始しました	AWS Directory Service は、AWS 管理ポリシーの変更の追跡を開始しました。	2024 年 9 月 17 日

でのアイデンティティベースのポリシー (IAM ポリシー) の使用 AWS Directory Service

このトピックでは、アカウント管理者がIAMアイデンティティ (ユーザー、グループ、ロール) へのアクセス権限ポリシーをアタッチする、アイデンティティベースのポリシーの例を示します。これらの例は、の IAM ポリシーを示しています AWS Directory Service。ニーズと環境に合わせて独自のポリシーを変更して作成する必要があります。

⚠ Important

まず、AWS Directory Service リソースへのアクセスを管理するために利用できる基本概念とオプションについて説明する入門トピックを確認することをお勧めします。詳細については、「[AWS Directory Service リソースへのアクセス許可の管理の概要](#)」を参照してください。

このセクションでは、次のトピックを対象としています。

- [AWS Directory Service コンソールを使用するために必要なアクセス許可](#)
- [AWS の 管理 \(事前定義\) ポリシー AWS Directory Service](#)
- [カスタマーマネージドポリシーの例](#)
- [IAM ポリシーでのタグの使用](#)

以下に示しているのは、アクセス許可ポリシーの例です。

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"
      }
    }
  }
]
}

```

ポリシーの 3 つのステートメントは、次のようにアクセス許可を付与します。

- 最初のステートメントは、AWS Directory Service ディレクトリを作成するアクセス許可を付与します。AWS Directory Service は、リソースレベルのアクセス権限をサポートしていないため、ポリシーは Resource 値としてワイルドカード文字 (*) を指定します。
- 次のステートメントでは、IAM アクションへのアクセスは付与され、AWS Directory Service がユーザーに代わって IAM ロールの読み取りと作成できるようになります。Resource 値の末尾のワイルドカード文字 (*) は、このステートメントで任意の IAM ロールに対して IAM アクションを実行するアクセス許可が付与されることを意味します。このアクセス許可を特定のロールに制限するには、リソース ARN 内のワイルドカード文字 (*) を特定のロール名に置き換えます。詳細については、「[IAM のアクション](#)」を参照してください。
- 3 番目のステートメントは、ディレクトリを作成、設定、および破棄するために必要な Amazon EC2 内の特定のリソースセット AWS Directory Service にアクセス許可を付与します。

ロール ARN を自分のロールに置き換えます。詳細については、「[Amazon EC2 Actions](#)」を参照してください。

アイデンティティに基づくポリシーでは、アクセス権限の付与先のプリンシパルを指定しないため、Principal 要素は指定されません。ユーザーにそのポリシーをアタッチすると、そのユーザーが暗黙のプリンシパルになります。IAM ロールにアクセス許可ポリシーをアタッチすると、ロールの信頼ポリシーで識別されたプリンシパルがアクセス許可を得ることになります。

すべての AWS Directory Service API アクションとそれらが適用されるリソースを示す表については、「」を参照してください[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)。

AWS Directory Service コンソールを使用するために必要なアクセス許可

AWS Directory Service コンソールを操作するユーザーには、前述のポリシーに記載されているアクセス許可、または「」で説明されている Directory Service フルアクセスロールまたは Directory Service 読み取り専用ロールによって付与されたアクセス許可が必要です[AWS の 管理 \(事前定義\) ポリシー AWS Directory Service](#)。

これらの最小限必要なアクセス許可よりも制限された IAM ポリシーを作成している場合、その IAM ポリシーを使用するユーザーに対してコンソールは意図したとおりには機能しません。

AWS の 管理 (事前定義) ポリシー AWS Directory Service

AWS は、によって作成および管理される事前定義された、または管理された IAM ポリシーを提供することで、多くの一般的なユースケースに対処します AWS。マネージドポリシーは、一般的なユースケースに必要なアクセス許可を付与するため、必要なアクセス許可を決定するのに役立ちます。詳細については、「[AWS の 管理ポリシー AWS Directory Service](#)」を参照してください。

カスターマネージドポリシーの例

このセクションでは、さまざまな AWS Directory Service アクションのアクセス許可を付与するユーザーポリシーの例を示します。

Note

例はすべて、米国西部 (オレゴン) リージョン (us-west-2) を使用し、架空のアカウント ID を使用しています。

例

- [例 1: ユーザーに任意の AWS Directory Service リソースに対して Describe アクションを実行することを許可する](#)
- [例 2: ディレクトリの作成をユーザーに許可する](#)

例 1: ユーザーに任意の AWS Directory Service リソースに対して Describe アクションを実行することを許可する

次のアクセス許可ポリシーは、のディレクトリ ID を使用して AWS Managed Microsoft AD Describe で始まるすべてのアクションを実行するアクセス許可をユーザーに付与します。AWS アカウント 111122223333。これらのアクションは、ディレクトリやスナップショットなどの、AWS Directory Service リソースに関する情報を表示します。とアカウント番号を、使用するリージョンとアカウント番号に変更 AWS リージョン してください。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ds:Describe*",
      "Resource": "arn:aws:ds:us-west-2:111122223333:directory/d-1234567890"
    }
  ]
}
```

例 2: ディレクトリの作成をユーザーに許可する

次のアクセス許可ポリシーによって、ディレクトリおよび関連するすべての他のリソース (スナップショットや信頼など) を作成するアクセス許可がユーザーに付与されます。そのためには、特定の Amazon EC2 サービスへのアクセス許可も必要です。

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:"
      }
    ]
  }
}

```

IAM ポリシーでのタグの使用

ほとんどの AWS Directory Service API アクションに使用する IAM ポリシーで、タグベースのリソースレベルのアクセス許可を適用できます。これにより、ユーザーがどのリソースを作成、変更、または使用できるかを制御しやすくなります。IAM ポリシーの以下の条件コンテキストのキーと値とともに Condition 要素 (Condition ブロックとも呼ばれる) を使用して、リソースのタグに基づいてユーザーアクセス (アクセス許可) を制御できます。

- 特定のタグを持つリソースに対してユーザーアクションを許可または拒否するには、aws:ResourceTag/**tag-key: tag-value** を使用します。

- タグが許可されているリソースを作成または変更する API リクエストを作成する場合に、特定のタグを使用する (または使用しない) ことを要求するには、aws:ResourceTag/tag-key: tag-value を使用します。
- タグが許可されているリソースを作成または変更する API リクエストを作成する場合に、特定の一連のタグキーを使用する (または使用しない) ことを要求するには、aws:TagKeys: [tag-key, ...] を使用します。

Note

IAM ポリシーの条件コンテキストのキーと値は、タグ付け可能なリソースの識別子が必須パラメータである AWS Directory Service アクションにのみ適用されます。

「IAM ユーザーガイド」の「[タグを使用したアクセスの制御](#)」には、タグの使用に関する追加情報が記載されています。このガイドの「[IAM JSON ポリシーリファレンス](#)」セクションには、IAM で JSON ポリシーの要素、変数、および評価ロジックの構文、説明、および例が詳細に記載されています。

次のタグポリシーでは、次のタグが使用されている限り、AWS Directory Service ディレクトリの作成を許可します。

- 環境:本稼働
- 所有者: インフラストラクチャチーム
- コストセンター: 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"
        }
    }
}
]
}

```

次のタグポリシーでは、次のタグが使用されている限り、AWS Directory Service ディレクトリの更新と削除を許可します。

- プロジェクト: Atlas
- 部門: エンジニアリング
- 環境: ステージング

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"
                }
            }
        }
    ]
}

```

次のタグポリシーは、リソースに次のいずれかのタグがある AWS Directory Service のリソースタグ付けを拒否します。

- 本番稼働
- セキュリティ
- 機密

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "ds:AddTagsToResource"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:TagKeys": ["Production", "Security", "Confidential"]
        }
      }
    }
  ]
}
```

ARN の詳細については、[「Amazon リソースネーム \(ARNs AWS 「サービス名前空間」を参照してください。](#)

次の AWS Directory Service API オペレーションのリストは、タグベースのリソースレベルのアクセス許可をサポートしています。

- [AcceptSharedDirectory](#)
- [AddIpRoutes](#)
- [AddTagsToResource](#)
- [CancelSchemaExtension](#)
- [CreateAlias](#)

- [CreateComputer](#)
- [CreateConditionalForwarder](#)
- [CreateSnapshot](#)
- [CreateLogSubscription](#)
- [CreateTrust](#)
- [DeleteConditionalForwarder](#)
- [DeleteDirectory](#)
- [DeleteLogSubscription](#)
- [DeleteSnapshot](#)
- [DeleteTrust](#)
- [DeregisterEventTopic](#)
- [DescribeConditionalForwarders](#)
- [DescribeDomainControllers](#)
- [DescribeEventTopics](#)
- [DescribeSharedDirectories](#)
- [DescribeSnapshots](#)
- [DescribeTrusts](#)
- [DisableRadius](#)
- [DisableSso](#)
- [EnableRadius](#)
- [EnableSso](#)
- [GetSnapshotLimits](#)
- [ListIpRoutes](#)
- [ListSchemaExtensions](#)
- [ListTagsForResource](#)
- [RegisterEventTopic](#)
- [RejectSharedDirectory](#)
- [RemoveIpRoutes](#)
- [RemoveTagsFromResource](#)

- [ResetUserPassword](#)
- [RestoreFromSnapshot](#)
- [ShareDirectory](#)
- [StartSchemaExtension](#)
- [UnshareDirectory](#)
- [UpdateConditionalForwarder](#)
- [UpdateNumberOfDomainControllers](#)
- [UpdateRadius](#)
- [UpdateTrust](#)
- [VerifyTrust](#)

AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス

[アクセスコントロール](#) をセットアップし、IAM ID (ID ベースのポリシー) にアタッチできるアクセス許可ポリシーを作成する際、[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#) の表をリファレンスとして使用できます。内の各 API エントリには以下が含まれます。

- API オペレーションの名前。
- 各 API オペレーションに対応するアクション、またはその実行のためのアクセス権限を付与できるアクションを示しています。
- アクセス許可を付与できる AWS リソース

ポリシーの Action フィールドでアクションを指定し、ポリシーの Resource フィールドでリソースの値を指定します。アクションを指定するには、API オペレーション名 (ds:CreateDirectory など) の前に ds: プレフィックスを使用します。

AWS アプリケーションによっては、ポリシー ds:UnauthorizeApplication で ds:AuthorizeApplication、ds:CheckAlias、ds:CreateIdentityPoolDirectory、ds:Update など、非公開 AWS Directory Service API ds:GetAuthorizedApplicationDetails オペレーションを使用する必要がある場合があります。

AWS Directory Service APIs は、[AWS Management Console](#) を介してのみ呼び出すことができます。これらはプログラムで呼び出すことができないという意味ではパブリック API ではなく、

どの SDK からでも提供されていません。このサーバーにはユーザー認証情報が必要です。これらの API オペレーションには `ds:DisableRoleAccess`、`ds:EnableRoleAccess`、およびが含まれます `ds:UpdateDirectory`。

AWS Directory Service および Directory Service Data ポリシーで AWS グローバル条件キーを使用して、条件を表現できます。AWS キーの完全なリストについては、IAM ユーザーガイドの「[利用可能なグローバル条件キー](#)」を参照してください。

AWS Directory Service API とアクションに必要なアクセス許可

AWS Directory Service Data API とアクションに必要なアクセス許可

Note

アクションを指定するには、API オペレーション名 (例えば、`ds-data:AddGroupMember`) の前に `ds-data:` プレフィックスを使用します。

Directory Service Data API オペレーション	必要な許可 (API アクション)	リソース
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>	*
ListGroup	<code>ds-data:ListGroup</code>	*
ListGroupMembers	<code>ds-data:ListGroupMembers</code>	*

Directory Service Data API オペレーション	必要な許可 (API アクション)	リソース
ListGroupMembers	ds-data:ListGroupMembers	*
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	*

関連トピック

- [アクセスコントロール](#)

Directory Service Data の条件キー

「[Directory Service Data](#)」条件キーを使用して、ユーザーおよびグループレベルのアクセスに特定のステートメントを追加します。これによって、ユーザーには、どのプリンシパルがどのリソースに対してどのような条件下でアクションを実行できるかを定めることができます。

条件要素、または条件ブロックを使用すると、ステートメントが有効になる条件を指定できます。Condition 要素はオプションです。イコール (=) や未満 (<) などの条件演算子を使用して条件式を作成することで、ポリシーの条件とリクエスト内の値を一致させることができます。

1 つのステートメントに複数の要素を指定する場合、または 1 つの条件要素に複数のキーを指定する場合、AWS は論理演算子 AND を使用してそれらを評価します。1 つの条件キーに複数の値を指定すると、は論理 OR オペレーションを使用して条件 AWS を評価します。ステートメントの権限が

付与される前にすべての条件が満たされる必要があります。条件を指定する際にプレースホルダー変数も使用できます。例えば、ユーザー名でタグが付けられている場合のみ、リソースにアクセスする IAM ユーザーアクセス許可を付与できます。詳細については、「IAM ユーザーガイド」の「[複数のキーまたは値を含む IAM 条件](#)」参照してください。

これらの条件キーをサポートするアクションのリストについては、「サービス認可リファレンス」の [AWS「Directory Service Data」で定義されるアクション](#)」を参照してください。

 Note

タグに基づくリソースレベルのアクセス権限の詳細については、「[IAM ポリシーでのタグの使用](#)」を参照してください。

ds-data:SAMAccountName

「[文字列演算子](#)」で動作します。

指定された SAMAccountName を使用するポリシーがリクエストで使用されたポリシーと一致するかどうかを確認します。各リクエストで提供できる SAM アカウント名は 1 つだけです。

 Note

この条件キーでは大文字と小文字は区別されません。[StringEqualsIgnoreCase](#) または [StringNotEqualsIgnoreCase](#) 条件演算子を使用して、文字の大文字と小文字に関係なく文字列の値を比較する必要があります。

ユーザーまたはグループが AD オブジェクトを検索できるようにする

次のポリシーでは、ユーザー jstyles または のメンバー test-group に、AWS Managed Microsoft AD ドメイン内のユーザー、メンバー、およびグループの検索を許可します。

 Important

SAMAccountName または MemberName を使用する場合は、ds-data:Identifier を SAMAccountName として指定することをお勧めします。これにより、などの AWS Directory Service Data がサポートする将来の識別子が既存のアクセス許可を破る SID のを防ぐことができます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SearchOnTrustedDomain",
      "Effect": "Allow",
      "Action": "ds-data:Search*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:SAMAccountName": [
            "jstyles",
            "test-group"
          ],
          "StringEqualsIgnoreCase": {
            "ds-data:identifier": [
              "SAMAccountName"
            ]
          }
        }
      }
    }
  ]
}
```

ds-data:Identifier

「[文字列演算子](#)」で動作します。

リクエストで使用する識別子のタイプを指定します。Directory Service Data でサポートされる今後の識別子が既存のアクセス権限を妨げないように、識別子条件キーで SAMAccountName を常に指定することをお勧めします。

 Note

現在、SAMAccountName は許可される唯一の値です。ただし、将来的にはさらに多くの値が許可される可能性があります。

ユーザーまたはグループがレルムでユーザーを更新することを許可する

次のポリシーでは、ユーザー `jstyles` または `test-group` のメンバーが `example-domain.com` レルム内のユーザー情報を更新することを許可します。識別子キーは、`SAMAccountName` がリクエストコンテキストで渡される ID タイプであることを保証します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateUseronDomain",
      "Effect": "Allow",
      "Action": "ds-data:UpdateUser",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ds-data:SAMAccountName": [
            "jstyles",
            "test-group"
          ],
          "StringEquals": {
            "ds-data:Identifier": [
              "SAMAccountName"
            ],
            "StringEquals": {
              "ds-data:Realm": [
                "example-domain.com"
              ]
            }
          }
        }
      }
    }
  ]
}
```

ds-data:MemberName

「[文字列演算子](#)」で動作します。

指定された MemberName を使用するポリシー名がリクエストで使用されたポリシー名と一致するかどうかを確認します。

Note

この条件キーでは、大文字と小文字は区別されません。[StringEqualsIgnoreCase](#) または [StringNotEqualsIgnoreCase](#) 条件演算子を使用して、文字の大文字と小文字に関係なく、文字列の値を比較する必要があります。

グループへのメンバーの追加を許可する

次のポリシーでは、グループに追加される MemberName が region-1 で始まる場合、ユーザーまたはロールが指定されたディレクトリ内のグループにメンバーを追加することを許可します。

Important

MemberName または SAMAccountName を使用する場合は、ds-data:Identifier を SAMAccountName として指定することをお勧めします。これにより、SID などの Directory Service Data がサポートする将来の識別子が既存のアクセス権限を妨げるのを防ぐことができます。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateGroupsWithRegionalMembers",
      "Effect": "Allow",
      "Action": "ds-data:UpdateGroup",
      "Resource": "arn:aws:ds::123456789012:directory/d-012345678",
      "Condition": {
        "StringEqualsIgnoreCase": {
          "ds-data:MemberName": [
            "region-1-*"
          ]
        }
      }
    }
  ]
}
```

```
}  
}  
]  
}
```

ds-data:MemberRealm

「[文字列演算子](#)」で動作します。

ポリシーの MemberRealm が、リクエストで使用するメンバーレルムと一致することを確認します。

Note

この条件キーでは、大文字と小文字は区別されません。[StringEqualsIgnoreCase](#) または [StringNotEqualsIgnoreCase](#) 条件演算子を使用して、文字の大文字と小文字に関係なく、文字列の値を比較する必要があります。

レルム内のグループへのメンバーの追加を許可する

次のポリシーでは、ユーザーまたはロールがクロスドメインに信頼されたレルムのグループにメンバーを追加することを許可します。

Note

次の例では、ds-data:MemberName コンテキストキーのみを使用します。

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "UpdateMembersInRealm",  
      "Effect": "Allow",  
      "Action": "ds-data:UpdateGroup",  
      "Resource": "arn:aws:ds::123456789012:directory/d-012345678",  
    }  
  ]  
}
```

```
    "Condition": {
      "StringEqualsIgnoreCase": {
        "ds-data:MemberRealm": [
          "region-1-*"
        ]
      }
    }
  }
}
```

ds-data:Realm

「[文字列演算子](#)」で動作します。

ポリシーの Realm がリクエストで使用されるレルムと一致することを確認します。

Note

この条件キーでは、大文字と小文字は区別されません。[StringEqualsIgnoreCase](#) または [StringNotEqualsIgnoreCase](#) 条件演算子を使用して、文字の大文字と小文字に関係なく文字列の値を比較する必要があります。

レルムへのグループの追加を許可する

次のポリシーでは、ユーザーまたはロールが指定されたレルムにグループを作成することを許可します。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UpdateGroupsInRealm",
      "Effect": "Allow",
      "Action": "ds-data:CreateGroup",
      "Resource": "*",
      "Condition": {
```

```
"StringEqualsIgnoreCase": {  
  "ds-data:Realm": [  
    "example-domain.com"  
  ]  
}  
}  
]  
}
```

を使用した AWS アプリケーションとサービスの認可 AWS Directory Service

このトピックでは、および AWS Directory Service Data を使用する AWS アプリケーション AWS Directory Service とサービスの認可について説明します。

Active Directory での AWS アプリケーションの認可

AWS Directory Service は、アプリケーションを承認するときに、選択した AWS アプリケーションに Active Directory とシームレスに統合するための特定のアクセス許可を付与します。AWS アプリケーションには、特定のユースケースに必要なアクセスのみが付与されます。承認後にアプリケーションとアプリケーション管理者に付与される内部アクセス許可のセットは次のとおりです：

Note

Active Directory の新しい AWS アプリケーションを認可するには、アクセス `ds:AuthorizationApplication` 許可が必要です。このアクションを実行するアクセス許可は、ディレクトリサービスとの統合を設定する管理者にのみ提供してください。

- AWS Managed Microsoft AD、Simple AD、AD Connector ディレクトリのすべての組織単位 (OU) の Active Directory ユーザー、グループ、組織単位、コンピュータ、または認証機関データへの読み取りアクセス、および信頼関係で許可されている場合は AWS Managed Microsoft AD の信頼されたドメインへの読み取りアクセス。
- AWS Managed Microsoft AD の組織単位のユーザー、グループ、グループメンバーシップ、コンピュータ、または認証機関データへの書き込みアクセス。Simple AD のすべての OU への書き込みアクセス。

- すべてのディレクトリタイプの Active Directory ユーザーの認証とセッション管理。

Amazon RDS や Amazon FSx などの特定の AWS Managed Microsoft AD アプリケーションは、Active Directory への直接ネットワーク接続を介して統合されます。この場合、ディレクトリインタラクションには LDAP や Kerberos などのネイティブの Active Directory プロトコルが使用されます。これらの AWS アプリケーションのアクセス許可は、アプリケーション認可中に AWS リザーブド組織単位 (OU) で作成されたディレクトリユーザーアカウントによって制御されます。これには、DNS 管理と、アプリケーション用に作成されたカスタム OU へのフルアクセスが含まれます。このアカウントを使用するには、アプリケーションに呼び出し元の認証情報または IAM ロールを介した `ds:GetAuthorizedApplicationDetails` アクションへのアクセス許可が必要です。

AWS Directory Service API アクセス許可の詳細については、「」を参照してください[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)。

AWS Managed Microsoft AD の AWS アプリケーションとサービスを有効にする方法の詳細については、「」を参照してください[AWS Managed Microsoft AD から AWS アプリケーションとサービスへのアクセス](#)。Simple AD の AWS アプリケーションとサービスを有効にする方法の詳細については、「」を参照してください[Simple AD から AWS アプリケーションとサービスへのアクセス](#)。AD Connector の AWS アプリケーションとサービスを有効にする方法については、「」を参照してください[AD Connector から AWS アプリケーションとサービスへのアクセス](#)。

Active Directory での AWS アプリケーションの認証解除

AWS アプリケーションが Active Directory にアクセスするため

の `ds:UnauthorizedApplication` アクセス許可を削除するには、アクセス許可が必要です。アプリケーションに表示される指示に従ってそれを無効化します。

AWS Directory Service Data を使用したアプリケーション認可

AWS Managed Microsoft AD ディレクトリの場合、Directory Service Data (ds-data) API は、ユーザーとグループの管理タスクへのプログラムによるアクセスを提供します。AWS アプリケーションの認可モデルは Directory Service Data のアクセスコントロールとは別のものです。つまり、Directory Service Data アクションのアクセスポリシーは、AWS アプリケーションの認可には影響しません。ds-data のディレクトリへのアクセスを拒否しても、AWS アプリケーション統合や AWS アプリケーションのユースケースが中断されることはありません。

AWS アプリケーションを許可する AWS Managed Microsoft AD ディレクトリのアクセスポリシーを作成するときは、承認された AWS Application または Directory Service Data API を呼び出すことで、ユーザーとグループの機能が利用可能になる可能性があることに注意してください。Amazon

WorkDocs、Amazon WorkMail、Amazon WorkSpaces、Amazon QuickSight、および Amazon Chime はすべて API でユーザーとグループの管理アクションを提供します。IAM ポリシーを使用して、この AWS アプリケーション機能へのアクセスを制御します。

例

次のスニペットは、WorkDocs や Amazon WorkMail などの AWS アプリケーションがディレクトリで承認されている場合に、正しくない方法で DeleteUser 機能を拒否する方法を示しています。

正確ではない

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser"
    ],
    "Resource": "*"
  }]
}
```

正確

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "VisualEditor0",
    "Effect": "Deny",
    "Action": [
      "ds-data:DeleteUser",
      "workmail:DeleteUser",
      "workdocs:DeleteUser"
    ],
  }]
```

```
        "Resource": "*"
    }
}
}
```

でのログ記録とモニタリング AWS Directory Service

ベストプラクティスとして、組織をモニタリングして、変更がログに記録されていることを確認します。これにより、予期しない変更を調査でき、不要な変更をロールバックできます。AWS Directory Service は現在、次の 2 つの AWS サービスをサポートしているため、組織とその中で発生するアクティビティをモニタリングできます。

- Amazon CloudWatch - AWS Managed Microsoft AD ディレクトリタイプで CloudWatch Events を使用できます。詳細については、「[AWS Managed Microsoft AD の Amazon CloudWatch Logs ログ転送の有効化](#)」を参照してください。さらに、CloudWatch メトリクスを使用して、ドメインコントローラーのパフォーマンスをモニタリングできます。詳細については、「[CloudWatch メトリクスを使用して、ドメインコントローラーを追加するタイミングを決定する](#)」を参照してください。
- AWS CloudTrail
 - CloudTrail は、すべての AWS Directory Service ディレクトリタイプで使用できます。詳細については、「[を使用した AWS Directory Service API コールのログ記録 AWS CloudTrail](#)」を参照してください。
 - Directory Service Data API で AWS Managed Microsoft AD で CloudTrail を使用できます。詳細については、「[を使用した AWS Directory Service Data API コールのログ記録 AWS CloudTrail](#)」を参照してください。

を使用した AWS Directory Service API コールのログ記録 AWS CloudTrail

AWS Managed Microsoft AD API は AWS CloudTrail、で AWS Managed Microsoft AD によって行われた、または Managed Microsoft AD に代わって行われた API コールをキャプチャ AWS アカウントし、指定した Amazon S3 バケットにログファイルを配信するサービスであると統合されています。CloudTrail は、AWS Managed Microsoft AD コンソールからの API コールと AWS Managed Microsoft AD APIs。CloudTrail で収集された情報を使用して、AWS Managed Microsoft AD に対してどのようなリクエストが行われたか、リクエスト元のソース IP アドレス、リクエスト者、リクエスト日時などを判断できます。CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

AWS CloudTrail の Managed Microsoft AD 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に 有効になります。AWS Managed Microsoft AD でアクティビティが発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。で最近のイベントを表示、検索、ダウンロードできます AWS アカウント。詳細については、[CloudTrail イベント履歴でのイベントの表示](#)を参照してください。

AWS Managed Microsoft AD のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成すると、証跡はすべての AWS リージョンに適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- [証跡の作成のための概要](#)
- [CloudTrail がサポートするサービスと統合](#)
- [CloudTrail 用 Amazon SNS 通知の構成](#)
- [複数のリージョンから CloudTrail ログファイルを受け取る](#) および [複数のアカウントから CloudTrail ログファイルを受け取る](#)

で CloudTrail ログ記録を有効にすると AWS アカウント、 AWS Managed Microsoft AD アクションに対して行われたすべての API コールがログファイルに記録されます。AWS マネージド Microsoft AD レコードは、他の AWS サービスレコードと一緒にログファイルに記録されます。CloudTrail は、期間とファイルサイズに基づいて、新しいファイルをいつ作成して書き込むかを決定します。AWS Directory Service API または CLI 呼び出しに対して行われたすべての呼び出しは、CloudTrail によってログに記録されます。

各ログエントリには、リクエストの生成者に関する情報が含まれます。ログのユーザー ID 情報は、リクエストがルートまたは IAM ユーザー認証情報を使用して行われたか、ロールまたはフェデレティッドユーザーの一時的なセキュリティ認証情報を使用して行われたか、または別の AWS サービスによって行われたかを判断するのに役立ちます。詳細については、[CloudTrail ログイベントリファレンス](#) の `userIdentity` フィールドを参照してください。

必要な場合はログファイルを自身のバケットに保管できますが、ログファイルを自動的にアーカイブまたは削除するように Amazon S3 ライフサイクルルールを定義することもできます。デフォルトでは Amazon S3 のサーバー側の暗号化 (SSE) を使用して、ログファイルが暗号化されます。

ログファイルの配信時にすぐにアクションを実行したいときは、新しいログファイルが配信されるたびに CloudTrail から Amazon SNS 通知を発行するよう選択します。詳細については、「[Amazon SNS 通知の設定](#)」を参照してください。

AWS Managed Microsoft AD ログファイルを複数の AWS リージョン AWS アカウント から 1 つの Amazon S3 バケットに集約することもできます。詳細については、「[CloudTrail ログファイルの単一の Amazon S3 バケットへの集約](#)」を参照してください。

AWS Managed Microsoft AD ログファイルエントリについて

CloudTrail ログファイルには、それぞれが複数の JSON 形式イベントで構成される複数のログエントリを含む可能性があります。ログエントリは任意の送信元からの単一のリクエストを表し、リクエストされたアクション、任意のパラメータ、アクションの日時などに関する情報を含みます。ログエントリは、特定の順序で生成されるわけではありません。つまり、パブリック API 呼び出しのスタックトレース順にはなりません。

パスワード、認証トークン、ファイルコメント、ファイルコンテンツなどの機密情報は、ログエントリには表示されません。

次の例は、AWS Managed Microsoft AD の CloudTrail ログエントリの例を示しています。

```
{
  "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>"
}
]
}

```

を使用した AWS Directory Service Data API コールのログ記録 AWS CloudTrail

AWS Directory Service Data は AWS CloudTrail、Directory Service Data のユーザー、ロール、または AWS のサービスによって実行されたアクションを記録するサービスと統合されます。CloudTrail は、Directory Service Data のすべての API コールをイベントとしてキャプチャします。キャプチャされた呼び出しには、Directory Service Data コンソールからの呼び出しと、Directory Service Data API オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、Directory Service Data のイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。CloudTrail で収集された情報を使用して、Directory Service Data に対するリクエスト、リクエスト元の IP アドレス、リクエスト者、リクエスト日時などの詳細を確認できます。

CloudTrail の詳細については、「[AWS CloudTrail ユーザーガイド](#)」を参照してください。

CloudTrail の Directory Service Data 情報

CloudTrail は、アカウントの作成 AWS アカウント 時に 有効になります。Directory Service Data でサポートされているイベントアクティビティ (管理イベント) が発生すると、そのアクティビティはイベント履歴の他の AWS サービスイベントとともに CloudTrail イベントに記録されます。最近 90 日間の管理イベントは、AWS アカウントで表示、検索、ダウンロードできます。詳細については、「[CloudTrail イベント履歴でのイベントの表示](#)」を参照してください。[イベント履歴] の表示には料金はかかりません。

Directory Service Data のイベントなど AWS アカウント、 のイベントの継続的な記録については、証跡を作成します。証跡により、CloudTrail はログファイルを Amazon S3 バケットに配信できます。デフォルトでは、コンソールで証跡を作成するときに、証跡がすべての AWS リージョンに適用されます。証跡は、AWS パーティション内のすべてのリージョンからのイベントをログに記録し、指定した Amazon S3 バケットにログファイルを配信します。さらに、CloudTrail ログで収集されたイベントデータをさらに分析して処理するように他の AWS サービスを設定できます。詳細については、次を参照してください:

- [追跡を作成するための概要](#)
- 「[CloudTrail がサポートされているサービスと統合](#)」
- 「[CloudTrail の Amazon SNS 通知の設定](#)」
- [複数のリージョンから CloudTrail ログファイルを受け取る](#) および [複数のアカウントから CloudTrail ログファイルを受け取る](#)

CloudTrail は、すべての Directory Service Data アクションを [Directory Service Data API 参照](#) で記録しています。例えば、AddGroupMember、DescribeUser、SearchGroups の各アクションを呼び出すと、CloudTrail ログファイルにエントリが生成されます。

各イベントまたはログエントリには、誰がリクエストを生成したかという情報が含まれます。アイデンティティ情報は、以下を判別するのに役立ちます。

- リクエストがルートまたは AWS Identity and Access Management (IAM) ユーザー認証情報を使用して行われたかどうか。
- リクエストがロールまたはフェデレーションユーザーのテンポラリなセキュリティ認証情報を使用して行われたかどうか。
- リクエストが別の AWS サービスによって行われたかどうか。

詳細については、「[CloudTrail userIdentity エレメント](#)」を参照してください。

Directory Service Data ログファイルエントリについて

「トレイル」は、指定した Amazon S3 バケットにイベントをログファイルとして配信するように設定できます。CloudTrail のログファイルは、単一か複数のログエントリを含みます。イベントは任意ソースからの単一リクエストを表し、リクエストされたアクション、アクションの日時、リクエストパラメータなどの情報を含みます。CloudTrail ログファイルは、パブリック API 呼び出しの順序付けられたスタックトレースではないため、特定の順序では表示されません。

次の例は、「[CreateUser](#)」アクションを表示する CloudTrail ログエントリを示します。

```
{
  "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"
  }
},

```

次の例は、「[ListUsers](#)」アクションを表示する CloudTrail ログエントリを示します。

オブジェクトを作成または変更しないアクションは、null レスポンスを返します。

```

{
  "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"
    }
}

```

次の例は、「[ListGroups](#)」アクションを表示する CloudTrail ログエントリを示します。

Note

NextToken 要素はすべてのログエントリによって編集されます。

```

{
    "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"
  }
}
```

例外エラーのログエントリ

次の例は、「アクセス拒否」エラーの CloudTrail ログエントリを示しています。このエラーのサポートについては、「IAM ユーザーガイド」の「[アクセス拒否エラーメッセージのトラブルシューティング](#)」を参照してください。

Note

アクセス拒否ログにはリクエストパラメータが表示されません。

```
{
  "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"
    }
  }
}

```

次の例は、「リソースが見つからない」エラーの CloudTrail ログエントリを示しています。

```

{
  "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"
}
}
```

のコンプライアンス検証 AWS Directory Service

AWS のサービス が特定のコンプライアンスプログラムの範囲内にあるかどうかを確認するには、[AWS のサービス「コンプライアンスプログラムによる対象範囲内」](#)を参照して、関心のあ
るコンプライアンスプログラムを選択します。一般的な情報については、[AWS「Compliance Programs Assurance」](#)を参照してください。

を使用して、サードパーティーの監査レポートをダウンロードできます AWS Artifact。詳細について
は、[「Downloading Reports in AWS Artifact」](#)を参照してください。

を使用する際のお客様のコンプライアンス責任 AWS のサービス は、お客様のデータの機密性、貴
社のコンプライアンス目的、適用される法律および規制によって決まります。 は、コンプライアンス
に役立つ以下のリソース AWS を提供します。

- [セキュリティのコンプライアンスとガバナンス](#) – これらのソリューション実装ガイドでは、アー
キテクチャ上の考慮事項について説明し、セキュリティとコンプライアンスの機能をデプロイする
手順を示します。
- [HIPAA 対応サービスのリファレンス](#) – HIPAA 対応サービスの一覧が提供されています。すべての
AWS のサービス が HIPAA の対象となるわけではありません。
- [AWS コンプライアンスリソース](#) – このワークブックとガイドのコレクションは、お客様の業界や
地域に適用される場合があります。
- [AWS カスタマーコンプライアンスガイド](#) – コンプライアンスの観点から責任共有モデルを理解し
ます。このガイドでは、複数のフレームワーク (米国国立標準技術研究所 (NIST)、Payment Card
Industry Security Standards Council (PCI)、国際標準化機構 (ISO) など) のセキュリティコント
ロールを保護し、そのガイダンスに AWS のサービス マッピングするためのベストプラクティス
をまとめています。
- [「デベロッパーガイド」の「ルールによるリソースの評価」](#) – この AWS Config サービスは、リ
ソース設定が内部プラクティス、業界ガイドライン、および規制にどの程度準拠しているかを評価
します。AWS Config

- [AWS Security Hub](#) – これにより AWS のサービス、内のセキュリティ状態を包括的に把握できます AWS。Security Hub では、セキュリティコントロールを使用して AWS リソースを評価し、セキュリティ業界標準とベストプラクティスに対するコンプライアンスをチェックします。サポートされているサービスとコントロールの一覧については、[Security Hub のコントロールリファレンス](#)を参照してください。
- [Amazon GuardDuty](#) – 不審なアクティビティや悪意のあるアクティビティがないか環境をモニタリングすることで AWS アカウント、ワークロード、コンテナ、データに対する潜在的な脅威 AWS のサービスを検出します。GuardDuty を使用すると、特定のコンプライアンスフレームワークで義務付けられている侵入検知要件を満たすことで、PCI DSS などのさまざまなコンプライアンス要件に対応できます。
- [AWS Audit Manager](#) – これにより AWS のサービス、AWS 使用状況を継続的に監査し、リスクの管理方法と規制や業界標準への準拠を簡素化できます。

の耐障害性 AWS Directory Service

AWS グローバルインフラストラクチャは、AWS リージョンとアベイラビリティーゾーンを中心に構築されています。AWS リージョンは、低レイテンシー、高スループット、冗長性の高いネットワークで接続された、物理的に分離された複数のアベイラビリティーゾーンを提供します。アベイラビリティーゾーンでは、アベイラビリティーゾーン間で中断せずに、自動的にフェイルオーバーするアプリケーションとデータベースを設計および運用することができます。アベイラビリティーゾーンは、従来の単一または複数のデータセンターインフラストラクチャよりも可用性、耐障害性、およびスケーラビリティが優れています。

AWS リージョンとアベイラビリティーゾーンの詳細については、[AWS 「グローバルインフラストラクチャ」](#)を参照してください。

AWS グローバルインフラストラクチャに加えて、はデータの耐障害性とバックアップのニーズをサポートするために、いつでもデータの手動スナップショットを作成する機能 AWS Directory Service を提供します。詳細については、「[スナップショットを使用した AWS Managed Microsoft AD の復元](#)」を参照してください。

のインフラストラクチャセキュリティ AWS Directory Service

マネージドサービスである AWS Directory Service は、AWS グローバルネットワークセキュリティで保護されています。AWS セキュリティサービスとインフラストラクチャ AWS を保護する方法については、[AWS 「クラウドセキュリティ」](#)を参照してください。インフラストラクチャセキュ

リテイのベストプラクティスを使用して AWS 環境を設計するには、「Security Pillar AWS Well-Architected Framework」の「[Infrastructure Protection](#)」を参照してください。

AWS が公開した API コールを使用して、ネットワーク AWS Directory Service 経由で にアクセスします。クライアントは以下をサポートする必要があります。

- Transport Layer Security (TLS)。TLS 1.2 が必須で、TLS 1.3 をお勧めします。
- DHE (楕円ディフィー・ヘルマン鍵共有) や ECDHE (楕円曲線ディフィー・ヘルマン鍵共有) などの完全前方秘匿性 (PFS) による暗号スイート。これらのモードは Java 7 以降など、ほとんどの最新システムでサポートされています。

また、リクエストにはアクセスキー ID と、IAM プリンシパルに関連付けられているシークレットアクセスキーを使用して署名する必要があります。または、[AWS Security Token Service](#) (AWS STS) を使用して、テンポラリセキュリティ認証情報を生成し、リクエストに署名することもできます。

サービス間の混乱した代理の防止

混乱した代理問題は、アクションを実行するためのアクセス許可を持たないエンティティが、より特権のあるエンティティにアクションの実行を強制できてしまう場合に生じる、セキュリティ上の問題です。では AWS、サービス間のなりすましにより、混乱した代理問題が発生する可能性があります。サービス間でのなりすましは、1 つのサービス (呼び出し元サービス) が、別のサービス (呼び出し対象サービス) を呼び出すときに発生する可能性があります。呼び出し元サービスは、本来ならアクセスすることが許可されるべきではない方法でその許可を使用して、別のお客様のリソースに対する処理を実行するように操作される場合があります。これを防ぐため、AWS では、アカウントのリソースへのアクセス権が付与されたサービスプリンシパルで、すべてのサービスのデータを保護するために役立つツールを提供しています。

Directory AWS Service for Microsoft Active Directory がリソースに別のサービスに付与するアクセス許可を制限するには、リソースポリシーで [aws:SourceArn](#) および [aws:SourceAccount](#) グローバル条件コンテキストキーを使用することをお勧めします。aws:SourceArn の値に Amazon S3 バケット ARN などのアカウント ID が含まれていない場合は、両方のグローバル条件コンテキストキーを使用して、アクセス許可を制限する必要があります。同じポリシーステートメントでこれらのグローバル条件コンテキストキーの両方を使用し、アカウント ID に aws:SourceArn の値が含まれていない場合、aws:SourceAccount 値と aws:SourceArn 値の中のアカウントには、同じアカウント ID を使用する必要があります。クロスサービスのアクセスにリソースを 1 つだけ関連付けたい場合は、aws:SourceArn を使用します。クロスサービスが使用できるように、アカウント内の任意のリソースを関連づけたい場合は、aws:SourceAccount を使用します。

次の例では、aws:SourceArn の値は CloudWatch ロググループである必要があります。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定しながら、aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合は、aws:SourceArn グローバルコンテキスト条件キーを使用して、ARN の未知部分をワイルドカード (*) で表します。例えば、arn:aws:service:*:123456789012:* です。

次の例は、AWS Managed Microsoft AD で aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題を防ぐ方法を示しています。

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ConfusedDeputyPreventionExamplePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/directoryservice/YOUR_LOG_GROUP:*"
      ],
      "Condition": {
        "ArnLike": {
          "aws:SourceArn":
            "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
        },
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        }
      }
    }
  ]
}
```

次の例では、aws:SourceArn の値はアカウントの SNS トピックである必要があります。例えば、arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f 「ap-southeast-1」が自分のリージョン、「123456789012」が顧客 ID、DirectoryMonitoring_d-966739499f が作成した Amazon SNS トピック名などを使用できます。

混乱した代理問題から保護するための最も効果的な方法は、リソースの完全な ARN を指定して aws:SourceArn グローバル条件コンテキストキーを使用することです。リソースの完全な ARN が不明な場合や、複数のリソースを指定する場合は、aws:SourceArn グローバルコンテキスト条件キーを使用して、ARN の未知部分をワイルドカード (*) で表します。例えば、arn:aws:service:*:123456789012:* です。

次の例は、AWS Managed Microsoft AD で aws:SourceArn および aws:SourceAccount グローバル条件コンテキストキーを使用して、混乱した代理問題を防ぐ方法を示しています。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": ["SNS:GetTopicAttributes",
      "SNS:SetTopicAttributes",
      "SNS:AddPermission",
      "SNS:RemovePermission",
      "SNS:DeleteTopic",
      "SNS:Subscribe",
      "SNS:ListSubscriptionsByTopic",
      "SNS:Publish"],
    "Resource": [
      "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
          "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

```
}  
}  
}
```

次の例は、コンソールアクセスが委任されているロールの IAM 信頼ポリシーを示しています。aws:SourceArn の値は、アカウント内のディレクトリリソースにする必要があります。詳細については、「[で定義されるリソースタイプ AWS Directory Service](#)」を参照してください。例えば、arn:aws:ds:us-east-1:123456789012:directory/d-1234567890 を使用できます。ここで、123456789012 はお客様 ID であり、d-1234567890 はディレクトリ ID です。

JSON

```
{  
  "Version": "2012-10-17",  
  "Statement": {  
    "Sid": "ConfusedDeputyPreventionExamplePolicy",  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "ds.amazonaws.com"  
    },  
    "Action": [  
      "sts:AssumeRole"  
    ],  
    "Condition": {  
      "ArnLike": {  
        "aws:SourceArn":  
          "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"  
      },  
      "StringEquals": {  
        "aws:SourceAccount": "123456789012"  
      }  
    }  
  }  
}
```

AWS Directory Service を使用した API とインターフェイスの Amazon VPC エンドポイント AWS PrivateLink

を使用して AWS PrivateLink、VPC AWS Directory Service と Directory Service Data APIs の間にプライベート接続を作成できます。これにより、インターネットゲートウェイ、NAT デバイス、VPN 接続、または AWS Direct Connect 接続を使用せずに、VPC にあったように および AWS Directory Service Directory Service Data APIs にアクセスできます。Amazon VPC 内のインスタンスは、AWS Directory Service および Directory Service Data APIs にアクセスするためにパブリック IP アドレスを必要としません。

プライベート接続を確立するには、AWS PrivateLink を使用するインターフェイス Amazon VPC エンドポイントを作成します。インターフェイスエンドポイントに対して有効にする各サブネットにエンドポイントネットワークインターフェイスを作成します。これらはリクエスト管理のネットワークインターフェイスであり、AWS Directory Service および AWS Directory Service Data 宛てのトラフィックのエントリポイントとして機能します。

詳細については、「AWS PrivateLink ガイド」の [「Access AWS のサービス through AWS PrivateLink」](#) を参照してください。

AWS Directory Service および Directory Service Data に関する考慮事項

AWS Directory Service および Directory Service Data を使用すると、インターフェイスエンドポイントを介して API アクションを呼び出すことができます。インターフェイスエンドポイントを作成する前に考慮すべき前提条件については、「AWS PrivateLink ガイド」の [「インターフェイス Amazon VPC エンドポイント AWS のサービスを使用してにアクセスする」](#) を参照してください。

AWS Directory Service および Directory Service Data Availability

AWS Directory Service は、以下のインターフェイスエンドポイントをサポートしています AWS リージョン。

- 米国東部 (バージニア北部)
- AWS GovCloud (米国東部)
- AWS GovCloud (米国西部)

Directory Service Data は、使用可能なすべての AWS リージョン でインターフェイスエンドポイントをサポートします。AWS Directory Service と Directory Service Data AWS リージョン をサポートする の詳細については、「[のリージョンの可用性 AWS Directory Service](#)」を参照してください。

AWS Directory Service および Directory Service Data のインターフェイス Amazon VPC エンドポイントを作成する

Amazon VPC コンソールまたは AWS Command Line Interface () を使用して、AWS Directory Service および Directory Service Data APIsのインターフェイスエンドポイントを作成できますAWS CLI。

例: AWS Directory Service

次のサービス名を使用して、AWS Directory Service APIsのインターフェイスエンドポイントを作成します。

```
com.amazonaws.region.ds
```

例: Directory Service データ

以下のサービス名を使用して、Directory Service Data API のインターフェイスエンドポイントを作成します:

```
com.amazonaws.region.ds-data
```

インターフェイスエンドポイントの作成の詳細については、「AWS PrivateLink ガイド」の「[インターフェイス Amazon VPC エンドポイント AWS のサービスを使用してにアクセスする](#)」を参照してください。

インターフェイスの Amazon VPC エンドポイントの Amazon VPC エンドポイントポリシーを作成する

エンドポイントポリシーは、インターフェイスエンドポイントに付加できる IAM リソースポリシーです。

Note

エンドポイントポリシーをインターフェイスエンドポイントに付加しない場合、AWS PrivateLink はユーザーに代わってデフォルトのエンドポイントポリシーをインターフェイスエンドポイントに付加します。詳細については、「[AWS PrivateLink の概念](#)」を参照してください。

エンドポイントポリシーは以下の情報を指定します。

- アクションを実行できるプリンシパル (AWS アカウント、IAM ユーザー、IAM ロール)
- 実行可能なアクション
- このアクションを実行できるリソース

詳細については[AWS PrivateLink Guide] (ガイド) の[\[Control access to services using endpoint policies\]](#) (エンドポイントポリシーを使用してサービスへのアクセスをコントロール) を参照してください。

Amazon VPC から API へのアクセスをコントロールするには、カスタムエンドポイントポリシーをインターフェイスエンドポイントに付加します。

例: AWS Directory Service API アクションの Amazon VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。このポリシーをインターフェイスエンドポイントにアタッチすると、すべてのリソースのすべてのプリンシパルに対して、リストされた AWS Directory Service アクションへのアクセスが許可されます。

action-1、*action-2*、および *action-3* を、ポリシーに含める AWS Directory Service APIs に必要なアクセス許可に置き換えます。詳細なリストについては、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds:action-1",
        "ds:action-2",
        "ds:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

例: Directory Service Data API アクションの Amazon VPC エンドポイントポリシー

以下は、カスタムエンドポイントポリシーの例です。インターフェイスエンドポイントに付加されると、このポリシーは、すべてのリソースですべてのプリンシパルに、リストされている Directory Service Data アクションへのアクセス権限を付与します。

action-1、*action-2*、*action-3* を、ポリシーに含める Directory Service Data API に必要なアクセス許可に置き換えます。詳細なリストについては、「[AWS Directory Service API アクセス許可: アクション、リソース、および条件リファレンス](#)」を参照してください

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "ds-data:action-1",
        "ds-data:action-2",
        "ds-data:action-3"
      ],
      "Resource": "*"
    }
  ]
}
```

のサービスレベルアグリーメント AWS Directory Service

AWS Directory Service は可用性の高いサービスであり、AWS管理されたインフラストラクチャで構築されています。また、当社のサービス可用性ポリシーを定義するサービスレベル (SLA) 契約によってバックアップされています。

- SLA は AWS Managed Microsoft AD、AD Connector、Simple AD に適用されます。
- SLA では、サービスクレジット、SLA の除外について説明し、「対象ディレクトリ」、「月間稼働率」、「リクエスト」などの用語を定義します。
- 詳細については、「[AWS Directory Serviceのサービスレベルアグリーメント](#)」を参照してください。

のリージョンの可用性 AWS Directory Service

次の表に、ディレクトリタイプでサポートされているリージョン固有のエンドポイントを示します。

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
米国東部 (バージニア北部)	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 はい	 はい	 はい
米国東部 (オハイオ)	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 はい	 はい	 いいえ
米国西部 (カリフォルニア)	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
米国西部 (オレゴン)	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	 はい	 はい	 はい
アフリカ (ケープタウン)	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connector	Simple AD
アジアパシフィック (香港)	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (台北)	ap-east-2	ds.ap-east-2.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (ハイデラバード)	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (ジャカルタ)	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 はい	 はい	 いいえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
アジアパシフィック (マレーシア)	ap-southeast-5	ds.ap-southeast-5.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (メルボルン)	ap-southeast-4	ds.ap-southeast-4.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (タイ)	ap-southeast-7	ds.ap-southeast-7.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (ムンバイ)	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
アジアパシフィック (大阪)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 はい	 はい	 いいえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
アジアパシフィック (ソウル)	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	 はい	 はい	 はい いえ
アジアパシフィック (シンガポール)	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	 はい	 はい	 はい
アジアパシフィック (シドニー)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 はい	 はい	 はい
アジアパシフィック (東京)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 はい	 はい	 はい
カナダ (中部)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 はい	 はい	 はい いえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
カナダ西部 (カルガリー)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 はい	 はい	 はい いえ
中国 (北京)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 はい	 はい	 はい いえ
中国 (寧夏)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	 はい	 はい	 はい いえ
欧州 (フランクフルト)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 はい	 はい	 はい いえ
欧州 (アイルランド)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	 はい	 はい	 はい
欧州 (ロンドン)	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	 はい	 はい	 はい いえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
欧州 (ミラノ)	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
欧州 (パリ)	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	 はい	 はい	 いいえ
欧州 (スペイン)	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	 はい	 はい	 いいえ
欧州 (ストックホルム)	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
欧州 (チューリッヒ)	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	 はい	 はい	 いいえ
イスラエル (テルアビブ)	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
メキシコ (中部)	mx-central-1	ds.mx-central-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
中東 (バーレーン)	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
中東 (アラブ首長国連邦)	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
南米 (サンパウロ)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
AWS GovCloud (米国西部)	us-gov-west-1	ds.us-gov-west-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
AWS GovCloud (米国東部)	us-gov-east-1	ds.us-gov-east-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ

AWS GovCloud (米国西部) リージョンおよび AWS GovCloud (米国東部) リージョン AWS Directory Service での の使用については、AWS GovCloud (US) 「ユーザーガイド」の「[サービスエンドポイント](#)」を参照してください。

北京および寧夏リージョン AWS Directory Service での の使用の詳細については、「[中国での の開始方法](#)」の「[中国でのアマゾン ウェブ サービスのエンドポイントと ARNs](#)」を参照してください。

AWS

Directory Service Data がサポートする FIPS エンドポイントの詳細については、「AWS 全般のリファレンス Reference Guide」の「[Directory Service Data endpoints and quotas](#)」を参照してください。

Directory Service Data AWS リージョン でサポート

次の表は、Directory Service Data がダイレクトリによってサポートするリージョン固有のエンドポイントの一覧です。

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
米国東部 (オハイオ)	us-east-2	ds-data.us-east-2.amazonaws.com	HTTPS	 はい	 はい え	 はい え
米国東部 (バージニア北部)	us-east-1	ds-data.us-east-1.amazonaws.com	HTTPS	 はい	 はい え	 はい え
米国西部 (カリフォルニア)	us-west-1	ds-data.us-west-1.amazonaws.com	HTTPS	 はい	 はい え	 はい え

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
米国西部 (オレゴン)	us-west-2	ds-data.us-west-2.amazonaws.com	HTTPS	 はい	 はい いいえ	 はい いいえ
アジアパシフィック (香港)	ap-east-1	ds-data.ap-east-1.amazonaws.com	HTTPS	 はい	 はい いいえ	 はい いいえ
アジアパシフィック (ムンバイ)	ap-south-1	ds-data.ap-south-1.amazonaws.com	HTTPS	 はい	 はい いいえ	 はい いいえ
アジアパシフィック (大阪)	ap-northeast-3	ds-data.ap-northeast-3.amazonaws.com	HTTPS	 はい	 はい いいえ	 はい いいえ
アジアパシフィック (ソウル)	ap-northeast-2	ds-data.ap-northeast-2.amazonaws.com	HTTPS	 はい	 はい いいえ	 はい いいえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
アジアパシフィック (シンガポール)	ap-southeast-1	ds-data.ap-southeast-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
アジアパシフィック (シドニー)	ap-southeast-2	ds-data.ap-southeast-2.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
アジアパシフィック (東京)	ap-northeast-1	ds-data.ap-northeast-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
カナダ (中部)	ca-central-1	ds-data.ca-central-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
欧州 (フランクフルト)	eu-central-1	ds-data.eu-central-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ

リージョン名	リージョン	エンドポイント	プロトコル	AWS Managed Microsoft AD	AD Connect	Simple AD
欧州 (アイルランド)	eu-west-1	ds-data.eu-west-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
欧州 (ロンドン)	eu-west-2	ds-data.eu-west-2.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
欧州 (パリ)	eu-west-3	ds-data.eu-west-3.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
欧州 (ストックホルム)	eu-north-1	ds-data.eu-north-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ
南米 (サンパウロ)	sa-east-1	ds-data.sa-east-1.amazonaws.com	HTTPS	 はい	 はい いえ	 はい いえ

Directory Service Data がサポートする FIPS エンドポイントの詳細については、「AWS 全般のリリース Reference Guide」の「[Directory Service Data endpoints and quotas](#)」を参照してください。

のブラウザ互換性 AWS Directory Service

AWS WorkSpaces、Amazon WorkMail、Amazon Connect、Amazon Chime、WorkDocs などのアプリケーションやサービス AWS IAM Identity Center には、互換性のあるブラウザからの有効なサインイン認証情報が必要です。次の表ではサインイン用に互換性のあるブラウザとブラウザバージョンのみを示しています。

ブラウザ	バージョン	互換性
Microsoft Edge	最新の 3 つのバージョン	互換性あり
Mozilla Firefox	最新の 3 つのバージョン	互換性あり
Google Chrome	最新の 3 つのバージョン	互換性あり
Apple Safari	最新の 3 つのバージョン	互換性あり

サポートされるバージョンのブラウザを使用していることが確認できたので、次のセクションを参照してブラウザが AWS で必要な Transport Layer Security (TLS) を使用する設定になっていることも確認することをお勧めします。

TLS とは何ですか？

TLS は、ネットワークを介してデータを安全にやり取りするためにウェブブラウザなどのアプリケーションが使用するプロトコルです。TLS によって、暗号化およびエンドポイント ID 検証が行われ、リモートエンドポイントへの接続が意図されたエンドポイントであることが確実になります。TLS のバージョンは、現在のところ、TLS 1.0、1.1、1.2、1.3 です。

IAM Identity Center でどの TLS バージョンがサポートされているか

AWS アプリケーションとサービスは、安全なサインインのために TLS 1.1、1.2、1.3 をサポートしています。2019 年 10 月 30 日をもって TLS 1.0 はサポートされなくなります。そのため、すべてのブラウザが TLS 1.1 以降をサポートするように設定されていることが重要です。つまり、TLS 1.0 を有効にしたアクセスでは、AWS のアプリケーションおよびサービスにサインインすることはできなくなります。上述の変更については、管理者にお問い合わせください。

サポートされている TLS バージョンをブラウザで有効にする方法

これはブラウザによって異なります。通常は、ブラウザの設定の高度な設定内でこの設定を見つけることができます。例えば Internet Explorer では、インターネットオプションの詳細設定タブのセキュリティセクションに複数の TLS オプションが見つかります。具体的な手順については、ブラウザメーカーのヘルプウェブサイトを確認してください。

ドキュメント履歴

次の表は、「AWS Directory Service 管理者ガイド」の前回リリースからの重要な変更点をまとめたものです。

変更	説明	日付
ログ記録とモニタリングのトピックを更新 – 新しいセクション	ログ AWS Directory Service 記録とモニタリングのトピックにと AWS Directory Service Data のセクションが含まれました。	2024 年 9 月 18 日
新しい Directory Service Data API と属性	AWS Directory Service Data は、組み込みのオブジェクト管理を提供します。「 サポートされている AD 属性のリスト 」を使用して、オブジェクトを検索および更新できるようになりました。	2024 年 9 月 18 日
AWS 管理ポリシー - 新しいポリシー	AWS Directory Service Data は、AWSDirectoryServiceDataFullAccess という新しい AWS 管理ポリシーを追加しますAWSDirectoryServiceDataReadOnlyAccess。このポリシーは、Directory Service Data オブジェクト管理へのアクセスを許可します。	2024 年 9 月 18 日
証明書ベースの認証設定	AWS Managed Microsoft AD の 2 つの新しいセキュリティ設定に関するコンテンツを追加しました。	2023 年 4 月 11 日

AWS PrivateLink	AWS PrivateLinkに関するコンテンツを追加しました。	2023 年 3 月 20 日
Simple AD VPC エンドポイント	設定すべきではない VPC エンドポイントに関する内容を追加しました。	2021 年 8 月 25 日
AD Connector VPC エンドポイント	設定すべきではない VPC エンドポイントに関する内容を追加しました。	2021 年 8 月 25 日
スマートカードのサポート	AWS GovCloud (米国西部) リージョンのスマートカードと Amazon WorkSpaces Application Manager のサポートに関する内容を追加しました。	2020 年 12 月 1 日
パスワードのリセット	AWS Management ConsolePowerShell および を使用してユーザーパスワードをリセットする方法に関するコンテンツを追加しました AWS CLI。	2019 年 1 月 2 日
ディレクトリ共有	AWS Managed Microsoft AD でディレクトリ共有を使用する方法に関するコンテンツを追加しました。	2018 年 9 月 25 日
内容を新しい「Amazon Cloud Directory デベロッパーガイド」に移行	このガイドに含まれていた Amazon Cloud Directory の内容を、新しい「Amazon Cloud Directory デベロッパーガイド」に移動しました。	2018 年 6 月 21 日

管理者ガイドの目次の全面改訂	お客様のニーズをより直接的に反映するようにコンテンツを再編成しました。また、必要に応じて新しいコンテンツを追加しました。	2018 年 4 月 5 日
AWS 委任グループ	オンプレミスユーザーに割り当てることができる AWS 委任グループのリストを追加しました。	2018 年 3 月 8 日
詳細なパスワードポリシー	パスワードポリシーに関する新しい内容を追加しました。	2017 年 7 月 5 日
追加のドメインコントローラー	AWS Managed Microsoft AD のディレクトリへのドメインコントローラーの追加に関する情報を追加しました。	2017 年 6 月 30 日
チュートリアル	AWS Managed Microsoft AD ラボ環境をテストするための新しいチュートリアルを追加しました。	2017 年 6 月 21 日
AWS Managed Microsoft AD を使用した MFA	AWS Managed Microsoft AD での MFA の使用に関するコンテンツを追加しました。	2017 年 2 月 13 日
Amazon Cloud Directory	新しいディレクトリタイプに関するコンテンツを追加しました。	2017 年 1 月 26 日
スキーマ拡張	AWS Directory Service for Microsoft Active Directory を使用したスキーマ拡張に関するコンテンツを追加しました。	2016 年 11 月 14 日

AWS Directory Service 管理者ガイドの大幅な再編成	お客様のニーズをより直接的に反映するようにコンテンツを再編成しました。	2016 年 11 月 14 日
SNS 通知	SNS 通知に関するコンテンツを追加しました。	2016 年 2 月 25 日
認可と認証	で IAM を使用する方法に関するコンテンツを追加しました AWS Directory Service。	2016 年 2 月 25 日
AWS Managed Microsoft AD	AWS Managed Microsoft AD に関するコンテンツを追加し、ガイドを 1 つのガイドにまとめました。	2015 年 11 月 17 日
Linux インスタンスの Simple AD ディレクトリへの結合を許可	Linux インスタンスの Simple AD ディレクトリへの結合に関するコンテンツを追加しました。	2015 年 7 月 23 日
ガイドの分割	AWS Directory Service 管理ガイドを複数のガイドに分割します。	2015 年 7 月 14 日
シングルサインオンのサポート	シングルサインオンのサポートに関するコンテンツを追加しました。	2015 年 3 月 31 日
新規ガイド	これは「AWS Directory Service 管理ガイド」の初版リリースです。	2014 年 10 月 21 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。