管理ガイド

AWS Directory Service

Version 1.0

AWS Directory Service: 管理ガイド

Table of Contents

とは AWS Directory Service

AWS Directory Service には、他の AWS のサービスで Microsoft Active Directory (AD) を使用する複数の方法があります。ディレクトリは、ユーザー、グループ、デバイスに関する情報を保存し、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、開発者がディレクトリによってユーザー、グループ、デバイス、およびアクセスを管理する場合にも、同じオプションを提供します。

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
クラウド上のアプリケーションで、Active Directory または LDAP が必要	AWS Directory Service for Microsoft Active Directory (Standard Edition または Enterprise Edition) は、 対応のワークロード、Amazon や Amazon Active Directoryなどの AWS アプリケーションやサービスをサポートする AWS クラウドMicrosoftActive Directoryで実際に が必要な場合 QuickSight、または Linux WorkSpaces アプリケーションの LDAP サポートが必要な場合に使用します。 AD Connector は、オンプレミスユーザーが Active Directory認証情報を使用してアプリケーションやサービスにログイン AWS することのみを許可する場合に使用します。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、低コストの低スケールディレクトリが必要な場合、または LDAP 対応アプリケー

目的	推奨 AWS Directory Service オプション
	ションに LDAP 互換性が必要な場合は、Simple AD を使用します。
SaaS アプリケーションを開発する	高スケールの 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、「 でActive Directoryソリューションを選択する方法 AWS」を参照してください。

AWS Directory Service オプション

AWS Directory Service には、選択できるディレクトリタイプがいくつか含まれています。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 とも呼ばれる AWS Directory Service for Microsoft Active Directory は、 AWS クラウド AWS で によって管理される実際の Microsoft Windows Server Active Directory (AD) を利用しています。これにより、幅広い 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 ServerAlways 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 、Amazon WorkDocs、Amazon Chime 、Amazon Connect 、Amazon Relational Database Service for Microsoft SQL Server (Amazon RDS for 、Amazon RDS for SQL Server、Amazon RDS for PostgreSQL) などの AWS マネージドアプリケーションOracleとサービスもサポートしています。 QuickSight

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、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 に保存したユーザー認証情報で動作します。または、信頼して既存の AD インフラストラクチャに接続し、オンプレミ

スまたは EC2 Windows でActive Directory実行されている の認証情報を使用できます。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ション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認証情報を取得したり、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したり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Active Directoryで 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。Managed Microsoft AD の多要素認証 (MFA) AWS 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を強化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) 認証やその他の LDAP 対応アプリケーションに AWS Managed Microsoft AD を使用することもできます。

AWS は、モニタリング、日次スナップショット、リカバリをサービスの一部として提供します。ユーザーとグループを AWS Managed Microsoft AD に追加し、 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実際のActive Directory機能が必要な場合に最適ですMicrosoft SQL Server。また、Office 365 をサポートするスタンドアロンActive DirectoryのAWS クラウドが必要な場合や、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、Windows Serverインスタンス用の Amazon 、Amazon WorkSpaces、QuickSightAmazon 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 を使用すると、 に 1 つのサービスアカウントを追加するだけで済みますActive Directory。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 などの AWS アプリケーションにユーザーを追加すると QuickSight、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 、Amazon WorkDocs、Amazon Chime QuickSight、Amazon Connect 、および Amazon を含む多くの AWS アプリケーションとサービスで動作します。 Amazon Connect WorkMail シームレスなActive Directoryドメイン結合 を使用して、AD Connector を介して EC2 Windowsインスタンスをオンプレミスドメインに参加させることもできます。 https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ad_connector_launching_instance.htmlAD 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、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。 AWS 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 では、現在のActive Directoryように を管理し続けます。例えば、新しいユーザーとグループを追加し、オンプレミスの の標準Active Directory管理ツールを使用してパスワードを更新しますActive Directory。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、アカウントの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 Microsoft Active Directory4 を搭載した からの互換性のあるディレクトリ AWS Directory Service 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 インスタンスへの参加、Kerberos ベースの SSO、グループポリシーなどの基本Active Directory機能をサポートしています。 AWS 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機能を必要とする、使い慣れた Active Directory対応のアプリケーションやツールを多数使用できます。Simple AD は、Amazon 、Amazon WorkSpaces 、Amazon WorkDocs、および Amazon QuickSightの AWS アプリケーションと互換性があります。 WorkMailSimple AD ユーザーアカウント AWS Management Console を使用して にサインインし、 リソースを管理する AWS こともできます。

Simple AD は、多要素認証 (MFA)、信頼関係、DNS 動的更新、スキーマ拡張、LDAPS 経由の通信、 PowerShell AD コマンドレット、または FSMO ロール転送を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 MicrosoftActive 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。

Amazon Cognito

Amazon Cognito は、モバイルアプリケーションまたはウェブアプリケーションに対して、Amazon Cognito ユーザープールを使用してサインアップとサインインを追加するユーザーディレクトリです。

どのようなときに使うか

カスタム登録フィールドを作成し、そのメタデータをユーザーディレクトリに格納する必要があるときにも、Amazon Cognito を使用できます。このフルマネージド型のサービスは、何百万というユーザーをサポートするように拡張できます。詳細については、「Amazon Cognito デベロッパーガイド」の「Amazon Cognito user pools」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。

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 EC2 ユーザーガイド」のAmazon EC2 とは」。
- 「Amazon EC2 ユーザーガイド」の「EC2 インスタンスの起動」。 Amazon EC2
- 「Amazon EC2 ユーザーガイド」の「セキュリティグループ」。 Amazon EC2
- 「Amazon VPC ユーザーガイド」の「Amazon VPC とは?」。
- 「Amazon VPC ユーザーガイド」の「Adding a Hardware Virtual Private Gateway to Your VPC」(ハードウェア仮想プライベートゲートウェイの VPC への追加)。

はじめに AWS Directory Service

まだ作成していない場合は、 AWS アカウントを作成し、 AWS Identity and Access Management サービスを利用してアクセスを制御する必要もあります。

を使用するには AWS Directory Service、Microsoft Active Directory、AD Connector、または Simple AD AWS 用Directory Service 前提条件を満たす必要があります。詳細については「AWS Managed Microsoft AD の前提条件」、「AD Connector の前提条件」または「Simple AD の前提条件」を参照してください。

にサインアップしてください AWS アカウント

をお持ちでない場合は AWS アカウント、次の手順を実行して作成してください。

にサインアップするには AWS アカウント

1. https://portal.aws.amazon.com/billing/signup を開きます。
2. オンラインの手順に従います。

   サインアップ手順の一環として、通話呼び出しを受け取り、電話キーパッドで検証コードを入力するように求められます。

   にサインアップすると AWS アカウント、AWS アカウントのルートユーザーが作成されます。ルートユーザーには、アカウントのすべての AWS のサービス とリソースへのアクセス権があります。セキュリティ上のベストプラクティスとして、ユーザーに管理アクセスを割り当て、root ユーザーアクセスを必要とするタスクを実行するときは root ユーザーのみを使用してください。

AWS サインアッププロセスが完了すると、確認メールが送信されます。https://aws.amazon.com/ の [マイアカウント] を選んで、いつでもアカウントの現在のアクティビティを表示し、アカウントを管理できます。

管理者権限を持つユーザーを作成します。

にサインアップしたら AWS アカウント、日常のタスクに root ユーザーを使用しないように AWS IAM Identity Center、管理ユーザーを保護し、有効にしてから作成してください。 AWS アカウントのルートユーザー

セキュリティを確保してください。 AWS アカウントのルートユーザー

1. [Root user] を選択し、 AWS アカウント メールアドレスを入力して、AWS Management Consoleアカウントオーナーとしてにログインします。次のページでパスワードを入力します。

   ルートユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「ルートユーザーとしてサインインする」を参照してください。

2. ルートユーザーの多要素認証 (MFA) を有効にします。

   手順については、IAM ユーザーガイドの「AWS アカウント root ユーザー (コンソール) の仮想 MFA デバイスを有効にする」を参照してください。

管理者権限を持つユーザーを作成します。

1. IAM アイデンティティセンターを有効にします。

   手順については、「AWS IAM Identity Center ユーザーガイド」の「AWS IAM Identity Centerの有効化」を参照してください。

2. IAM Identity Center で、ユーザーに管理アクセスを付与します。

   IAM アイデンティティセンターディレクトリ をアイデンティティソースとして使用するチュートリアルについては、『ユーザーガイド』の「 IAM アイデンティティセンターディレクトリデフォルトでのユーザーアクセスの設定」を参照してください。AWS IAM Identity Center

管理者権限を持つユーザーとしてサインインします。

- IAM アイデンティティセンターのユーザーとしてサインインするには、IAM アイデンティティセンターのユーザーの作成時に E メールアドレスに送信されたサインイン URL を使用します。

  IAM Identity Center ユーザーを使用してサインインする方法については、AWS サインイン ユーザーガイドの「 AWS アクセスポータルへのサインイン」を参照してください。

追加のユーザーにアクセス権を割り当てます。

1. IAM Identity Center で、最小権限権限を適用するというベストプラクティスに従った権限セットを作成します。

手順については、『ユーザーガイド』の「権限セットの作成」を参照してください。AWS IAM Identity Center

2. ユーザーをグループに割り当て、そのグループにシングルサインオンアクセスを割り当てます。

   手順については、『AWS IAM Identity Center ユーザーガイド』の「グループの追加」を参照してください。

詳細情報

- IAM Identity Center AWS Management Console ユーザーとしてにサインインする方法の詳細については、「IAM Identity Center アクセスポータルへのサインイン」を参照してください。
- IAM ユーザーとしてにサインインする方法の詳細については、「IAM AWS Management Console ユーザーとしてにサインインする」を参照してください。 AWS Management Console
- IAM AWS Directory Service ポリシーを使用してリソースへのアクセスを制御する方法の詳細については、「」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

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 Microsoft AD とも呼ばれ、WindowsServer AWS 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、Virtual Private Cloud (Amazon VPC) に接続された可用性の高いドメインコントローラーの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ー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、 MicrosoftSharePoint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 クラウドの AWS Managed Microsoft AD と既存のオンプレミス Microsoft と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、リソースを既存のオンプレミス Microsoft に接続したりできます AWS 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 とMicrosoft Windowsワークロードのデプロイと管理を簡素化する
- AWS Managed Microsoft AD を使用すると、既存の RADIUS ベースの MFA インフラストラクチャと統合して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セキュリティを強化できます。
- Amazon EC2 Linux とWindowsインスタンスに安全に接続する

> **Note**
>
> AWS はサーバーWindows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、 Managed Microsoft AD AWS とオンプレミスディレクトリ間の信頼関係の作成、および Managed Microsoft AD AWS 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
- AWS Managed Microsoft AD のベストプラクティス
- AWS Managed Microsoft AD のユースケース
- Managed Microsoft AD AWS を管理する方法
- AWS Managed Microsoft AD クォータ
- AWS マネージド Microsoft AD のアプリケーション互換性
- AWS Managed Microsoft AD テストラボのチュートリアル
- 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の 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 Microsoft 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

- オンプレミスの Active Directory を使用して AWS サービスに簡単にログオンする方法

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 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、「追加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。

トピック

- AWS Managed Microsoft AD の前提条件
- AWS Managed Microsoft AD を作成する
- AWS Managed Microsoft AD Active Directory で作成される内容
- 管理者アカウントのアクセス権限

AWS Managed Microsoft AD 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 IAM Identity Center 前提条件

Managed Microsoft AD で IAM Identity Center AWS を使用する予定の場合は、次の点に当てはま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 の前提条件」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、オンプレミスまたはクラウドベースの Remote Authentication Dial-In User Service (RADIUS) サーバーを次の方法で設定して、 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ことができるようにする必要があります AWS。

1. RADIUS サーバーで、2 つの RADIUS クライアントを作成して、 の AWS Managed Microsoft AD ドメインコントローラー (DCsの両方を表します 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): AWS これは Managed Microsoft AD DCs。両方の DNS アドレスは、 AWS 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 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。あるいは、各 AWS Managed Microsoft AD DC 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 を使用する方法の詳細については、「」を参照してくださいAWS マネージド Microsoft AD のマルチファクタ認証を有効にする。

AWS Managed Microsoft AD を作成する

新しいディレクトリを作成するには、以下の手順を実行します。この手順を開始する前に、「AWS Managed Microsoft AD 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 ディレクトリを作成するには

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。

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。

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。

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ー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 Active Directory で作成される内容

AWS Managed Microsoft AD で Active Directory 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 Interfaces」を参照してください。 AWS Managed Microsoft AD のデフォルトの DNS サーバーは、Classless Inter-Domain Routing (CIDR)+2 の VPC DNS サーバーActive Directory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 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。

- 耐障害性と高可用性のために、2 つのドメインコントローラーを使用して VPC 内で Active Directory がプロビジョニングされます。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、「追加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を作成します。デフォルトのアウトバウンドルールは、作成された AWS セキュリティグループにアタッチされたすべてのトラフィック ENIs またはインスタンスを許可します。デフォルトのインバウンドルールでは、任意のソース (0.0.0.0/0) からの Active Directory の必須ポートを経由したトラフィックのみが許可されます。0.0.0.0/0 ルールでは、ドメインコントローラーへのトラフィックは VPC、他のピア接続された VPCs、または AWS Direct Connect、 AWS Transit Gateway、または仮想プライベートネットワークを使用して接続したネットワークからのトラフィックに制限されるため、セキュリティの脆弱性は発生しません。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、 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 と VPC がルーティングしたトラフィックのみです。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」を参照してください。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	0.0.0.0/0	Ping	LDAP キープアライブ、DFS

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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	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	0.0.0.0/0	Windows タイム	Windows タイム、信頼
UDP	138	0.0.0.0/0	DFSN と NetLogon	DFS、グループポリシー
すべて	すべて	sg-###### ############	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	sg-###### ############	すべてのトラフィック	

- Active Directory で使用される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。
- 「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、Users OU (例えば、Corp > Users) の下にあります。このアカウントを使用して、 AWS クラウドでディレクトリを管理します。詳細については、「管理者アカウントのアクセス権限」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、 AWS Directory Service コンソールまたは ResetUserPassword API を使用してパスワードをリセットできます。

- 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 委任グループ	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 予約済み	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 されており、 AWS

OU 名	説明

	関連のディレクトリオブジェクトがすべて含まれており、フルコントロールが付与されています。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

- AWS 委任グループ OU に次のグループを作成します。

グループ名	説明
AWS 委任アカウントオペレーター	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 委任された Active Directory ベースのアクティベーション管理者	このセキュリティグループのメンバーは、Active Directory ボリュー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 がドメインユーザーにワークステーションを追加を委任	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 委任された管理者	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、委任グループ OU に含まれる AWS グループを管理できます。
AWS オブジェクトの認証が許可されている委任	このセキュリティグループのメンバーには、AWS リザーブド OU 内のコンピュータリソー

グループ名	説明
	スに対して認証する機能が提供されます (選択認証が有効な信頼を持つオンプレミスオブジェクトにのみ必要) 。
AWS ドメインコントローラーへの認証を許可する委任	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 OU 内のコンピュータリソースに対する認証を許可されます (信頼に選択的な認証を適用できるオンプレミスオブジェクトにのみ必要)。
AWS が委任した削除済みオブジェクトのライフタイム管理者	このセキュリティグループのメンバーは、削除されたオブジェクトが AD ごみ箱から復旧できる期間を定義する msDS -DeletedObjectLifetime オブジェクトを変更できます。
AWS 委任分散ファイルシステム管理者	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 委任されたドメイン名システム管理者	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 委任された動的ホスト設定プロトコル管理者	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 委任されたエンタープライズ認証機関管理者	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 委任されたきめ細かなパスワードポリシー管理者	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。

グループ名	説明
AWS 委任された FSx 管理者	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 が委任したグループポリシー管理者	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 委任された Kerberos 委任管理者	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
AWS が委任した Managed Service アカウント管理者	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 委任された MS-NPRC 非準拠デバイス	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 委任されたリモートアクセスサービス管理者	このセキュリティグループのメンバーは、RAS および IAS サーバーグループに対して RAS サーバーを追加および削除できます。
AWS 委任されたレプリケートディレクトリの変更管理者	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 サーバーと同期できます。
AWS 委任サーバー管理者	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 委任されたサイトとサービス管理者	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。

グループ名	説明
AWS 委任されたシステム管理者	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 委任されたターミナルサーバーライセンス管理者	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ライセンスサーバーグループに属するターミナルサーバーライセンスサーバーを追加および削除できます。
AWS 委任されたユーザープリンシパル名のサフィックス管理者	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。

- 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
デフォルトのドメインポリシー	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	AWS 「委任サーバー管理者」を BUILTIN\Administrators Group のメンバーとして追加します。
AWS 予約ポリシー：ユーザー	AWS 予約済みユーザーアカウント	AWS リザーブド OU 内のすべてのユーザーアカウントに

グループポリシー名	適用対象	説明
		推奨されるセキュリティ設定を設定します。
AWS マネージド Active Directory ポリシー	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。
ドメインコントローラーのデフォルトポリシー	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る 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。

管理者アカウントのアクセス権限

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 Active Directory で作成される内容」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 でユーザーとグループを管理する」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 モジュールと DNS Windows PowerShellモジュールを実行します。
- 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。

> **Important**
>
> 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。 AWS が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。

> **Note**
>
> 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。

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 日ごとに自動的にランダムなパスワードにローテーションします。組み込みの管理者パスワードが人間による使用を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 管理チームのみが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、パスワードボー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 正常にローテーションすると、 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行う必要がある AWS 場合があります。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 オートメーションは、ドメイン管理者のアクセス許可を持つ時間制限付きユーザーアカウントをディレクトリに作成します。 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。この機能により、AD セキュリティイベントをシステムに転送し、モニタリングソリューションを実装できます CloudWatch。詳細については、「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。イベントビューワー Microsoft 管理コンソール (MMC) を使用すると、ドメインに結合している Windows コンピュータから各 DC の Windows セキュリティイベントログを表示できます。またログ転送の有効化、すべてのセキュリティイベントログをアカウントの CloudWatch ログ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、およびアクセスと管理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、 AWS Directory Service が自動化を使用してドメイン管理者の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、まれに、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場合、 AWS Directory Service エンジニアが使用できるように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

以下の主要なコンセプトを理解すると、AWS Managed Microsoft AD をさらに活用できます。

トピック

- アクティブディレクトリのスキーマ
- 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

アクティブディレクトリのスキーマ

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。例として、User クラスの属性には、ユーザーの姓、名、電話番号などを含めることができます。

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。AWS Managed 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必要がある、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。クラスの特性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 (別名: AWS DS for AWS Managed Microsoft AD) とは、実際には Microsoft Active Directory のドメインサービス (AD DS) であり、マネージド型サービスとして提供されています。システムはドメインコントローラー (DC) 用に Microsoft Windows Server 2019 を使用し、AWS は サービス管理の目的で DC にソフトウェアを追加します。また、AWS は DC を更新 (パッチ適用) して新しい機能の追加を行うと同時に、Microsoft Windows Server ソフトウェアを最新の状態に保ちます。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、DC を追加で導入することをお勧めします。AWS は DC に対しパッチを順番に適用します。がパッチ適用処理を実行している DC AWS は利用できなくなります。1 つ以上の DC が一時的に使用停止状態になった場合、AWS は、ディレクトリに少なくとも 2 つの運用可能な DC が検出されるまでパッチ適用を延期します。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

お使いの DC の Microsoft Windows Server ソフトウェアを最新の状態に保つために、AWS は Microsoft アップデートを利用しています。Microsoft による、Windows Server 用の月次ロールアップパッチが利用可能になったため、AWS は、すべての顧客 DC に対するロールアップを 3 週間以内にテストならびに適用するよう、最善を尽くしています。さらに、DC への適用性と緊急性に基づいて、AWS は、Microsoft が毎月のロールアップ外でリリースする更新のレビューを行います。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に設定します。

AWS Managed Microsoft AD のユーザーに対し、gMSA を作成するための許可を付与するには、そのユーザーのアカウントをセキュリティグループ (AWS Delegated Managed Service Account Administrators) のメンバーに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。

AWS セキュリティブログの関連記事

- Managed Microsoft AD Helps to Simplify the Deployment and Improve the Security of Active Directory–Integrated .NET Applications (AWS Managed Microsoft AD によってデプロイを簡素化し Active Directory と統合された .NET アプリケーションのセキュリティを強化する方法)

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の代わりに行う処理の範囲を制限することで、アプリケーションの信頼の境界を指定し適用できます。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。

例えば、ユーザー jsmith が HR アプリケーションにログインする場合を考えます。この時、SQL Server で jsmith のデータベースへのアクセス許可を適用する必要があります。ただし、SQL Server のデフォルトでは、データベース接続を開く際に jsmith で設定済みのアクセス許可を使用せず、(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ます。HR 給与アプリケーションが SQL Server データベースにアクセスするために、jsmith の認証情報を使用できるように設定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。

Kerberos の制約付き委任を設定するアクセス許可を、AWS Managed Microsoft AD のユーザーに付与するには、それらのユーザーのアカウントをセキュリティグループ (AWS Delegated Kerberos Delegation Administrators) のメンバーとして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

ここでは、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。

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 Active Directoryに接続するだけです 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互換性を備えた低コストの低スケールディレクトリです。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 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 Active Directory」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 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、その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 の通信に必要なトラフィックを許可します。 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。デフォルト設定では、セキュリティグループは任意の IP アドレスから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ア AWS 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 0.0.0.0/0 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ます。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。AWS 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、この practice. AWS 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 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。ディレクトリのセキュリティグ

ループは、必要な Active Directory ポートで任意の IP アドレスからのトラフィックを受け付けます。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。

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る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。そのアカウント ID は Managed Microsoft AD AWS 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、「DHCP オプションセットを作成または変更する」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消えるのを防ぐことができます。

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ーゾーンに存在する 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ー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 Locator Service 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、、Amazon 、Amazon 、または Amazon 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 WorkSpaces、文字制限が適用されます WorkDocs WorkMail QuickSight。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。

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。

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。そうすることで、ディレクトリに自分自身と の両方が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 Active Directory で作成される内容」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 ドメインの一部である 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環としてドメインに参加するのが最も簡単です。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 にシームレスに結合する 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との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、「信頼関係の作成」を参照してください。

ディレクトリを管理する

ディレクトリを管理するための以下の推奨事項を考慮してください。

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、「パフォーマンスメトリクスを使用してドメインコントローラーをモニタリングする」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 のスケーリングを自動化する方法 AWS 」を参照してください。

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、「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。Microsoft の Active Directory (AD) は、外部ロードバランシングを使用せずに応答性の最も高い運用中の DC を検出する、ドメインコントローラー (DC) 探索アルゴリズムと共に使用するように設計されています。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 のロードバランサーと Active Directory」を参照してください。 TechNet このバージョンでは、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、「ディレクトリをスナップショットまたは復元する」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、 からメッセージを受信する SNS トピックがある場合は AWS Directory Service、Amazon SNS コンソールからそのトピックを削除する前に、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 SNS でディレクトリステータス通知を設定する」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 では、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、 のステップまたは UpdateSettings API ディレクトリセキュリティ設定の編集を使用してコンソールで実行できます。

詳細については、「ディレクトリセキュリティ設定の構成」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

Amazon WorkSpaces Application Manager、Amazon 、Amazon WorkSpaces、Amazon Relational Database Service (Amazon RDS) などの 1 つ以上の Amazon Enterprise Applications に関連付けられているディレクトリを削除する前に WorkDocs WorkMail 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 管理対象Microsoft AD を削除する」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。SMBv1 の無効化とシステム上の新しい SMB バージョンへの更新の詳細については、Microsoft TechNet および Microsoft ドキュメント のこれらの投稿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、 Windows PowerShell コマンドレット Set- を使用しますSmbServerConfiguration。

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、「追加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。

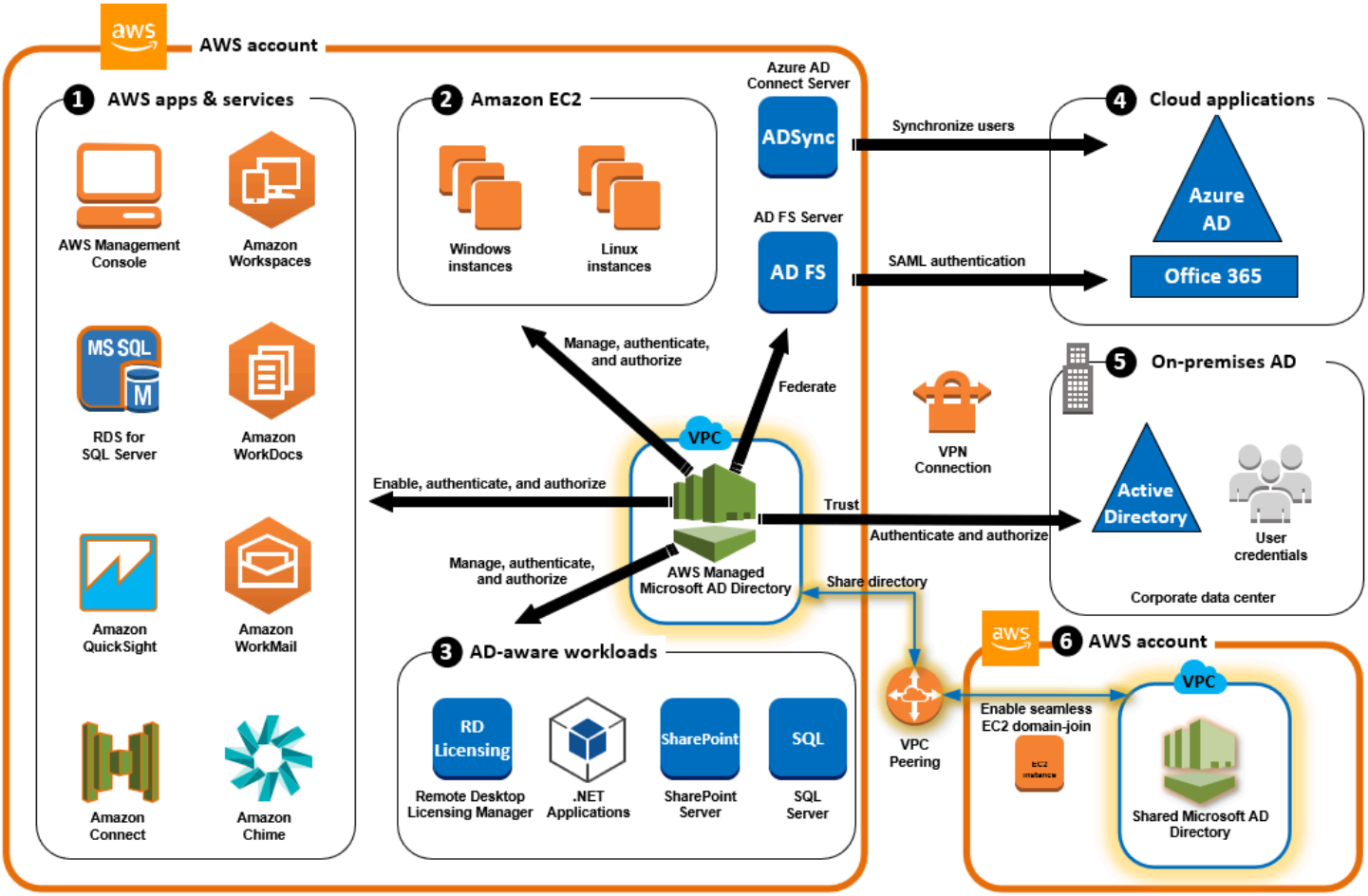
効率的な LDAP クエリを使用する

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、複数のユースケースで単一のディレクトリを共有できます。例えば、1 つのディレクトリを共有して、NET アプリケーションや 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 へのアクセスを認証および承認できます。

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: オンプレミスの Active Directory を AWS クラウドに拡張する
- ユースケース 6: 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

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WorkSpacesを使用するにはAWS Client VPN、、AWS Management Console、AWS IAM Identity Center、Amazon Chime 、Amazon Connect 、Amazon FSx 、Amazon 、Amazon RDS for SQL Server QuickSight、Amazon 、Amazon 、およびWorkDocs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。WorkMail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。

例えば、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 にサインインすると 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、Amazon 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 WorkDocs、ユーザーは、認証情報を個別に入力しなくても、ディレクトリに結合されたコンピュータ WorkDocs から Amazon 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 と AWS Managed Microsoft AD を統合すると、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ます。これにより、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 に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、一般的な FSx for Windows File Server と AWS Managed Microsoft AD の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、フルマネージド型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 FSx with AppStream 2.0 は、Amazon FSx を使用する個人用の永続ストレージドライブを提供し、共通のファイルにアクセスするための共有フォルダを提供す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 での Amazon FSx の使用
- 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 を使用すると、Active Directory ユーザーのホームフォルダおよび My Documents からデータを一元的な場所に保存できます。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
- での FSx for Windows File Server の使用 WorkSpaces

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
- での FSx for Windows File Server の使用 WorkSpaces

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でインストールする

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。

- ディレクトリの共有
- 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 AWS と Amazon RDS で始まり、Amazon RDS を AWS Managed Microsoft AD と統合する方法をカバーします。

- 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。

- ディレクトリの共有
- 「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、Windows または Linux インスタンス用の Amazon EC2 を一元管理できます。 AWS

また、ユーザーは 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、リモートデスクトップライセンスマネージャー、Microsoft SharePoint および Microsoft SQL Server Always On などの従来の Active Directory 対応ワークロードを クラウドで実行できる実際の Microsoft Active Directory です。Managed Microsoft AD は、グループ Managed Service Accounts (gMSAs) と Kerberos 制約付き委任 (KCD) を使用して、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。AWS AWS

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 AWS IAM Identity Center に 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 およびその他の 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 動画を参照してください。

> **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: オンプレミスの Active Directory を AWS クラウドに拡張する

Active Directory 対応のワークロードを AWS クラウドに移行するときに Active Directory インフラストラクチャを既に使用したい場合は、 AWS マネージド Microsoft AD が役立ちます。Active Directory の信頼を使用して、 AWS Managed Microsoft AD を既存の Active Directory に接続できます。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、オンプレミスの 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。

例えば、ユーザーは既存の Active Directory ユーザー名とパスワード WorkSpaces を使用して AWS Management Console と Amazon にサインインできます。また、 AWS Managed Microsoft AD SharePoint で などの Active Directory 対応アプリケーションを使用すると、ログインした Windows ユーザーは認証情報を再度入力しなくてもこれらのアプリケーションにアクセスできます。

Active Directory Migration Toolkit (ADMT) と Password Export Service (PES) を使用して、オンプレミスの Active Directory ドメインを に移行し AWS 、Active Directory 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。 https://aws.amazon.com/blogs/security/how-to-migrate-your-on-premises-domain-to-aws-managed-microsoft-ad-using-admt/

ユースケース 6: 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

複数のアカウント間でディレクトリを共有すると、 AWS 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 間で簡単に管理することができるようになりました。

AWS Managed Microsoft AD ディレクトリを別のアカウントと共有する場合 AWS 、Amazon EC2 コンソールまたは を使用してAWS Systems Manager、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、「ディレクトリの共有」を参照してください。

Managed Microsoft AD AWS を管理する方法

このセクションでは、 AWS Managed Microsoft AD 環境を運用および保守するためのすべての手順を一覧表示します。

トピック

- AWS Managed Microsoft AD ディレクトリを保護する
- AWS Managed Microsoft AD をモニタリングする
- マルチリージョンレプリケーション
- ディレクトリの共有
- Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する Active Directory
- AWS Managed Microsoft AD でユーザーとグループを管理する
- 既存の Active Directory インフラストラクチャに接続する
- AWS Managed Microsoft AD を に接続する Microsoft Entra Connect Sync
- スキーマを拡張する
- AWS Managed Microsoft AD ディレクトリの維持
- ユーザーおよびグループに AWS リソースへのアクセス権限を付与する
- 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 認証情報による AWS Management Console へのアクセスを有効化する
- 追加ドメインコントローラーのデプロイ
- Active Directory から AWS Managed Microsoft AD へユーザーを移行する

AWS Managed Microsoft AD ディレクトリを保護する

このセクションでは、AWS Managed Microsoft 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

- AWS マネージド Microsoft AD のパスワードポリシーの管理
- AWS マネージド Microsoft AD のマルチファクタ認証を有効にする
- セキュア LDAP または LDAPS を有効にする
- AWS マネージド Microsoft AD のコンプライアンスを管理
- AWS Managed Microsoft AD のネットワークセキュリティ設定を強化する

- ディレクトリセキュリティ設定の構成
- AWS Private CA Connector for AD をセットアップする

AWS マネージド Microsoft AD のパスワードポリシーの管理

AWS Managed Microsoft AD では、 AWS Managed Microsoft AD ドメインで管理するユーザーグループに対して、さまざまなパスワードおよびアカウントロックアウトポリシー (詳細設定可能なパスワードポリシーとも呼ばれます) を定義して割り当てることができます。 AWS 管理対象の 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
可逆的暗号化を使用したパスワードの保存	無効

* 注意: パスワードの最長有効期間 (42 日間) 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。

MicrosoftActive Directoryきめ細かいパスワードポリシーとセキュリティポリシーについて詳しく知るためのリソースは次のとおりです。

- セキュリティポリシー設定を行います。
- パスワードの複雑さの要件
- パスワードの複雑さ、セキュリティ上の考慮事項

AWS AWS Managed Microsoft AD には、設定してグループに割り当てることができる、きめ細かい一連のパスワードポリシーが用意されています。ポリシーを構成するには、MicrosoftActive Directory管理センターなどの標準のポリシーツールを使用できます。Microsoftポリシーツールを使い始めるには、を参照してください管理対象の Microsoft AD AWS 用アクティブディレクトリ管理ツールのインストール。

パスワードポリシーの適用方法

パスワードがリセットされたのか、パスワードが変更されたのかによって、きめ細かいパスワードポリシーの適用方法が異なります。ドメインユーザーは自分のパスワードを変更できます。Active Directory管理者または必要な権限を持つユーザーは、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、次の表を参照してください。

ポリシー	パスワードリセット	パスワード変更
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

ポリシー	パスワードリセット	パスワード変更
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。たとえば、ユーザーのパスワードがリセットされるたびに、「パスワード履歴の強制」ポリシーと「パスワードの最低有効期間」ポリシーは適用されません。詳細については、パスワード履歴およびパスワードの最低有効期間ポリシーの適用に関するセキュリティ上の考慮事項に関する Microsoft のドキュメントを参照してください。

トピック

- サポートされているポリシー設定
- パスワードポリシーの管理権限を委任する
- パスワードポリシーをユーザーに割り当てる

AWS 関連する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ようにさらに強力なパスワードポリシーを設定する方法

サポートされているポリシー設定

AWS 管理対象の Microsoft AD には、編集不可の優先順位値を持つ 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 定義済みのパスワードポリシー

次の表は、 AWS 管理対象の Microsoft AD ディレクトリに含まれている 5 つのポリシーと、それらに割り当てられている優先順位値を示しています。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強制に与える影響について詳しくは、Microsoft Web サイトの「AD DS: きめ細かい設定が可能なパスワードポリシー」を参照してください。 TechNetこれらのポリシーに関する一般的な情報については、Microsoft TechNet Web サイトの「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

これらのポリシーに関する一般的な情報については、Microsoft TechNet Web サイトの「アカウントロックアウトポリシー」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 の Web サイトの「AD DS: きめ細かいパスワードポリシー」を参照してください。 TechNet

パスワードポリシーの管理権限を委任する

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権限を委任するには、AWS それらのアカウントを委任されたファイングレインパスワードポリシー管理者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. マネージド Microsoft AD ドメインに参加した任意のマネージド 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 Active Directory で作成される内容」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。

パスワードポリシーをユーザーに割り当てる

[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. マネージド Microsoft AD ドメインに参加した任意のマネージド 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 定義済みの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、 PowerShell以下の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 管理対象の Microsoft AD ディレクトリにある 5 つのパスワードポリシーのいずれも設定しない場合、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 マネージド Microsoft AD のマルチファクタ認証を有効にする

AWS 管理対象の Microsoft AD ディレクトリで多要素認証 (MFA) を有効にすると、ユーザーが AD 認証情報を指定してアクセスする際のセキュリティを強化できます。サポートされている Amazon エンタープライズアプリケーション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、許可、アカウント管理の機能を提供します。 AWS マネージド 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 管理対象の Microsoft AD は次に 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 管理対象の 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 AWS を介した通信を有効にするセキュリティグループを構成する必要があります。

次の手順を実行して、 AWS 管理対象の Microsoft AD ディレクトリの多要素認証を有効にできます。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 管理対象の Microsoft AD の多要素認証に関する考慮事項は次のとおりです。

- 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Multi-Factor Authenticationを有効にする」を参照してください。

- MFA AWS はマネージド Microsoft AD の地域機能です。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 Managed Microsoft AD を外部通信に使用する場合は、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Internet Gateway AWS をネットワーク外の通信用に構成することをお勧めします。
  - AWS 管理対象の Microsoft AD AWS とネットワーク上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したい場合は、お問い合わせくださいAWS Support。

AWS マネージド Microsoft AD のマルチファクタ認証を有効にする

次の手順は、 AWS 管理対象の Microsoft AD の多要素認証を有効にする方法を示しています。

1. RADIUS MFA AWS サーバーと管理対象の 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 管理対象の Microsoft AD IP エンドポイントと RADIUS MFA サーバー間のポート 1812 を介した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 管理対象の 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 AWS Management Console、または Amazon や Amazon Amazon Chime WorkSpaces などの Amazon エンタープライズ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。 QuickSightEC2 インスタンスで実行されている Windows ワークロードに MFA を提供したり、EC2 インスタンスにサインインしたりするための MFA は提供されません。 AWS Directory Service RADIUS チャレンジ/レスポンス認証は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 SMS out-of-band テキスト検証などの MFA を実行するソリューションを使用する必要があります。 out-of-band MFA ソリューションでは、RADIUS タイムアウト値をソリューションに適切に設定する必要があります。 out-of-band MFA ソリューションを使用する場合、サインインページでユーザーに 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、サーバーからのデフォルトの RADIUS サーバーポート (UDP: 1812) を介したインバウンドトラフィックを許可する必要があります。 AWS Directory Service

[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。

サポートされている Amazon エンタープライズアプリケーション

Amazon、Amazon WorkSpaces、Amazon を含むすべての Amazon WorkDocs エンタープライズ IT アプリケーション WorkMail QuickSight、および MFA AWS 付きマネージド Microsoft AD および AD Connector AWS IAM Identity Center AWS Management Console へのアクセスがサポートされます。

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、および使用の設定方法については AWS Directory Service、「」と「」を参照してください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。 AWS Management Console AD 認証情報による AWS Management Console へのアクセスを有効化する

AWS 関連するセキュリティブログ記事

- AWS Managed Microsoft AD AWS とオンプレミスの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

セキュア LDAP または LDAPS を有効にする

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、または検索を行なったり、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。

このようなデータ漏えいを軽減するために、 AWS Managed Microsoft ADには次のオプションがあります。LDAPSとも呼ばれるセキュア・ソケット・レイヤー (SSL) /トランスポート・レイヤー・セキュリティ (TLS) を介したLDAPを有効にできます。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 マネージド Microsoft AD は、以下の導入シナリオで LDAPS をサポートします。

- サーバー側LDAPSは、商用または自社開発のLDAP対応アプリケーション (LDAPクライアントとして動作) AWS と管理対象Microsoft AD (LDAPサーバーとして動作) 間のLDAP通信を暗号化します。詳細については、「マネージド Microsoft AD AWS を使用してサーバー側の LDAPS を有効にする」を参照してください。
- クライアント側の LDAPS は、(LDAP クライアントとして動作) AWS などのアプリケーションと、自己管理 (オンプレミス) の Active WorkSpaces Directory (LDAP サーバーとして動作) との間の LDAP 通信を暗号化します。詳細については、「マネージド Microsoft AD AWS を使用してクライアント側の LDAPS を有効にする」を参照してください。

トピック

- マネージド Microsoft AD AWS を使用してサーバー側の LDAPS を有効にする
- マネージド Microsoft AD AWS を使用してクライアント側の LDAPS を有効にする

マネージド Microsoft AD AWS を使用してサーバー側の LDAPS を有効にする

サーバー側のライトウェイトディレクトリアクセスプロトコルセキュアソケットレイヤー (SSL) /トランスポートレイヤーセキュリティ (TLS) (LDAPS) サポートにより、商用または自社製の LDAP 対応アプリケーションと管理対象の Microsoft AD ディレクトリ間の LDAP 通信が暗号化されます。AWS 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LDAPSと認証局 (CA) サーバーをセットアップおよび構成する方法の詳細については、セキュリティブログの「 AWS 管理対象Microsoft ADディレクトリのサーバー側LDAPSを有効にする方法」を参照してください。 AWS

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。以下の手順は、クラウド内のドメインの LDAPS を有効にする手順を示しています。 AWS

PKI インフラストラクチャの設定を自動化したい場合は、AWS QuickStart ガイドの Microsoft 公開鍵インフラストラクチャを使用できます。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 このガイドを使用したことがある場合は、ステップ 3: 証明書テンプレートを作成するに直接ジャンプできます。

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、Managed Microsoft AD AWS ディレクトリの管理者グループまたは委任エンタープライズ認証局管理者グループのメンバーである必要があります。 AWS 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。

その場合は、そのユーザーを AWS Managed Microsoft AD AWS ディレクトリの管理者グループまたは委任エンタープライズ認証局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 管理対象の 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 管理対象の Microsoft AD を使用するサーバー側 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。

- 下位の Microsoft エンタープライズ CA の作成 — (推奨) このオプションを使用すると、下位の Microsoft エンタープライズ CA サーバーをクラウドに展開できます。 AWS 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。下位の 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、「管理対象の Microsoft AD ディレクトリのサーバー側 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
- ルートマイクロソフトエンタープライズ CA の作成 — このオプションでは、Amazon EC2 AWS を使用してクラウドにルート Microsoft エンタープライズ CA を作成し、 AWS それをマネージド Microsoft AD ドメインに参加させることができます。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、「AWS 管理対象の Microsoft AD ディレクトリのサーバー側 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構成する」を参照してください。

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 Active Directory」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. 証明書の受信者を Windows 10/Windows Server 2016 に変更してください。

      > **Note**
      > AWS マネージドMicrosoft AD は Windows Server 2019 を搭載しています。

   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。

- [ソース] の横のボックスに、 AWS ディレクトリのセキュリティグループ (例:sg-123456789) を入力します。
- [保存] を選択します。

6. 次に、 AWS 管理対象の Microsoft AD AWS ディレクトリ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。
- [宛先] 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 管理対象の 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、「管理対象の Microsoft AD AWS 用アクティブディレクトリ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LDAPSの詳細と設定方法のユースケースについては、セキュリティブログの「AWS 管理対象Microsoft ADディレクトリのサーバー側LDAPSを有効にする方法」を参照してください。 AWS

マネージド Microsoft AD AWS を使用してクライアント側の LDAPS を有効にする

AWS Managed Microsoft AD におけるクライアント側のライトウェイトディレクトリアクセスプロトコルセキュアソケットレイヤー (SSL) /トランスポートレイヤーセキュリティ (TLS) (LDAPS) サポートにより、自己管理 (オンプレミス) の Microsoft Active Directory (AD) とアプリケーション間の通信が暗号化されます。 AWS このようなアプリケーションの例としては WorkSpaces、、、Amazon AWS IAM Identity Center QuickSight、Amazon Chime などがあります。この暗号化により、組織の ID データの保護を強化し、セキュリティ要件を満たすことができます。

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

- マネージド Microsoft AD AWS とセルフマネージドの間に信頼関係を構築する Microsoft Active Directory
- Active Directory にサーバー証明書をデプロイする
- 認証局の証明書要件
- ネットワーク要件

マネージド Microsoft AD AWS とセルフマネージドの間に信頼関係を構築する Microsoft Active Directory

まず、クライアント側の LDAPS Microsoft Active Directory を有効にするために、 AWS 管理対象の Microsoft AD と自己管理型の間に信頼関係を確立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。

認証局の証明書要件

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。

- クライアント側の LDAPS を有効にするにはエンタープライズ認証局 (CA) が必要です。Active Directory証明書サービス、サードパーティの商用認証局、またはのいずれかを使用できます。AWS Certificate ManagerMicrosoftエンタープライズ認証局について詳しくは、Microsoftドキュメントを参照してください。

- 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。
- AWS 管理対象の Microsoft AD ディレクトリごとに最大 5 つの 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。
- 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 アプリケーションの 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。マネージド Microsoft AD (アウトバウンド) AWS 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 メソッドとメソッドのどちらでも使用できます。 AWS CLI

> **Note**
>
> クライアント側 LDAPS AWS はマネージド Microsoft AD のリージョナル機能です。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: に証明書を登録する 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: に証明書を登録する AWS Directory Service

次のいずれかの方法を使用して、 AWS Directory Serviceに証明書を登録します。

方法 1: AWS Directory Service (AWS Management Console) に証明書を登録する

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) 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: AWS Directory Service (AWS CLI) に証明書を登録するには

- 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。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 Service (AWS Management Console) で証明書の登録状況を確認するには

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 Service (AWS CLI) で証明書の登録状況を確認するには

- 以下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

以下のいずれかの方法を使用して、クライアント側の LDAPS in を有効にします。 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: () でクライアント側の LDAPS を有効にする AWS Directory ServiceAWS 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. [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: () でクライアント側の LDAPS を有効にする AWS Directory ServiceAWS CLI

- 以下のコマンドを実行します。

```
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

以下のいずれかの方法を使用して、LDAPS のステータスを確認します。 AWS Directory Service

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

- 以下のコマンドを実行します。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 メソッドとメソッドのどちらでも使用できます。 AWS CLI

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 Service (AWS 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 Service (AWS 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ます。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 Service ()AWS Management Consoleで証明書を登録解除するには

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 Service で証明書を登録解除するにはAWS CLI

- 以下のコマンドを実行します。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: () でクライアント側の LDAPS を無効にする AWS Directory ServiceAWS 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: () でクライアント側の LDAPS を無効にする AWS Directory ServiceAWS CLI

- 以下のコマンドを実行します。

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

証明書登録に関する問題

AWS 管理対象の 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。証明書の登録に問題があり、 AWS 管理対象の Microsoft AD ドメインコントローラーを再起動したい場合は、お問い合わせください。 AWS Supportサポートケースを作成するには、「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 マネージド Microsoft AD のコンプライアンスを管理

AWS Managed Microsoft AD を使用すると、以下のコンプライアンス要件の対象となる Active Directory AWS 対応アプリケーションをクラウドでサポートできます。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、以下の規格の監査を受けており、コンプライアンス認証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、連邦リスクおよび承認管理プログラム (FedRAMP) のセキュリティ要件を満たしており、FedRAMP の中程度および高レベルの基準で FedRAMP 共同承認委員会 (JAB) の暫定運用権限 (P-ATO) を受けています。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、サービスプロバイダーレベル 1 で、ペイメントカード業界 (PCI) データセキュリティ標準 (DSS) バージョン 3.2 への準拠証明書を取得しています。 AWS 製品やサービスを使用してカード会員データを保存、処理、または送信するお客様は、 AWS Managed Microsoft AD を使用して独自の PCI DSS コンプライアンス証明書を管理できます。

PCI コンプライアンスPackage コピーをリクエストする方法など、PCI DSS の詳細については、 AWS PCI DSS レベル 1 を参照してください。重要なのは、 AWS Managed Microsoft AD では、PCI DSS バージョン 3.2 標準と一致するように、きめ細かいパスワードポリシーを設定する必要があるということです。どのポリシーを適用する必要があるかについて詳しくは、以下の「 AWS 管理対象の 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、Health 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大し、HIPAA AWS 対象サービスとして Managed Microsoft AD を追加しました。とビジネスアソシエイト契約 (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 AWS 医療情報の処理と保存にどのように活用できるかについて詳しく知りたいお客様向けに、HIPAA に焦点を当て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るわけでは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 AWS がサポートするさまざまなコンプライアンスプログラムの全一覧については、「AWS コンプライアンスプログラム別の対象サービス」を参照してください。

AWS 管理対象の 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 管理対象の Microsoft AD ディレクトリで PCI コンプライアンスを有効にするには、が提供する PCI DSS コンプライアンス証明書 (AOC) および責任の概要ドキュメントで指定されているように、きめ細かい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 マネージド Microsoft AD のパスワードポリシーの管理」を参照してください。

AWS Managed Microsoft AD のネットワークセキュリティ設定を強化する

AWS Managed Microsoft AD ディレクトリ用にプロビジョニングされている AWS セキュリティグループには、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が設定済みとなっています。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 Active Directory で作成される内容」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、以下に示す一般的なシナリオに応じて AWS セキュリティグループを変更できます。

トピック

- AWS アプリケーションのみのサポート
- 信頼がサポートされる AWS アプリケーション
- AWS アプリケーションとネイティブの Active Directory ワークロードのサポート
- 信頼の使用が可能な AWS アプリケーションとネイティブの Active Directory ワークロードのサポート

AWS アプリケーションのみのサポート

すべてのユーザーアカウントは、以下に挙げるようなサポートされた AWS アプリケーション専用として、AWS Managed Microsoft AD にプロビジョニングされます。

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

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

> **Note**
>
> - 以下のサービスでは、この AWS セキュリティグループ設定を使用できません。
>   - 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。

信頼がサポートされる AWS アプリケーション

すべてのユーザーアカウントは、AWS Managed Microsoft AD 、または信頼された Active Directory にプロビジョニングされており、これをサポートしている以下の AWS アプリケーションにおいて使用が可能です。

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

プロビジョニングされている AWS セキュリティグループ設定を変更すると、AWS Managed Microsoft AD ドメインコントローラーへの、重要ではないすべてのトラフィックをブロックすることができます。

Note

- 以下のサービスでは、この AWS セキュリティグループ設定を使用できません。
  - 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、「オンプレミス CIDR」ネットワークのセキュリティを確保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	トラフィックのタイプ	Active Directory の使用
TCP と UDP	53	オンプレミス 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	オンプレミス 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	オンプレミス CIDR	LDAP	ディレクトリ、レプリケーショ

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
				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	オンプレミス 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	オンプレミス 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	オンプレミス CIDR	レプリケーション	RPC、EPM
TCP	636	オンプレミス 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	オンプレミス 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

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
TCP	3268 - 3269	オンプレミス 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	オンプレミス 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	トラフィックのタイプ	Active Directory の使用
すべて	すべて	オンプレミス 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の Active Directory ワークロードのサポート

ユーザーアカウントは、以下に挙げるようなサポートされた AWS アプリケーション専用として、AWS Managed Microsoft AD にプロビジョニングされています。

- Amazon Chime
- Amazon Connect
- Amazon EC2 インスタンス
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server

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

プロビジョニングされている AWS セキュリティグループ設定を変更すると、AWS Managed Microsoft AD ドメインコントローラーへの、重要ではないすべてのトラフィックをブロックすることができます。

> **Note**
>
> - AWS Managed Microsoft AD ディレクトリとオンプレミスドメインとの間では、Active Directory の信頼を作成し維持することはできません。
> - そのためには、「クライアント CIDR」ネットワークのセキュリティを確保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。
> - この設定エンタープライズ CA を使用する場合は、アウトバウンドルールとして「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	トラフィックのタイプ	Active Directory の使用
TCP と UDP	53	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	クライアント CIDR	Kerberos	ユーザーとコンピュータの認

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
				証、フォレストレベルの信頼
TCP と UDP	389	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	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認証、グループポリシー、信頼
TCP と UDP	464	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	クライアント CIDR	レプリケーション	RPC、EPM
TCP	636	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

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
TCP	49152 - 65535	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	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	クライアント CIDR	SOAP	AD DS ウェブサービス
UDP	123	クライアント CIDR	Windows タイム	Windows タイム、信頼
UDP	138	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。

信頼の使用が可能な AWS アプリケーションとネイティブの Active Directory ワークロードのサポート

すべてのユーザーアカウントは、AWS Managed Microsoft AD 、または信頼された Active Directory にプロビジョニングされており、これをサポートしている以下の AWS アプリケーションにおいて使用が可能です。

- Amazon Chime
- Amazon Connect

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

プロビジョニングされている AWS セキュリティグループ設定を変更すると、AWS Managed Microsoft AD ドメインコントローラーへの、重要ではないすべてのトラフィックをブロックすることができます。

> **Note**
>
> - そのためには、「オンプレミス CIDR」と「クライアント CIDR」のネットワークで、セキュリティを確保する必要があります。
> - 「オンプレミス CIDR」での TCP 445 は、信頼の作成時にのみ使用され、信頼の確立後は削除できます。
> - 「クライアント CIDR」での 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。
> - この設定エンタープライズ CA を使用する場合は、アウトバウンドルールとして「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	トラフィックのタイプ	Active Directory の使用
TCP と UDP	53	オンプレミス 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	オンプレミス 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	オンプレミス 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	オンプレミス 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	オンプレミス 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	オンプレミス CIDR	レプリケーション	RPC、EPM
TCP	636	オンプレミス 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

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
				認証、グループポリシー、信頼
TCP	49152 - 65535	オンプレミス 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	オンプレミス 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	オンプレミス CIDR	Windows タイム	Windows タイム、信頼
TCP と UDP	53	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	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	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

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
TCP と UDP	445	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認証、グループポリシー、信頼
TCP と UDP	464	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	クライアント CIDR	レプリケーション	RPC、EPM
TCP	636	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	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	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

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
TCP	9389	クライアント CIDR	SOAP	AD DS ウェブサービス
UDP	123	クライアント CIDR	Windows タイム	Windows タイム、信頼
UDP	138	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

プロトコル	ポート範囲	ソース	トラフィックのタイプ	Active Directory の使用
すべて	すべて	オンプレミス CIDR	すべてのトラフィック	

ディレクトリセキュリティ設定の構成

AWS Managed Microsoft AD のディレクトリ設定をきめ細かく設定することで、運用ワークロードを増やすことなく、コンプライアンスやセキュリティの要件を満たすことができます。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。例えば、RC4 や DES などの個々のレガシーの暗号や、SSL 2.0/3.0 や TLS 1.0/1.1 などのプロトコルを無効にできる柔軟性があります。AWSManaged 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 AWS リージョン をスケールアウトまたはデプロイするときにこの構成を維持します。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、AWS で https://console.aws.amazon.com/directoryservicev2/ 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. [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 AAES 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。これらを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	CERTIFICATE_BACKDATING_COMPENSATION	年: 0〜50 月: 0〜11 日: 0〜30 時間: 0〜23 分: 0 ~ 59 秒: 0 ~ 59	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。

タイプ	設定名	API 名	考えられる値	設定の説明
				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。 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
	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 (デフォルト): 証明書をユーザーに強くマッピングできない場合に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。 • 互換性: 証明書をユーザーに強くマッピング

タイプ	設定名	API 名	考えられる値	設定の説明
				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
	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。
セキュアチャネル: プロトコル	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 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。Active Directory 用 AWS Private CA コネクタを使用すると、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、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 の完全マネージド型 AWS Private CA ドロップインリプレースメントを使用できます。

> **Note**
>
> Connector for Active Directory を使用した AWS AWS Private CA Managed Microsoft AD ドメインコントローラーのサーバー側の LDAPS 証明書登録はサポートされていません。ディレクトリのサーバー側 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 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、Directory Service コンソール、 AWS Private CA Connector for Active Directory コンソール、または `CreateTemplate` API を呼び出して設定できます。 AWS Private CA Connector for Active Directory コンソールを使用して Private 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手順については、以下を参照してください。

AWS Private CA Connector for AD をセットアップするには

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. ネットワークとセキュリティ タブの AWS Private CA Connector for AD で、 AWS Private CA Connector for AD のセットアップ を選択します。のプライベート CA 証明書を作成するActive Directoryページが表示されます。コンソールの手順に従って、 Private CA に登録するActive Directoryコネクタ用の Private CA を作成します。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、以下の手順に従って、コネクタのステータスや関連するプライベート CA のステータスなどの詳細を表示します。

AWS Private CA Connector for AD を表示するには

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. [ネットワークとセキュリティ] の [AWS Private CA Connector for AD] 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。クリックすると、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 コネクタと 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 コネクタが作成された日。

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。

AWS Managed Microsoft AD をモニタリングする

AWS Managed Microsoft AD ディレクトリは以下の方法でモニタリングできます。

トピック

- ディレクトリのステータスを把握する
- Amazon SNS でディレクトリステータス通知を設定する
- AWS Managed Microsoft AD ディレクトリのログを確認する
- ログ転送の有効化
- パフォーマンスメトリクスを使用してドメインコントローラーをモニタリングする

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 Support 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については、40 AWS 分以内に問題を解決します。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 Support 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、「ディレクトリをスナップショットまたは復元する」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

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 Support 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 SNS でディレクトリステータス通知を設定する

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。ディレクトリがアクティブステータス から障害ステータス になると、通知を受け取ります。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。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。

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. [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 の権限が追加で必要です。

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。

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. [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。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、 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。

AWS Managed Microsoft AD ディレクトリのログを確認する

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。また、AWS Managed 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、「ログ転送の有効化」を参照してください。

AWS は、コンプライアンスに関する以下のイベントをログに記録します。

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
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

モニタリングカテゴリ	ポリシー設定	監査の状態
	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
	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ジングの監査	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

モニタリングカテゴリ	ポリシー設定	監査の状態
	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

ログ転送の有効化

AWS Directory Service コンソールまたは API を使用して、ドメインコントローラーセキュリティイベントログを 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。

また、CloudWatch Logs では、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。

ログ転送を有効化するには

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. 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. [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。

ログ転送を無効化するには

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. 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. [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。

CLI を使用したログ転送の有効化

`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 を使用してログ転送を有効にするには、以下のすべてのステップを完了します。

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 コマンドの例

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

PowerShell コマンドの例

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

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権限を AWS Directory Service に付与する CloudWatch Logs リソースポリシーを作成します。ロググループに ARN をそのまま指定して他のロググループへの AWS Directory Service のアクセスを制限することも、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もできます。次のポリシーのサンプルでは、ワイルドカードを使用する方法で、ディレクトリが存在する AWS アカウントに対して /aws/directoryservice/ で始まるすべてのロググループが含まれるように指定しています。

```
{
    "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 コマンドの例

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

PowerShell コマンドの例

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

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

ステップ 3: AWS Directory Service ログの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 コマンドの例

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

PowerShell コマンドの例

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

パフォーマンスメトリクスを使用してドメインコントローラーをモニタリングする

AWS Directory Service は Amazon CloudWatch と統合されているため、内の各ドメインコントローラの重要なパフォーマンスメトリックスを提供できます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 AWS Lambda トピックを使用して関数などの自動化を開始し、使用するドメインコントローラーの数を増やすことができます。Active Directory

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いつ追加するかを決めてください。」を参照してください。

Amazon には手数料がかかります CloudWatch。詳細については、「CloudWatch請求と費用」を参照してください。

> **Important**
>
> CloudWatch とのドメインコントローラーのパフォーマンス指標は、カナダ西部 (カルガリー) リージョンではご利用いただけません。

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以下で確認できます。 CloudWatch

Amazon CloudWatch コンソールでは、特定のサービスのメトリックスが最初にサービスの名前空間によってグループ化されます。ユーザーは、その名前空間に従属するメトリクスフィルターを追加できます。以下の手順に従って、 AWS で管理対象の Microsoft AD ドメインコントローラメトリックを設定するのに必要な正しい名前空間と従属メトリックを見つけてください。 CloudWatch

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

1. AWS Management Console にサインインし、https://console.aws.amazon.com/cloudwatch/ CloudWatch の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) をクリックします。
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のメトリクスを設定する方法については、 AWS セキュリティブログの「 AWS 使用率メトリックに基づいてマネージド 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。

CloudWatch メトリクスを使用してドメインコントローラーをいつ追加するかを決めてください。

すべてのドメインコントローラーの負荷分散は、の回復力とパフォーマンスにとって重要です。Active Directory AWS Managed Microsoft AD 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、 CloudWatch まず重要なメトリックを監視してベースラインを作成することをお勧めします。このプロセスでは、Active Directory時間の経過に伴う使用率を分析して、Active Directory平均使用率とピーク使用率を特定します。ベースラインを決定したら、これらのメトリックを定期的に監視して、ドメインコントローラーをいつ追加するかを判断できますActive Directory。

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。で利用できるドメインコントローラーのメトリックスの全リストについては CloudWatch、を参照してくださいAWS マネージド Microsoft AD パフォーマンスカウンター。

- 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 管理対象の Microsoft AD ディレクトリ固有の指標。例:

- 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のメトリクスを設定する方法については、 AWS セキュリティブログの「 AWS 使用率メトリックに基づいてマネージド 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。のメトリックスに関する一般的な情報については CloudWatch、『Amazon CloudWatch ユーザーガイド』の「Amazon CloudWatch メトリクスの使用」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 Web サイトの「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 マネージド Microsoft AD パフォーマンスカウンター

次の表は、 AWS Managed Microsoft AD CloudWatch の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の Amazon で使用できるすべてのパフォーマンスカウンターの一覧です。

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

メトリクスカテゴリ	メトリクス名
	Recursive Query Failure/sec
	TCP Query Received/sec
	Total Query Received/sec
	Total Response Sent/sec
	UDP Query Received/sec
LogicalDisk	Avg。Disk Queue Length
	% Free Space
メモリ	% Committed Bytes in Use
	Long-Term Average Standby Cache Lifetime (s)
ネットワークインターフェイス	Bytes Sent/sec
	Bytes Received/sec
	Current Bandwidth
NTDS	ATQ Estimated Queue Delay
	ATQ Request Latency
	DS Directory Reads/Sec
	DS Directory Searches/Sec
	DS Directory Writes/Sec
	LDAP Client Sessions
	LDAP Searches/sec
	LDAP Successful Binds/sec

メトリクスカテゴリ	メトリクス名
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

マルチリージョンレプリケーション

マルチリージョンレプリケーションを使用すると、 AWS Managed Microsoft AD ディレクトリデータを複数の に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、ネイティブの 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。

自動マルチリージョンレプリケーションは、 AWS Managed Microsoft AD が提供されているほとんどのリージョンで使用できます。

Important

マルチリージョンレプリケーションでは、次のオプトインリージョンでは利用できません。

- 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
- 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

オプトインリージョンとその有効化方法の詳細については、「 ガイド」の AWS リージョン「アカウントで使用できる を指定する」を参照してください。 AWS Account Management

利点

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して高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、迅速にデプロイでき、グローバル Active Directory インフラストラクチャを自己管理する手間が省けます。
- これにより、Windows と Linux の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。可用性の高い 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 Managed 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、および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

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強化してリージョン対応にします。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) とは表示されないので、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 Managed Microsoft AD は次の 2 種類のリージョンを使用して、グローバル機能またはリージョン機能をディレクトリ全体に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、「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。

マルチリージョンレプリケーションの仕組み

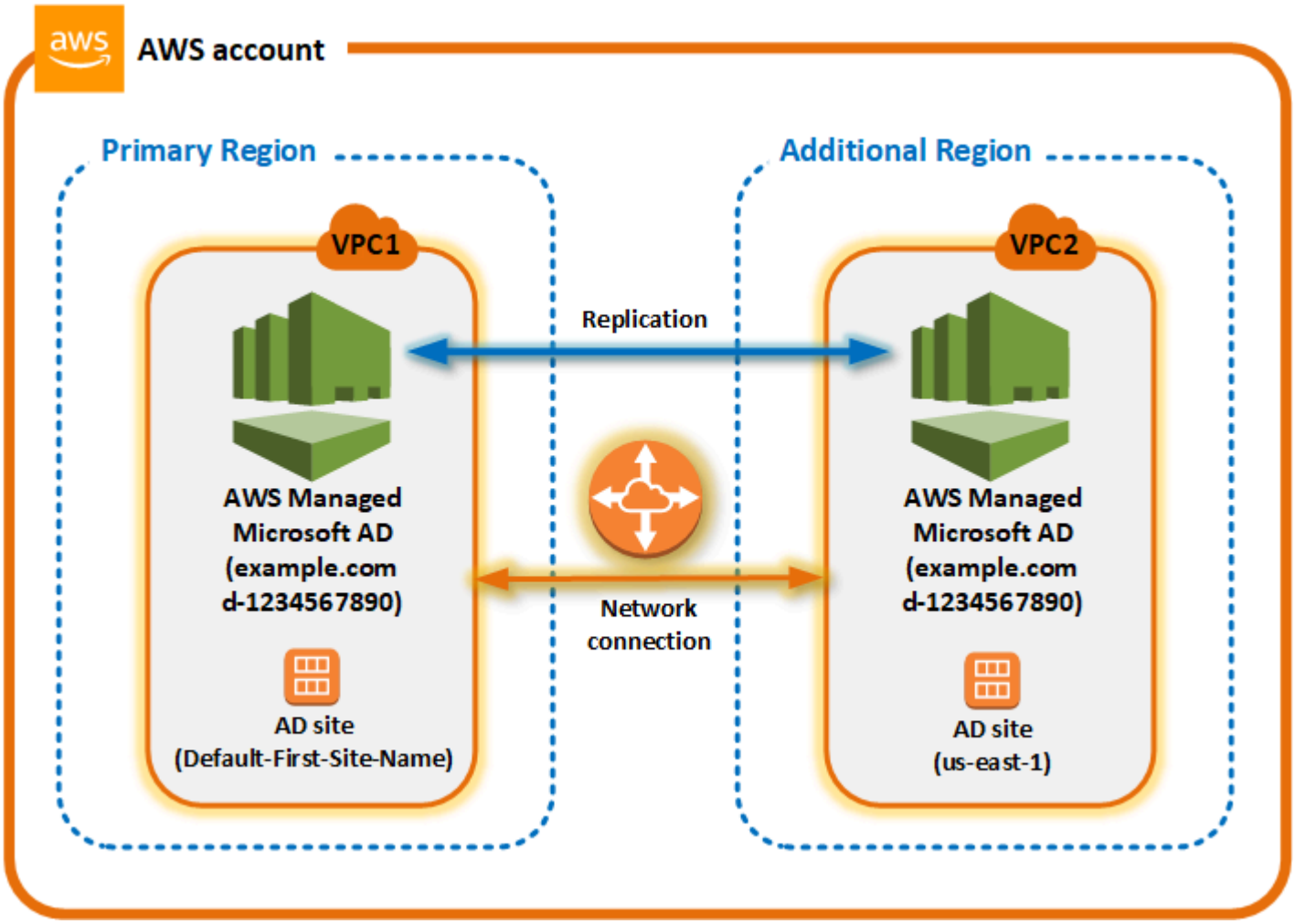
マルチリージョンレプリケーション機能を使用すると、 AWS Managed Microsoft AD は、グローバル Active Directory インフラストラクチャを管理するという、差別化されていない負荷の大きい作業を排除します。設定すると、ユーザー、グループ、グループポリシー、スキーマを含むすべてのカスタマーディレクトリデータが複数の AWS リージョンに AWS レプリケートされます。

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。
- 追加したリージョンが初めての場合、 AWS Managed 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 のサイト

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や AWS 、任意の AWS リージョンの Amazon RDS for SQL Server などの AWS サービスに 1 回サインインできます。これを行うには、 AWS Managed Microsoft AD との信頼がある場合、ユーザーは AWS Managed Microsoft AD またはオンプレミスの Active Directory から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
- FSx for Windows File Server
- Amazon RDS for SQL Server
- 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 Managed Microsoft AD はドメインコントローラーを復旧し、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。

レプリケートされたリージョンの追加

マルチリージョンレプリケーション 機能を使用してリージョンを追加すると、 AWS Managed 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 Managed 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、ディレクトリがすでにデプロイされているのと同じ 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 セットアップ、サブネットセットアップがあることを確認します。
- 既存のオンプレミスの Active Directory 認証情報を使用して の Active Directory 対応ワークロードにアクセスし、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、「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。

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、リージョンのステータスが Active と表示されます。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、「追加のドメインコントローラーの追加または削除」を参照してください。
- リージョンごとに他の AWS アカウントとディレクトリを共有します。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、「ディレクトリの共有」を参照してください。
- 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、「ログ転送の有効化」を参照してください。
- 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 SNS でディレクトリステータス通知を設定する」を参照してください。

レプリケートされたリージョンを削除する

AWS Managed 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。

ディレクトリの共有

AWS Managed Microsoft AD は、複数の AWS アカウント間でシームレスなディレクトリの共有ができるように、AWS Organizations と緊密に統合されています。同じ組織内で他の信頼済み AWS アカウントと単一のディレクトリを共有したり、組織外の他の AWS アカウントとディレクトリを共有したりできます。また、使用する AWS アカウントが現在組織に属していない場合にも、ディレクトリを共有することができます。

> **Note**
>
> AWS ではディレクトリの共有に追加料金が発生します。詳細については、AWS Directory Service ウェブサイトの「料金」ページを参照してください。

ディレクトリの共有によって、AWS Managed Microsoft AD では、複数のアカウントおよび VPC で Amazon EC2 と統合する際のコスト効率が高くなります。ディレクトリの共有は、AWS Managed Microsoft AD が提供されているすべての AWS リージョンで利用できます。

> **Note**
>
> AWS 中国 (寧夏) リージョンでは、AWS Systems Manager (SSM) を使用している場合にのみ、この機能を使用して Amazon EC2 インスタンスにシームレスに結合することができます。

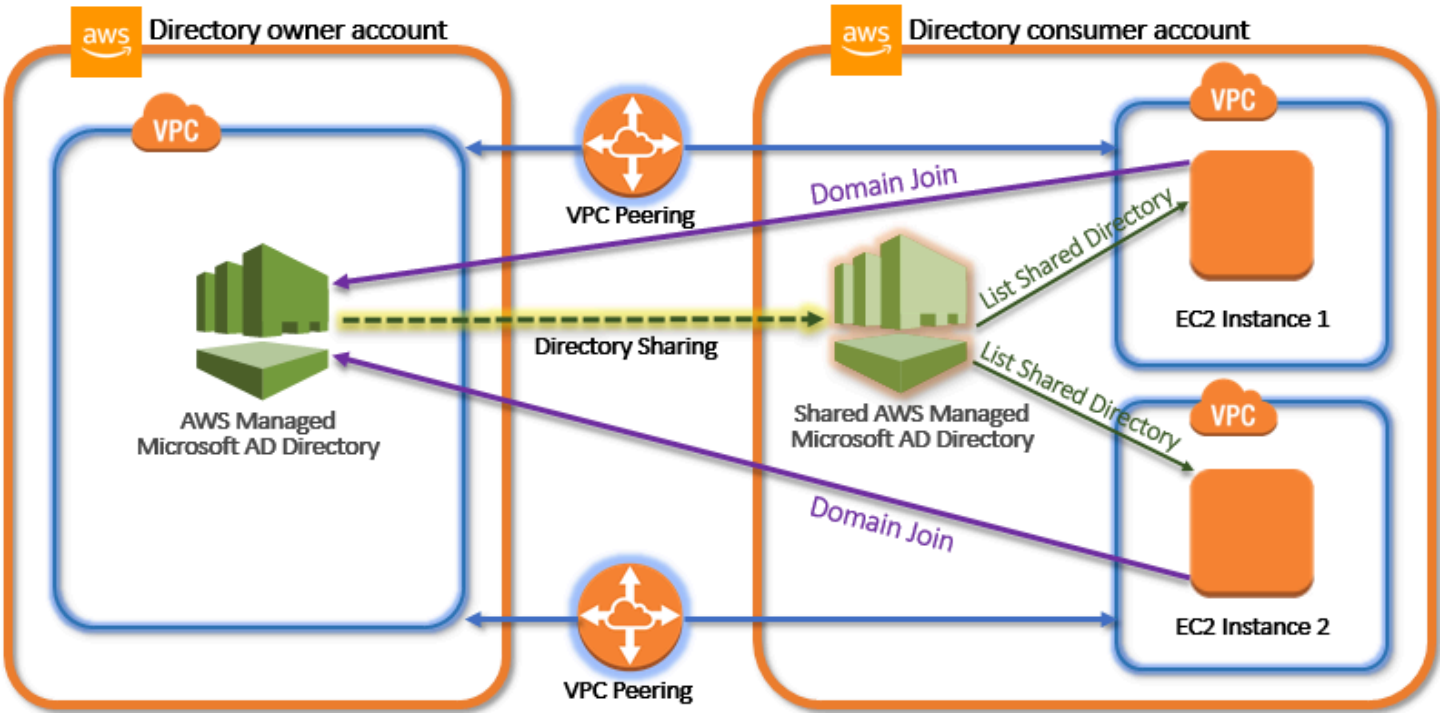
ディレクトリの共有に関する詳細と AWS Managed Microsoft AD ディレクトリが到達する範囲を AWS アカウント境界を超えて拡張する方法については、以下のトピックを参照してください。

トピック

- 主要なディレクトリ共有の概念
- チュートリアル: シームレスな EC2 ドメイン結合のための AWS Managed Microsoft AD ディレクトリの共有
- ディレクトリの共有解除

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

ディレクトリの所有者とは、共有ディレクトリ関係において、元のディレクトリを所有している AWS アカウント の持ち主です。このアカウントの管理者は、ディレクトリを共有する AWS アカウント を指定して、ディレクトリ共有の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る場合もあります。

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 は、次の 2 つのディレクトリ共有メソッドを用意しています。

- 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、このメソッドは [Share this directory with AWS アカウント inside your organization] (このディレクトリを組織内の AWS アカウント と共有) と表示されます。
- 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、AWS アカウント 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 は、VPC を接続するための多くのソリューション (VPC ピアリング、Transit Gateway、VPN など) をサポートしています。開始するには、「チュートリアル: シームレスな EC2 ドメイン結合のための AWS Managed Microsoft AD ディレクトリの共有」を参照してください。

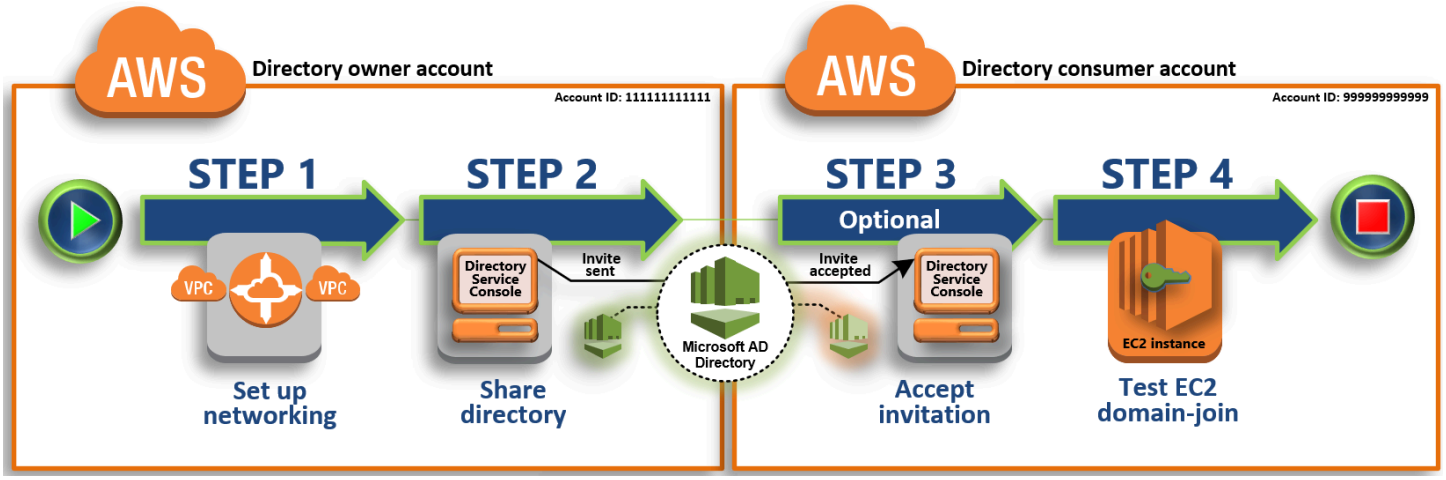
チュートリアル: シームレスな EC2 ドメイン結合のための AWS Managed Microsoft AD ディレクトリの共有

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 間で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け入れる - オプション

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ときに、 AWS Directory Service コンソールを開き、ディレクトリ共有の招待を承諾します。

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

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 アカウント 用に 2 つの新しい を作成します。を作成すると AWS アカウント、各アカウントに専用の Virtual Private Cloud (VPC) が自動的に作成されます。各アカウントの 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。
- このステップの手順に従い、これら 2 つのアカウントにある VPC 間に VPC ピアリング接続を作成します。

> **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、ディレクトリのコンシューマーの VPC とディレクトリの所有者の VPC 間に配置されます。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 (https://console.aws.amazon.com/vpc/) を開きます。ディレクトリの所有者アカウントに、管理者の認証情報を使用するユーザーとしてサインインしていることを確認します。
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 (Accepter)] (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。

両方の VPC は同じリージョンにあるため、VPC ピアリングのリクエストを送信したディレクトリの所有者アカウントの管理者は、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のリクエストを承諾することもできます。

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 (https://console.aws.amazon.com/vpc/) を開きます。
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 Managed Microsoft AD AWS 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. [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、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 組織の で、ディレクトリ AWS アカウント を共有する を選択し、 の追加 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け入れる - オプション

ステップ 3: 共有ディレクトリの招待を受け入れる - オプション

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用します。

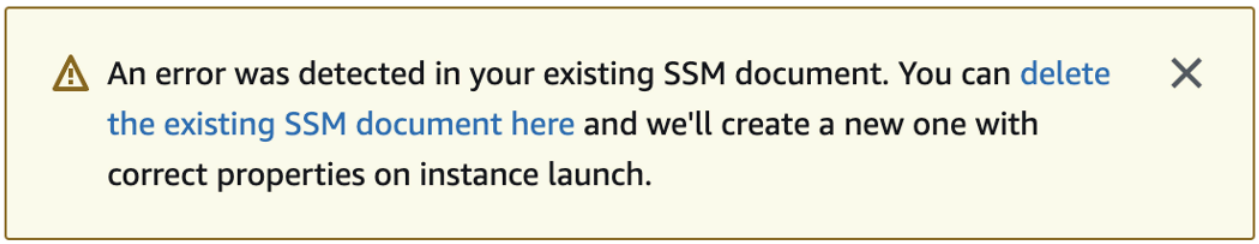
1. にサインイン AWS Management Console し、https://console.aws.amazon.com/ec2/ で Amazon EC2 コンソールを開きます。
2. ナビゲーションバーで、既存のディレクトリ AWS リージョン と同じ を選択します。
3. [EC2 ダッシュボード] の [インスタンスを起動する] セクションで、[インスタンスを起動する] を選択します。
4. [インスタンスを起動する] ページの [名前とタグ] セクションで、Windows EC2 インスタンスに使用する名前を入力します。
5. (オプション) [補足タグを追加] で、タグとキーの値のペアを 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、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。
    a. 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。
    b. 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。
    c. 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。
    d. [キーペアの作成] を選択します。
    e. 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。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>

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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
- 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持つ 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。AmazonSSMManagedInstanceCore がアAmazonSSMDirectoryServiceAccessタッチされた AWS 管理ポリシーを持つ 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 プロファイルリンクの作成 を選択し、次の操作を行います。

    1. [ロールの作成] を選択します。
    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] を選択します。
    4. アクセス許可の追加 で、ポリシーのリストで 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] をクリックします。

    > **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] を選択します。
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. [Launch instance (インスタンスの起動)] を選択します。

方法 2: を使用してドメイン結合をテストする AWS Systems Manager

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用します。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

- をセットアップします 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、「実行中の EC2 Windows インスタンス AWS Systems Manager を AWS Directory Service ドメインに参加させるにはどうすればよいですか？」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 、および DNS IP アドレスを見つけるには、 AWS Directory Service コンソールに戻り、自分と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 には、 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 には、 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、 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) AWS 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ときは、以下の手順に従います。

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. [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、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] (スケールリングと共有) 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。

その他のリソース

- 「ユースケース: AWS アカウント間でディレクトリを共有して、Amazon EC2 インスタンスを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)

Amazon EC2 インスタンスを AWS Managed Microsoft AD に結合する Active Directory

インスタンスの起動時に、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 にシームレスに結合する 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。

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、適切なリージョンと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 でディレクトリ管理インスタンスを起動する Active Directory
- Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD にシームレスに結合する Active Directory
- Amazon EC2 Windowsインスタンスを AWS Managed Microsoft AD に手動で結合する Active Directory
- 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 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 ManaggedMicrosoft AD Active Directoryに手動で結合します
- Amazon EC2 Mac インスタンスを AWS Managed Microsoft AD Active Directory に手動で結合する
- AWS Managed Microsoft AD のディレクトリ結合権限を委任する
- DHCP オプションセットを作成または変更する

AWS Managed Microsoft AD でディレクトリ管理インスタンスを起動する Active Directory

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 で起動します。これを行うには、オートメーションコンソールで Automation AWS-CreateDSManagementInstance AWS Systems Manager を直接実行します。

前提条件

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、アカウントで次の権限が有効になっている必要があります。

- 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

でディレクトリ管理 EC2 インスタンスを起動するには 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. ディレクトリ管理 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. Actions ドロップダウンリストで、Launch directory administration EC2 instance 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. （オプション) 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) AWS CLI コマンドを表示 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 で使用する例が表示されます。
7. [送信] を選択します。
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には

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 にシームレスに結合する Active Directory

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: シームレスな EC2 ドメイン結合のための AWS Managed Microsoft AD ディレクトリの共有。Amazon EC2 の詳細については、「Amazon EC2 とは」を参照してください。

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、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。

   a. 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。

b. 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。

c. 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。

d. [キーペアの作成] を選択します。

e. 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。

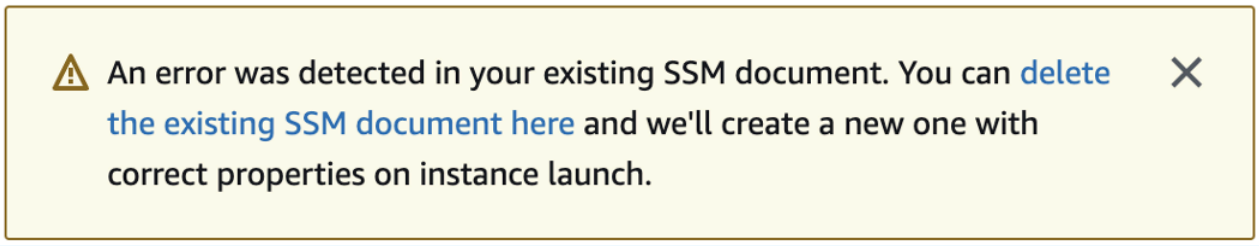
11. [自動割り当てパブリック IP] で、[有効化] を選択します。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>
>
> 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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
> - 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持つ 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。AmazonSSMManagedInstanceCore がアAmazonSSMDirectoryServiceAccessタッチされた AWS 管理ポリシーを持つ 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 プロファイルリンクの作成 を選択し、次の操作を行います。

    1. [ロールの作成] を選択します。
    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] を選択します。
    4. アクセス許可の追加 で、ポリシーのリストで 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] をクリックします。

    > **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。

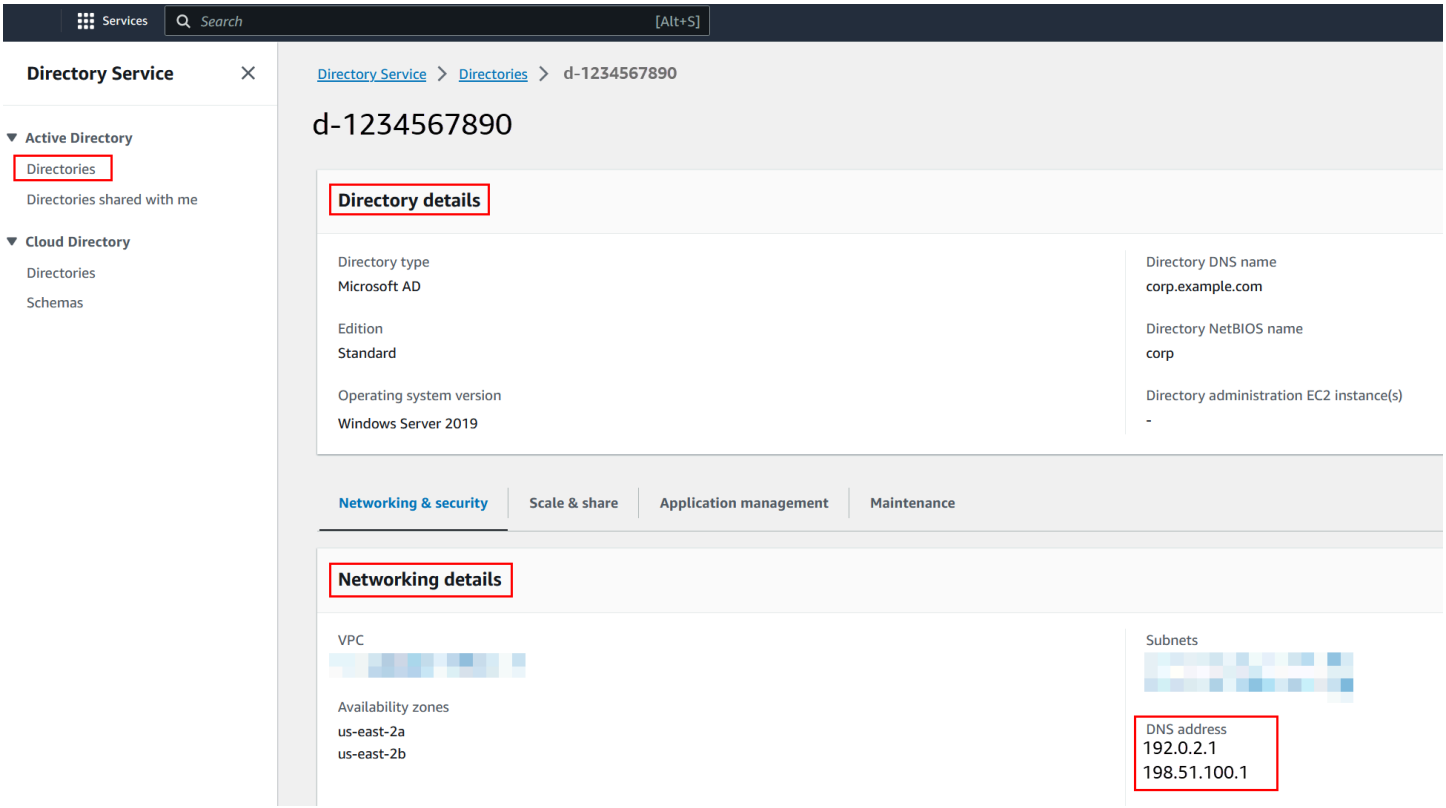
5. [名前、確認、作成] ページで、[ロール名] を入力します。EC2 インスタンスにアタッチするには、このロール名が必要です。
6. (オプション) IAM インスタンスプロファイルの説明を [説明] フィールドに入力できます。
7. [ロールの作成] を選択します。
8. [インスタンスを起動する] ページに戻り、[IAM インスタンスプロファイル] の横にある更新アイコンを選択します。新しい IAM インスタンスプロファイルが [IAM インスタンスプロファイル] ドロップダウンリストに表示されるはずです。新しいプロファイルを選択し、残りの設定はデフォルト値のままにします。

16. [Launch instance (インスタンスの起動)] を選択します。

Amazon EC2 Windowsインスタンスを AWS Managed Microsoft AD に手動で結合する Active Directory

既存の Amazon EC2 Windowsインスタンスを AWS Managed Microsoft AD に手動で結合するにはActive Directory、 で指定され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Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD にシームレスに結合する Active Directory。

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。



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。

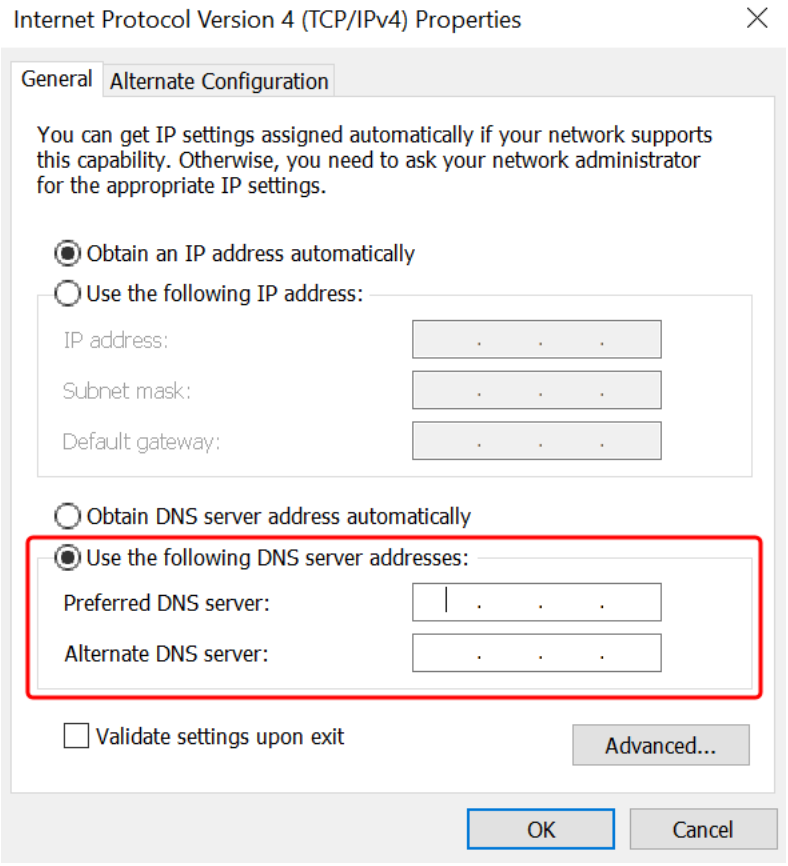
   a. ネットワーク接続を開きます。

   > **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. 次の DNS サーバーアドレスを使用する を選択し、優先 DNS サーバーと代替 DNS サーバーのアドレスを AWS Managed Microsoft AD が提供する 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。

> **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. 「 のメンバー」フィールドに「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。ユーザー名は管理者 になります。例えば、**corp.example.com\admin**、**corp\admin** などです。

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、「管理対象の Microsoft AD AWS 用アクティブディレクトリ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 解決を と統合 Amazon Route 53 Resolver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 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。複数の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 AWS 、オプションでディレクトリ共有 を有効にすることができます。

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 より前のディストリビューションでは、シームレスなドメイン結合機能はサポートされていません。

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ンストレーションについては、次の YouTube 動画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

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 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参加させるために必要な最小限の権限を持つアカウントを委任するには、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、管理対象の Microsoft AD AWS 用アクティブディレクトリ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

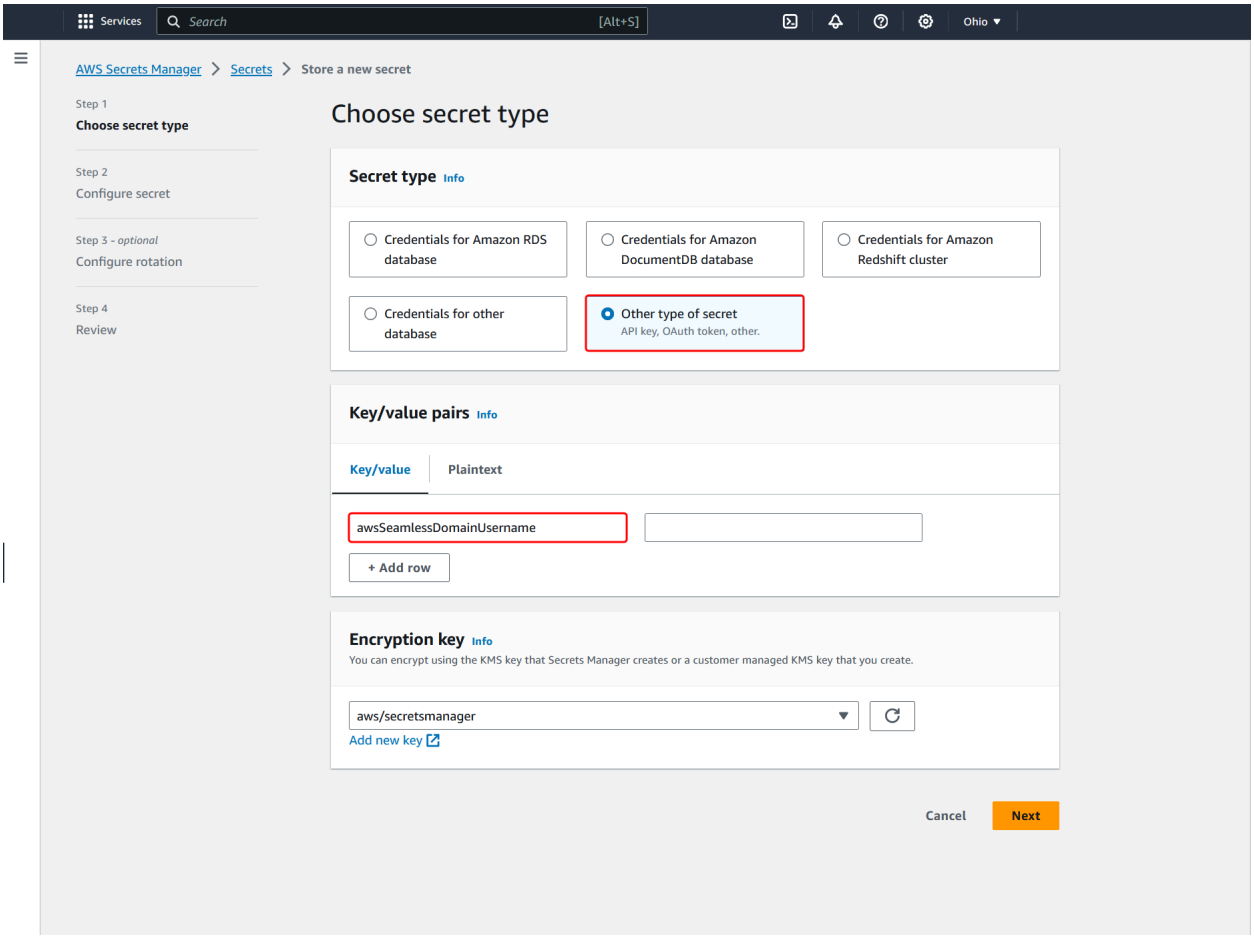
AWS Secrets Manager を使用してドメインサービスアカウントを保存できます。

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 になりますawsSeamlessDomain。

> **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。



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。

> **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/secretsmanagerが作成する AWS マネージドキーを使用して、シークレットを無料で暗号化できます。独自の KMS キーを作成してシークレットを暗号化すると、 は現在の AWS KMS レートで AWS 課金します。詳細については、「AWS Key Management Service の料金」を参照してください。

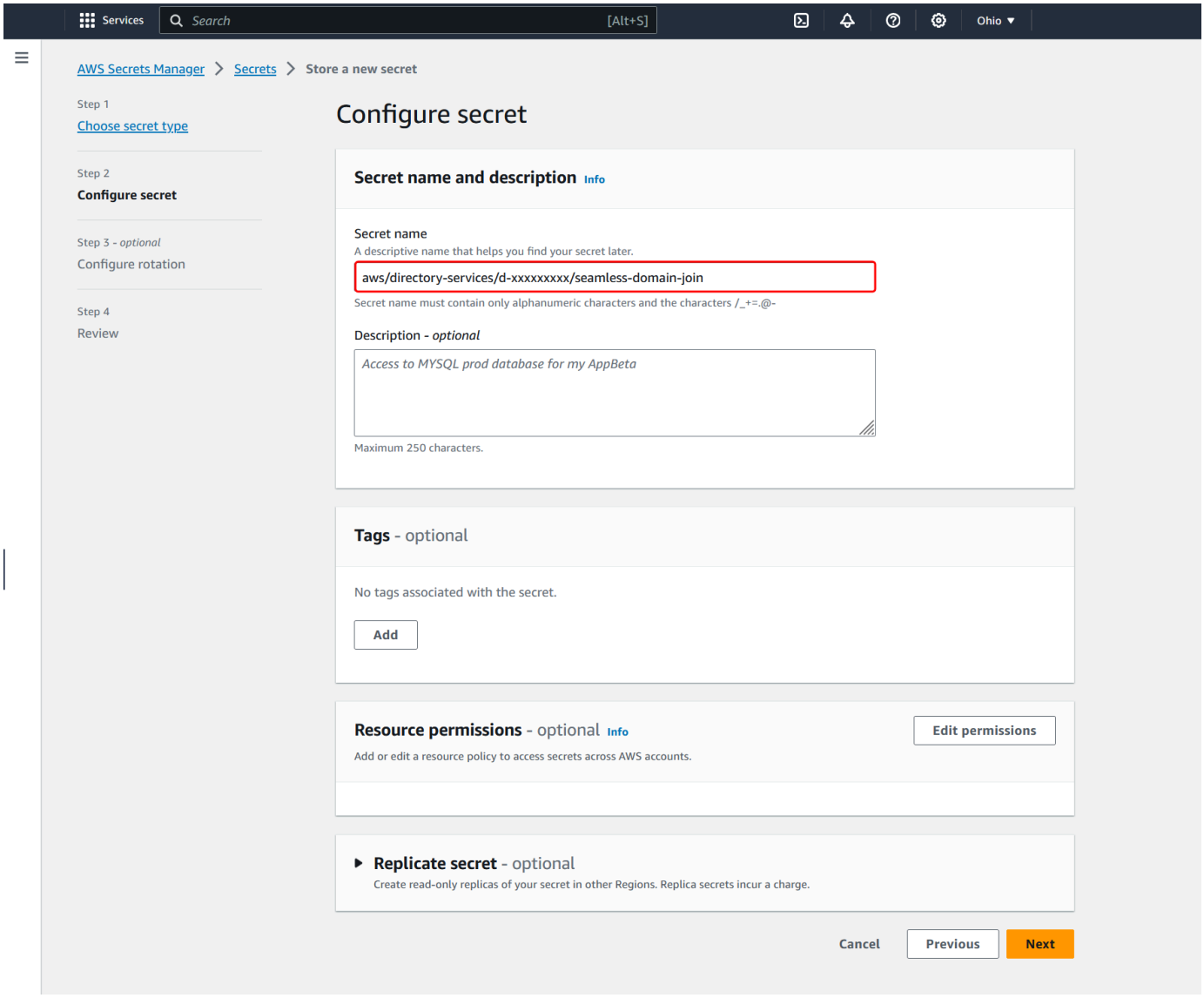
v. [次へ] をクリックします。

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-xxxxxxxxx/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-xxxxxxxxx*/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。



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 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。

  ステップ 5 では、「 AWS Secrets Manager ユーザーガイド」の「Microsoft Active Directory の認証情報」のローテーションテンプレートを使用します。

  ヘルプについては、「 ユーザーガイド」の AWS Secrets Manager 「ローテーションのトラブルシューティングAWS Secrets Manager 」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

以下の前提条件のステップを使用して、Secrets Manager のシームレスなドメイン結合シークレット (以前に作成したもの) 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。

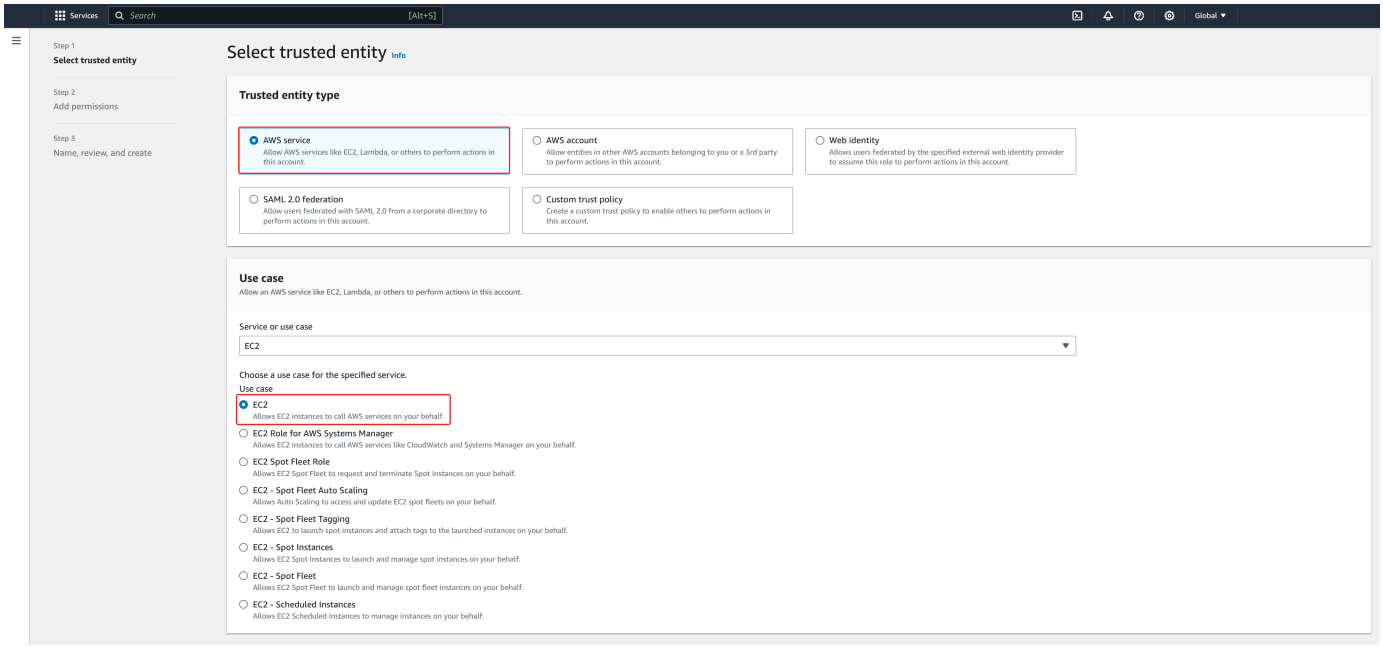
> **Note**
>
> シークレットごとに 1 つのポリシーを作成することをお勧めします。そうすることで、インスタンスが適切なシークレットにのみアクセスできるようになり、インスタンスが侵害された場合の影響を最小限に抑えることができます。

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。



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] を選択します。

Linux インスタンスをシームレスに結合する

すべての前提条件タスクを設定したので、次の手順に従い EC2 Linux インスタンスをシームレスに結合できます。

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. (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. 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ときにaws:domainJoinプラグインを使用します。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。

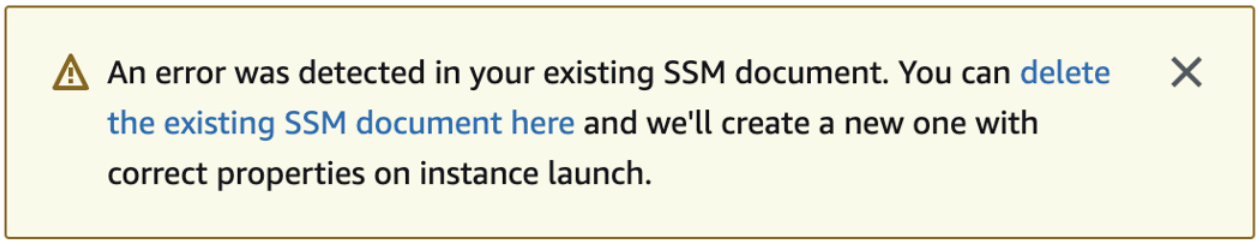
11. [自動割り当てパブリック IP] で、[有効化] を選択します。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>
>
> 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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
> - 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持つ 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 で、前提条件セクション「ステップ 2: LinuxEC2DomainJoin role を作成する」で以前に作成した IAM ロールを選択します。
16. [Launch instance (インスタンスの起動)] 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 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。

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 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構いません。

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 -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

ドメイン結合権限を持つ *example.com* ドメイン内のアカウントの 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. 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AccountName の sAM。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/sssd.service; enabled; vendor
 preset: disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
           ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
           ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11. 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。

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
```

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 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構いません。

```
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* ドメイン内のアカウントの 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/sssd/sssd.conf に追加する必要があります。

テキストエディタで /etc/sssd/sssd.conf ファイルを開きます。

```
sudo vi /etc/sssd/sssd.conf
```

この操作を行った後、sssd.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=admins,ou=Testou,dc=example,dc=com)
```

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
```

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/sssd/sssd.conf に追加する必要があります。

1. テキストエディタで /etc/sssd/sssd.conf ファイルを開きます。

```
sudo vi /etc/sssd/sssd.conf
```

2. この操作を行った後、sssd.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=admins,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、UNIX/Linux ユーザー識別子 (UID) とグループ識別子 (GID) と Windows および Active Directoryセキュリティ識別子 (SID) のアイデンティティ間の統一されたエクスペリエンスを維持するために、2 つの方法で実行できます。

1. 一元化
2. 分散型

> **Note**
>
> の一元化されたユーザー ID 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または POSIX Active Directory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、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)

から 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Active Directory、sssd.conf ファイル`ldap_id_mapping = False`で を設定します。この値を設定する前に、 のユーザーとグループに UID、UID 番号、および GID 番号を追加していることを確認しますActive Directory。

分散型ユーザー ID マッピング

Active Directory に POSIX 拡張機能がない場合、または ID マッピングを一元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。

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 ManaggedMicrosoft AD Active Directoryに手動で結合します

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. 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. 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 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AccountName の sAM。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「静的 DNS サーバーをプライベート Amazon EC2 インスタン

スに割り当てる方法」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
```

```
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 Active Directory に手動で結合する

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 専有ホストが必要です。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 インスタンスの起動」を参照してください。 Amazon EC2
- 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、「DHCP オプションセットを作成または変更する」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。 Amazon EC2

Linux インスタンスを手動で結合するには

1. 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
   ```

2. 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
```

3. 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。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」の手順に従って、オペレーティングシステムとソフトウェアを更新できます。

4. 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、組織単位は、必ず AWS Managed Microsoft AD Active Directory の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。ハイフンを使用すると、 AWS Managed Microsoft AD Active Directory へのバインドが妨げられる可能性があります。

```
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を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"
```

5. 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
```

6. 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 インスタンスを AWS Managed Microsoft AD Active Directory に正常に接続しました。 AWS Managed Microsoft AD Active Directory の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。

ドメインユーザーで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) に接続する」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。

AWS Directory Service for Microsoft Active Directory では、管理者グループとAWS 委任された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。

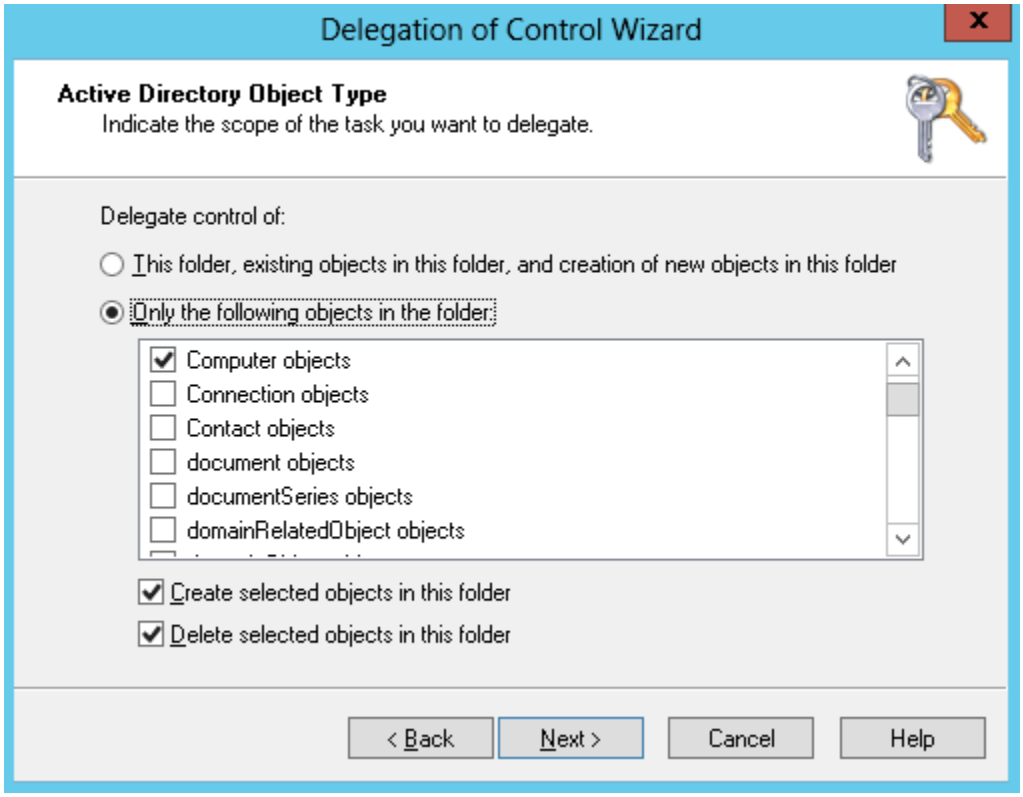
AWS Managed Microsoft AD の参加権限を委任するには

1. [Active Directory 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に NetBIOS 名が表示されている組織単位 (OU) を選択し、[Users] (ユーザー) OU を選択します。

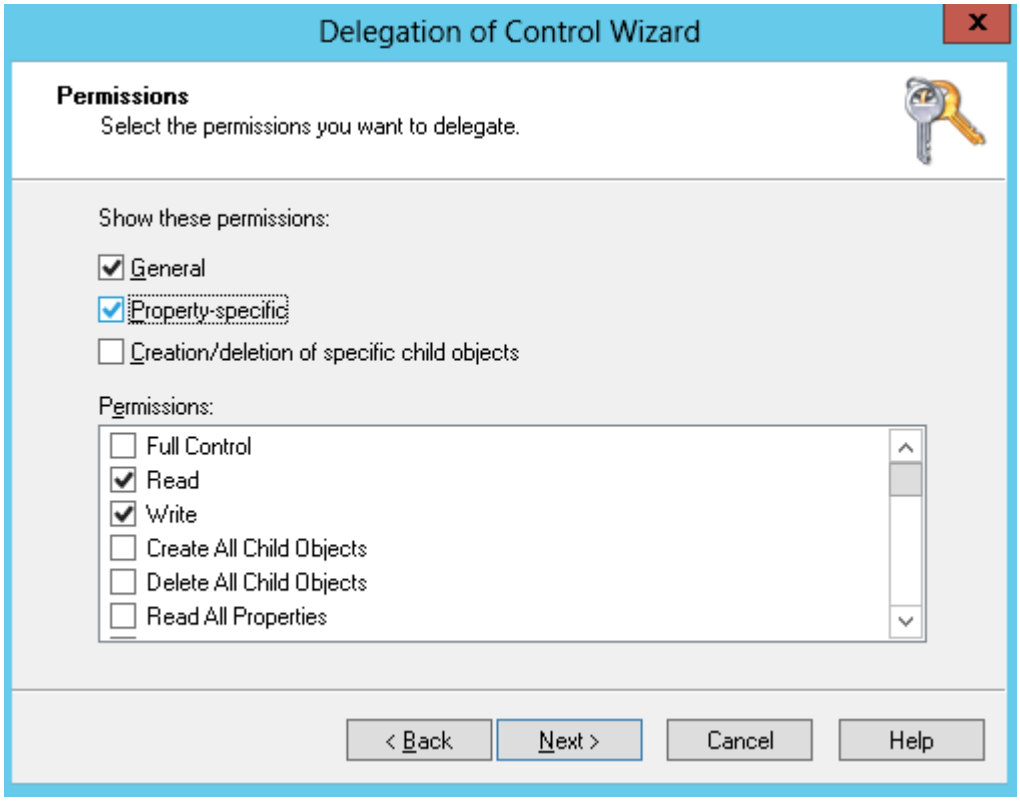
> **Important**
>
> AWS Directory Service for Microsoft Active Directory を起動すると、 はディレクトリのすべてのオブジェクトを含む組織単位 (OU) AWS を作成します。この OU はドメインルートにあります。OU にはディレクトリを作成する際に入力した NetBIOS 名がありま

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。



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。このユーザーは、NetBIOS 名の下の [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。

DHCP オプションセットを作成または変更する

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

   が提供するディレクトリの AWS 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、アクション、VPC 設定の編集 を選択します。
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、以下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 でユーザーとグループを管理する

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。

ユーザーとグループを AWS Directory Service ディレクトリに作成するには、AWS Directory Service ディレクトリに結合されたいずれかのインスタンスを (オンプレミスまたは EC2 から) 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している必要があります。さらに、Active Directory のツールを EC2 インスタンスにインストールし、[Active Directory Users and Computers] (Active Directory ユーザーとコンピュータ) スナップインを使用してユーザーとグループを EC2 インスタンスに追加できるようにする必要があります。

AWS Directory Service 管理コンソールから、プリインストールされた Active Directory 管理ツールを使用して、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 でディレクトリ管理インスタンスを起動する Active Directory」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 AWS インスタンスをデプロイしてマネージド Microsoft AD アクティブディレクトリを管理する」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

- 管理対象の Microsoft AD AWS 用アクティブディレクトリ管理ツールのインストール

- ユーザーの作成
- ユーザーの削除
- ユーザーパスワードをリセットする
- グループを作成する
- ユーザーをグループに追加する

管理対象の Microsoft AD AWS 用アクティブディレクトリ管理ツールのインストール

Amazon EC2 Windows Server Active Directory インスタンスからを管理するには、Active Directory Domain Services and Active Directory Lightweight Directory Services Toolsインスタンスに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.

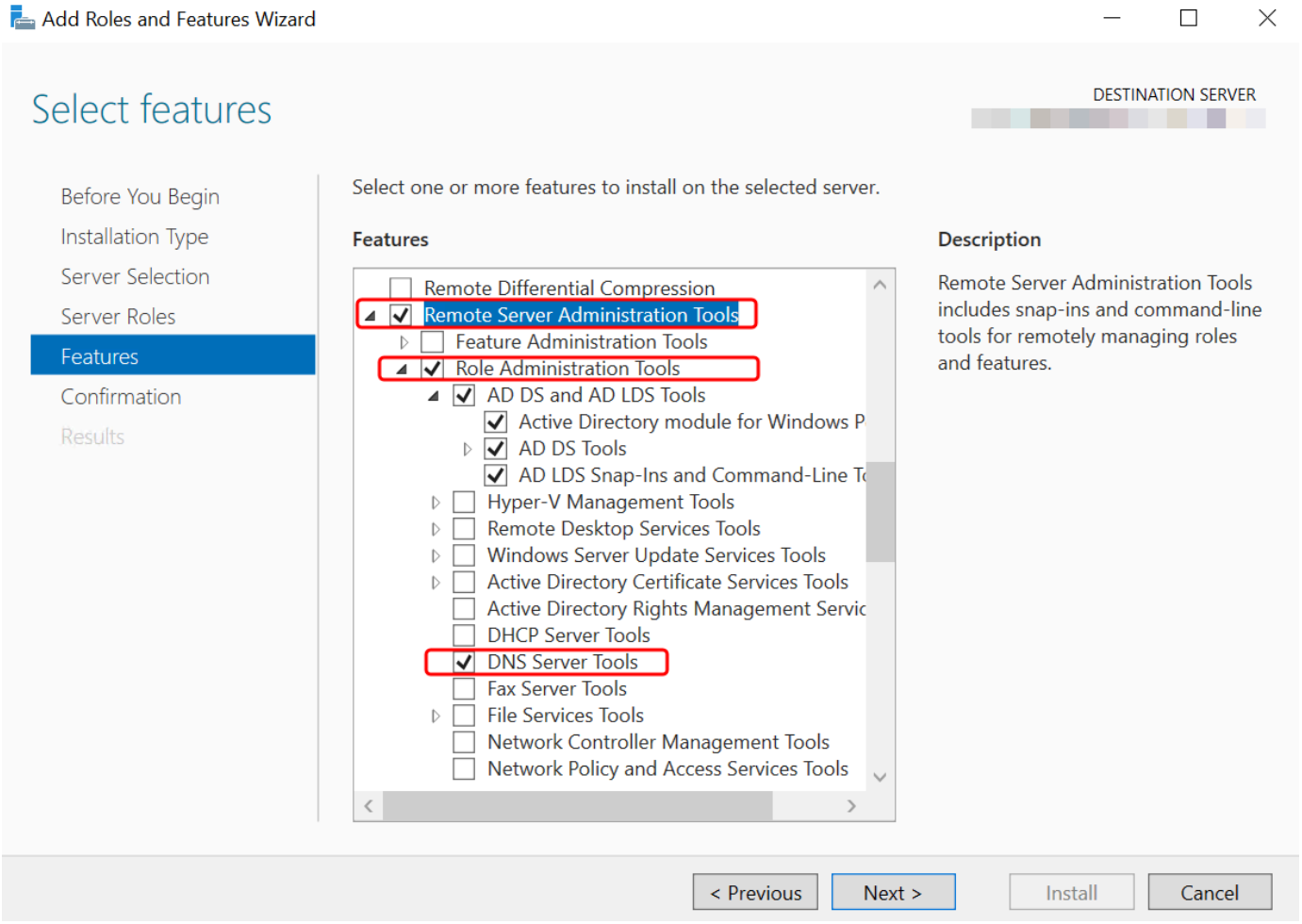
1. AWS マネージド型Microsoft AD を作成しますActive Directory。詳細については、「AWS Managed Microsoft AD を作成する」を参照してください。
2. EC2 Windows Server インスタンスを起動し、 AWS マネージド Microsoft AD アクティブディレクトリに参加させます。EC2 インスタンスでユーザーとグループを作成するには、以下のポリシーが必要です **`AmazonSSMDirectoryServiceAccess`** と **`AWSSSMManagedInstanceCore`**。詳細については、「AWS Managed Microsoft AD でディレクトリ管理インスタンスを起動する Active Directory」および「Amazon EC2 Windows インスタンスを AWS Managed Microsoft AD にシームレスに結合する 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 管理対象の Microsoft AD の作成時に作成されました。AWS Managed Microsoft 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\admin`**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

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 (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。ユーザー名には、***NetBIOS-Name*\admin**または**の形式を使用できます*DNS-Name*\admin**。たとえば、AWS Managed Microsoft AD を作成する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 と AD LDS ツールを選択すると、AD DS ツール、AD LDS Active Directoryスナップインとコマンドラインツールのモジュールが選択されます。Windows PowerShell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。

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代替方法

- Active Directory 管理ツールをインストールする方法は他にもいくつかあります。
  - オプションとして、を使用してActive Directory管理ツールをインストールすることもできますWindows PowerShell。たとえば、Active Directory PowerShell リモート管理ツールはを使用するプロンプトからインストールできます`Install-WindowsFeature RSAT-ADDS`。詳細については、Microsoft の Web WindowsFeature サイトの「インストール-」を参照してください。
  - に記載されている手順に従って、Active Directory ドメインサービスと Active Directory ライトウェイトディレクトリサービスツールがすで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AWS Managed Microsoft AD でディレクトリ管理インスタンスを起動する Active Directory。 AWS Management Console

ユーザーの作成

AWS Managed Microsoft AD ディレクトリに結合された 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。

ユーザーを作成するには、以下のいずれかの方法を使用できます。

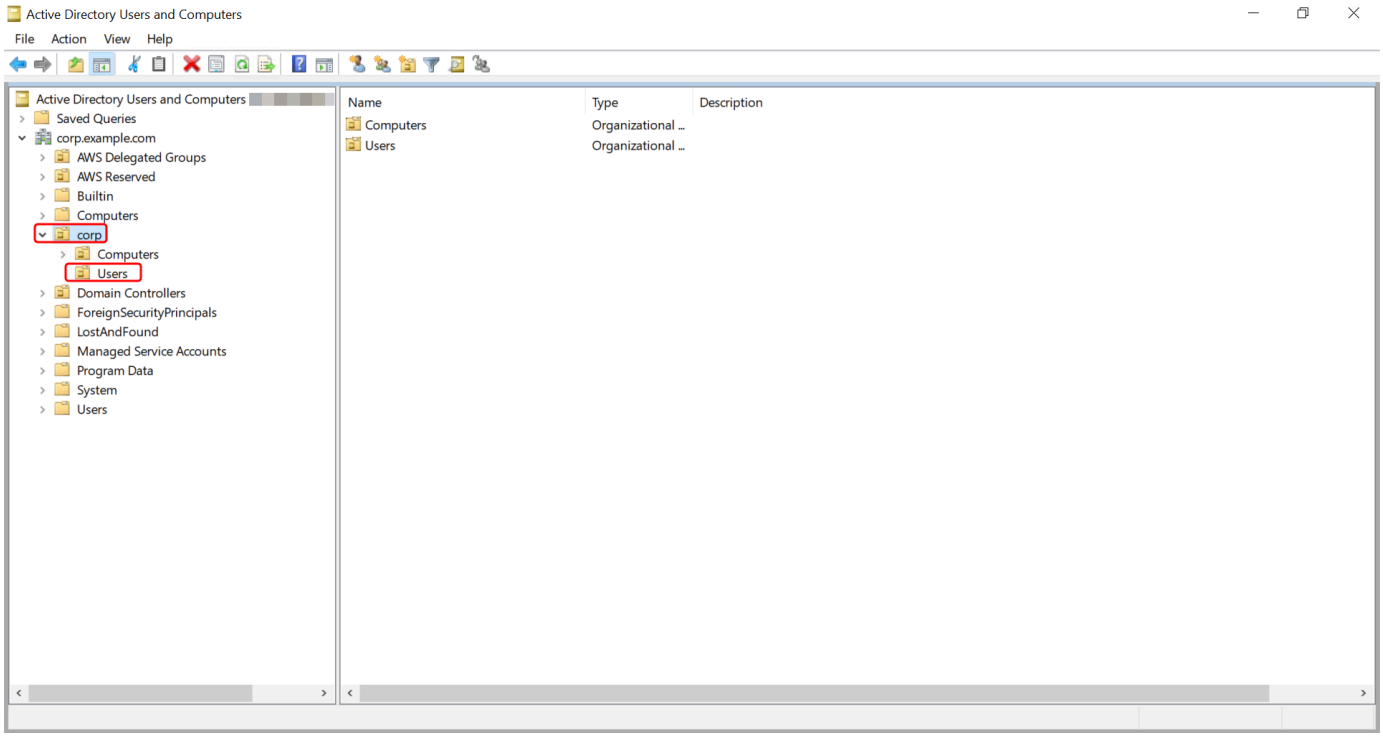
- Active Directory管理ツール
- Windows PowerShell

Active Directory管理ツールでユーザーを作成する

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 OU の下にある、ユーザーを保存する OU (例:**corp\Users**) 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 Active Directory で作成される内容。



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。

でユーザーを作成します。Windows PowerShell

1. Active DirectoryActive Directoryドメインに管理者として参加しているインスタンスConnect。
2. Windows PowerShell を開きます。
3. **`jane.doe`**ユーザー名を、作成するユーザーのユーザー名に置き換えて、次のコマンドを入力します。Windows PowerShell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について詳しくは、Microsoftドキュメントを参照してください。New-ADUser コマンドについて詳しくは、ドキュメントを参照してください。Microsoft

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

ユーザーの削除

次の手順を使用して、 AWS 管理対象の Microsoft AD に参加しているユーザーを削除しますActive Directory。

ユーザーを削除するには、以下のいずれかの方法を使用できます。

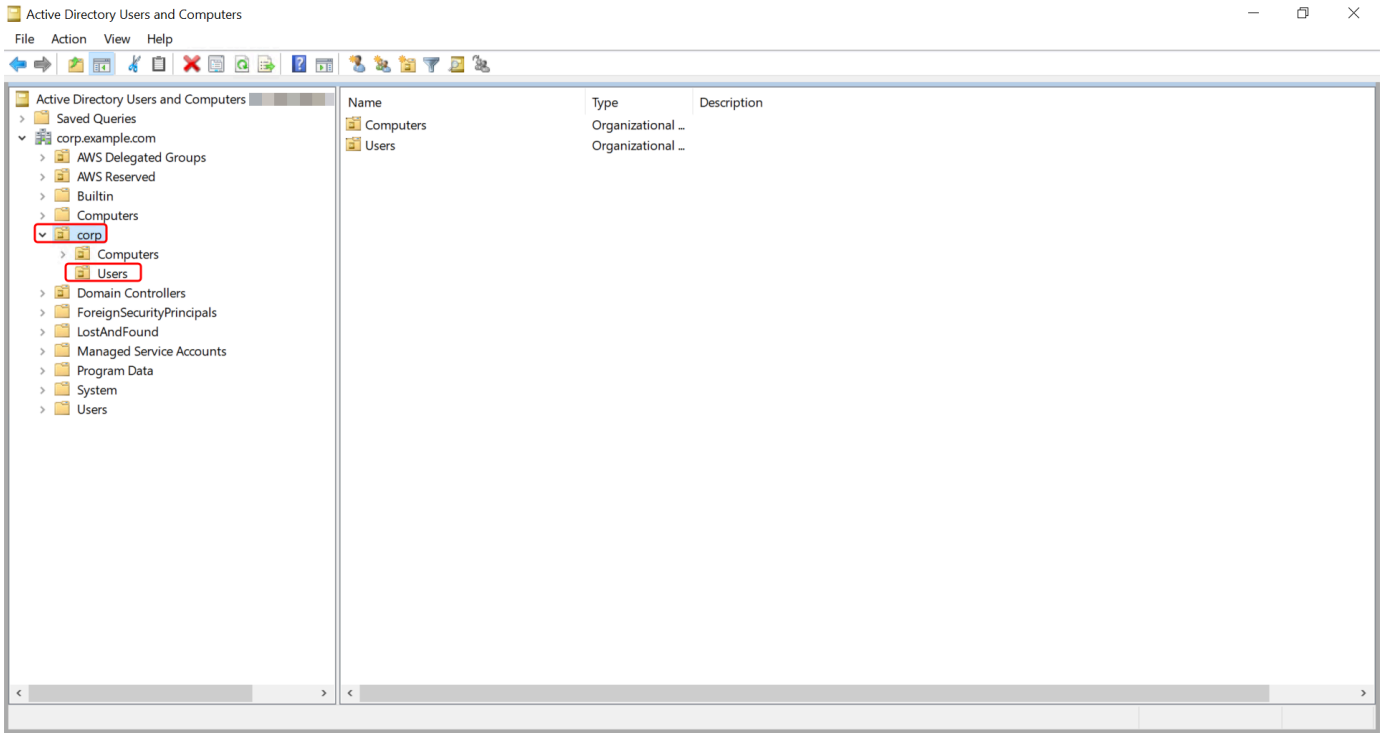
- Active Directory管理ツール
- Windows PowerShell

Active Directory管理ツールでユーザーを削除する

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、削除するユーザーを含む OU (例:**corp\Users**) を選択します。



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。

内のユーザーを削除します。Windows PowerShell

1. Active DirectoryActive Directoryドメインに管理者として参加しているインスタンスConnect。
2. Windows PowerShell を開きます。
3. **jane.doe**ユーザー名を削除するユーザーのユーザー名に置き換えて、次のコマンドを入力します。Remove-ADUser コマンドの詳細については、ドキュメントを参照してください。Microsoft

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

AD ごみ箱に関する考慮事項

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、「Ask the Directory Services Microsoft Team ブログ」の「AD のごみ箱:概要、実装、ベストプラクティス、トラブルシューティング」を参照してください。

ユーザーパスワードをリセットする

ユーザーは、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。Active DirectoryActive Directory管理者を含むユーザの最善を尽くしても、パスワードを忘れてしまうことがあります。このような場合は、 AWS Managed Microsoft AD AWS Directory Service にユーザーがいる場合は、そのユーザーのパスワードを簡単にリセットできます。

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ご参照ください。

以下の例外を除いて、内のすべてのユーザーのパスワードをリセットできます。Active Directory

- の作成時に使用した NetBIOS 名に基づいて、組織単位 (OU) 内のすべてのユーザのパスワードをリセットできます。Active Directoryたとえば、手順に従って 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。AWS Managed Microsoft AD を作成する
- の作成時に使用した NetBIOS 名に基づく OU 外のユーザのパスワードはリセットできません。Active Directoryたとえば、AWS 予約済み OU のユーザーのパスワードはリセットできません。 AWS マネージド 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 Active Directory で作成される内容。

AWS Managed Microsoft AD でパスワードをリセットしたときにパスワードポリシーがどのように適用されるかについての詳細は、を参照してくださいパスワードポリシーの適用方法。

以下の方法のいずれかを使用してユーザーパスワードをリセットできます。

- AWS Management Console
- AWS CLI
- Windows PowerShell

でユーザーパスワードをリセットします。 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、[ディレクトリ] を選択し、一覧からユーザーパスワードをリセットする場所を選択します。Active Directory
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。

でユーザーパスワードをリセットします。 AWS CLI

1. をインストールするには AWS CLI、「の最新バージョンのインストールまたは更新」を参照してください AWS CLI。
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**、**P@ssw0rd**Active Directory パスワードをディレクトリ ID と必要な認証情報に置き換えます。詳細についてはreset-user-password、『AWS CLI コマンドリファレンス』の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"
```

でユーザーパスワードをリセットします。Windows PowerShell

1. Active DirectoryActive Directoryドメインに管理者として参加しているインスタンスConnect。
2. Windows PowerShell を開きます。
3. ユーザー名**jane.doe**、ディレクトリ ID、**P@ssw0rd**Active Directoryパスワードをディレクトリ ID と必要な認証情報に置き換えて、次のコマンドを入力します。詳細については、「UserPassword Reset-DS 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"
```

グループを作成する

Managed Microsoft AD ディレクトリに結合された 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。

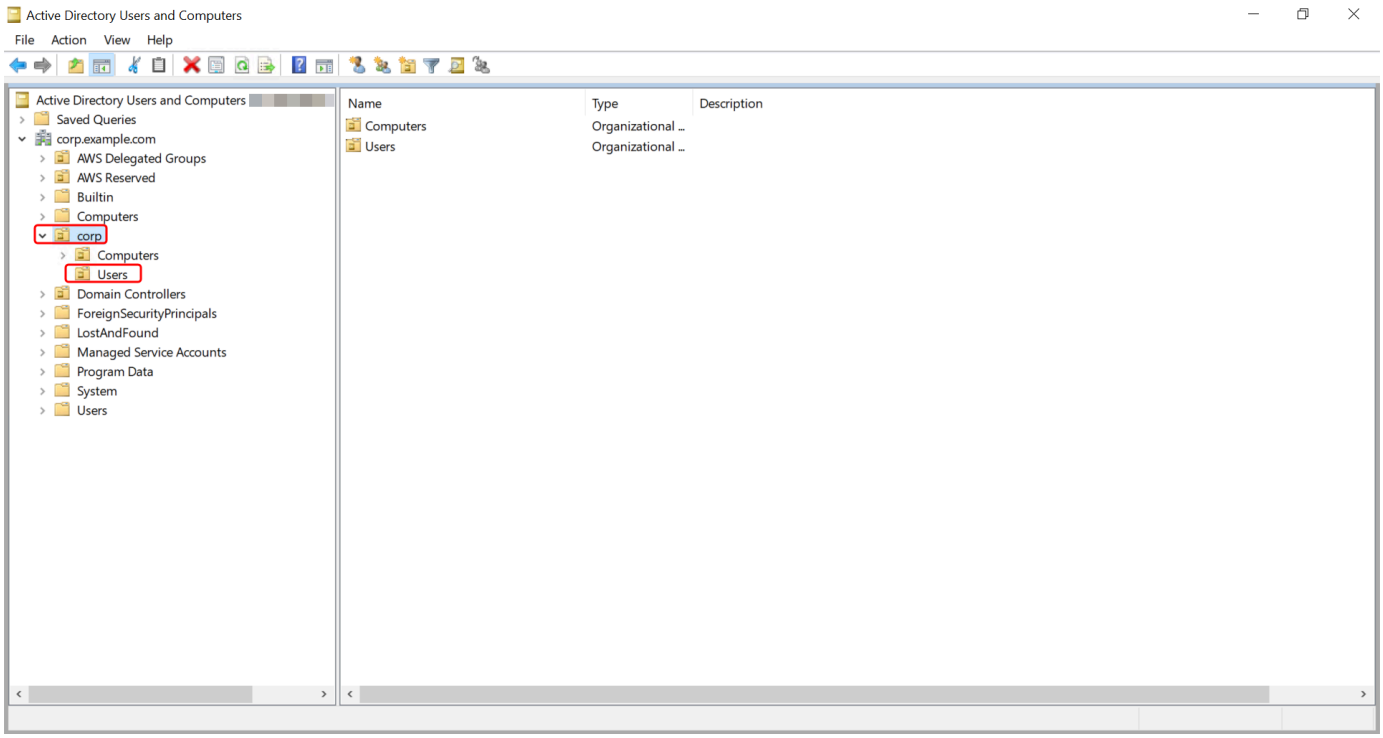
Windows PowerShell コマンドを使用してグループを作成することもできます。詳細については、Windows Server 2022 PowerShell ドキュメントの「New-ADGroup」を参照してください。

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 Active Directory で作成される内容。



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。

ユーザーをグループに追加する

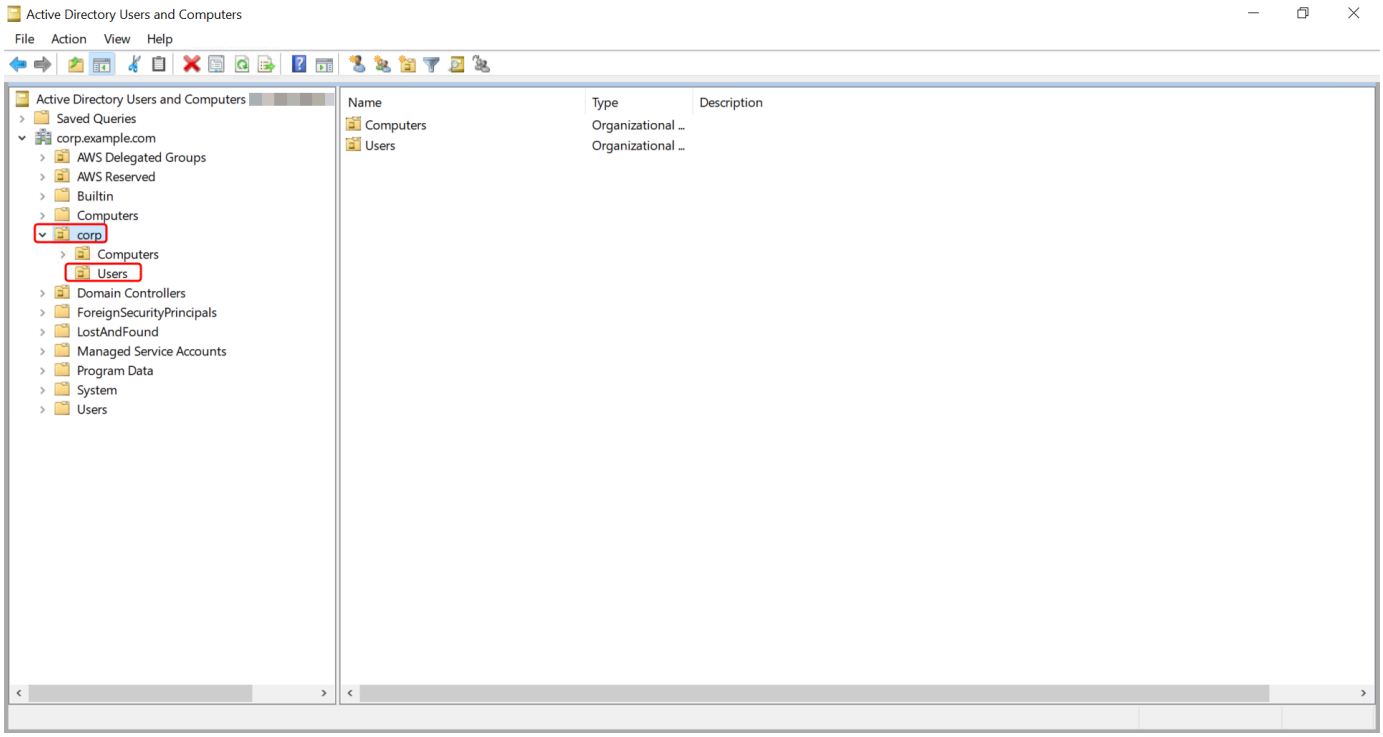
AWS Managed Microsoft AD ディレクトリに結合された EC2 インスタンスを使用するセキュリティグループにユーザーを追加するには、次の手順に従います。

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。

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との信頼関係を設定する方法について説明します。

トピック

- 信頼関係の作成
- パブリック IP アドレス使用時の IP ルートを追加する

- 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

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、一方向および双方向の外部とフォレストの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 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 AWS Directory Service。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、Amazon 、、Amazon 、Amazon QuickSight AWS IAM Identity Center、Amazon WorkDocs、Amazon WorkMail、Amazon などの AWS エンタープライズアプリケーション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 WorkSpaces、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。

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

セルフマネージドディレクトリとの信頼関係を作成する場合は、まずセルフマネージドネットワークを Managed Microsoft AD を含む Amazon VPC AWS に接続する必要があります。セルフマネージド型および 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 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 名を使用するには QuickSight、ポート 9389 を許可する必要があります。Active Directory の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「 のサービス概要とネットワークポート要件Windows」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 での事前認証」を参照してください TechNet。

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 のドメイン名に条件付きフォワーダーを割り当てる」を参照してください。 TechNet

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。
11. プライマリサーバーの IP アドレスを選択し、前にメモした 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 での信頼の管理」を参照してください TechNet。

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 Managed Microsoft AD AWS のグローバル機能です。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、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。選択的認証の一般的な情報については、「Microsoft での信頼のセキュリティに関する考慮事項」を参照してください TechNet。
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。例えば、既に一方向の「受信の信頼」が存在し、その上で「送信方向」で別の信頼関係の設定が必要な場合は、まず既存の信頼関係を削除してから、新たに「双方向」の信頼を作成します。

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。

このプロセスは、双方向信頼の送信方向のみを検証します。受信信頼の検証は AWS サポートされていません。セルフマネージド Active Directory との信頼を検証する方法の詳細については、「Microsoft での信頼の検証」を参照してください TechNet。

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。

パブリック IP アドレス使用時の IP ルートを追加する

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、Active Directory の多数の強力な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、「信頼関係の作成」を参照してください。

同様に、VPC でパブリック IP アドレス範囲が使用されている場合は、AWS の AWS Managed Microsoft AD から、ピア接続する AWS VPC にトラフィックをルーティングする際にも、IP アドレス情報を入力する必要があります。

「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 と自己管理型 (オンプレミス) の Microsoft Active Directory との間で信頼関係を設定するために必要な各手順について説明します。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。

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、シングルラベルドメインによる信頼をサポートしていません。

- AWS Managed Microsoft AD ディレクトリが AWS に作成されていること。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。
- Windows を実行している EC2 インスタンスが AWS Managed Microsoft AD に追加されていること。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 に手動で結合する 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、このインスタンスに対する管理者のアクセス権限が必要です。

- 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ること。
  - 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、「管理対象の Microsoft AD AWS 用アクティブディレクトリ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使用が可能な状態にする必要があります。
- 自己管理型ネットワークと、AWS Managed Microsoft AD を含む VPC との間で、アクティブな接続が確立されていること。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、「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 と自己管理型ドメインはすでに作成されています。自己管理型ネットワークは、AWS Managed Microsoft AD の VPC に接続済みです。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 AWS Managed Microsoft AD

- 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

VPC 内にある AWS Managed Microsoft AD の ID: vpc-12345678

自己管理型または AWS Managed Microsoft AD のドメイン

- 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 Microsoft AD を含む VPC が使用するすべてのサブネットの CIDRs に次のポートが開放されるように、セルフ AWS 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) からの受信トラフィックと送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 - ライトウェイトディレクトリアクセスプロトコル (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 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) QuickSight。

> **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。

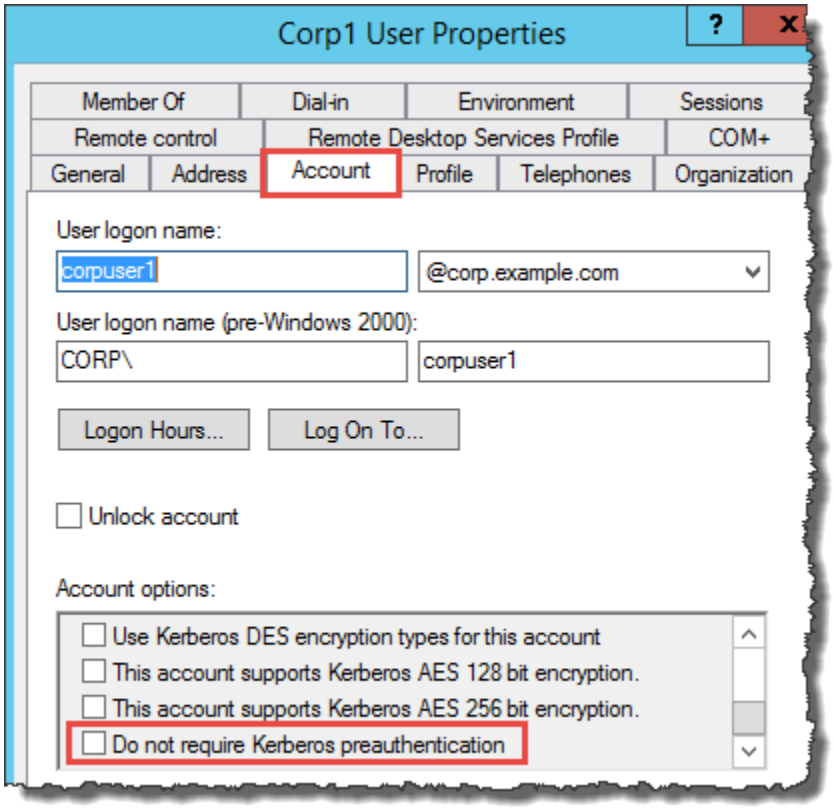
Kerberos の事前認証が有効化されていることを確認する

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

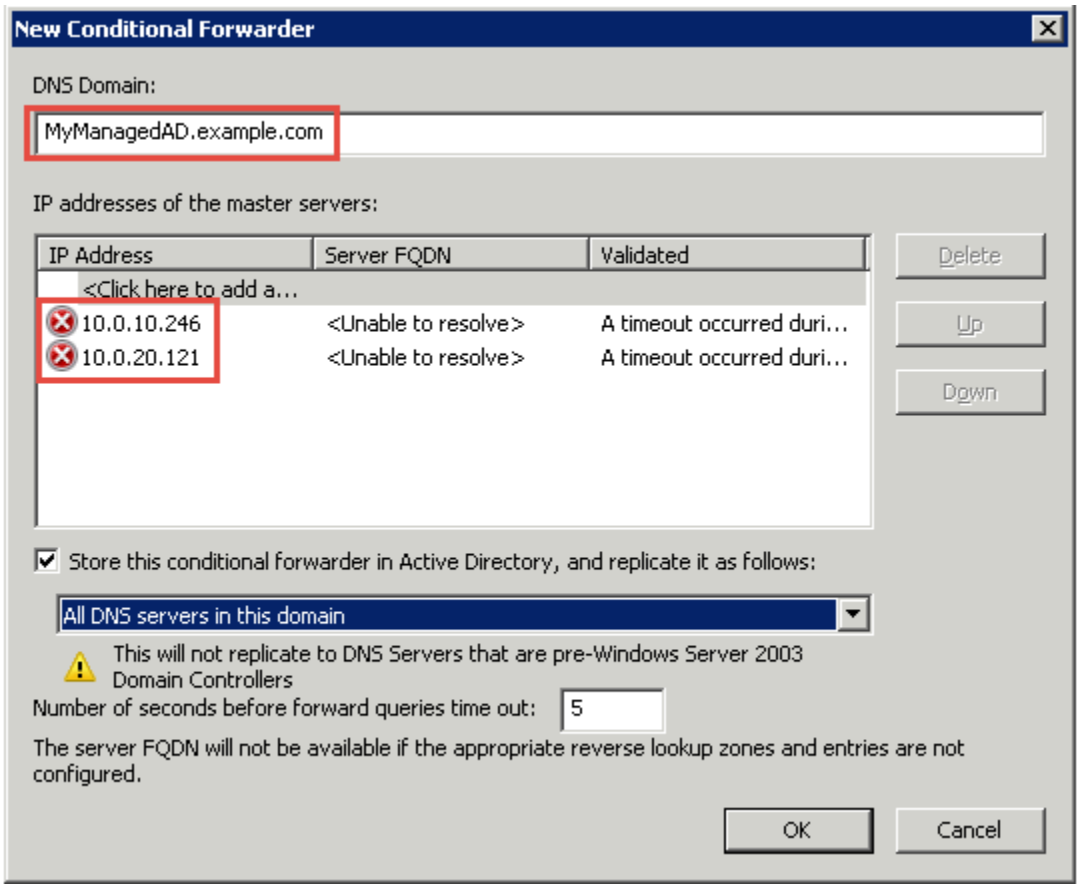
DNS の条件付きフォワーダーは、各ドメインで設定する必要があります。セルフマネージドドメインでこれを行う前に、まず AWS Managed Microsoft AD に関する情報を取得します。

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、前にメモした 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

それでは、 AWS 管理対象の Microsoft AD を信頼関係に備えましょう。以下の手順の多くは、自己管理型ドドメインで行ったものとほぼ同じです。ただし、今回は、 AWS 管理対象の Microsoft AD を使用して作業しています。

VPC サブネットとセキュリティグループを設定する

自己管理型ネットワークから管理対象の 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。 AWS そのためには、 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 ACL と、ドメインコントローラに設定されている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。

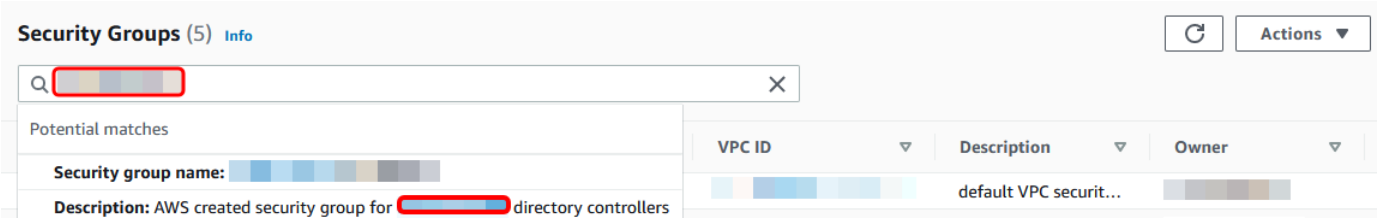
アウトバウンド

- 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 管理対象の 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

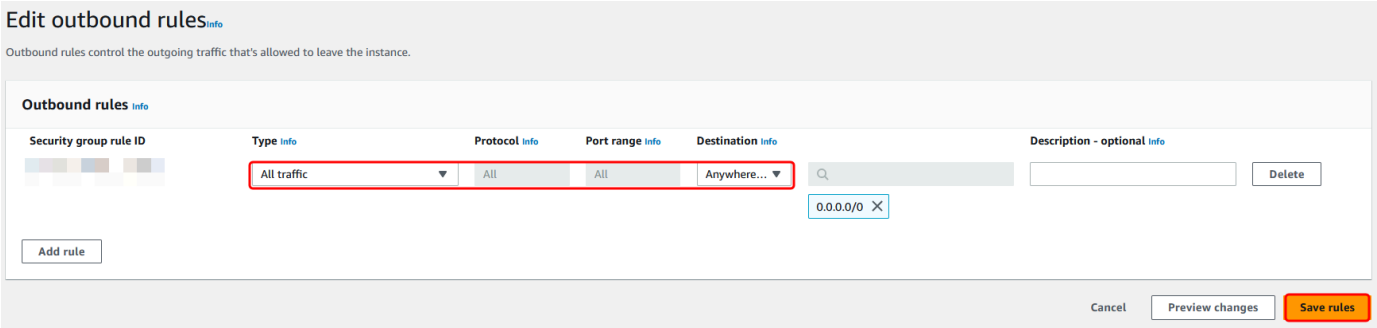
1. AWS Directory Service コンソール に戻ります。ディレクトリのリストで、 AWS 管理対象の Microsoft AD ディレクトリのディレクトリ ID を書き留めます。
2. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
3. ナビゲーションペインで、セキュリティグループ] を選択します。
4. 検索ボックスを使用して、 AWS 管理対象の Microsoft AD ディレクトリ ID を検索します。検索結果で、**`AWS created security group for yourdirectoryID 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。

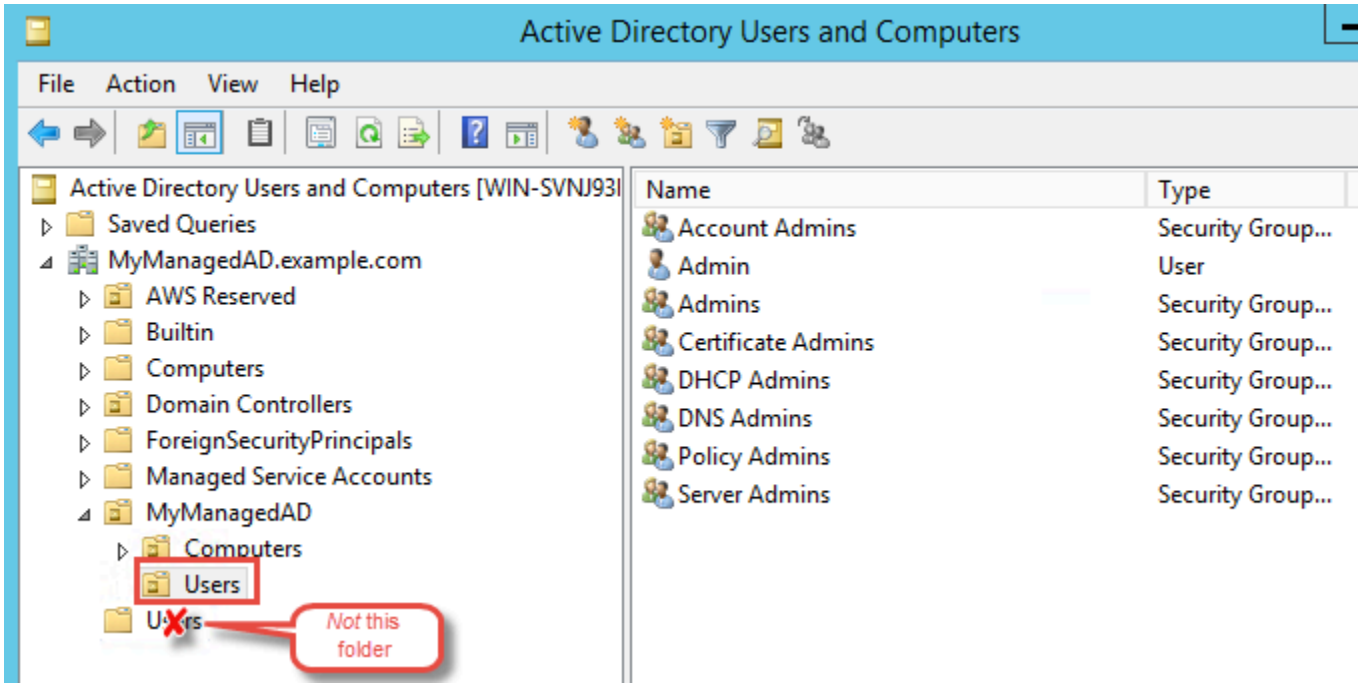


Kerberos の事前認証が有効化されていることを確認する

次に、 AWS 管理対象の 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する必要があります。これは、自己管理型ディレクトリで実施したものと同じプロセスです。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. ドメインのまたはドメイン内のユーザーを管理する権限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。管理者アカウントのアクセス権限
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、「管理対象の Microsoft AD AWS 用アクティブディレクトリ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。まず、自己管理型ドメインで信頼を作成した上で、最後に AWS Managed Microsoft AD でも信頼を作成します。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留意ください。例えば、自己管理型ドメインで一方向の送信の信頼を作成した場合には、もう一方の、AWS Managed Microsoft AD では一方向の受信の信頼を作成する必要があります。

> **Note**
>
> AWS Managed Microsoft AD は、外部の信頼を使用することもできます。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、[Next] (次へ) をクリックします。
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。このパスワードは AWS Managed Microsoft AD の信頼を設定する際に必要になるので記録しておきます。
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) をクリックします。

AWS Managed Microsoft AD ディレクトリ内で信頼を設定する

最後に、AWS Managed Microsoft AD ディレクトリでフォレストの信頼関係を設定します。自己管理型ドメインにフォレストの信頼を双方向で作成したので、AWS Managed Microsoft AD ディレクトリを使用する信頼も双方向で作成します。

> **Note**
>
> 信頼関係は、AWS Managed Microsoft AD でグローバルに使用できる機能です。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、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 ディレクトリ内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. [Directories] (ディレクトリ) ページで、使用する 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、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。この段階で、自己管理型ドメイン (corp.example.com) と AWS Managed Microsoft AD (MyManagedAD.example.com) との間に信頼関係が作成されました。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、「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 ドメイン間に信頼関係を設定するために必要な各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。

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、管理対象の Microsoft AD AWS AWS が別の管理対象 Microsoft AD との信頼関係に対応できるように準備します。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、 AWS 管理対象の Microsoft AD 環境が相互に連携するように構成しています。

VPC サブネットとセキュリティグループを設定する

管理対象の Microsoft AD AWS AWS ネットワークから他の管理対象 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。そのためには、 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 ACL と、ドメインコントローラに設定されている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

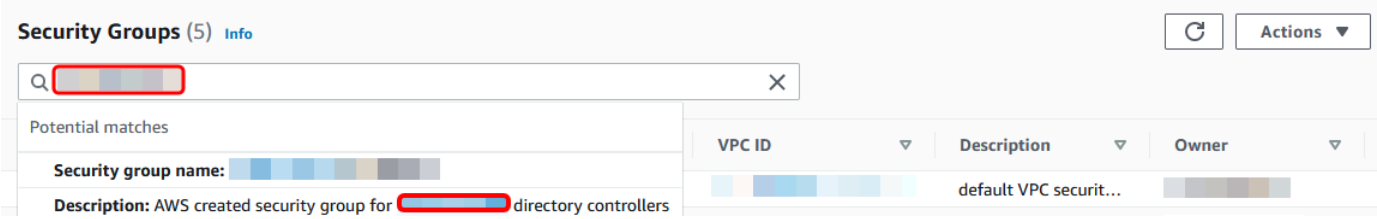
- すべて

> **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 管理対象の 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。

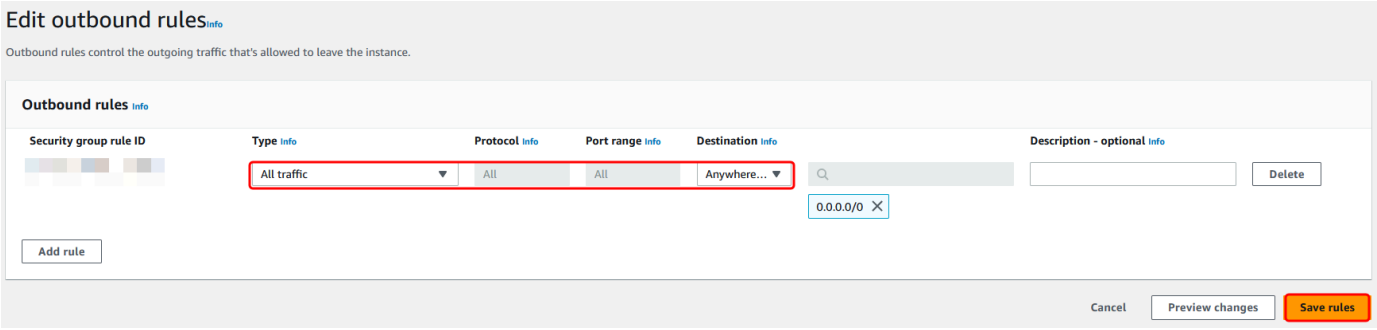
1. AWS Directory Service コンソールに移動します。ディレクトリのリストで、 AWS 管理対象の Microsoft AD ディレクトリのディレクトリ ID を書き留めます。
2. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
3. ナビゲーションペインで、セキュリティグループ] を選択します。
4. 検索ボックスを使用して、 AWS 管理対象の Microsoft AD ディレクトリ ID を検索します。検索結果で、**`AWS created security group for yourdirectoryID 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。

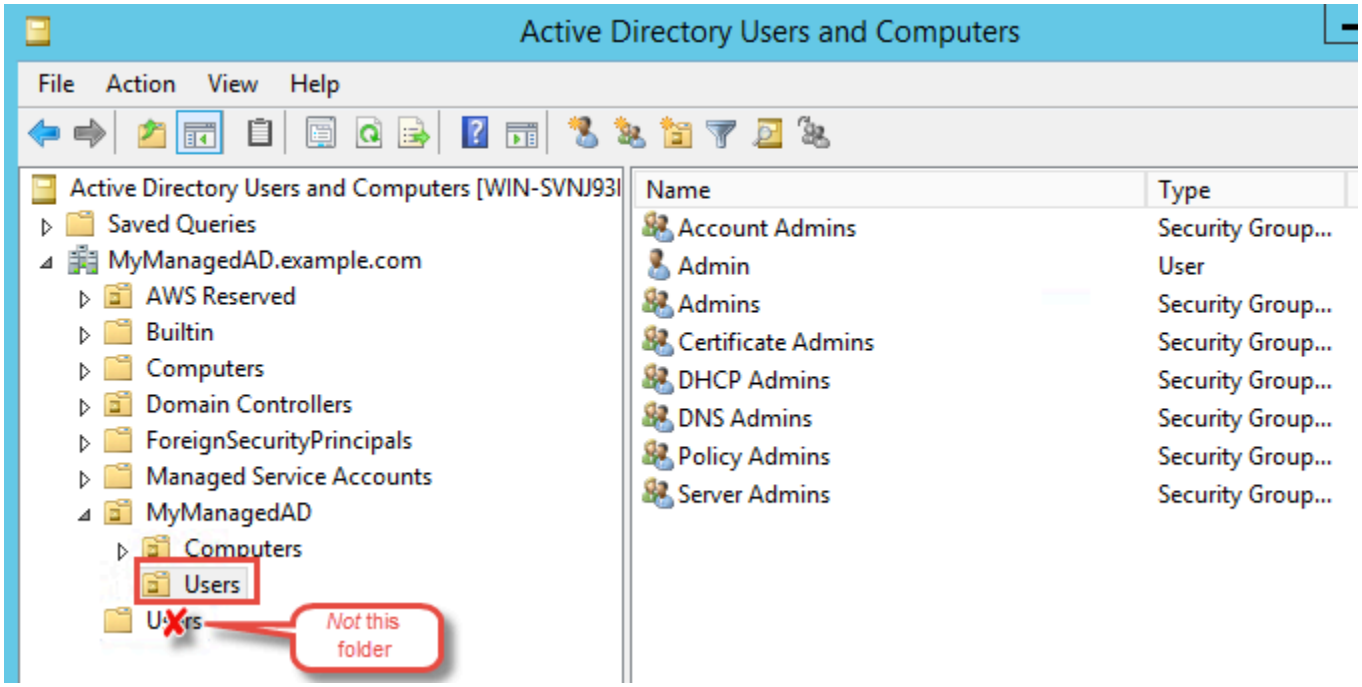


Kerberos の事前認証が有効化されていることを確認する

次に、 AWS 管理対象の 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する必要があります。これは、オンプレミスディレクトリで実施したものと同じプロセスです。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. ドメインのまたはドメイン内のユーザーを管理する権限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。管理者アカウントのアクセス権限
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、「管理対象の Microsoft AD AWS 用アクティブディレクトリ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

ここまでで準備が完了したので、最後の手順では 2 つの AWS Managed Microsoft AD ドメイン間で信頼関係を作成します。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。

1 番目の 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留意ください。例えば、1 番目のドメインで一方向の送信の信頼を作成した場合、2 番目の AWS Managed Microsoft AD には、一方向の受信の信頼を作成する必要があります。

> **Note**
>
> AWS Managed Microsoft AD は、外部の信頼を使用することもできます。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。

1 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 コンソールを開きます。
2. [Directories] (ディレクトリ) ページで、1 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. [Add a trust relationship] (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。このパスワードは、2 番目の AWS Managed Microsoft AD の信頼を設定する際に必要になるので、必ず記録しておきます。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、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) [Add another IP address] (別の IP アドレスの追加) 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 ドメインの信頼を設定する

次に、2 番目の AWS Managed Microsoft AD ディレクトリでフォレストの信頼関係を設定します。1 番目の AWS Managed Microsoft AD ドメインに双方向のフォレスト信頼を作成したので、この AWS Managed Microsoft AD ドメインに対しても双方向の信頼を作成します。

2 番目の AWS Managed Microsoft AD ドメインの信頼を設定するには

1. AWS Directory Service コンソール に戻ります。
2. [Directories] (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. [Add a trust relationship] (信頼関係の追加) ページで、1 番目の 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も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) [Add another IP address] (別の IP アドレスの追加) をクリックし、1 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確立されました。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 を に接続する Microsoft Entra Connect Sync

このチュートリアルでは、 をインストールして AWS Managed Microsoft AD Microsoft Entra IDにMicrosoft Entra Connect Sync同期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. Windows PowerShell を使用してスクリプトを実行し、新しく作成したユーザーに適切なアクセス許可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 を作成する”」を参照してください。
- Managed Microsoft AD に参加している Amazon EC2 Windows Server AWS インスタンス。詳細については、「Windows インスタンスにシームレスに接続する」を参照してください。
- AWS Managed Microsoft AD を管理するために Active Directory Administration Tools がインストールされた EC2 Windowsサーバー。詳細については、「the section called “管理対象の Microsoft AD 用の AD AWS 管理ツールのインストール”」を参照してください。

ステップ 1: Active Directory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た EC2 Windows Server インスタンスが既にあることを前提とActive DirectoryAdministration Toolsしています。詳細については、「the section called “管理対象の Microsoft AD 用の AD AWS 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 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. 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 Active Directory Directory Service (AD DS) Connector accountの になりますEntra Connect Sync。このプロセスの詳細な手順については、「」を参照してくださいthe section called “ユーザーの作成”。

ステップ 2: ダウンロード Entra Connect Sync

- Managed Microsoft AD 管理者である EC2 AWS インスタンスにMicrosoftウェブサイトEntra Connect Syncからダウンロードします。

> **Warning**
>
> この時点では を開いたEntra Connect Sync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許可をプロビジョニングします。

ステップ 3: Windows PowerShell スクリプトを実行する

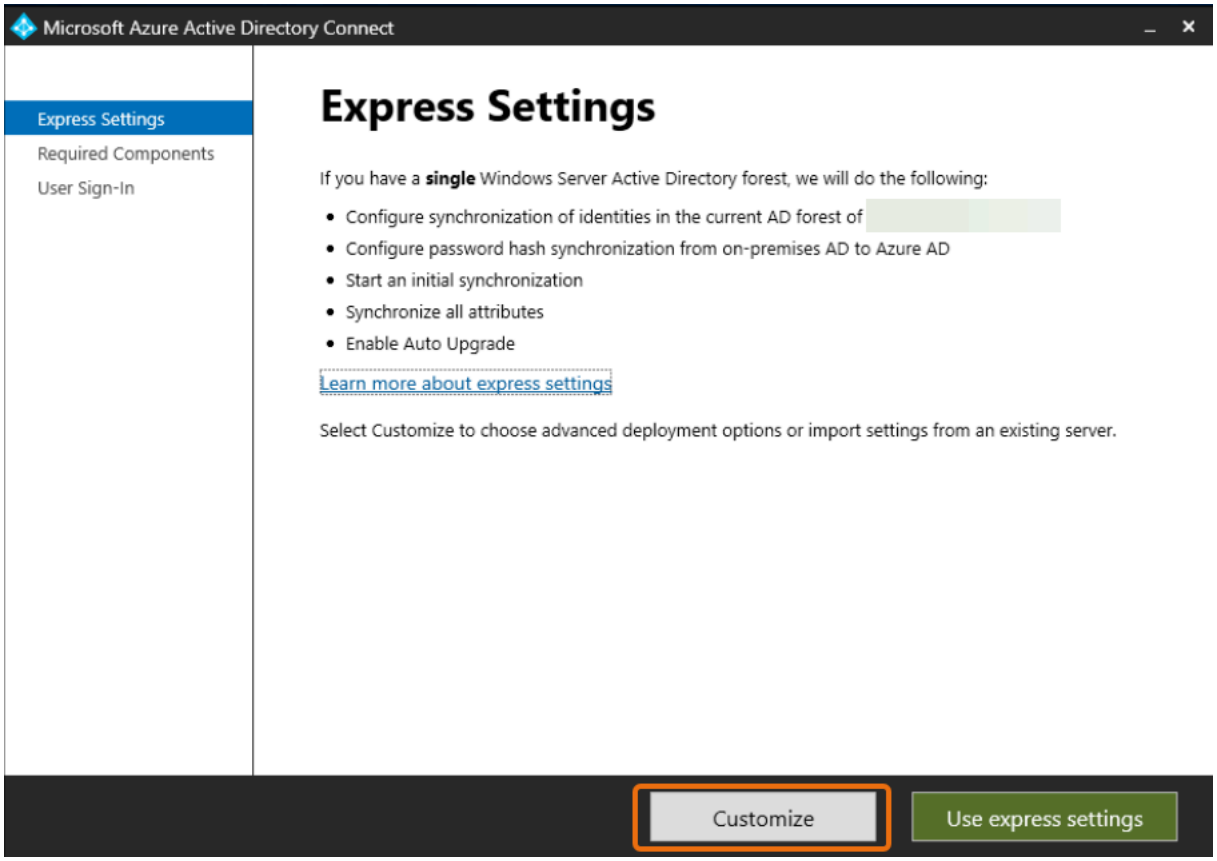
- 管理者PowerShellとして を開き、次のスクリプトを実行します。スクリプトの実行中に、ステップ 1 で新しく作成したドメインユーザーの sAMAccountName を入力するように求められます。

```
$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
```

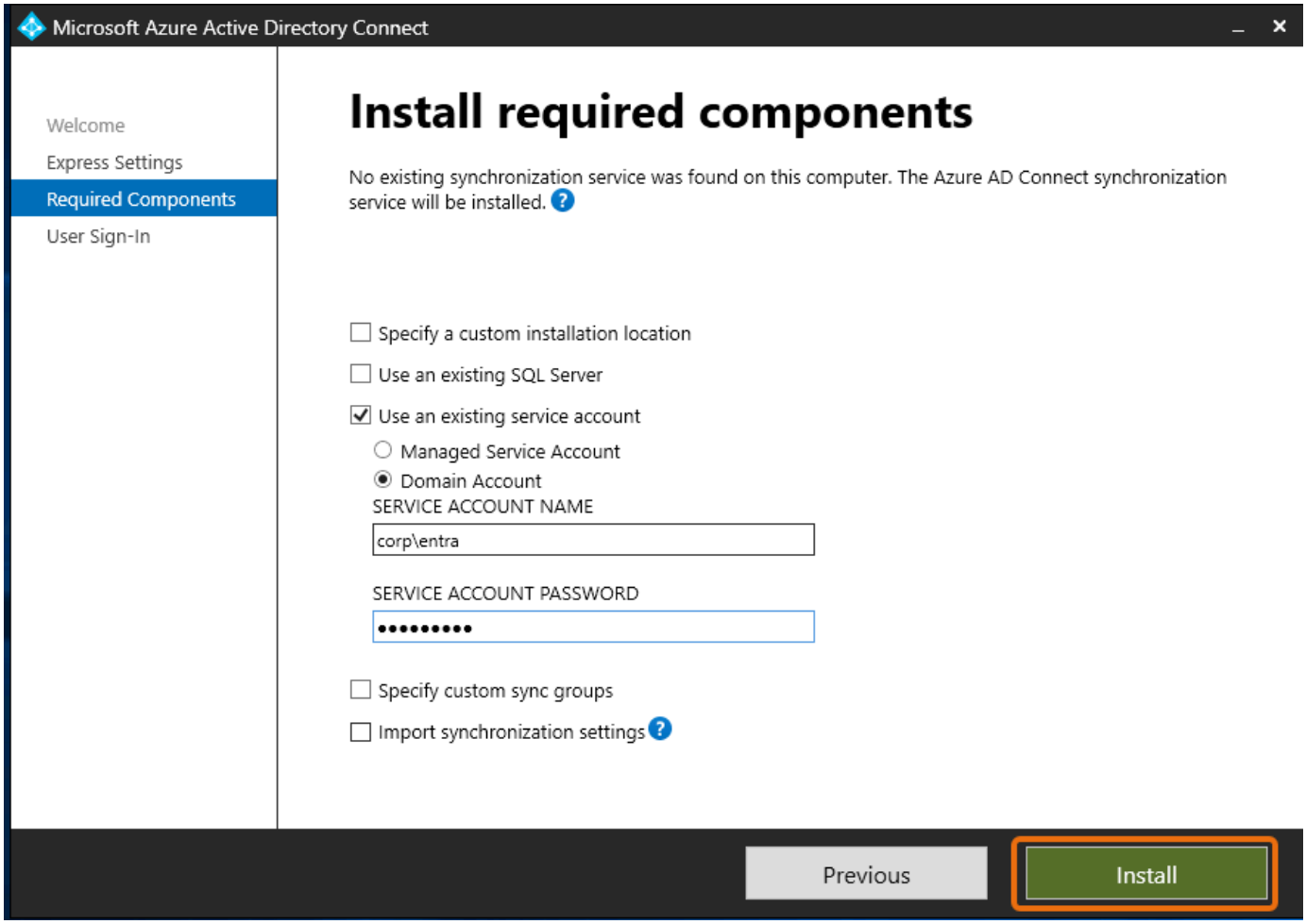
```
    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $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 : $_"
    }
    }
}
```

ステップ 4: 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 と呼ばれていましたAzure Active Directory Connect) 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すると、MicrosoftAzure Active Directory Connectウィンドウが開きます。Express Settings ウィンドウで、 の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。SERVICE ACCOUNT NAME と SERVICE ACCOUNT PASSWORD で、ステップ 1 で作成したユーザーAD DS Connector accountの名前とパスワードを入力します。例えば、AD DS Connector account名前が の場合`entra`、アカウント名は になります`corp\entra`。次に、インストール を選択します。



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Active Directoryを使用して にサインインできます。

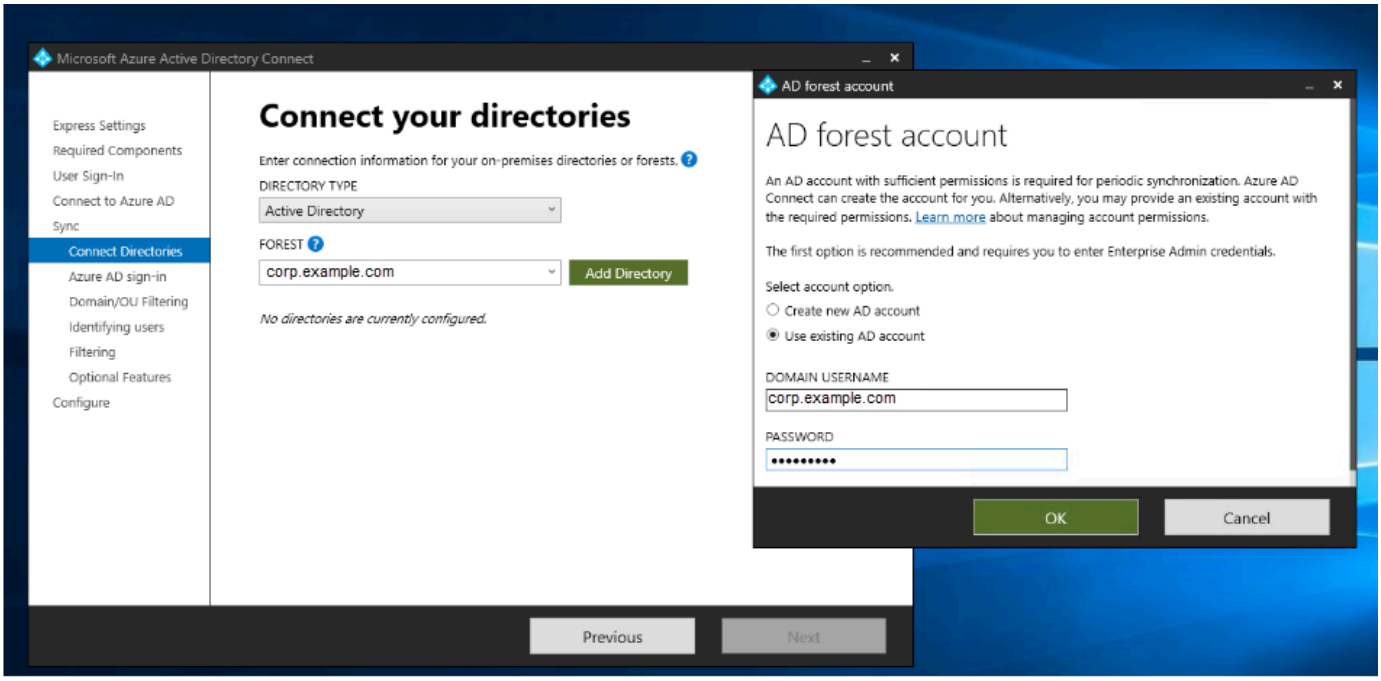
   b. 設定しないでください - これにより、 Microsoft Entra (旧称 Azure Active Directory (Azure AD)) または でフェデレーティッドサインインを使用できますOffice 365。

   [次へ] を選択します。

5. Connect to Azure ウィンドウで、 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Entra ID、次へ を選択します。

6. ディレクトリの接続ウィンドウで、ディレクトリタイプ Active Directoryを選択します。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ユーザー名とパスワードを入力し、OK 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、検証済みバニティドメインが 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ドメイン に一致させることなく続行を選択しますEntra ID。[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、ニーズに合った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「: フィルタリングの設定」]を参照してください。[次へ] を選択します。
10. ユーザーの識別、フィルタリング、およびオプションの機能ウィンドウで、デフォルト値のままにして、次へ を選択します。
11. Configure ウィンドウで、設定を確認し、Configure を選択します。のインストールEntra Connect Syncが確定し、ユーザーは との同期を開始しますMicrosoft Entra ID。

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を保存する方法の管理と適用を行います。スキーマに定義を追加するプロセスは、「スキーマの拡張」と呼ばれています。スキーマの拡張により、有効な LDAP データ交換形式 (LDIF) ファイルを使用して、AWS Microsoft AD ディレクトリのスキーマを変更できるようになります。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。

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 スキーマを拡張するタイミング

新しいオブジェクトクラスおよび属性を追加することで、AWS Managed Microsoft AD スキーマを拡張できます。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 に依存している企業内アプリケーションを AWS クラウドに移行する必要がある場合に特に有効です。

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 ID は、AD の オブジェクト識別子 (OID) 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

- スキーマを拡張する
- スキーマの要素

チュートリアル: AWS Managed Microsoft AD スキーマの拡張

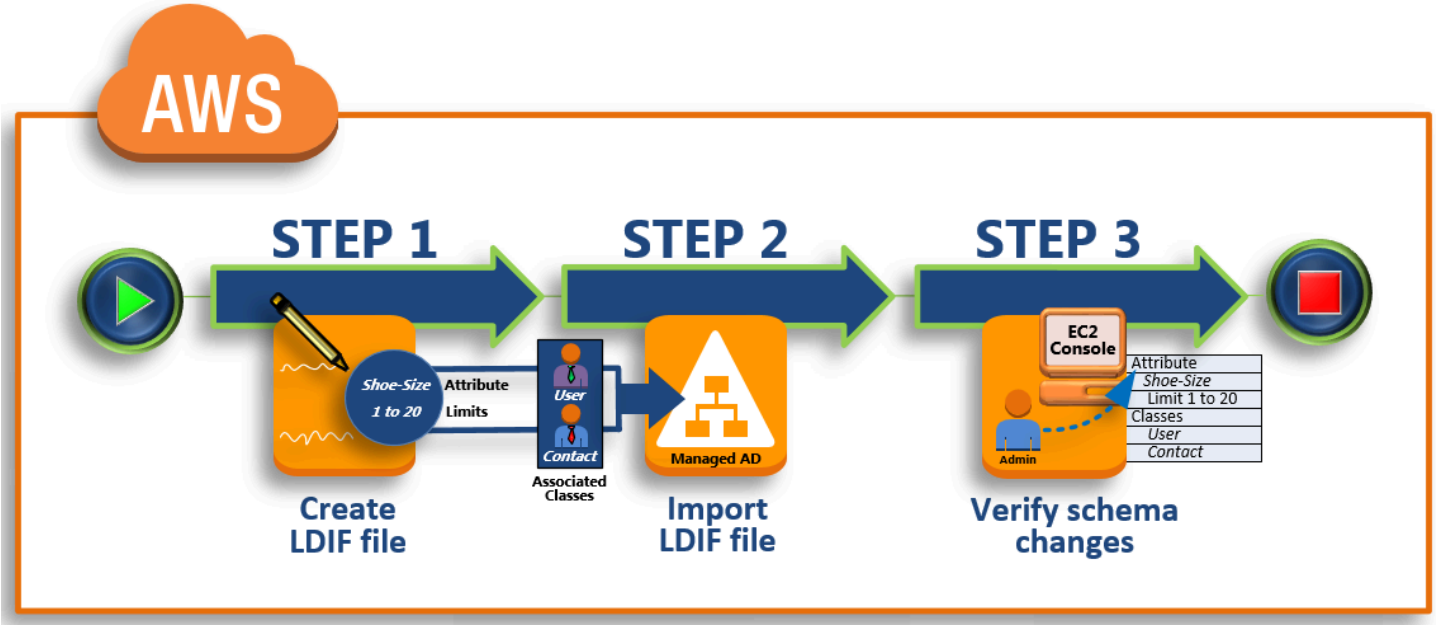
このチュートリアルでは、特定の要件を満たす一意の属性とクラスを追加して、 AWS Managed Microsoft AD とも呼ばれる AWS Directory Service for Microsoft Active Directory ディレクトリのスキーマを拡張する方法について説明します。 AWS マネージド Microsoft AD スキーマ拡張は、有効な LDIF (Lightweight Directory Interchange Format) スクリプトファイルを使用してのみアップロードおよび適用できます。

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、コンソールを使用して AWS Directory Service 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) ディ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 ディレクトリで`ldifde.exe`アプリケーションを実行することで、スキーマが変更された 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 を識別します。また、ディレクトリのためのドメインコンポーネントが含まれている必要があります。例えば、このチュートリアル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。
  - への変更は defaultSecurityDescriptor サポートされていません。

LDIF ファイルの構築方法の詳細と、 AWS Managed Microsoft AD スキーマ拡張のテストに使用できるサンプル LDIF ファイルについては、 AWS セキュリティブログのAWS 「 Managed Microsoft AD Directory スキーマを拡張する方法」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しても、オペレーションは元に戻せません。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、過去のある時点にロールバックされてます。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 Managed 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維持します。

> **Note**
>
> スキーマ拡張は Managed Microsoft AD AWS のグローバル機能です。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、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 はディレクトリをエラーから保護するためのステップを実行します。変更は次の順序で適用されます。

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、いずれかの DCs 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、プライマリスキーマとなる DCs の 1 つを選択し、その DC をディレクトリレプリケーションから削除して、 を使用して LDIF ファイルを適用しますLdifde.exe。
4. レプリケーションDCs AWS 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 スキーマスナップイン および/または PowerShell を使用して、スキーマの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 にドメインに参加し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 ウェブサイトの指示に従って Active Directory スキーマ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。

を使用して を検証するには PowerShell

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 - オプション

新しい属性に値を追加する - オプション

このオプションのステップは、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に使用します。

属性に値を追加するには

1. Windows 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

AWS Managed Microsoft AD ディレクトリの維持

このセクションでは、 AWS Managed Microsoft AD 環境の一般的な管理タスクを維持する方法について説明します。

トピック

代わりの UPN サフィックスを追加する

AWS Managed Microsoft AD ディレクトリに代わりとなるユーザープリンシパル名 (UPN) サフィックスを追加することで、Active Directory (AD) のログイン名の管理を簡素化し、ユーザーの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 Active Directory で作成される内容」を参照してください。

代わりの 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 ディレクトリに結合している Amazon EC2 インスタンスを探します。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 管理対象Microsoft AD を削除する

AWS 管理対象の Microsoft AD を削除すると、ディレクトリデータとスナップショットはすべて削除され、復元することはできません。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。

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。 AWS リージョン Active Directory自分が導入されている場所にいることを確認してください。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. AWS 削除するディレクトリの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 アプリケーションが有効になっていると、 AWS 管理対象の 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 アプリとサービス] セクションには、 AWS ディレクトリで有効になっている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へのアクセスを無効にする」を参照してください。
      - Amazon を無効にするには WorkSpaces、 WorkSpaces コンソールの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「ディレクトリからの登録解除」を参照してください。
      - Amazon を無効にするには WorkDocs、Amazon WorkDocs コンソールで Amazon 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 管理ガイド』の「サイトの削除」を参照してください。
      - Amazon を無効にするには WorkMail、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 管理者ガイド』の「組織の削除」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 ユーザーガイド』の「FSx for Windows File Server 操作」を参照してください。Active Directory
      - 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、Client 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』Active Directoryの「認証」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「Amazon Connect インスタンスの削除」を参照してください。
- アマゾンを無効にするには QuickSight、アマAmazon QuickSight ンの購読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 アカウントの解約」を参照してください。

> **Note**
>
> AWS IAM Identity Center 使用していて、 AWS 削除する予定の管理対象Microsoft ADディレクトリに以前に接続したことがある場合は、削除する前にまずアイデンティティ・ 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。

ディレクトリのサイト名を変更する

AWS Managed Microsoft AD ディレクトリのデフォルトのサイト名を、既存 Microsoft Active Directory (AD) でのサイト名と一致するように変更できます。これにより、オンプレミスディレクトリ内で既存の AD ユーザーを、AWS Managed Microsoft AD がより速く見つけ出し、認証できるようになります。結果として、AWS Managed Microsoft AD ディレクトリに結合した AWS リソース (Amazon EC2 や Amazon RDS for SQL Server インスタンスなど) にログインする際のユーザーエクスペリエンスが向上します。

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 Active Directory で作成される内容」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 のサイト名を変更するには

1. Amazon EC2 コンソール (https://console.aws.amazon.com/ec2/) を開きます。
2. AWS Managed Microsoft AD ディレクトリに結合している Amazon EC2 インスタンスを探します。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。

ディレクトリをスナップショットまたは復元する

AWS Directory Service は、毎日の自動スナップショットと、 AWS Managed Microsoft AD Active Directory 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。これらのスナップショットを使用して、Active Directory の point-in-time 復元を実行できます。 AWS Managed Microsoft AD Active Directory 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。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 Managed Microsoft AD AWS のグローバル機能です。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、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。

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. [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。

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 Support 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. [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 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

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. [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 マネージド Microsoft AD をアップグレードしてください

AWS スタンダードエディションのマネージド Microsoft AD Active Directory をエンタープライズエディションにアップグレードするには、お問い合わせください AWS Support。詳細については、AWS Support ユーザーガイドの「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。

> **Note**
>
> マルチリージョンレプリケーションは、 AWS 以下のリージョンのマネージド Microsoft AD エンタープライズエディション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)
> - アフリカ (ケープタウン)
> - アジアパシフィック (香港)
> - アジアパシフィック (ムンバイ)
> - アジアパシフィック (ハイデラバード)
> - 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 (ジャカルタ)
> - アジアパシフィック (メルボルン)
> - アジアパシフィック (東京)
> - カナダ (中部)
> - カナダ西部 (カルガリー)
> - 中国 (北京)

- 中国 (寧夏)
- 欧州 (フランクフルト)
- 欧州 (チューリッヒ)
- 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)
- 欧州 (ミラノ)
- 欧州 (スペイン)
- イスラエル (テルアビブ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 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際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費用が発生します。詳細については、「AWS Directory Service 料金表」を参照してください。
- Active Directory をアップグレードすると、以前のエディションに戻すことはできません。
- Active Directoryアップグレード後は、以前のスナップショットを使用してを復元することはできません。
- アップグレードは、合意したスケジュールされた日時に行われます。 AWS Supportアップグレードは、月曜日から金曜日の午前 9 時 ~ 午後 5 時 (太平洋標準時) の間に行われます。
- アップグレードには 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 1 つずつアップグレードされます。これはパフォーマンスに悪影響を及ぼし、メンテナンス期間中にダウンタイムが発生する可能性があります。

- アプリケーションが Active Directory のドメイン名の代わりにドメインコントローラーのホスト名または IP アドレスを使用している場合は、これらのアプリケーションを更新する必要があります。
- LDAPS (SSL 経由のライトウェイトディレクトリアクセスプロトコル) を使用している場合は、ドメインコントローラーに新しい証明書が必要になります。

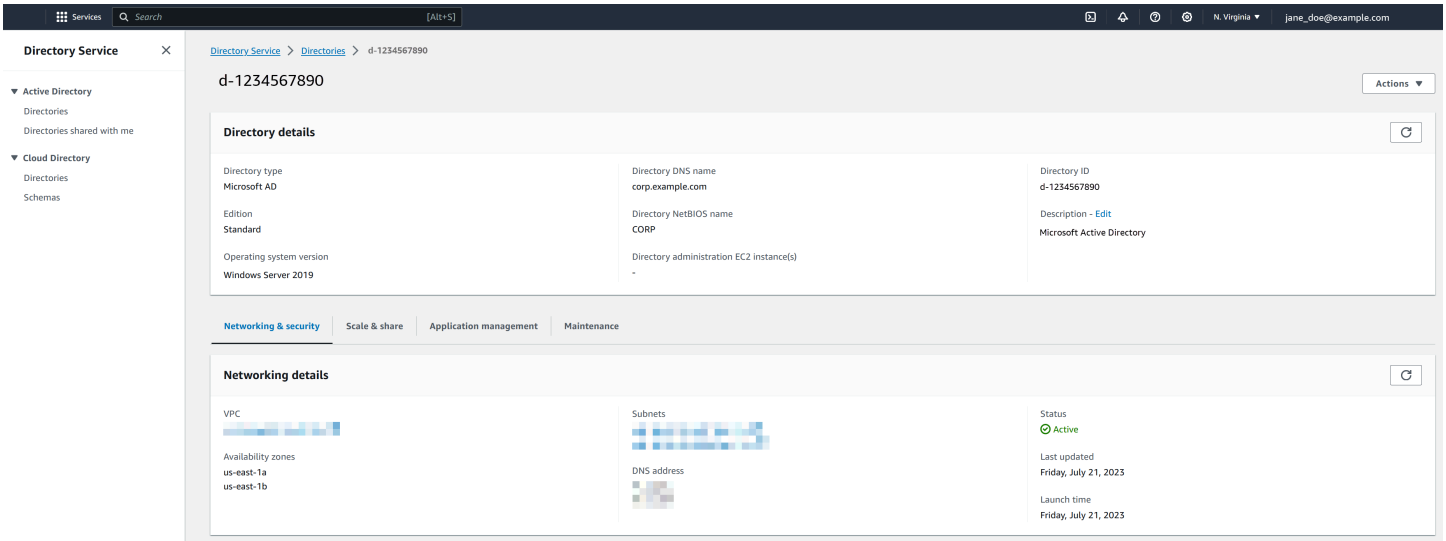
ディレクトリ情報の表示

ディレクトリに関する詳細情報を表示できます。

詳細なディレクトリ情報を表示するには

1. AWS Directory Service コンソールナビゲーションペインの でActive Directory、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 リンクをクリックします。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。



ユーザーおよびグループに AWS リソースへのアクセス権限を付与する

AWS Directory Service は、ディレクトリユーザーとグループに、Amazon EC2 コンソールへのアクセスなど、 AWS サービスとリソースへのアクセスを許可する機能を提供します。で説明したように、ディレクトリを管理するためのアクセス権限を IAM ユーザーに付与するのと同様にアイデン

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 AWS などの他の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、を参照してください。 AWS Management ConsoleAD 認証情報による AWS Management Console へのアクセスを有効化する

トピック

- 新しいロールの作成
- 既存のロールの信頼関係の編集
- ユーザーまたはグループの既存のロールへの割り当て
- ロールに割り当てられたユーザーとグループの表示
- ユーザーまたはグループからのロールの削除
- AWS Directory Service での AWS 管理ポリシーの使用

新しいロールの作成

で使用する IAM ロールを新規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。ロールを作成したら、コンソールにそのロールが表示されるようにするには、そのロールとの信頼関係を設定する必要があります。 AWS Directory Service 詳細については、「既存のロールの信頼関係の編集」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
> - リアム:GetRole
> - リアム:CreateRole
> - リアム: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 (たとえば AmazonEC2 FullAccess) の横にあるチェックボックスを選択し、[Next] を選択します。
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に、Amazon EC2 コンソールへのアクセス権限を特定のディレクトリユーザーに許可する新しいロールの作成のために、完了する必要があるタスクの例を示します。

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。ポリシーの入力を求められたら、[AmazonEC2] を選択します。FullAccess
2. 既存のロールの信頼関係の編集 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、 AWS Management Console 次のステップでへのアクセスを有効にした直後にロールが表示されるようにするために必要です。
3. AD 認証情報による AWS Management Console へのアクセスを有効化する 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. ユーザーまたはグループの既存のロールへの割り当て 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。

既存のロールの信頼関係の編集

既存の IAM AWS Directory Service ロールを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、そのためには、 AWS Directory Serviceそのロールがと信頼関係にある必要があります。 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ロールの作成、この信頼関係は自動的に設定されます。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。

既存の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。

```
{
  "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。

ユーザーまたはグループの既存のロールへの割り当て

既存の IAM AWS Directory Service ロールをユーザーまたはグループに割り当てることができます。そのためには、以下を完了していることを確認してください。

前提条件

- AWS マネージド型Microsoft AD を作成します。
- ユーザーを作成するか、グループを作成します。
- AWS Directory Serviceと信頼関係のあるロールを作成してください。既存のロールの信頼関係は編集できます。

> **Note**
>
> ディレクトリ内でネストされたグループのユーザーによる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。

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。
   - [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。
   - [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セクションまでスクロールし、[アクション] と [有効化] 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、ユーザーを割り当てる既存の 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

ロールに割り当てられたユーザーとグループを表示するには、以下の手順を実行します。

前提条件

- ユーザーまたはグループを既存のロールに割り当てます。

ロールに割り当てられた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。
   - [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。
   - [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. [コンソールアクセスの委任] セクションで、表示する IAM ロールを選択します。
5. [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。

ユーザーまたはグループからのロールの削除

ユーザーまたはグループからロールを削除するには、以下の手順を実行します。

ユーザーまたはグループから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。

- [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。
- [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、表示するロールを選択します。
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。

AWS Directory Service での AWS 管理ポリシーの使用

AWS Directory Service では、以下の AWS 管理ポリシーを使用して、ユーザーおよびグループに AWS のサービスやリソース (Amazon EC2 コンソールなど) へのアクセスを提供します。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
- 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 Example policies for administering AWS resources を参照してください。

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、 AWS Managed Microsoft AD を許可して WorkSpaces、Amazon AWS などのアプリケーションやサービスにあなたへのアクセスを許可することができますActive Directory。 AWS 以下のアプリケーションとサービスは、 AWS Managed Microsoft AD と連携するように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、「Amazon Chime 管理ガイド」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 FSx for Windows File Server	詳細については、「Microsoft Active Directory AWS のDirectory Service で Amazon FSx を使用する」を参照してください。
Amazon QuickSight	詳細については、Amazon QuickSight ユーザーガイドを参照してください。
Amazon Relational Database Service	詳細については、「Amazon RDS ユーザーガイド」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
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	シンプル AD、 AWS マネージド Microsoft AD、または AD Connector をから直接作成できます WorkSpaces。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 Client VPN	詳細については、『AWS Client VPN ユーザーガイド』を参照してください。
AWS IAM Identity Center	詳細については、『AWS IAM Identity Center ユーザーガイド』を参照してください。
AWS License Manager	詳細については、「 License Manager ユーザーガイド」を参照してください。
AWS Management Console	詳細については、「AD 認証情報による AWS Management Console へのアクセスを有効化する」を参照してください。
AWS Private Certificate Authority	詳細については、「AWS Private CA 用コネクタ」を参照してくださいActive Directory。
AWS Transfer Family	詳細については、『AWS Transfer Family ユーザーガイド』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、そのディレクトへのアクセスを管理します。 AWS AWS Directory Service 上記のアプリケーションとサービスのリンクをコンソールで見つけるには、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。

AWS AWS Directory Serviceを使用してアプリケーションとサービスを認証または認証解除する方法の詳細については、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承認 AWS Directory Service

トピック

- アクセス URL の作成
- シングルサインオン

アクセス URL の作成

Amazon WorkDocs などの AWS アプリケーションとサービスで使用するアクセス URL を使用して、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。

> **Note**
>
> 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。

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。
   - [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 によって Amazon WorkDocs のサインインページが表示されます。

シングルサインオン

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 WorkDocs から Amazon 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がそれ自体でサービスプリンシパル名属性を追加または削除できるようにするアクセス許可を委任できます。AD Connector サービスアカウントのアクセス許可を変更するアクセス許可を持つアカウントを使用して、ドメインに参加しているコンピュータから以下の PowerShell コマンドを実行できます。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"
```

Amazon でシングルサインオンを有効または無効にするには WorkDocs

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、「有効化」を選択して Amazon のシングルサインオンを有効にします WorkDocs。

   [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、「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 Amazon でシングルサインオンを無効にする場合は WorkDocs、 を無効にするを選択し、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、もう一度無効化を選択します。

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ティング () を有効にしますJavaScript。
- 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

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AuthServerAllowlistを実行して、ポリシーにアクセス URL を追加します。

```
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 ポリシーを使用してドメイン内のコンピュータで Chrome ウェブブラウザを管理する場合は、AuthServerAllowlistポリシーにアクセス URL を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。

AD 認証情報による AWS Management Console へのアクセスを有効化する

AWS Directory Service を使用すると、ディレクトリのメンバーに AWS Management Console へのアクセス権限を付与することができます。デフォルトでは、ディレクトリのメンバーに AWS リソースに対するアクセス権限は付与されません。ディレクトリのメンバーに IAM ロールを割り当てることで、さまざまな AWS サービスやリソースにアクセスできるようにします。IAM ロールでは、ディレクトリメンバーに付与するをサービス、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、「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、「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「ユーザーおよびグループに AWS リソースへのアクセス権限を付与する」を参照してください。

トピック

- AWS Management Console へのアクセスを有効にする
- AWS Management Consoleへのアクセスを無効にする
- 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の記事

- AWS Microsoft ADとオンプレミスの資格情報を使用して AWS Management Console にアクセスする方法

> **Note**
>
> AWS Management Console へのアクセスは、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 へのアクセスを有効にする

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。

- [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、AWS Management Console へのアクセスを有効に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 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。

   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、先に、そのユーザーを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、「ユーザーまたはグループの既存のロールへの割り当て」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へのアクセスを無効にする

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、AWS Management Console へのアクセスを無効に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 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. [Manage Access to AWS Resource] (AWS リソースへのアクセスの管理) ダイアログボックスで、[Continue] (続行) を選択します。

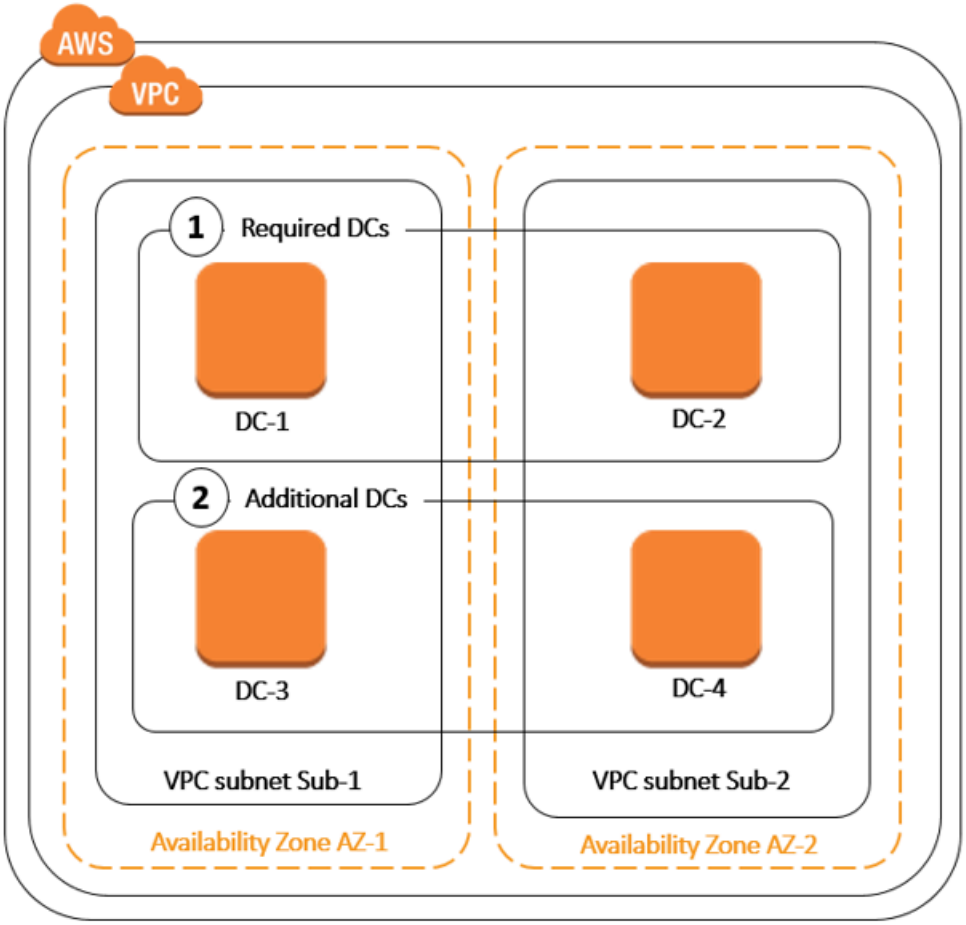
6. [Assign users and groups to IAM roles] (ユーザーおよびグループの IAM ロールへの割り当て) ページの [Set login session length] (ログインセッション期間の設定) で数値を編集し、[Save] (保存) をクリックします。

追加ドメインコントローラーのデプロイ

追加のドメインコントローラーをデプロイすると、冗長性が高まり、その結果として耐障害性と可用性が高まります。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。たとえば、 AWS マネージド Microsoft AD を使用して、大規模な Amazon EC2 および Amazon RDS for SQL Server インスタンス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。

最初にディレクトリを作成すると、 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。これは高可用性を実現するために必要です。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 コンソールから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 Managed 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配布します。

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ドメインコントローラーを Required と呼びます。 AWS Managed Microsoft AD は、ディレクトリ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意図的に別々のアベイラビリティーゾーンに配置します。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 Managed 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異なる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 の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。UpdateNumberOfDomainControllersAPI を使用して、 AWS 管理対象の Microsoft AD 用の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こともできます。

> **Note**
>
> 追加のドメインコントローラーは、 AWS マネージド Microsoft AD の地域機能です。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。

追加のドメインコントローラーの追加または削除

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の詳細を確認してください。

- 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。
- AWS 管理対象の Microsoft AD で LDAPS を有効にするように設定した場合、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、「セキュア LDAP または LDAPS を有効にする」を参照してください。

AWS Managed Microsoft AD ディレクトリの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、以下の手順に従います。

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

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] (スケールリングと共有) 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のステータスが Active になり、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。

関連するセキュリティブログ記事 AWS

- AWS ドメインコントローラーを追加して管理対象の Microsoft AD の冗長性とパフォーマンスを向上させる方法 AWS Directory Service

Active Directory から AWS Managed Microsoft AD へユーザーを移行する

自己管理型 Active Directory から AWS Managed Microsoft AD ディレクトリへのユーザーの移行には、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) を使用します。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 How to migrate your on-premises domain to AWS Managed Microsoft AD using ADMT を参照してください。

AWS Managed Microsoft AD 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 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 *	Managed Microsoft AD あたり AWS 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

リソース	デフォルトのクォータ
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
単一の AWS Managed Microsoft AD (Enterprise Edition) ディレクトリ **** の合計 AWS リージョンの最大数	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、「アプリケーションをプログラミングする」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 マネージド Microsoft AD のアプリケーション互換性

AWS Microsoft Active Directory 用Directory Service (AWS Managed Microsoft AD) は、 AWS 複数のサービスおよびサードパーティアプリケーションと互換性があります。

AWS 以下は互換性のある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。
- 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 Active Directory」を参照してください。
- Amazon QuickSight -詳細については、「Amazon QuickSight エンタープライズエディションのユーザーアカウントの管理」を参照してください。
- Amazon RDS for MySQL - 詳細については、「MySQL での Kerberos 認証の使用」を参照してください。
- Amazon RDS for Oracle - 詳細については、「Amazon RDS for Oracle の Kerberos 認証の設定」を参照してください。
- Amazon RDS for PostgreSQL - 詳細については、「Amazon RDS for PostgreSQL で Kerberos 認証を使用する」を参照してください。
- Amazon RDS for SQL Server - 詳細については、「Amazon RDS for SQL Server DB インスタンスでの Windows 認証の使用」を参照してください。
- Amazon WorkDocs -詳細な手順については、「AWS マネージド Microsoft AD による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、「Amazon WorkMail を既存のディレクトリと統合する (標準設定)」を参照してください。
- AWS Client VPN -詳細な手順については、「クライアントの認証と承認」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 Connect する」を参照してください。
- AWS License Manager -詳細については、の「ユーザーベースのサブスクリプション」を参照してください。 AWS License Manager
- AWS Management Console — 詳細については、を参照してください。AD 認証情報による AWS Management Console へのアクセスを有効化する
- FSx for Windows File Server – 詳細については、「FSx for Windows File Server とは？」を参照してください。

- WorkSpaces -詳細な手順については、「AWS 管理対象の Microsoft AD WorkSpace を使用してを起動する」を参照してください。

Active Directory off-the-shelf を使用するカスタムアプリケーションおよび商用アプリケーションの規模は非常に大きいため、Microsoft Active Directory AWS 用Directory Service (AWS Managed Microsoft AD) AWS とのサードパーティアプリケーションの互換性を正式または広範囲に検証することは行っておらず、実施することもできません。は、 AWS お客様が直面する可能性のあるアプリケーションのインストール上の問題を解決するためにお客様と協力していますが、 AWS Managed Microsoft AD とのアプリケーションの互換性を保証することはできませんし、今後も互換性があることを保証することはできません。

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

- Active Directory によるライセンス認証 (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 (AzureADAzure Active Directory) と呼ばれていました)
- Microsoft Entra Connect(旧称) Azure Active Directory Connect
- 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 (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server(SQL Server 常時接続可用性グループを含む)
- 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が、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 を管理対象サービスとして提供するには、 AWS この権限レベルの排他的制御を維持する必要があるため、ドメイン管理者としてこ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、 AWS 権限の低い特定のサポート対象権限をインストール担当者に委任することで、このようなアプリケーションをインストールできます。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。 AWS 委任できる権限の詳細については、を参照してください。AWS Managed Microsoft AD Active Directory で作成される内容
- Active Directory特権コンテナへのアクセス — AWS Managed Microsoft AD はディレクトリ内に、管理者が完全に管理できる組織単位 (OU) を提供します。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 の管理の詳細については、「Managed Microsoft AD AWS を管理する方法」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 — Active Directory 一部のアプリケーションでは、既定の 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の一部としてそれらの変更をインストールしようとする場合があります。スキーマ拡張には特権があるため、 AWS Directory Service コンソール、CLI、または SDK からのみライトウェイトディレクトリ交換フォーマット (LDIF) AWS 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、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 ファイルが付属していることがよくあります。 AWS Directory Service 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 で動作する構成が見つからない、 off-the-shelf よく要求される商用アプリケーションの一覧です。 AWS 非生産的な作業を避けるため、この一覧は独自の裁量で随時更新されています。 AWS この情報は、現在またはfuture 互換性に関する保証や主張なしに提供してください。

- 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 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 AWS すことができるテストラボ環境を で構築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: AWS ベースとなるマネージド Microsoft AD テストラボのセットアップ 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: AWS ベースとなるマネージド Microsoft AD テストラボのセットアップ 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 AWS インスタンスを使用するマネージド Microsoft AD の新規インストールに備えて、 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 AWS インスタンスからマネージド Microsoft AD 環境を管理する方法を説明します。チュートリアルを完了する頃には、ネットワークの前提条件を設定し、 AWS 新しい管理対象の Microsoft AD フォレストを構成しているはずです。

次の図に示すように、このチュートリアルから作成するラボは、Managed Microsoft AD の実地学習の基礎となります。 AWS 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 マネージド Microsoft AD AWS アクティブディレクトリの環境をセットアップする]

前提条件となるタスクを完了したら、EC2 インスタンスに Amazon VPC を作成して設定します。

[ステップ 2: AWS 管理対象の Microsoft AD アクティブディレクトリを作成する]

このステップでは、 AWS マネージド Microsoft AD AWS を初めてセットアップします。

[ステップ 3: Amazon EC2 AWS インスタンスをデプロイしてマネージド Microsoft AD アクティブディレクトリを管理する]

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たら、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 AWS Tools for Windows PowerShell コマンドまたは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 AWS Tools for Windows PowerShell または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 にをダウンロードしてインストールします。インストールしたら、Windows PowerShellコマンドプロンプトまたはウィンドウを開き、と入力しますaws configure。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留意ください。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 [なし]: 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留意ください。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 マネージド Microsoft AD AWS アクティブディレクトリの環境をセットアップする

AWS AWS テストラボでマネージド Microsoft AD を作成する前に、すべてのログインデータが暗号化されるように Amazon EC2 key pair 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。

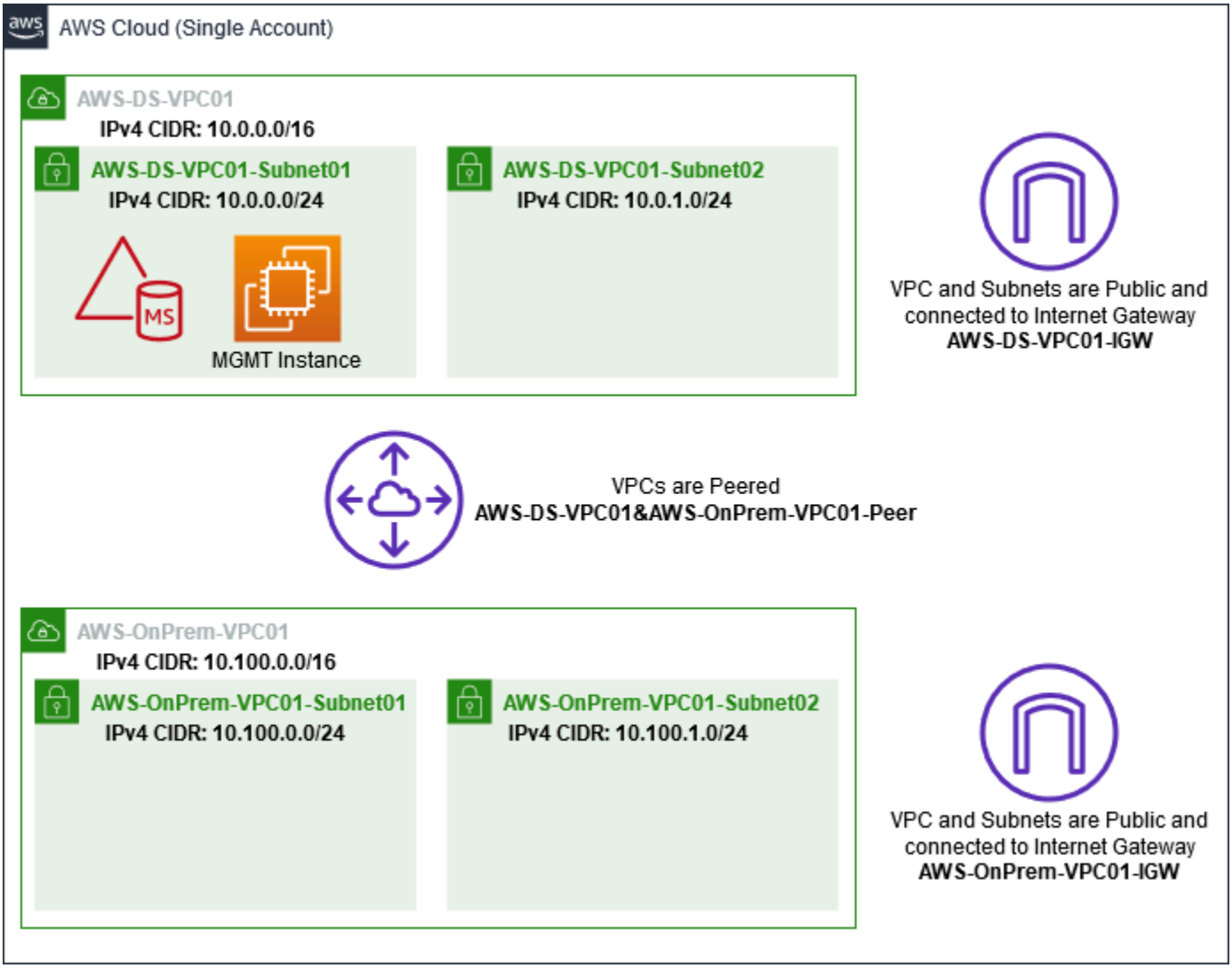
キーペアを作成するには

1. AWS Management Console にサインインし、https://console.aws.amazon.com/ec2/ にある 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 の作成、設定、およびピアリングを行う

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 PowerShell およびサンプルはすべて、以下のVPC 情報を使用しており、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、次の表に指定されているパラメータを使用して、同じアカウントに 2 つの VPC を作成する必要があります。 AWS マネージド Microsoft AD では、ディレクトリの共有この機能により個別のアカウントの使用がサポートされます。最初の VPC AWS はマネージド型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」で使用します。

マネージド Active DirecVPC 情報	オンプレミス VPC 情報
ネームタグ: AWS-DS-VPC01	ネームタグ:--VPC01 AWS OnPrem
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 の前提条件 の 1 つです。

AWS-DS-VPC01 サブネット情報:	AWS--VPC01 サブネット情報 OnPrem
ネームタグ:-DS-VPC01-Subnet01 AWS VPC: AWS vpc-xxxxxxxxxxxxxxxxx-DS-VPC01 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	ネームタグ:--VPC01-Subnet01 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem アベイラビリティーゾーン: us-west-2a IPv4 CIDR ブロック: 10.100.0.0/24
ネームタグ:-ds-VPC01-Subnet02 AWS VPC: AWS vpc-xxxxxxxxxxxxxxxxx-DS-VPC01 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	ネームタグ:--VPC01-Subnet02 AWS OnPrem VPC: vpc-xxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem アベイラビリティーゾーン: us-west-2b 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 Internet Gateway 情報
ネームタグ:-DS-VPC01-IGW AWS	ネームタグ:--VPC01-IGW AWS OnPrem
VPC: AWS vpc-xxxxxxxxxxxxxxxxx-DS-VPC01	VPC: vpc-xxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem

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--VPC01 の間の VPC ピアリング接続を設定します AWS OnPrem

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 を接続する方法はたくさんありますが、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、VPC 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。その中には、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:-DS-VPC01&--VPC01-Peer AWSAWS OnPrem
VPC (リクエスタ): vpc-xxxxxxxxxxxxxxx-DS-VPC01 AWS
アカウント: My Account
リージョン: 使用しているリージョン
VPC (アクセプター): AWS vpc-xxxxxxxxxxxxxxx-VPC01 OnPrem

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 ネームタグ (AWS-DS-VPC01 または--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 OnPrem

AWS-DS-VPC01 ルート 1 情報	AWS-DS-VPC01 ルート 2 情報	AWS--VPC01 ルート 1 情報 OnPrem	AWS-OnPrem-VPC01 ルート 2 情報
送信先: 0.0.0.0/0 ターゲット:igw-xxxxxxxxxxxxxxxxx-DS-VPC01-IGW AWS	送信先: 10.100.0.0/16 ターゲット: AWS pcx-xxxxxxxxxxxxxxxxx-DS-VPC01&--VPC01-Peer AWS OnPrem	送信先: 0.0.0.0/0 ターゲット: AWS igw-xxxxxxxxxxxxxxxxx-onprem-VPC01	送信先: 10.0.0.0/16 ターゲット: AWS pcx-xxxxxxxxxxxxxxxx-DS-VPC01 &--vpc01-Peer AWS OnPrem

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 Managed 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 テストラボセキュリティグループ
VPC: AWS vpc-xxxxxxxxxxxxxxxxx-DS-VPC01

-DS-VPC01 のセキュリティグループインバウンドルール AWS

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

-DS-VPC01 のセキュリティグループアウトバウンドルール AWS

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--VPC01 セキュリティグループ情報:OnPrem
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 テストラボセキュリティグループ。
VPC: vpc-xxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem

--VPC01 のセキュリティグループインバウンドルール AWS OnPrem

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

--VPC01 のセキュリティグループアウトバウンドルール AWS OnPrem

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 管理対象の Microsoft AD アクティブディレクトリを作成する

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。 AWS Management Console 手順 (このチュートリアルでは推奨) を使用するか、 AWS CLI AWS Tools for Windows PowerShell またはの手順を使用してディレクトリを作成できます。

方法 1: AWS 管理対象の 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 マネージド Microsoft AD を作成するには (Windows PowerShell) (オプション)

1. Windows PowerShell を開きます。
2. 次のコマンドを入力します。 AWS Management Console 前の手順のステップ 4 で指定した値を必ず使用してください。

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
 -Description “AWS DS Managed” - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

方法 3: AWS マネージド 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。 AWS Management Console 前の手順のステップ 4 で指定した値を必ず使用してください。

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

ステップ 3: Amazon EC2 AWS インスタンスをデプロイしてマネージド Microsoft AD アクティブディレクトリを管理する

このラボでは、どこからでも管理インスタンスに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ています。本番環境では、VPN AWS Direct Connect またはリンクを介してのみアクセスできるプライベート 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: AWS-DS-VPC01 にディレクトリ用の DHCP オプションセットを作成します。

このオプションの手順では、VPC の EC2 AWS インスタンスがマネージド Microsoft AD を自動的に使用して DNS 解決を行うように、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見つけるには、[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 AWS インスタンスを管理対象の Microsoft AD ドメインに参加させるロールを作成します。

この手順を使用して、Amazon EC2 Windows インスタンスをドメインに参加させる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 にシームレスに結合する 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。

   - AmazonSSM ManagedInstanceCore 管理ポリシーの横にあるボックスを選択します。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。
   - DirectoryServiceAccessAmazonSSM 管理ポリシーの横にあるボックスを選択します。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 には、EC2 などのドメインにインスタンスを結合するために使用されることを説明するロールの名前を入力します。DomainJoin
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、自動的にディレクトリに参加する

この手順では、EC2 インスタンスに Windows サーバーシステムをセットアップします。このシステムを使用して、後で Active Directory のユーザー、グループ、ポリシーを管理できます。

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-***xxxxxxxxxxxxxxxxx]*** 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-***xxxxxxxxxxxxxxxxx*** | 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-***xxxxxxxxxxxxxxxxx*** | 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 ロールには、インスタンスロールに付けた名前 (EC2 Windows AWS インスタンスを管理対象の Microsoft AD ドメインに参加させるロールを作成します。 など) を選択します。DomainJoin
- 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) 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。サーバーマネージャー UI (このチュートリアルでは推奨) Windows PowerShell またはを使用できます。

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
- 用の Active Directory モジュール Windows PowerShell
- 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 (Windows PowerShell) (オプション)

1. Windows 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 サーバーが適切に構成されていること、corp.example.com ドメインに接続できること、および管理対象の Microsoft AD フォレストの管理に使用できることを確認します。 AWS

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] に、このチュートリアルのステップ 2 AWS で管理対象の 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目してください。

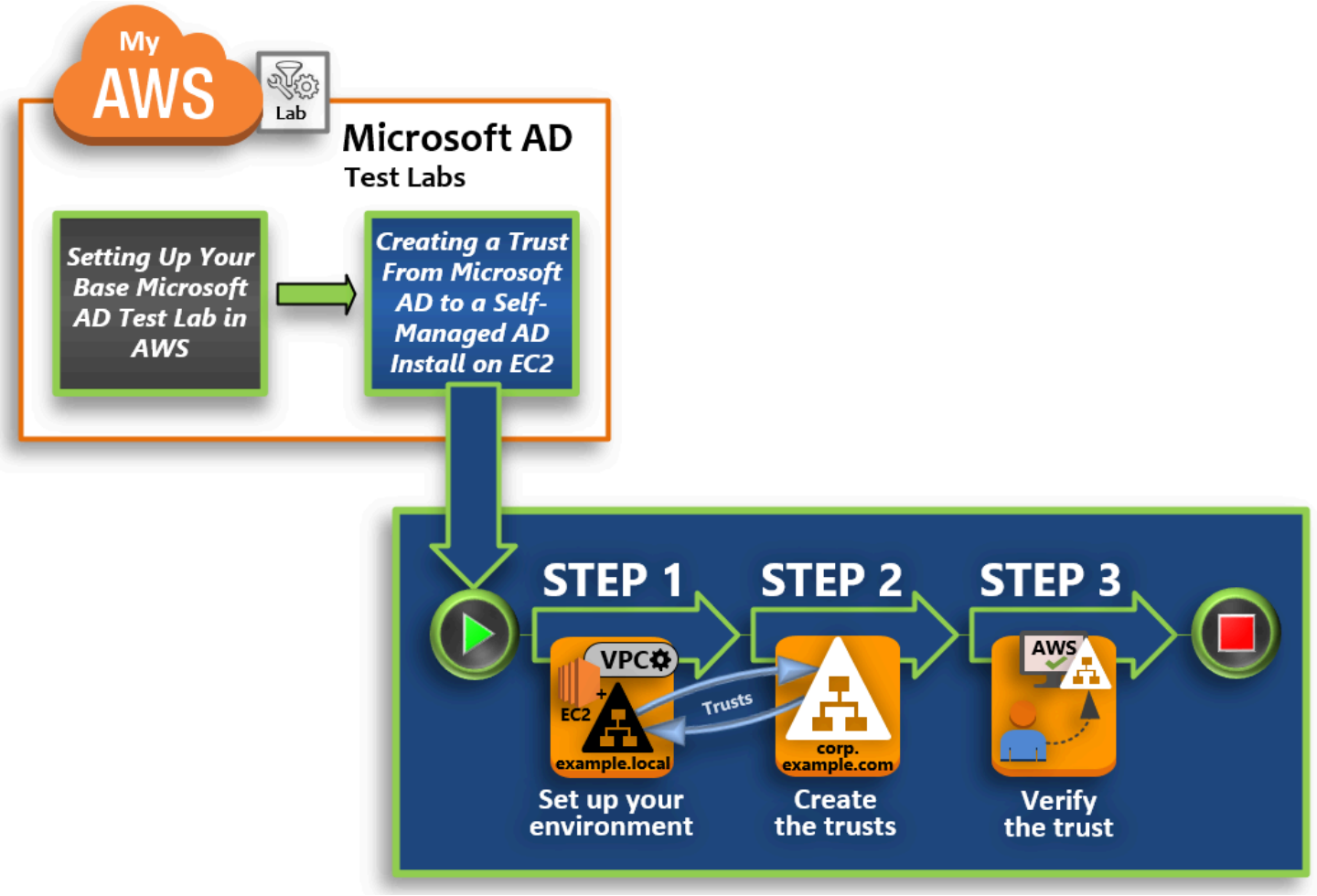
お疲れ様でした。これで、 AWS マネージド Microsoft AD ベーステストラボ環境が設定されました。このシリーズの次のテストラボを追加する準備が整いました。

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のクラウドベースの 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

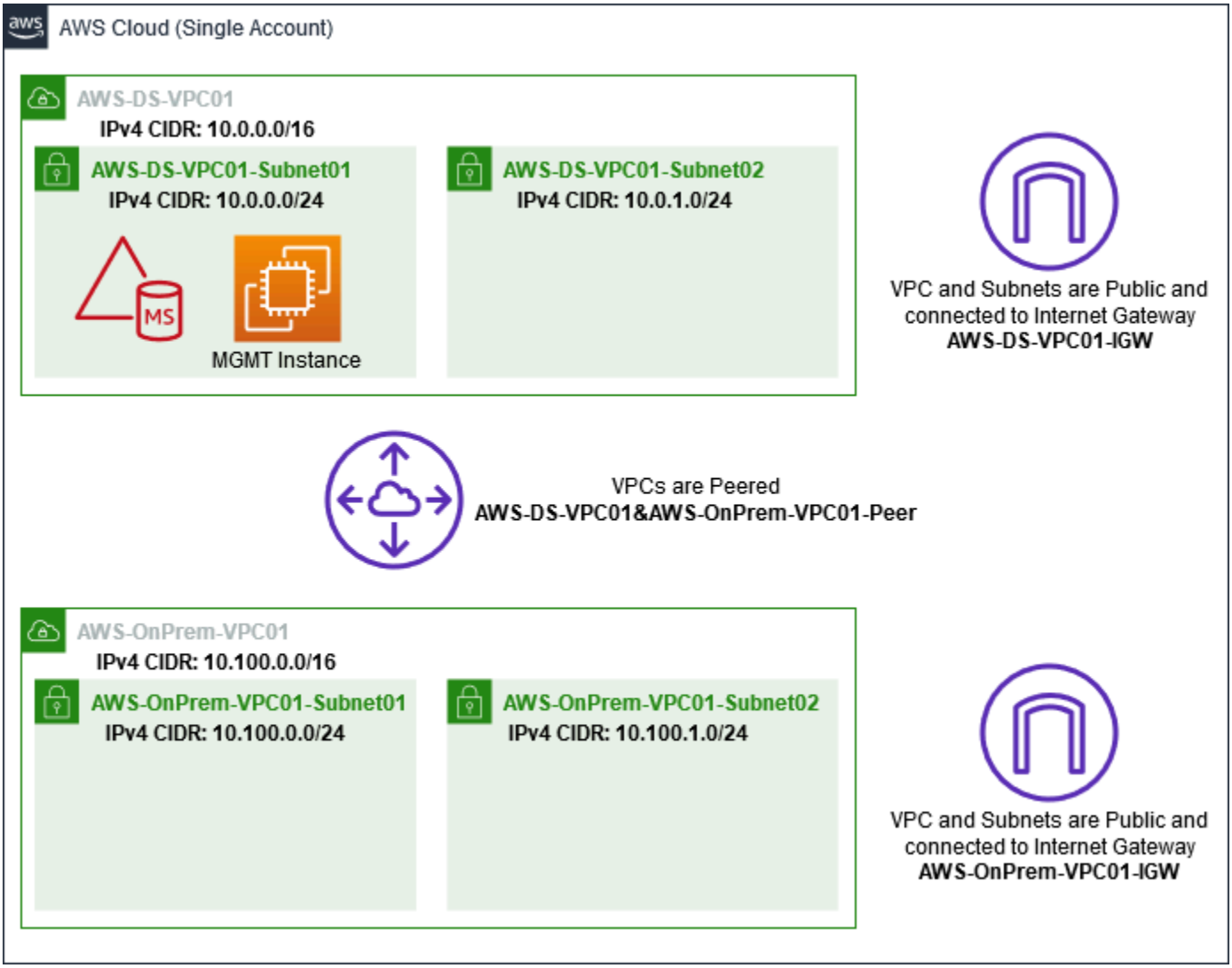
このステップでは、Amazon EC2 でホストされる新しく作成された Active Directory フォレストと の AWS Managed Microsoft AD フォレストの間に双方向のフォレスト信頼関係を作成しますAWS。

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、新しい信頼が動作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、 との信頼のために 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-***xxxxxxxxxxxxxxxx***] 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。
   - ネットワーク で、vpc-***xxxxxxxxxxxxxxxxx*** AWS-OnPrem-VPC01 を選択します (以前に基本チュートリアル で設定した) 。
   - サブネット で、subnet-***xxxxxxxxxxxxxxxxx*** | 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 で作成する場合は、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機能を指定」で、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. 追加オプションページで、EXAMPLE が NetBios ドメイン名としてリスト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、セキュリティグループ] 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で作成されます。

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、 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 を押します。2 つ目の 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「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 Managed Microsoft AD AWS のグローバル機能です。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、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。

Managed Microsoft AD から EC2 AWS 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と一致することを確認してください (EC2 ドメインから AWS Managed Microsoft AD への信頼を作成するには) 。

- [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じ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「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、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 のトラブルシューティング

以下のセクションは、ディレクトリ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。

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、 でのみ完了できます AWS Support。タスクの一部を次に示します。

- 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 マネージド Microsoft AD をアップグレードしてください.

サポートケースを作成するには、「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、パッチ適用をリリースしました。これらの安全な Netlogon の変更が導入されたため、一部の Netlogon 接続 (サーバー、ワークステーション、信頼検証) は AWS Managed Microsoft AD で受け入れられない場合があります。

問題が Netlogon または安全なチャネル通信に関連しているかどうかを確認するには、Amazon CloudWatch Logs でイベント IDs 5827 (デバイス認証関連の問題の場合) または 5828 (AD 信頼検証関連の問題の場合) を検索します。 AWS Managed Microsoft AD CloudWatch の については、「」を参照してください[ログ転送の有効化]。

CVE-2020-1472 に対する緩和策の詳細については、Microsoft ウェブサイトの、「CVE-2020-1472 に関連する Netlogon のセキュリティで保護されたチャネルの接続の変更を管理する方法」を参照してください。

ユーザーパスワードのリセットに関する問題

ユーザーのパスワードをリセットしようとすると、次のようなエラーメッセージが表示されます。

```
Response Status: 400 Bad Request
```

この問題は、同じユーザーログオン名を持つ 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、Simple AD または 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 ConsoleWindows PowerShellまたは を使用してパスワードをリセットできます AWS CLI。

詳細については、「ユーザーパスワードをリセットする」を参照してください。

追加リソース

以下のリソースは、 を使用する際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検索できます。
- AWS サポートセンター — テクニカルサポートを受けることができます。
- 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

- Microsoft イベントビューアーによる DNS サーバーの監視
- Linux ドメイン結合のエラー
- Active Directory の利用可能なストレージスペースの低下
- スキーマ拡張のエラー
- 信頼作成ステータスの理由

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 での DNS イベントを監査することで、DNS の問題の特定とトラブルシューティングがより簡単になります。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 Active Directory で作成される内容」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で、[Instances] (インスタンス) をクリックします。
3. AWS Managed Microsoft AD ディレクトリに結合している Amazon EC2 インスタンスを探します。対象のインスタンスを選択し、[Connect] (接続) をクリックします。
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. イベントビューワーウィンドウで [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. [Another computer] (別のコンピュータ) をクリックし、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た上で、[OK] をクリックします。
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。

Linux ドメイン結合のエラー

以下は、EC2 Linux インスタンスを AWS Managed Microsoft AD ディレクトリに結合する時に表示されることがある、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 Active Directory とオンプレミス AD との間で一方向の送信の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、ドメインに結合している Linux インスタンスに対し認証を試みた際に、認証に失敗することがあります。

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
```

Active Directory の利用可能なストレージスペースの低下

Active Directory の使用可能なストレージ領域が少ないために AWS Managed Microsoft AD が機能しなくなった場合は、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 ストレージの料金情報については、「 のAWS Directory Service 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、 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) AWS 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、 が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場合は、汎用名前付け規則 (UNC) によるパスを使用して SYSVOL 共有にアクセスできます。例えば、ドメインの完全修飾ドメイン名 (FQDN) が example.com である場合、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 分経っ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、リサイクルされた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、「 のAWS Directory Service 料金」を参照してください。

削除されたオブジェクトを含むディレクトリ内のオブジェクトの総数を取得するには、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 でユーザーとグループを管理する」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、空き領域の AWS Directory Service 再利用をリクエストします。

2. ディレクトリタイプが Standard Edition の場合、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する AWS Support でケースを開きます。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 委任された削除済み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 のごみ箱に保持される日数を設定する `msDS-DeletedObjectLifetime` 属性を変更できます。

> **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、「ディレクトリをスナップショットまたは復元する」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。この期間の長さを調整したい場合は、「30」を必要

な数値に置き換えます。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拡張の際に表示されることがある、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: AtrErr: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ましたが、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

信頼の作成が失敗した場合、その追加情報を含むステータスメッセージが表示されます。ここでの内容は、それらのメッセージの理解に役立ちます。

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、またはリモートドメインのセキュリティ設定で信頼を設定することを許可していません。この問題を解決するには、以下の手順を実行します。

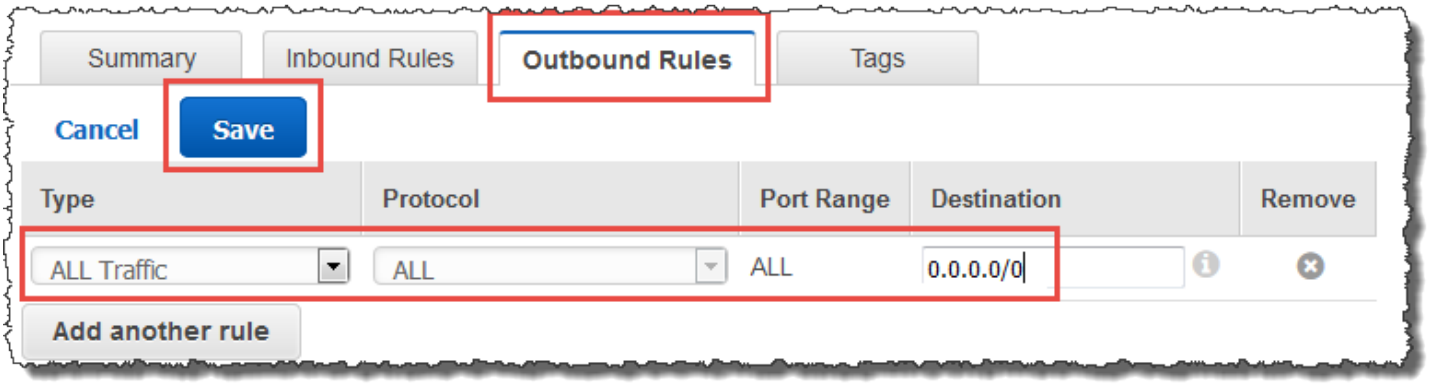
- AWS Managed Microsoft AD Active Directoryと信頼関係Active Directoryを作成するセルフマネージド は、同じファーストサイト名である必要があります。最初のサイト名は に設定されていますDefault-First-Site-Name。これらの名前がドメイン間で異なる場合、アクセス拒否エラーが発生します。
- リモートドメインで対応する信頼を作成する際に使用したものと、同じ信頼パスワードを使用していることを確認します。
- ドメインのセキュリティ設定で、信頼の作成を許可していることを確認します。
- ローカルセキュリティポリシーが正しく設定さ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NullSessionPipesレジストリパス HKLM\SYSTEM\servicesCurrentControlSet\LanmanServerParameters にあるレジストリキーの値 (複数) として存在することを確認します。これらの値は、別々の行に挿入される必要があります。

> **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 にあります。これらは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 (常時): 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 (サーバーが署名されている場合): 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 (常時): 有効
  - Microsoft ネットワークサーバー: 通信にデジタル署名 (クライアントが同意した場合): デフォルト: 有効

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。

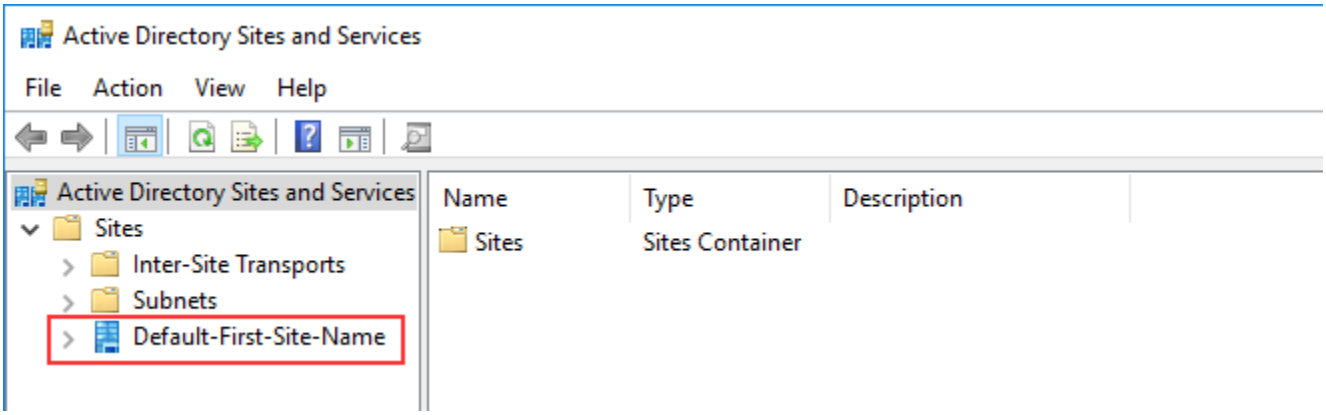
The Internet Assigned Numbers Authority (IANA) は、プライベートインターネット用に次の 3 つの IP アドレス空間ブロックを予約しています。

- 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。

これの仕組みの詳細については、 Microsoftウェブサイトの「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。



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のみです。また、以下の点を考慮してください。

- AWS Managed Microsoft AD は、シングル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、Microsoft「シングルラベルドメイン のサポート」を参照してください。
- RFC 1123 (https://tools.ietf.org/html/rfc1123) の規定では、DNSラベルで使用できる文字は「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のみです。

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への準拠」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 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、Systems Manager Automation を活用して、 用の定義済みランブックを提供します AWS Directory Service。 AWS AWSSupport-TroubleshootDirectoryTrust ランブックツールは、 AWS Managed Microsoft AD とオンプレミスMicrosoftの の間で発生する信頼作成に関する一般的な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 とオンプレミスの 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の例については、 Microsoftウェブサイトの「Netdom」と「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、Microsoft Active Directoryクラウドに情報をキャッシュせずにディレクトリ要求をオンプレミスにリダイレクト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を処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を処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 Directorey 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 Acti e 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 AWS は他のアカウントと共有できません。これが必要な場合は、 AWS マネージド Microsoft AD を使用して次のことを行うことを検討してくださいディレクトリの共有。また、AD ConnectorはマルチVPCに対応していないため、 AWS WorkSpacesこのような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 や Amazon AWS などのアプリケーションにログオンできます WorkMail。
- への IAM ロールベースのアクセスにより、Amazon EC2 インスタンスや Amazon S3 AWS バケットなどのリソースを管理できます。 AWS Management Console
- ユーザーや IT 管理者がオンプレミスインフラストラクチャまたはクラウド内のリソースにアクセスしてい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、アカウントロックアウトなど) を一貫して適用できます。 AWS
- 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できます。これにより、ユーザーがアプリケーションにアクセスする際のセキュリティを強化できます。 AWS

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 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すると、すべてのディレクトリデータはドメインコントローラーに残ります。 AWS Directory Service はディレクトリデータをレプリケートしません。

トピック

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

の詳細については AWS Direct Connect、「 AWS Direct Connect ユーザーガイド」を参照してください。

既存 Active Directory

Active Directory ドメインを使用して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
- コンピュータをドメインに結合する - シームレスなドメイン結合と を使用する場合にのみ必要です WorkSpaces
- 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 を使用する場合にのみ必要です WorkSpaces
- サービスアカウントのパスワードは、 AWS パスワード要件に準拠している必要があります。AWS パスワードは、次の条件を満たす必要があります。
  - 8 ~ 128 文字の長さ。
  - 次の 4 つのカテゴリのうち 3 つから少なくとも 1 文字を含む。
    - 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許可に 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ユーザーとして LDAP オペレーションを実行する 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 の SRV リソースレコードを参照してください TechNet。

サブネット用のポート

AD Connector がディレクトリリクエストを既存のActive Directoryドメインコントローラーに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 内の両方のサブネットの CIDRs に次のポートが開いている必要があります。

- 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 を使用する場合は WorkSpaces、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 と連携できなくなります Amazon WorkSpaces。

> **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、そ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 内の両方のサブネットの CIDRs に対して上記のポートを開く必要があります。

その他のポート要件については、 Microsoftドキュメントの「AD および 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。この設定の一般的な情報については、「 の事前認証」を参照してください Microsoft TechNet。

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Multi-Factor Authentication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、 という名前の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。

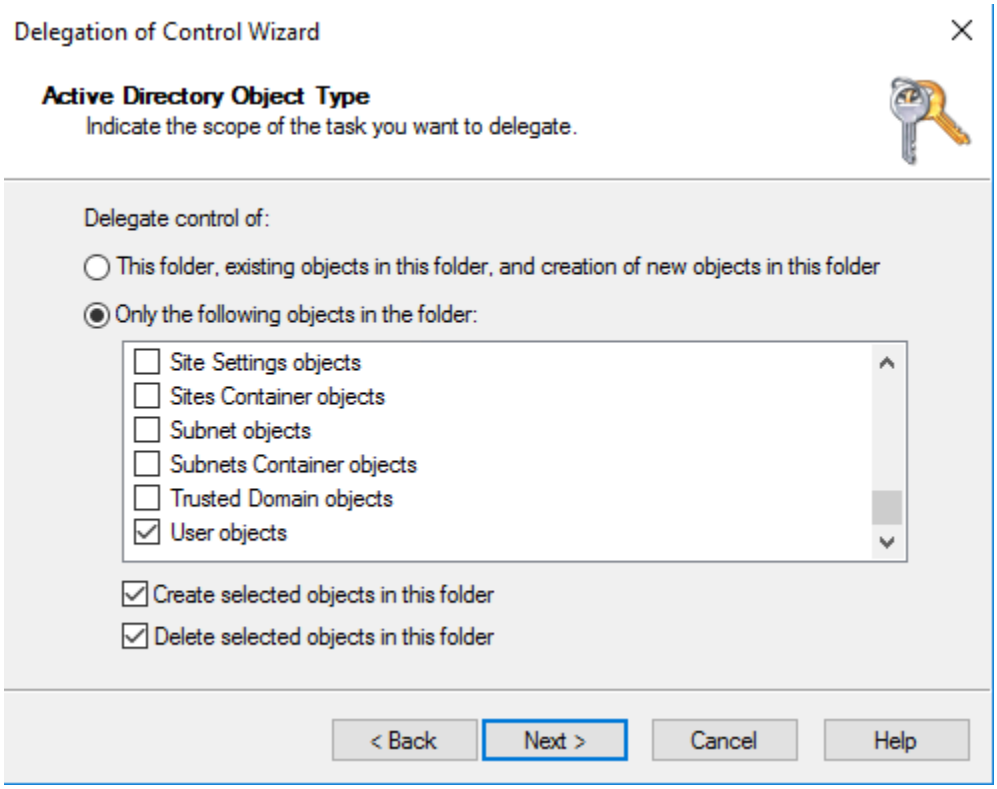
権限をサービスアカウントに委任するには

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

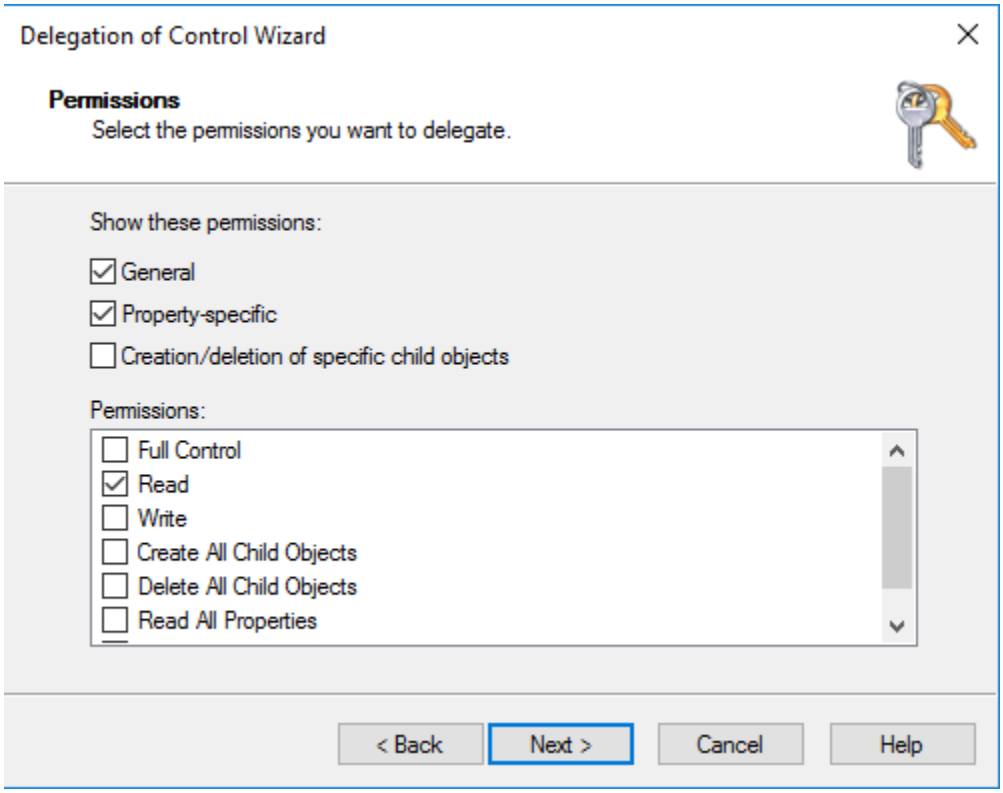
4. [Active Directory User and Computers] (Active Directory ユーザーとコンピュータ) ナビゲーションツリーで、ドメインルートを選択します。メニューで [Action] (アクション) を選択し、[Delegate Control] (制御を委任する) を選択します。AD Connector が AWS Managed Microsoft AD に接続されている場合、ドメインのルートレベルで制御を委任するアクセス権限はありません。この場合、制御を委任するには、コンピュータオブジェクトが作成されるディレクトリ OU で OU を選択します。
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**
>
> シームレスドメイン結合または を使用する場合は WorkSpaces、Active Directory がコンピュータオブジェクトを作成できるように、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、Connectors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ます。

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、ドメインと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.Write("Checking UDP port {0}: ", port);

                UdpClient udpClient = new UdpClient();

                try
                {
                    udpClient.Connect(_ipAddr, port);
                    udpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }
    }
}
```

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ー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ー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ー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 は自己管理型 Active Directory のドメインコントローラーにリクエストを転送して認証を行います。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 の管理方法

このセクションでは、AD Connector 環境を運用および維持するすべての手順を一覧表示します。

トピック

- 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
- Amazon EC2 インスタンスを に結合する Active Directory
- AD Connector ディレクトリを維持する
- 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 DNS アドレスを更新する

AD Connector ディレクトリをセキュリティで保護する

このセクションでは、AD Connector 環境をセキュリティで保護する際の考慮事項について説明します。

トピック

- AWS Directory Service の AD Connector サービスアカウントの認証情報を更新する
- AD Connector のMulti-Factor Authenticationを有効にする
- AD Connector を使用してクライアント側 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 認証を有効にする
- AWS Private CA Connector for AD をセットアップする

AWS Directory Service の AD Connector サービスアカウントの認証情報を更新する

AWS Directory Service で指定した AD Connector の認証情報は、既存のオンプレミスのディレクトリへのアクセスに使用するサービスアカウントを表します。AWS Directory Service のサービスアカウントの認証情報を変更するには、次の手順を実行します。

> **Note**
>
> ディレクトリに対して AWS IAM Identity Center が有効になっている場合、AWS Directory Service 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。

AWS Directory Service の AD Connector サービスアカウントの認証情報を更新するには

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 [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。

AD Connector のMulti-Factor Authenticationを有効にする

オンプレミスまたは EC2 インスタンスで Active Directory を実行している場合は、AD Connector の Multi-Factor·Authentication を有効にすることができます。AWS Directory Service でのMulti-Factor Authenticationを使用の詳細については、「AD Connector の前提条件」を参照してください。

> **Note**
>
> Multi-Factor Authenticationは、Simple AD では使用できません。ただし、MFA は AWS Managed Microsoft AD ディレクトリで有効にすることができます。詳細については、「AWS マネージド Microsoft AD のマルチファクタ認証を有効にする」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、AWS Management Console へのアクセス、または、WorkSpaces、Amazon QuickSight、Amazon Chime などの Amazon エンタープライズ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。EC2 インスタンス上で実行されている、または EC2 インスタンスにサインインするための Windows ワークロードに MFA を入力することはありません。 AWS Directory Service では、RADIUS チャレンジ/レスポンス認証はサポートされていません。
   > 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。オンプレミスのネットワークで、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) を介したインバウンドトラフィックが許可されている必要があります。

[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 LDAPS を有効にする

AD Connector のクライアント側 LDAPS のサポートにより、Microsoft Active Directory (AD) と AWS アプリケーション間の通信が暗号化されます。このようなアプリケーションには、WorkSpaces、AWS IAM Identity Center、Amazon QuickSight、Amazon Chime などがあります。この暗号化により、組織の ID データの保護を強化し、セキュリティ要件を満たすことができます。

トピック

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

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 アプリケーションの LDAP トラフィックは TCP ポート 636 で排他的に実行され、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 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、AD Connector のポート 636 (アウトバウンド) および自己管理型 Active Directory (インバウンド) での TCP 通信を許可します。

クライアント側 LDAPS を有効にする

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。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。次の AWS Management Console または AWS CLI のいずれかの方法を使用します。

トピック

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

以下のいずれかの方法を使用して、AWS Directory Service で証明書を登録します。

方法 1: AWS Directory Service で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. [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: AWS Directory Service で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。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 Service で証明書登録ステータスを確認するには (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. [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 Service で証明書登録ステータスを確認するには (AWS CLI)

- 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

以下のいずれかの方法を使用して、AWS Directory Service でクライアント側 LDAPS を有効にします。

> **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 でクライアント側 LDAPS を有効にするには (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. [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 でクライアント側 LDAPS 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-ldaps --directory-id your_directory_id --type Client
```

ステップ 4: LDAPS ステータスを確認する

以下のいずれかの方法を使用して、AWS Directory Service の LDAPS ステータスを確認します。

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

- 次のコマンドを実行します。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。次の AWS Management Console または AWS CLI のいずれかの方法を使用します。

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 Service で証明書の詳細を表示するには (AWS Management Console)

1. AWS Directory Service コンソールのナビゲーションペインで、[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 Service で証明書の詳細を表示するには (AWS CLI)

- 次のコマンドを実行します。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 Service で証明書を登録解除するには (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. 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 Service で証明書を登録解除するには (AWS CLI)

- 次のコマンドを実行します。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 でクライアント側 LDAPS を無効にするには (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. [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 でクライアント側 LDAPS を無効にするには (AWS CLI)

- 次のコマンドを実行します。

```
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 認証を有効にする

スマートカードによる証明書ベースの相互トランスポート層セキュリティ (mTLS) 認証を使用して、自己管理型の Active Directory (AD) と AD Connector WorkSpaces を通じて Amazon へのユーザーを認証できます。有効にすると、 WorkSpaces ユーザーはログイン画面でスマートカードを選択し、ユーザー名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 AWS リージョン、次の場合にのみ使用でき、とのみ使用できます WorkSpaces。現時点では、 AWS 他の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)

トピック

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証明書ベースの相互トランスポート層セキュリティ (mTLS) 認証を有効にするには、セルフマネージド型と統合された運用可能なスマートカードインフラストラクチャが必要です。Active DirectoryAmazon WorkSpaces およびでのスマートカード認証の設定方法の詳細についてはActive Directory、『Amazon WorkSpaces 管理ガイド』を参照してください。

のスマートカード認証を有効にする前に WorkSpaces、以下の考慮事項を確認してください。

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。
- 証明書伝達サービスが [自動] に設定され、実行中であ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は次のとおりです。

- ユーザーのスマートカード証明書には、ユーザーの UPN (サブジェクト代替名) のサブジェクト代替名 userPrincipalName (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) として拡張キー使用法が設定されています。
- 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、権限情報アクセスの「アクセス方法」=「オンライン証明書ステータスプロトコル (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。ログイン、パスワードのリセット、接続などの Amazon WorkSpaces の問題のトラブルシューティングについては、Amazon WorkSpaces ユーザーガイドの「 WorkSpaces クライアントの問題のトラブルシューティング」を参照してください。WorkSpaces WorkSpaces

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 に準拠している必要があります。さらに、OCSP サーバーは、合計 255 バイト以下の要求に対する GET メソッドを使用する要求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。

その他の考慮事項

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。他の種類の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でも動作するかもしれませんが、 WorkSpacesストリーミングプロトコル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、ユーザー名とパスワードによる認証に代わるものです。 WorkSpaces

  スマートカード認証が有効になっている AD Connector AWS ディレクトリに他のアプリケーションが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する

AD WorkSpaces Connectorで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。 AWS Directory Service コンソール、API、または CLI

を使用して CA 証明書を 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。

トピック

- ステップ 1: AD Connector サービスアカウントの Kerberos 制約付き委任を有効にする
- ステップ 2: AD Connector に CA 証明書を登録する
- ステップ 3: 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する

ステップ 1: AD Connector サービスアカウントの Kerberos 制約付き委任を有効にする

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。この機能により、管理者は、アプリケーションサービスがユーザーを代行できる範囲を制限することによって、アプリケーションの信頼の境界を指定および適用できます。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 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 SAM AccountName と一致する必要があります。SAM AccountName は 20 文字に制限されています。SAM AccountName 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いました。

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、を使用してこのプロセスを自動化することもできます PowerShell。

ステップ 2: AD Connector に CA 証明書を登録する

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。

ステップ 3: 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する

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)

1. [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。
2. [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。

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 メソッドとメソッドのどちらでも使用できます。 AWS CLI

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 Service (AWS 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 Service (AWS 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ます。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 Service ()AWS Management Consoleで証明書を登録解除するには

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 Service で証明書を登録解除するにはAWS CLI

- 以下のコマンドを実行します。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ます。

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

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

セルフマネージド Active Directory (AD) を AWS Private Certificate Authority AD Connector と統合して、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。AD 用 AWS Private CA コネクタを使用すると、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、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 の完全マネージド型 AWS Private CA ドロップインリプレースメントを使用できます。

ディレクトリと AWS Private CA の統合は、Directory Service コンソール、 AWS Private CA Connector for AD コンソール、または `CreateTemplate` API を呼び出して設定できます。 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、「AWS Private CA Connector for Active Directory」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手順については、以下を参照してください。

前提条件

AD Connector を使用するには、サービスアカウントに追加のアクセス許可を委任する必要があります。サービスアカウントにアクセスコントロールリスト (ACL) を設定して、次の操作を行えるようにします。

- サービスプリンシパル名 (SPN) をそれ自体に対して追加および削除します。
- 以下のコンテナで証明機関を作成および更新します。

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

- 次の例のように、NT AuthCertificates 認証機関オブジェクトを作成して更新します。NT AuthCertificates 認証機関オブジェクトが存在する場合は、そのオブジェクトのアクセス許可を委任する必要があります。オブジェクトが存在しない場合は、Public Key Services コンテナに子オブジェクトを作成する権限を委任する必要があります。

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

> **Note**
>
> AWS Managed Microsoft AD を使用している場合、ディレクトリで AWS Private CA Connector for AD サービスを承認すると、追加のアクセス許可が自動的に委任されます。

次の PowerShell スクリプトを使用して、追加のアクセス許可を委任し、NT AuthCertifiates 認証機関オブジェクトを作成できます。「myconnectoraccount」をサービスアカウント名で置き換えてください。

```
$AccountName = 'myconnectoraccount'

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

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

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

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

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

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

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

```
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

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

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

AWS Private CA Connector for AD をセットアップするには

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. Connector for AD のネットワークとセキュリティタブで、 AWS Private CA Connector for AD の設定を選択します。 AWS Private CA のプライベート CA 証明書を作成する Active Directory ページが表示されます。コンソールの手順に従って、 Private CA に登録するActive Directoryコネクタ用の Private CA を作成します。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、以下の手順に従って、コネクタのステータスや関連するプライベート CA のステータスなどの詳細を表示します。

AWS Private CA Connector for AD を表示するには

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. [ネットワークとセキュリティ] の [AWS Private CA Connector for AD] 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。クリックすると、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 コネクタと 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 コネクタが作成された日。

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 Connector ディレクトリをモニタリングする

AD Connector ディレクトリは以下の方法でモニタリングできます。

トピック

- ディレクトリのステータスを把握する
- Amazon SNS でディレクトリステータス通知を設定する

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 Support 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については、40 AWS 分以内に問題を解決します。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 Support 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、「ディレクトリをスナップショットまたは復元する」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 でディレクトリステータス通知を設定する

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 AWS Directory Service トピックに発行者として を追加できます。Amazon SNS 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。

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**
>
> DirectoryServiceFullAccess マネージド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 の権限が追加で必要です。

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 コンソールからこれを行うことができます。

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、 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 EC2 インスタンスを に結合する Active Directory

AD Connector は、クラウドに情報をキャッシュMicrosoftActive Directoryすることなく、ディレクトリリクエストをオンプレミスにリダイレクトできるディレクトリゲートウェイです。Amazon EC2 を Active Directory に結合する方法の詳細について説明します

- インスタンスの起動時に、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、「AD Connector を使用して Amazon EC2 Windowsインスタンスを AWS Managed Microsoft AD にシームレスに結合する」を参照してください。
- 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**
>
> インスタンスをセルフマネージド Active Directory (オンプレミス) に結合すると、インスタンスは と直接通信Active Directoryし、AD Connector をバイパスします。

トピック

- AD Connector を使用して Amazon EC2 Windowsインスタンスを AWS Managed Microsoft AD にシームレスに結合する
- AD Connector を使用して Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD にシームレスに結合する

AD Connector を使用して Amazon EC2 Windowsインスタンスを AWS Managed Microsoft AD にシームレスに結合する

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Active Directory。

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、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。

   a. 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。

   b. 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。

   c. 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。

   d. [キーペアの作成] を選択します。

   e. 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。

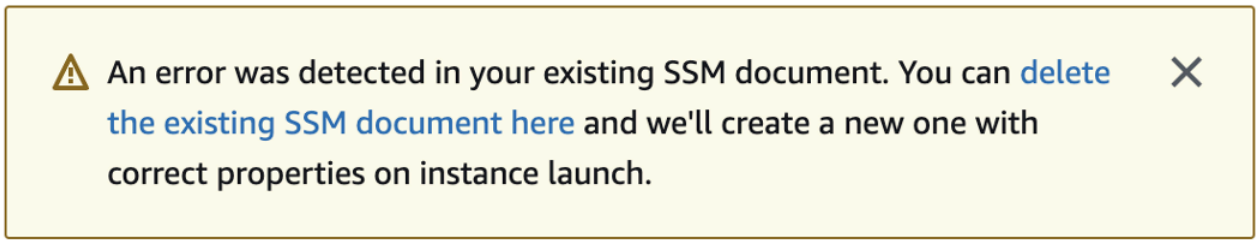
11. [自動割り当てパブリック IP] で、[有効化] を選択します。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>
>
> 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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
> - 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持つ 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。AmazonSSMManagedInstanceCore がアAmazonSSMDirectoryServiceAccessタッチされた AWS 管理ポリシーを持つ 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 プロファイルリンクの作成 を選択し、次の操作を行います。

    1. [ロールの作成] を選択します。
    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] を選択します。
    4. アクセス許可の追加 で、ポリシーのリストで 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] をクリックします。

> **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] を選択します。
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. [Launch instance (インスタンスの起動)] を選択します。

AD Connector を使用して Amazon EC2 Linux インスタンスを 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 AWS Managed Microsoft AD ディレクトリ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 より前のディストリビューションでは、シームレスなドメイン結合機能はサポートされていません。

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

AD Connector を使用して、Linux コンピュータをオンプレミス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、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。必要に応じて、AD Connector サービスアカウントを使用できます。または、コンピュータをドメインに結合するのに十分な権限を持つ他のアカウントを使用することもできます。ドメイン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ための十分な権限を持っている場合がありますが、これらを使用することはお勧めしません。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の必要最小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。

コンピュータをドメインに結合するために必要な最小限の権限を持つアカウントを委任するには、次の PowerShell コマンドを実行します。これらのコマンドは、 管理対象の Microsoft AD AWS 用アクティブディレクトリ管理ツールのインストールがインストールされているドメインに参加している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。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。

```
$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 の説明に従って手動プロセスを使用できます。

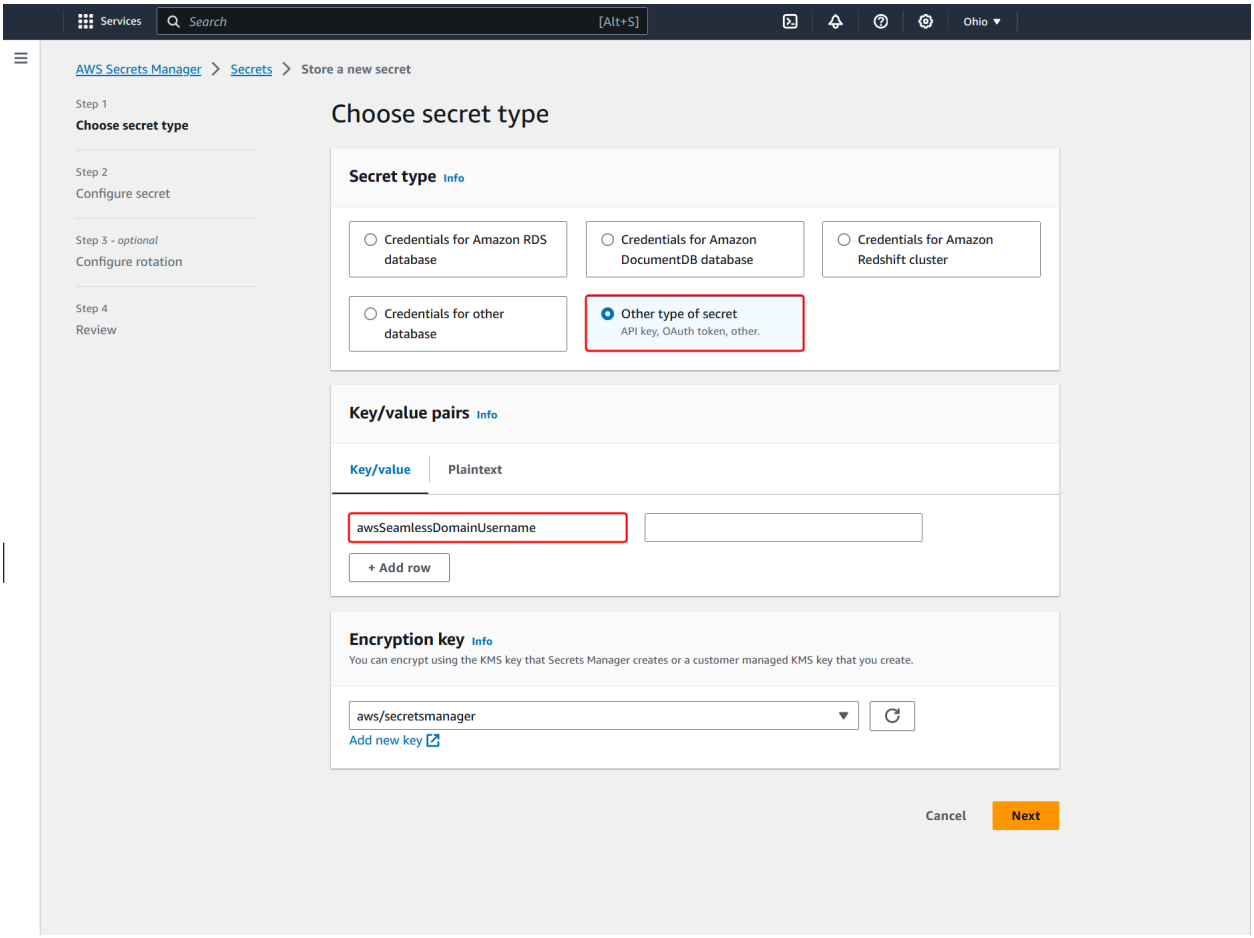
ドメインサービスアカウントを保存するシークレットを作成する

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。

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 になります**awsSeamlessDomain**。

> **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。



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。

> **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/secretsmanagerが作成する AWS マネージドキーを使用して、シークレットを無料で暗号化できます。独自の KMS キーを作成してシークレットを暗号化すると、 は現在の AWS KMS レートで AWS 課金します。詳細については、「AWS Key Management Service の料金」を参照してください。

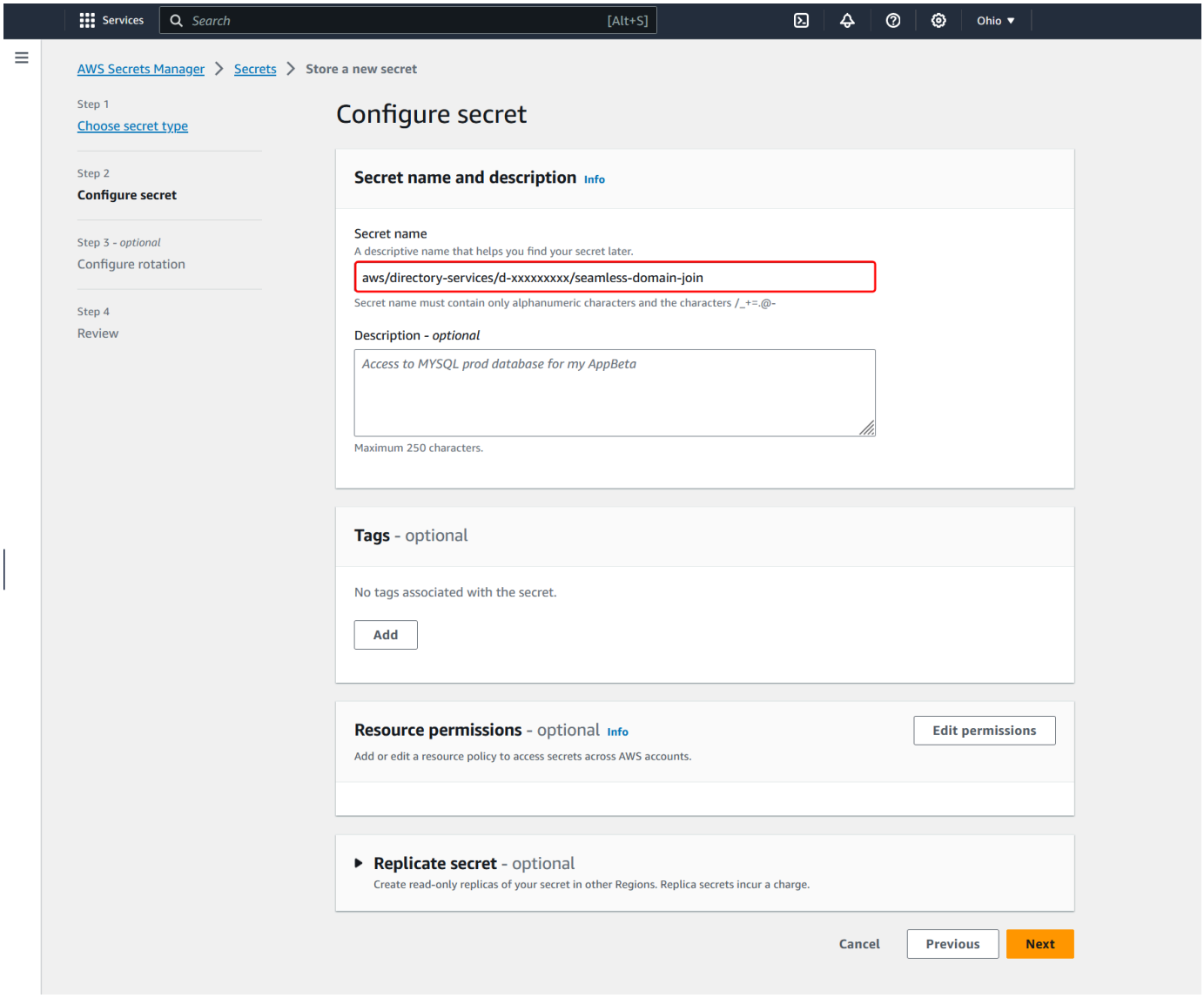
v. [次へ] をクリックします。

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-xxxxxxxxx/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-xxxxxxxxx*/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。



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 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。

  ステップ 5 では、「 AWS Secrets Manager ユーザーガイド」の「Microsoft Active Directory の認証情報」のローテーションテンプレートを使用します。

  ヘルプについては、「 ユーザーガイド」の AWS Secrets Manager 「ローテーションのトラブルシューティングAWS Secrets Manager 」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

以下の前提条件のステップを使用して、Secrets Manager のシームレスなドメイン結合シークレット (以前に作成したもの) 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。

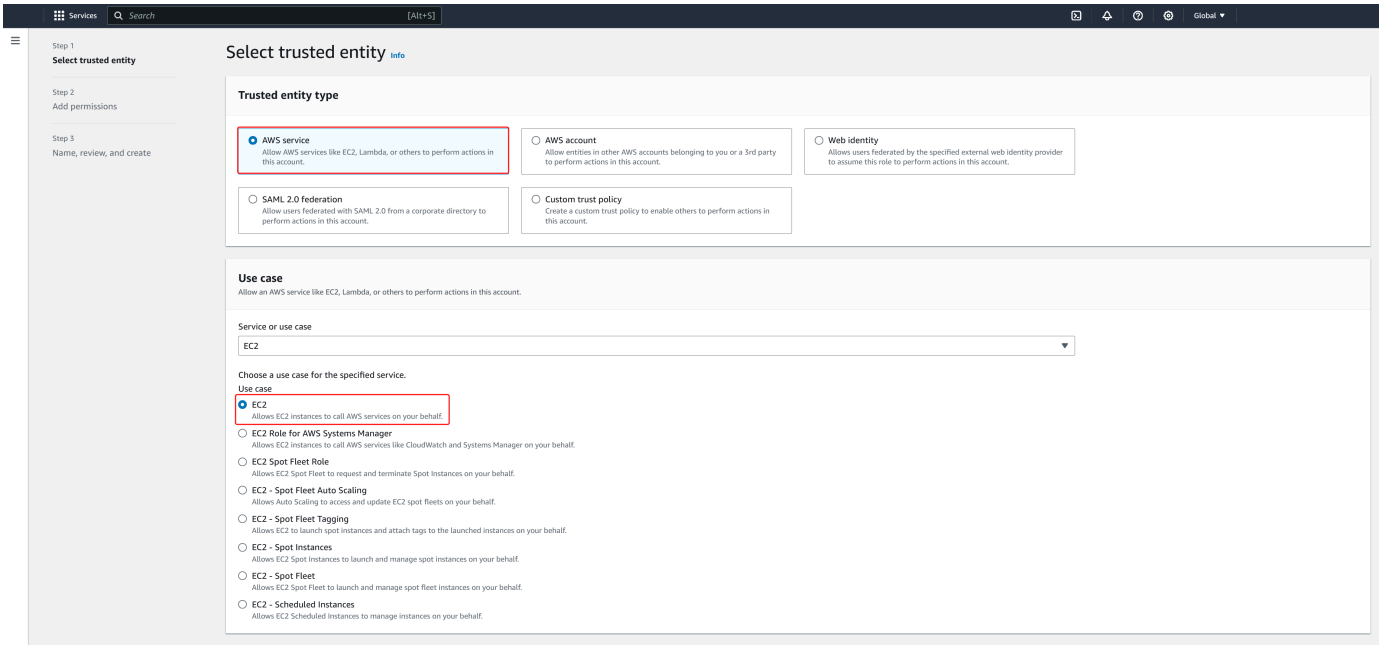
> **Note**
>
> シークレットごとに 1 つのポリシーを作成することをお勧めします。そうすることで、インスタンスが適切なシークレットにのみアクセスできるようになり、インスタンスが侵害された場合の影響を最小限に抑えることができます。

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。



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] を選択します。

Amazon EC2 Linux インスタンスを AWS Managed Microsoft AD にシームレスに結合する Active Directory

すべての前提条件タスクを設定したので、次の手順に従い EC2 Linux インスタンスをシームレスに結合できます。

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. (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. 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ときにaws:domainJoinプラグインを使用します。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。

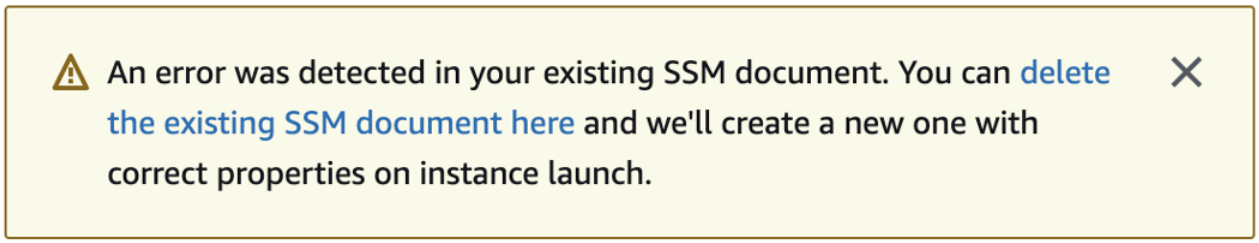
11. [自動割り当てパブリック IP] で、[有効化] を選択します。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>
>
> 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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
> - 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持つ 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 で、「前提条件」セクションの「ステップ 2: LinuxEC2DomainJoin role を作成する」で以前に作成した IAM ロールを選択します。
16. [Launch instance (インスタンスの起動)] 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。

AD Connector ディレクトリを維持する

このセクションでは、AD Connector 環境の一般的な管理タスクを維持する方法について説明します。

トピック

- AD Connector を削除する
- ディレクトリ情報の表示

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 AWS リージョン Connectorが導入されている場所にいることを確認してください。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 AWS Connectorの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 アプリケーションが有効になっていると、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 アプリとサービス] セクションには、AD AWS Connectorで有効になっている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へのアクセスを無効にする」を参照してください。
- Amazon を無効にするには WorkSpaces、 WorkSpaces コンソールの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「ディレクトリからの登録解除」を参照してください。
- Amazon を無効にするには WorkDocs、Amazon WorkDocs コンソールで Amazon 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 管理ガイド』の「サイトの削除」を参照してください。
- Amazon を無効にするには WorkMail、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 管理者ガイド』の「組織の削除」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 ユーザーガイド』の「FSx for Windows File Server 操作」を参照してください。Active Directory
- 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、Client 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』Active Directoryの「認証」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「Amazon Connect インスタンスの削除」を参照してください。
- アマゾンを無効にするには QuickSight、アマAmazon QuickSight ンの購読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 アカウントの解約」を参照してください。

> **Note**
>
> AWS IAM Identity Center 使用していて、 AWS 削除する予定の管理対象Microsoft ADディレクトリに以前に接続したことがある場合は、削除する前にまずアイデンティティ・ 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。

ディレクトリ情報の表示

ディレクトリに関する詳細情報を表示できます。

詳細なディレクトリ情報を表示するには

1. AWS Directory Service コンソールナビゲーションペインの でActive Directory、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 リンクをクリックします。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。

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 に、Amazon などの AWS アプリケーションやサービスに WorkSpaces へのアクセスを許可する場合がありますActive Directory。AD Connector と連携するには、以下の 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、「Amazon Chime 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
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、「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	Simple AD、 AWS Managed Microsoft AD、または AD Connector は、 から直接作成できます WorkSpaces。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 Client VPN	詳細については、『AWS Client VPN ユーザーガイド』を参照してください。
AWS IAM Identity Center	詳細については、『AWS IAM Identity Center ユーザーガイド』を参照してください。
AWS Management Console	詳細については、「AD 認証情報による AWS Management Console へのアクセスを有効化する」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検索するには、次のステップを実行します。

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承認または承認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承認 AWS Directory Service]。

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 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 Active Directoryに接続するだけです 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互換性を備えた低コストの低スケールディレクトリです。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 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 Active Directory」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 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、ピア接続またはサイズ変更された VPCs 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、セキュリティグループ AWS を設定して、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ます。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、ディレクトリに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**
>
> 技術的には、ディレクトリのセキュリティグループを、ユーザー作成した他の EC2 インスタンスと関連付けることができます。ただし、この方法にはお勧め AWS しません。 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、セキュリティグループを予告なしに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、、Amazon 、 WorkSpacesAmazon 、または Amazon 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 WorkDocs WorkMail QuickSight。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、「AWS Directory Service の AD Connector サービスアカウントの認証情報を更新する」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 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 AWS Directory Service。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 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
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 のアプリケーションの互換性ポリシー

Microsoft Active Directory (AWS Managed Microsoft AD) の AWS Directory Service の代替として機能する AD Connector は、AWS で作成されたアプリケーションとサービスのみの 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ログインするとき、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。

互換性のある AWS のアプリケーションとサービスのリストを次に示します。

- 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 Acttive Directorty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 に結合する Active Directory」を参照してください。
- AWS Management Console – AD Connector を使用して、AWS Management Console ユーザーを Active Directory の認証情報を使用して認証できます。SAML インフラストラクチャを設定する必要はありません。詳細については、「AD 認証情報による AWS Management Console へのアクセスを有効化する」を参照してください。
- Amazon QuickSight - 詳細については、「Amazon 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、「オンプレミスの Active Directory にIAM Identity Center を接続する」を参照してください。
- AWS Transfer Family - 詳細な手順については、「AWS Directory Service for Microsoft Active Directory を使用する」を参照してください。
- AWS Client 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。
- Amazon WorkDocs - 詳細な手順については、「Connecting to your on-premises directory with AD Connector」(オンプレミスのディレクトリを AD Connector に接続する) 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 のみと互換性があり、AD Connector との互換性はありません。詳細については、「AWS Directory Service よくある質問」ページの AWS Managed Microsoft AD のセクションを参照してください。

AD Connector のトラブルシューティング

以下は、AD Connectorを作成または使用するときに発生する可能性の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。

トピック

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

2012 AWS 年以前に作成されたアカウントの中には、 AWS Directory Service ディレクトリをサポートしない米国東部 (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ーゾーンにアクセスできるものがあります。の作成時にこのよう

なエラーが表示された場合はActive Directory、別のアベイラビリティーゾーンのサブネットを選択し、ディレクトリをもう一度作成してみてください。

AD Connector を作成しようとすると、「接続の問題が検出されました」というエラーが表示されます

AD Connectorを作成しようとしたときに「接続の問題が検出されました」というエラーが表示される場合は、ポートの可用性またはAD Connectorの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、以下のポートが使用できる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、を参照してくださいAD Connector をテストする。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参加している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したら、AD Connector のパスワードを確認します。AD Connector AWS はパスワードの複雑さの要件を満たす必要があります。詳細については、の「サービスアカウント」を参照してくださいAD Connector の前提条件。

お使いの 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で AD Connector を再作成してください。

接続の問題

AD Connector の一般的な接続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と、「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と、「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と、「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と、「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。

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

AD Connector 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、以下のリストを参照してください。が使用するポートについて詳しくはActive Directory、Microsoftドキュメントの「Active Directoryドメインとトラスト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と、「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と、「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。

認証に関する問題

AD Connector の一般的な認証問題を次に示します。

- Amazon WorkSpaces スマートカードを使用して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ます。
- 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、「Unable to Authenticate」というエラーが表示されます。
- AD Connector サービスアカウントを更新しようとすると、ディレクトリの認証情報に関するエラーが表示されます
- 一部のユーザーがディレクトリで認証されない

Amazon WorkSpaces スマートカードを使用して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ます。

WorkSpaces スマートカードを使用してにサインインしようとすると、次のようなエラーメッセージが表示されます。

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

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、を参照してください前提条件。

次の手順に従って、スマートカードがユーザーの証明書ストアに証明書を保存できるかどうかをトラブルシューティングします。

1. 証明書にアクセスできないデバイスで、Microsoft Management Console (MMC) にアクセスします。

   > **Important**
   >
   > 次に進む前に、スマートカードの証明書のコピーを作成してください。

2. MMC の証明書ストアに移動します。ユーザーのスマートカード証明書を証明書ストアから削除します。MMC で証明書ストアを表示する方法の詳細については、ドキュメントの「方法:MMC スナップインで証明書を表示する」を参照してください。Microsoft
3. スマートカードを取り外します。
4. スマートカードを再挿入して、スマートカード証明書をユーザーの証明書ストアに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ユーザーストアに再入力していない場合、スマートカード認証には使用できません。 WorkSpaces

AD Connector のサービスアカウントには以下が必要です。

- my/spnサービスプリンシパル名に追加
- LDAP サービスに委任されました。

証明書がスマートカードに再入力されたら、オンプレミスの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名 (UPN) マッピングからブロックされているかど

うかを確認する必要があります。この変更について詳しくは、ドキュメントの「UPN マッピングのサブジェクト代替名を無効にする方法」を参照してください。Microsoft

以下の手順に従って、ドメインコントローラーのレジストリキーを確認してください。

1. レジストリエディターで、次の Hive キーに移動します。

   HKEY_LOCAL_MACHINE\ SYSTEM\\ Services\ Kdc\ CurrentControlSet UseSubjectAltName

2. UseSubjectAltName選択。値が 0 に設定されていることを確認します。

> **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に設定されている場合、AD Connectorは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。Active Directory

認証局 (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 の追加要件を以下に示します。

- 証明書は、ドメインコントローラ、認証局サーバ、およびの信頼されたルート認証局にある必要があります WorkSpaces。
- オフライン証明書とルート 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、失効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 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 NTAuth ストアに公開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、認証局サーバー、およびの信頼されたルート機関にインストールする必要があります。 WorkSpaces
  - 以下のコマンドを使用して、証明書を Active Directory NTAuth ストアに公開できます。

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

証明書を NAuth ストアに公開する方法の詳細については、『Access Amazon WorkSpaces with Common Access Cards インストールガイド』の「発行元の CA 証明書を Enterprise NAuth ストアにインポートする」を参照してください。

次の手順に従って、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できます。

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、エクスポートし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 Certficate_name.cer
```

4. コマンドの後に、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。ステータスは「確認済み」に戻るはずです。

certutil コマンドの詳細については、ドキュメンテーションの certutil を参照してください。
Microsoft

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。

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、「Unable to Authenticate」というエラーが表示されます。

AD Connectorのステータスがアクティブであっても QuickSight、 AWS WorkSpaces またはAmazon などのアプリケーションを使用しているときにユーザーを検索すると、エラーが発生することがあります。認証情報が期限切れになると、AD Connector が Active Directory 内のオブジェクトのクエリを完了できなくなる可能性があります。に記載されている手順に従って、Amazon EC2 インスタンスのシームレスドメイン参加が機能しなくなったサービスアカウントのパスワードを更新します。

AD Connector サービスアカウントを更新しようとすると、ディレクトリの認証情報に関するエラーが表示されます

AD Connector サービスアカウントを更新しようとすると、次の 1 つまたは複数のエラーメッセージが表示されます。

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

```
Your directory needs a credential update. Please update the directory credentials.
```

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

```
Message:
An Error Has Occurred
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

時刻同期と Kerberos に問題がある可能性があります。AD Connector は Kerberos 認証リクエストをに送信します。Active Directoryこれらの要求は時間的制約があり、要求が遅れると失敗します。この問題を解決するには、ドキュメンテーションの「推奨事項-信頼できるタイムソースを使用してルート PDC を構成する」と「広範囲にわたるタイムスキューの回避」を参照してください。Microsoftタイムサービスと同期について詳しくは、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誤差
- Windowsタイムサービスのツールと設定

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。この設定について詳しくは、「事前認証オン Microsoft TechNet」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の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ドメイン参加が機能しなくなった

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 Support. (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ドメイン参加が機能しなくなった

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。認証情報の有効期限が切れていると、AD Connector Active Directory がにコンピューター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. のサービスアカウントのパスワードを更新してください。Active Directory
2. で AD Connector AWS Directory Service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、「AWS Directory Service の AD Connector サービスアカウントの認証情報を更新する」を参照してください。

> **Important**
>
> AWS Directory Service でのみパスワードを更新しても、Active Directoryパスワードの変更は既存のオンプレミスには反映されないため、前の手順に示した順序で行うことが重要です。

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 を削除するために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、を参照してくださいAD Connector を削除する。それでもAD Connectorを削除できない場合は、からサポートをリクエストできますAWS Support。

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 には、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が用意されています。ただし、Simple AD は、多要素認証 (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 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をサポートしていないことに注意してください。

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 インスタンスの管理と、Windows AWS アプリケーションのクラウドへのデプロイが容易になります。
- 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 や Amazon AWS WorkMail などのアプリケーションへのアクセスを許可します。
- IAM AWS 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
- 毎日自動スナップショットを作成することで、復旧が可能になります。 point-in-time

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 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 の管理方法
- チュートリアル:Simple AD の作成 Active Directory
- Simple AD のベストプラクティス
- Simple AD のクォータ
- Simple AD のアプリケーション互換性ポリシー
- 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 で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 Active Directory
- Simple AD で作成されるもの Active Directory

- Simple AD: DNS を設定する

Simple AD の前提条件

Simple AD を作成するにはActive Directory、以下を含む 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。
- VPC は次の VPC エンドポイントを使用して設定することはできません。
  - 非パブリック AWS IP アドレスに解決される *.amazonaws.com の DNS 条件付きオーバーライドを含む Route53 VPC エンドポイント
  - CloudWatch VPC エンドポイント
  - Systems Manager VPC エンドポイント
  - Security Token Service VPC エンドポイント
- 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ーゾーンに存在している。サブネットは同じクラスレスドメイン間ルーティング (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。

Simple AD を作成する Active Directory

新しい Simple 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、Simple AD 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。

Simple AD を作成するには Active Directory

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、 の起動の一部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 WorkSpaces。

   [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。

[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ー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 で作成されるもの Active Directory

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、 AWS Directory Service コンソールまたは 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-*xxxxxxxx* 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 Interfaces」を参照してください。 AWS Managed Microsoft AD のデフォルトの DNS サーバーは、Classless Inter-Domain Routing (CIDR)+2 の VPC DNS サーバーActive Directory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: DNS を設定する

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。

> **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。

Simple AD の管理方法

このセクションでは、Simple AD 環境の運用および維持におけるすべての手順を示します。

トピック

- Simple AD のユーザーおよびグループを管理する
- Simple AD ディレクトリのモニタリング
- Amazon EC2 インスタンスを Simple AD Active Directoryに結合する
- Simple AD ディレクトリの維持
- 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 認証情報による AWS Management Console へのアクセスを有効化する

Simple AD のユーザーおよびグループを管理する

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。

ユーザーとグループを AWS Directory Service ディレクトリに作成するには、AWS Directory Service ディレクトリに結合されたいずれかのインスタンスを (オンプレミスまたは EC2 から) 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している必要があります。さらに、Active Directory のツールを EC2 インスタンスにインストールし、[Active Directory Users and Computers] (Active Directory ユーザーとコンピュータ) スナップインを使用してユーザーとグループを EC2 インスタンスに追加できるように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 Active Directoryに結合する」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 ユーザーを作成する
- Simple AD ユーザーを削除する
- Simple AD ユーザーパスワードのリセット
- Simple AD グループを作成する
- 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 Windows Server インスタンスからActive Direcotryを管理するには、インスタンスに Active Directory ドメインサービスとActive Directory ライトウェイトディレクトリサービス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.

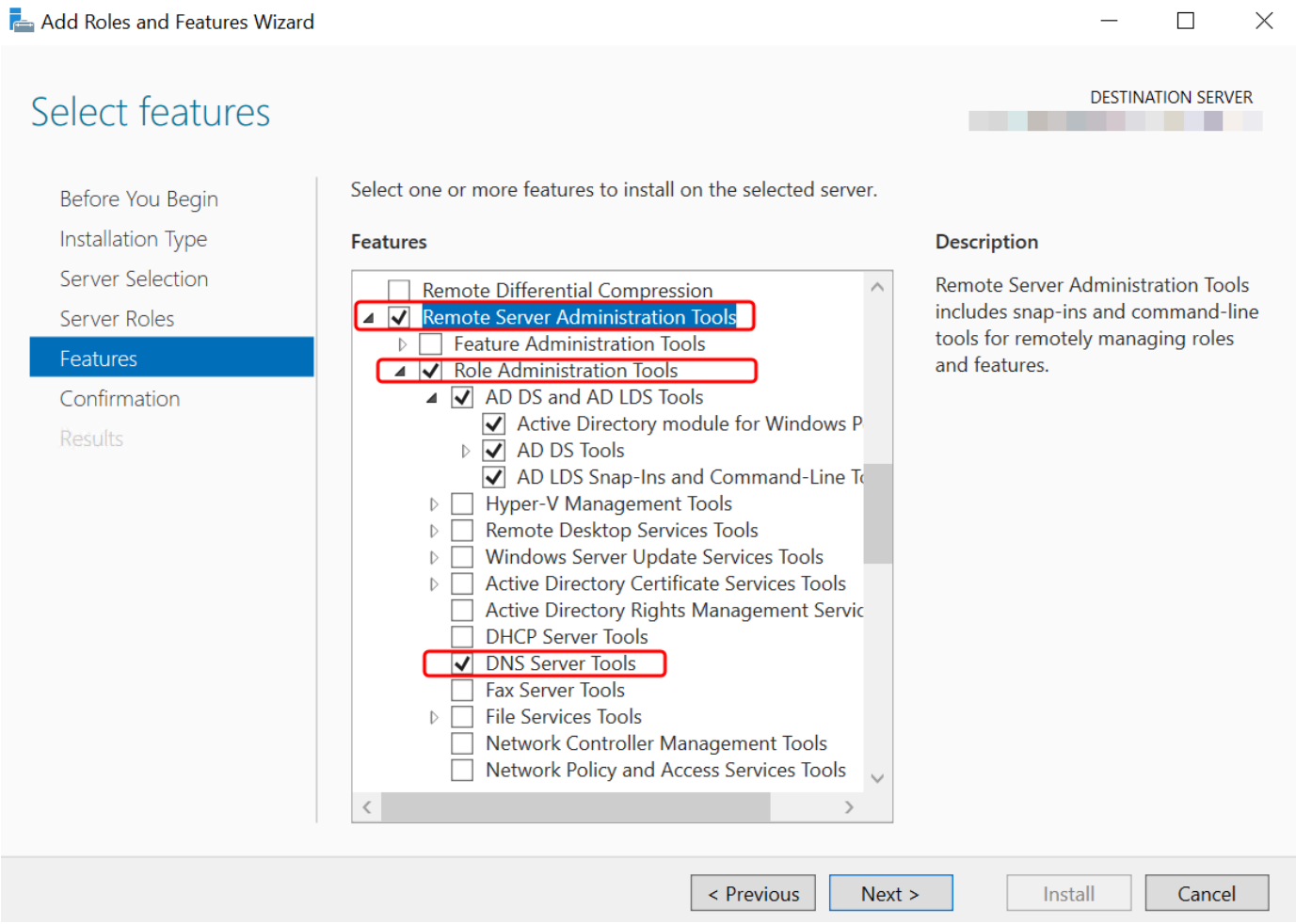
1. Simple Active Directoryを作成するには 詳細については、「Simple AD を作成する Active Directory」を参照してください。
2. EC2 Windows Server インスタンスを起動し、Simple AD アクティブディレクトリに参加させます。EC2 インスタンスでユーザーとグループを作成するには、以下のポリシーが必要です **AmazonSSMDirectoryServiceAccess** と **AWSSSMManagedInstanceCore**。詳細については、「Amazon EC2 Windows スタンスを Simple AD Active Directory にシームレスに結合する」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、Simple AD の作成時に作成されました。Simple AD を作成する Active Directory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

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 (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。ユーザー名には、***NetBIOS-Name*\administrator**または**の形式を使用できます*DNS-Name*\administrator**。たとえば、Simple AD を作成する Active Directory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 と AD LDS ツールを選択すると、AD DS ツール、AD LDS Active Directoryスナップインとコマンドラインツールのモジュールが選択されます。Windows PowerShell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。

EC2 Windows Server インスタンスにアクティブディレクトリ管理ツールをインストールする代替方法

- Active Directory 管理ツールをインストールする別の方法を次に示します。
  - オプションとして、を使用してActive Directory管理ツールをインストールすることもできますWindows PowerShell。たとえば、Active Directory PowerShell リモート管理ツールはを使用するプロンプトからインストールできます`Install-WindowsFeature RSAT-ADDS`。詳細については、Microsoft の Web WindowsFeature サイトの「インストール-」を参照してください。

Simple AD ユーザーを作成する

Simple AD ディレクトリに参加している Amazon EC2 インスタンスを持つ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、次のいずれかの方法を使用できます。

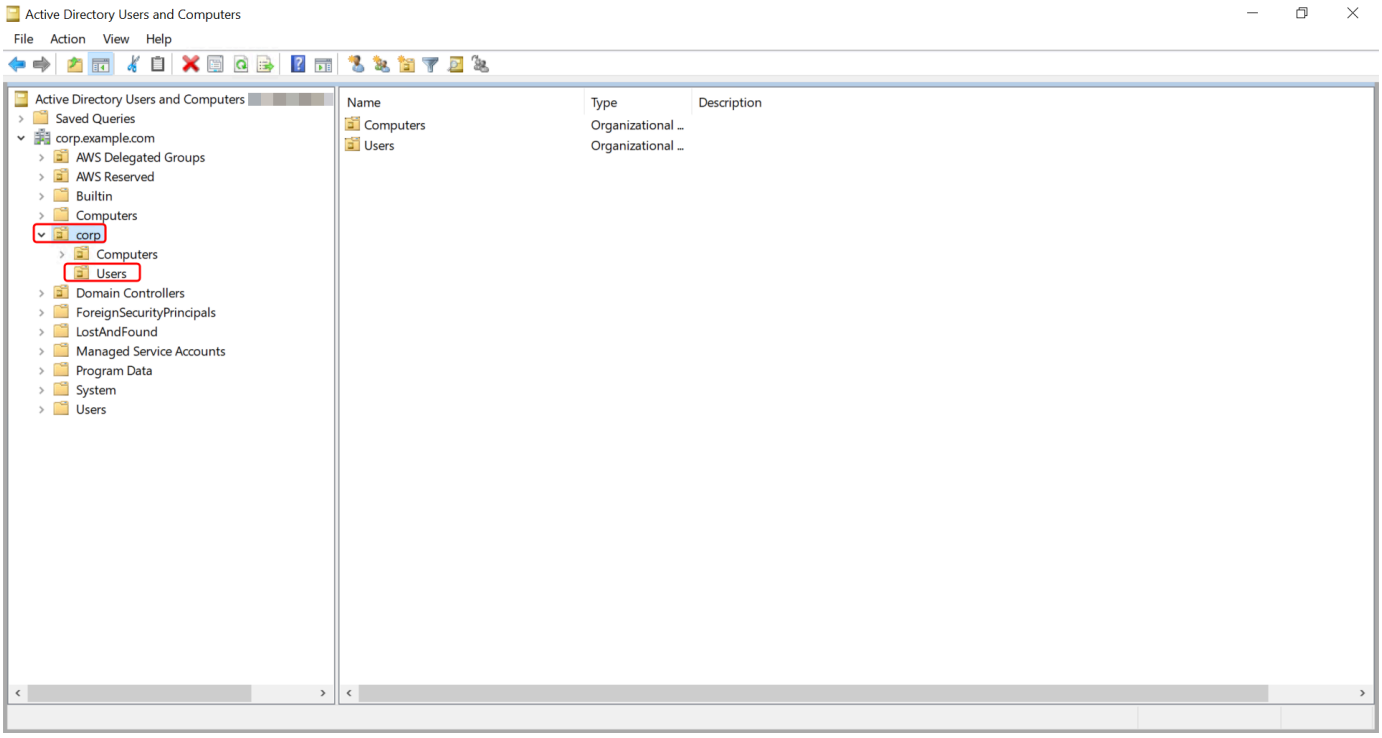
- Active Directory 管理ツール
- Windows PowerShell

Active Directory 管理ツールを使用してユーザーを作成する

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、ユーザーを保存するディレクトリの NetBIOS 名 OU で OU を選択します (例: **`corp\Users`**)。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 Active Directory で作成される内容。



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] をクリックします。

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。

でユーザーを作成する Windows PowerShell

1. Active Directory 管理者としてActive Directoryドメインに参加しているインスタンスに接続します。
2. Windows 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て、次のコマンドを入力します。によって、新しいユーザーのパスワードを入力するWindows PowerShellように求められます。Active Directory パスワードの複雑さの要件の詳細については、Microsoft「 のドキュメント」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')
```

Simple AD ユーザーを削除する

Simple AD ディレクトリに参加している Amazon EC2 Windows 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。

ユーザーを削除するには、次のいずれかの方法を使用できます。

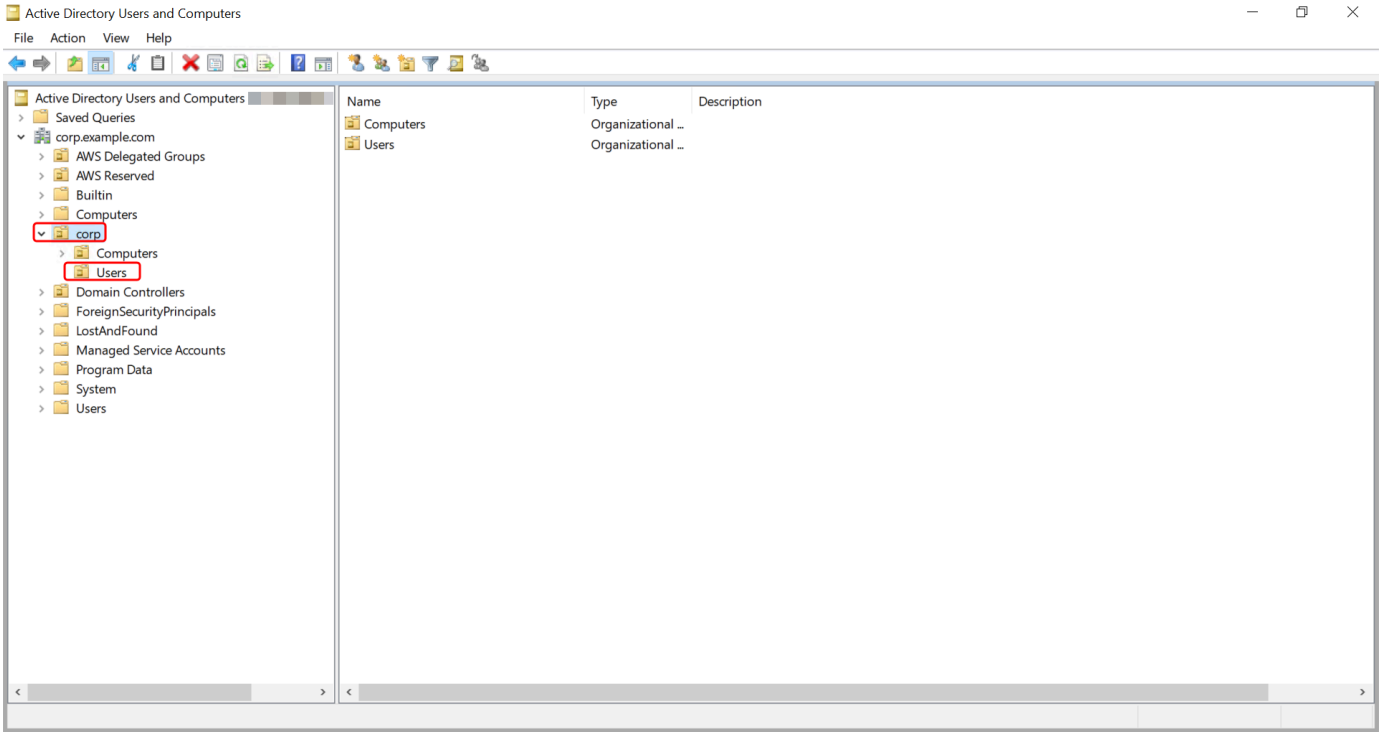
- Active Directory 管理ツール
- Windows PowerShell

Active Directory 管理ツールでユーザーを削除する

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、削除するユーザーを含む 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。

でユーザーを削除する Windows PowerShell

1. Active Directory 管理者としてActive Directoryドメインに参加しているインスタンスに接続します。
2. Windows PowerShell を開きます。

3. ユーザー名を削除するユーザーのユーザー名**jane.doe**に置き換えて、次のコマンドを入力します。Remove-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。

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

Simple AD ユーザーパスワードのリセット

ユーザーは、 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Active Directory。これにより、Active Directory管理者を含むユーザーの能力が最大限に高まり、パスワードを忘れることがあります。この場合、ユーザーが Simple AD にいる場合、 を使用して AWS Directory Service 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ご参照ください。

Active Directory 以下の例外を除き、 内の任意のユーザーのパスワードをリセットできます。

- 組織単位 (OU) 内のユーザーのパスワードは、 の作成時に使用した NetBIOS 名に基づいてリセットできますActive Directory。例えば、 の手順に従った場合Simple AD を作成する Active Directory、NetBIOS 名は CORP になり、リセットできるユーザーパスワードは Corp/Users OU のメンバーになります。
- の作成時に使用した NetBIOS 名に基づく OU の外部では、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Active Directory。Simple AD の OU 構造の詳細については、「」を参照してくださいSimple AD で作成されるもの Active Directory。
- 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。また、管理者ユーザーを除くドメイン管理者グループまたはエンタープライズ管理者グループ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。
- 管理者ユーザーを除き、ドメイン管理者グループまたはエンタープライズ管理者グループ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。

ユーザーパスワードをリセットするには、次のいずれかの方法を使用できます。

- AWS Management Console
- AWS CLI

- Windows PowerShell

でユーザーパスワードをリセットする AWS Management Console

1. AWS Directory Service コンソールのナビゲーションペインの でActive Directoryディレクトリ を選択し、ユーザーパスワードをリセットするリストActive Directoryで 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。

でのユーザーパスワードのリセット 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**、パスワードをActive Directoryディレクトリ ID と必要な認証情報に置き換え**P@ssw0rd**ます。詳細についてはreset-user-password、 AWS CLI コマンドリファレンスの「」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"
```

でのユーザーパスワードのリセット Windows PowerShell

1. Active Directory 管理者としてActive Directoryドメインに参加しているインスタンスに接続します。
2. Windows PowerShell を開きます。
3. ユーザー名 **jane.doe**、ディレクトリ ID、パスワードをActive Directoryディレクトリ ID と必要な認証情報に置き換え**P@ssw0rd**て、次のコマンドを入力します。詳細については、「Reset-DS UserPassword 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"
```

Simple AD グループを作成する

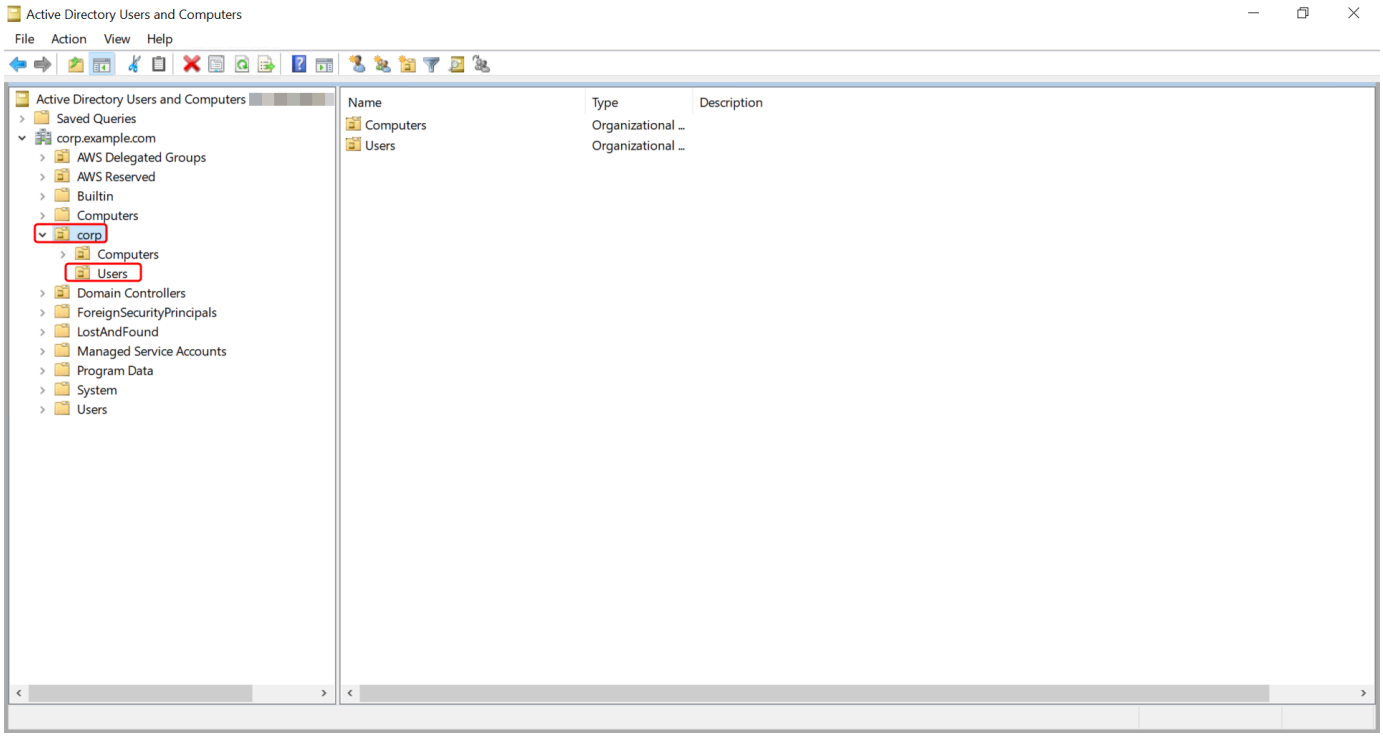
Simple AD ディレクトリに参加している Amazon EC2 インスタンスを使用してセキュリティグループを作成するには、次の手順に従います。セキュリティグループを作成する前に、「Active Directory 管理ツールのインストール」の手順を完了する必要があります。

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 Active Directory で作成される内容。



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

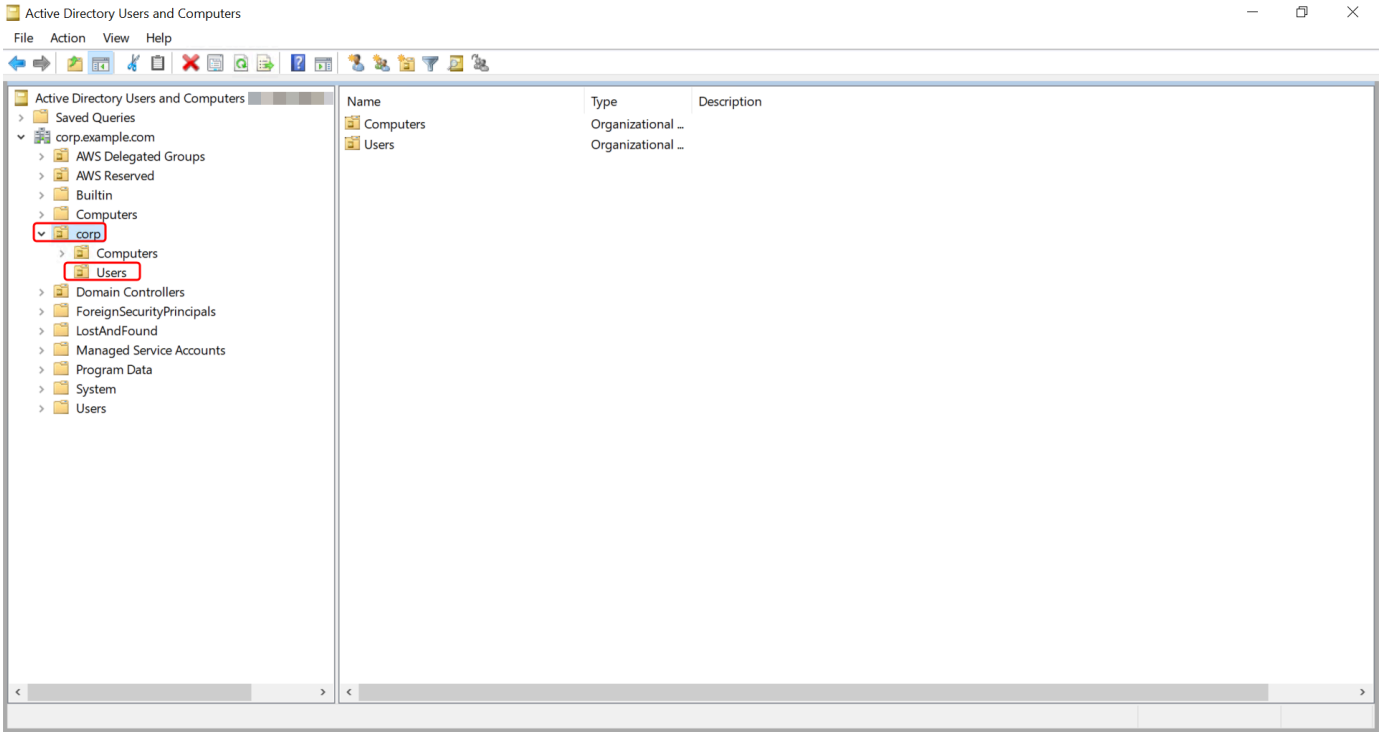
Simple AD ディレクトリに結合された EC2 インスタンスを持つセキュリティグループにユーザーを追加するには、次の手順に従います。

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 ディレクトリのモニタリング

Simple AD ディレクトリは次の方法でモニタリングできます。

トピック

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 Support 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については、40 AWS 分以内に問題を解決します。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 Support 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、「ディレクトリをスナップショットまたは復元する」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

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 Support 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の原因」を参照してください。

Amazon SNS でディレクトリステータス通知を設定する

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 AWS Directory Service トピックに発行者として を追加できます。Amazon SNS 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。

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**
>
> DirectoryServiceFullAccess マネージド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 の権限が追加で必要です。

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 コンソールからこれを行うことができます。

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、 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 EC2 インスタンスを Simple AD Active Directoryに結合する

インスタンスの起動時に、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 にシームレスに結合する Active Directory」を参照してください。また、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。

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、適切なリージョンと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 スタンスを Simple AD Active Directory にシームレスに結合する
- Amazon EC2 Windows 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
- 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
- Simple AD のディレクトリ結合権限を委任する
- DHCP オプションセットの作成

Amazon EC2 Windows スタンスを Simple AD Active Directory にシームレスに結合する

この手順は、Amazon EC2 Windows インスタンスを Simple AD Active Directory ディレクトリにシームレスに結合します。

EC2 Winodws 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、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。

   a. 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。
   b. 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。
   c. 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。
   d. [キーペアの作成] を選択します。
   e. 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。

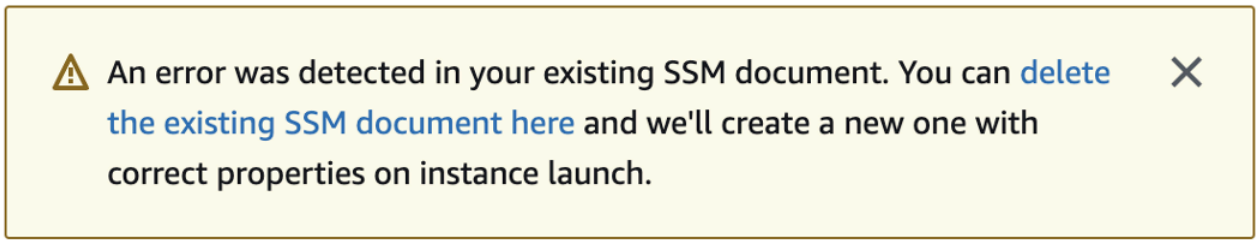
11. [自動割り当てパブリック IP] で、[有効化] を選択します。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>
>
> 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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
> - 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持つ 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。AmazonSSMManagedInstanceCore がアAmazonSSMDirectoryServiceAccessタッチされた AWS 管理ポリシーを持つ 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 プロファイルリンクの作成 を選択し、次の操作を行います。

    1. [ロールの作成] を選択します。
    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] を選択します。
    4. アクセス許可の追加 で、ポリシーのリストで 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] をクリックします。

        > **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。

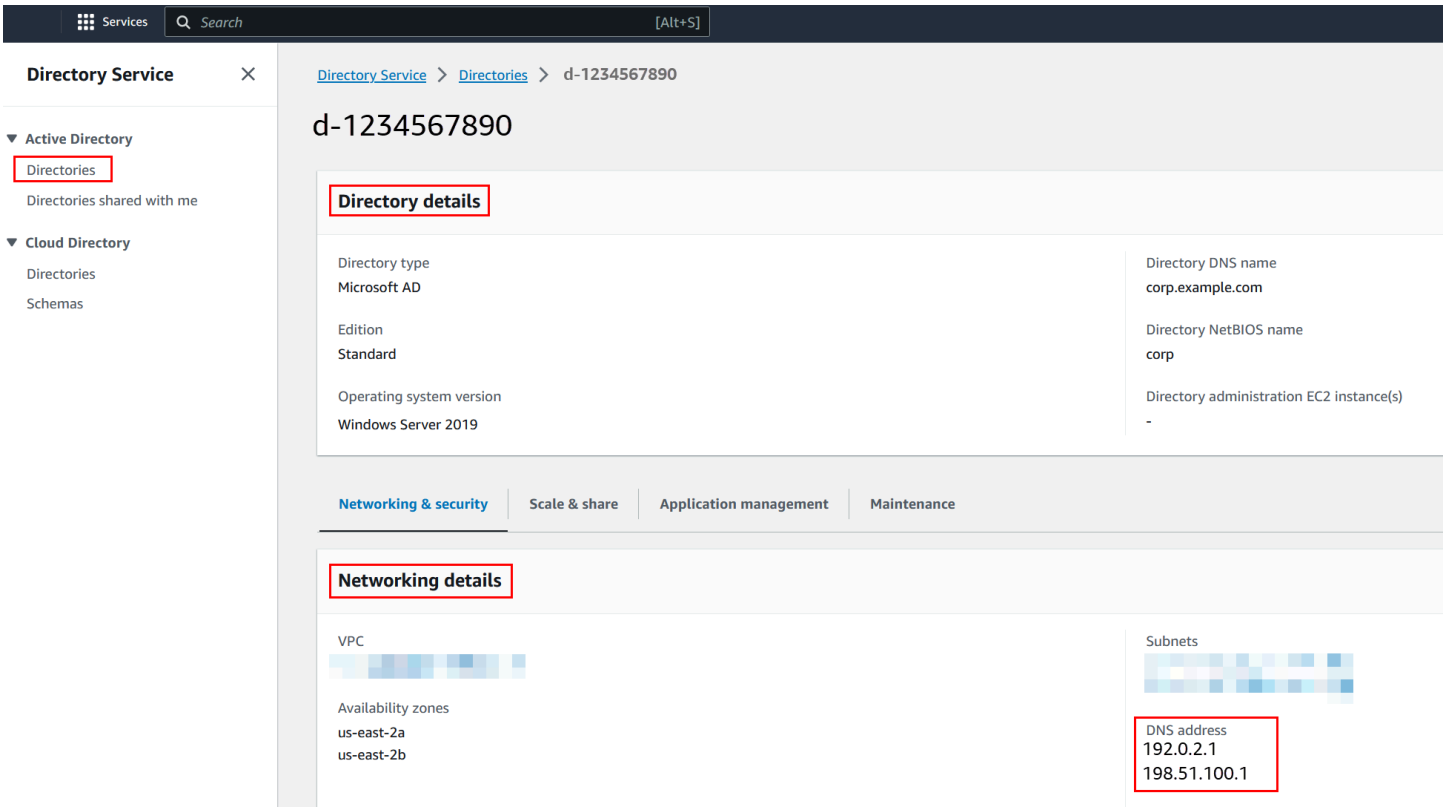
    5. [名前、確認、作成] ページで、[ロール名] を入力します。EC2 インスタンスにアタッチするには、このロール名が必要です。
    6. (オプション) IAM インスタンスプロファイルの説明を [説明] フィールドに入力できます。
    7. [ロールの作成] を選択します。
    8. [インスタンスを起動する] ページに戻り、[IAM インスタンスプロファイル] の横にある更新アイコンを選択します。新しい IAM インスタンスプロファイルが [IAM インスタンスプロファイル] ドロップダウンリストに表示されるはずです。新しいプロファイルを選択し、残りの設定はデフォルト値のままにします。

16. [Launch instance (インスタンスの起動)] を選択します。

Amazon EC2 Windows 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

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、で指定され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Amazon EC2 Windows スタンスを Simple AD Active Directory にシームレスに結合する。

Simple AD DNS サーバーの IP アドレスが必要になります。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。



Windows 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

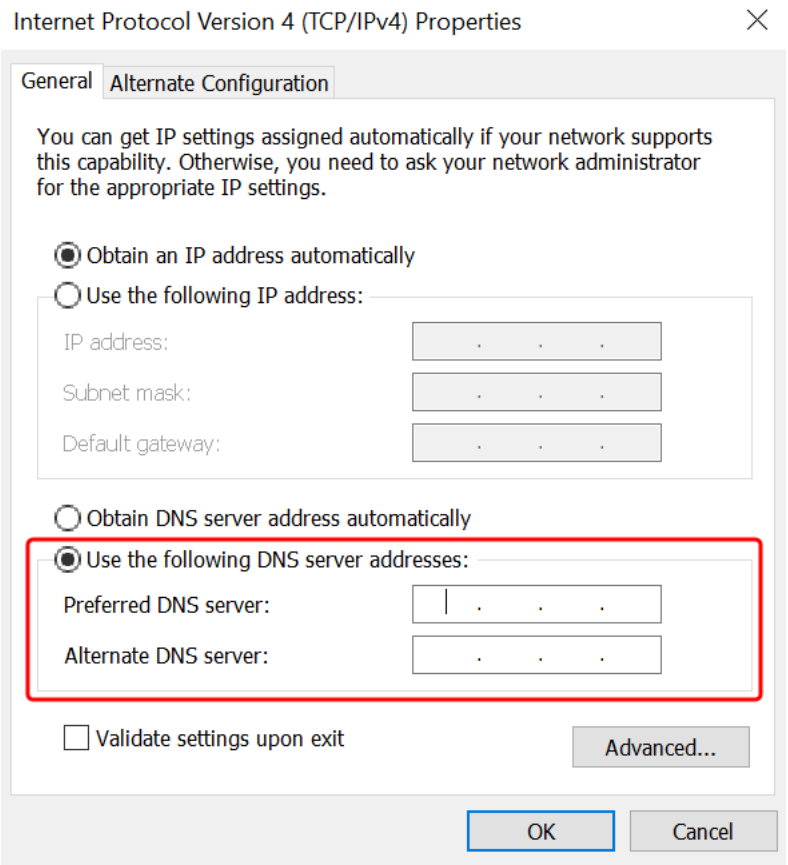
1. リモートデスクトッププロトコルクライアントを使用してインスタンスに接続します。
2. インスタンスの TCP / IPv4 プロパティダイアログボックスを開きます。
    a. ネットワーク接続を開きます。

> **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 サーバーアドレスを使用する を選択し、優先 DNS サーバーと代替 DNS サーバーのアドレスを Simple AD が提供する 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。

> **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. 「メンバー」フィールドに、「ドメイン」を選択し、Simple AD アクティブディレクトリ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、「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。ユーザー名は管理者 になります。例えば、**corp.example.com\administrator**、**corp\administrator** などです。

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 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、「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 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 より前のディストリビューションでは、シームレスなドメイン結合機能はサポートされていません。

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。

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

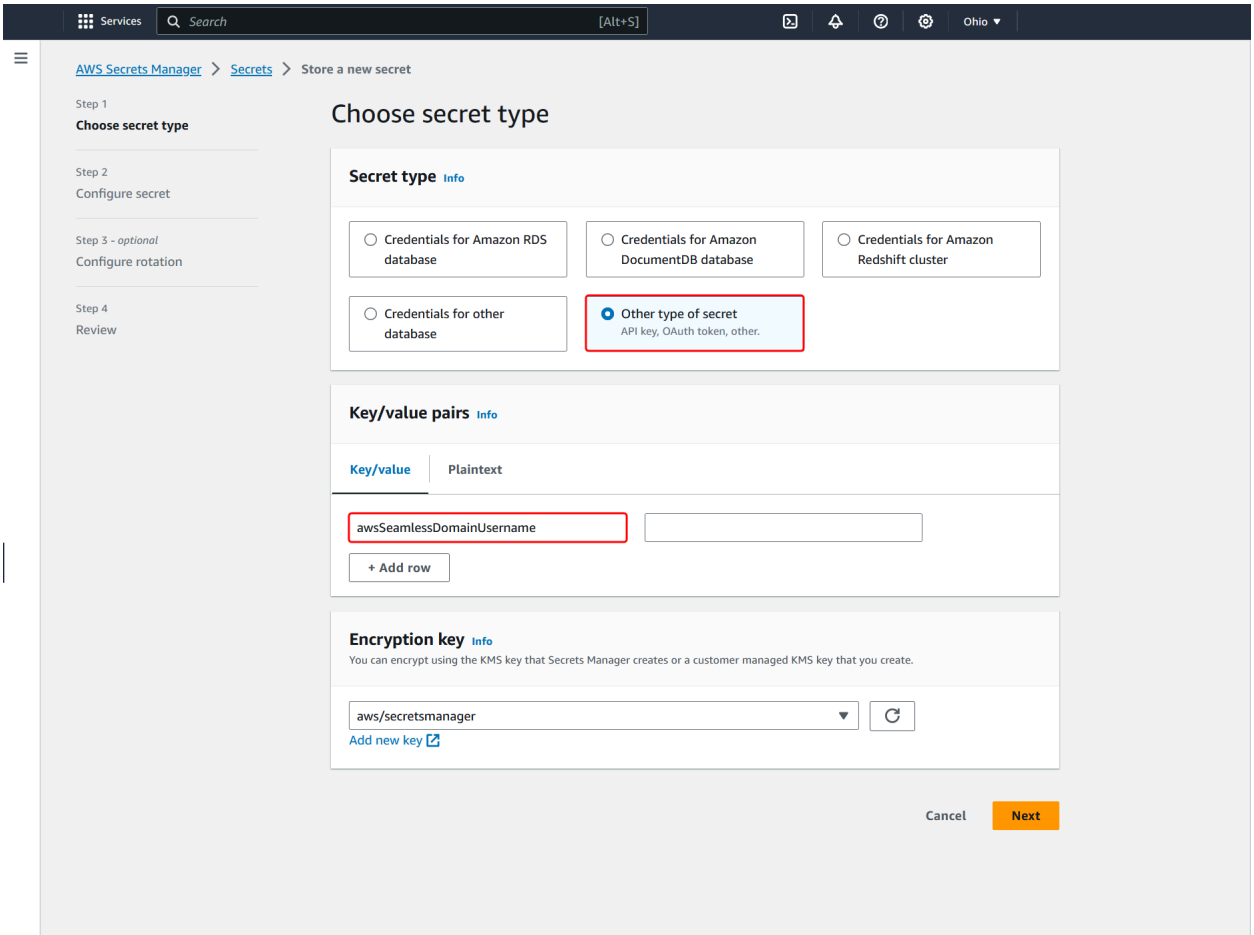
1. にサインイン AWS Management Console し、https://console.aws.amazon.com/secretsmanager/ で AWS Secrets Manager コンソールを開きます。
2. [Store a new secret] (新しいシークレットの保存) を選択します。
3. [Store a new secret] (新しいシークレットを保存する) のページで、次の操作を行います：

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 になります**awsSeamlessDomain**。

> **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。



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。

> **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/secretsmanagerが作成する AWS マネージドキーを使用して、シークレットを無料で暗号化できます。独自の KMS キーを作成してシークレットを暗号化すると、 は現在の AWS KMS レートで AWS 課金します。詳細については、「AWS Key Management Service の料金」を参照してください。

v. [次へ] をクリックします。

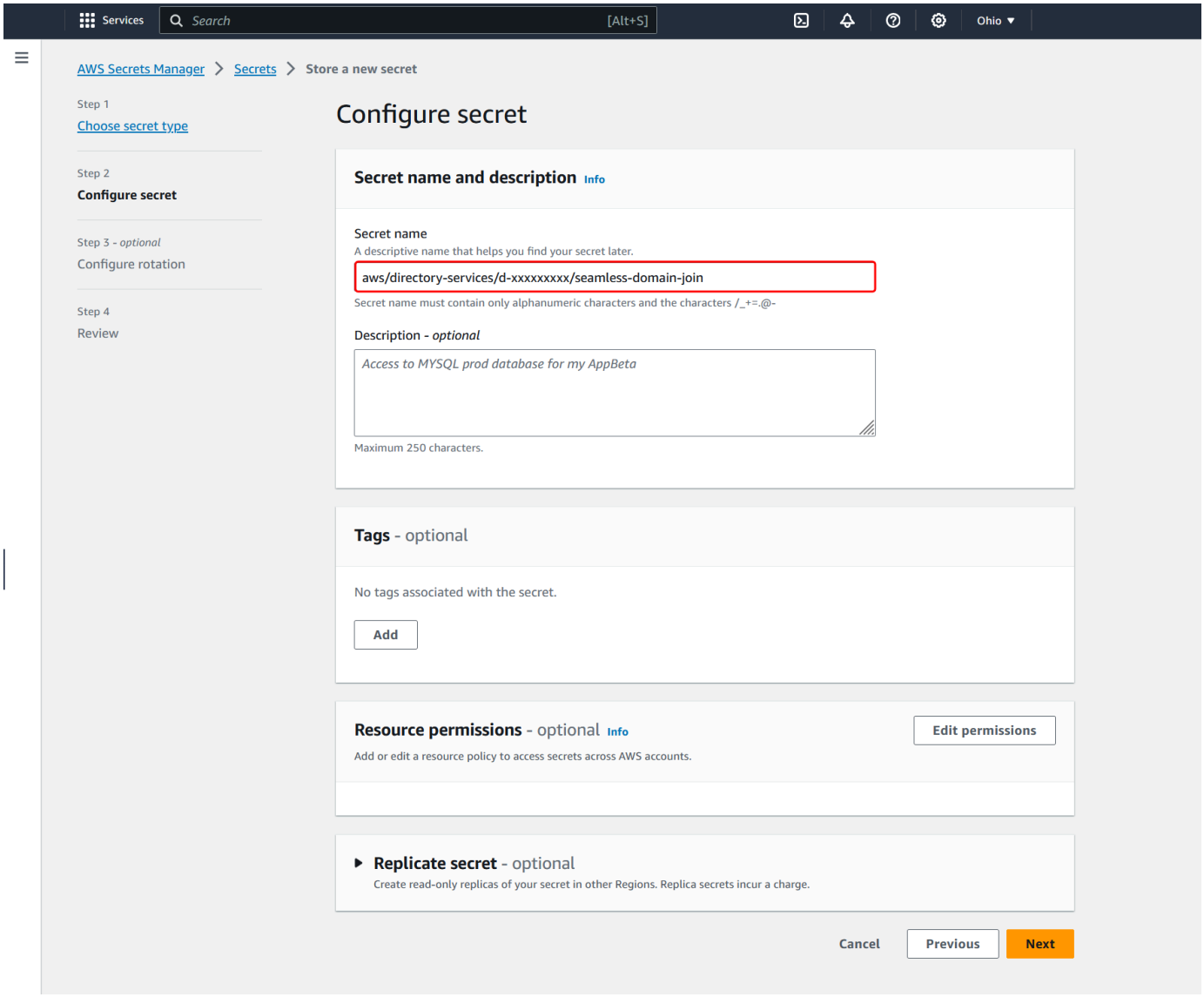
4. [Secret name]の下に、*d-xxxxxxxxxx*をディレクトリIDに置き換えて、以下のフォーマットでディレクトリIDを含むsecret nameを入力します：

```
aws/directory-services/d-xxxxxxxxx/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-xxxxxxxxx*/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。



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 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。

  ステップ 5 では、「 AWS Secrets Manager ユーザーガイド」の「Microsoft Active Directory の認証情報」のローテーションテンプレートを使用します。

  ヘルプについては、「 ユーザーガイド」の AWS Secrets Manager 「ローテーションのトラブルシューティングAWS Secrets Manager 」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

以下の前提条件のステップを使用して、Secrets Manager のシームレスなドメイン結合シークレット (以前に作成したもの) 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。

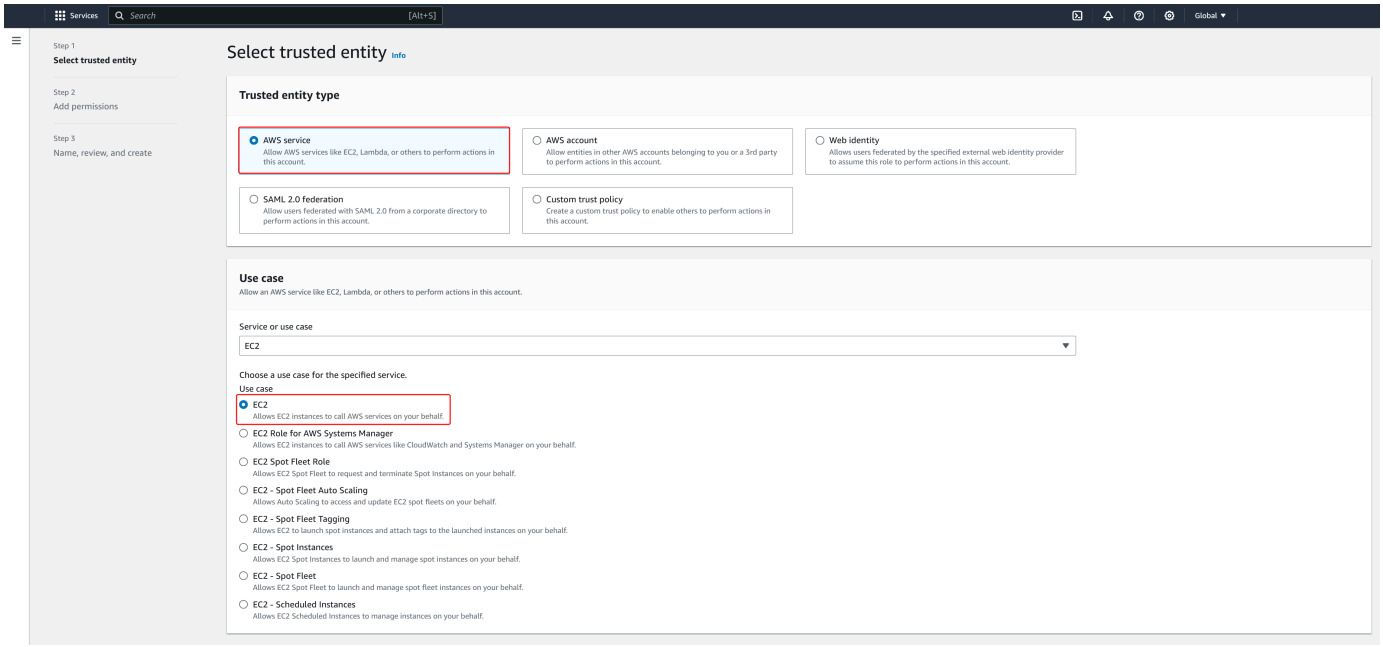
> **Note**
>
> シークレットごとに 1 つのポリシーを作成することをお勧めします。そうすることで、インスタンスが適切なシークレットにのみアクセスできるようになり、インスタンスが侵害された場合の影響を最小限に抑えることができます。

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。



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] を選択します。

Linux スタンスを Simple AD Active Directoryにシームレスに結合する

すべての前提条件タスクを設定したので、次の手順に従い EC2 Linux インスタンスをシームレスに結合できます。

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. (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. 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ときにaws:domainJoinプラグインを使用します。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。

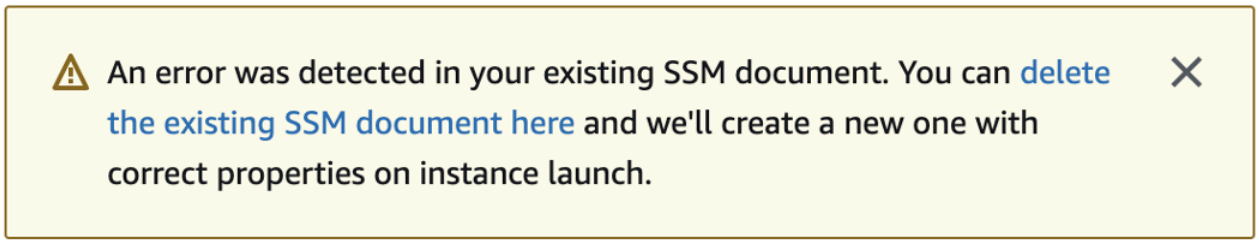
11. [自動割り当てパブリック IP] で、[有効化] を選択します。

    パブリック 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 ユーザーガイド」の「Amazon EC2 インスタンス IP アドレス指定Amazon EC2」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、以下が表示されることがあります。
>
> 
>
>
> 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、プロパティが想定されている場合は、閉じるを選択して EC2 インスタンスを起動します。変更はありません。
> - 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持つ 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 で、前提条件セクション「ステップ 2: LinuxEC2DomainJoin role を作成する」で以前に作成した IAM ロールを選択します。
16. [Launch instance (インスタンスの起動)] 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 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構いません。

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 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 -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 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

ドメイン結合権限を持つ *example.com* ドメイン内のアカウントの 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構いません。

```
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* ドメイン内のアカウントの 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/sssd/sssd.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、sssd サービスを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 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。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/sssd/sssd.conf に追加する必要があります。

テキストエディタで /etc/sssd/sssd.conf ファイルを開きます。

```
sudo vi /etc/sssd/sssd.conf
```

この操作を行った後、sssd.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=admins,ou=Testou,dc=example,dc=com)
```

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、UNIX/Linux ユーザー識別子 (UID) とグループ識別子 (GID) と Windows および Active Directoryセキュリティ識別子 (SID) のアイデンティティ間の統一されたエクスペリエンスを維持するために、2 つの方法で実行できます。

1. 一元化
2. 分散型

> **Note**
>
> の一元化されたユーザー ID 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または POSIX Active Directory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、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)

から 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Active Directory、sssd.conf ファイル`ldap_id_mapping = False`で を設定します。この値を設定する前に、 のユーザーとグループに UID、UID 番号、および GID 番号を追加していることを確認しますActive Directory。

分散型ユーザー ID マッピング

Active Directory に POSIX 拡張機能がない場合、または ID マッピングを一元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。

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。

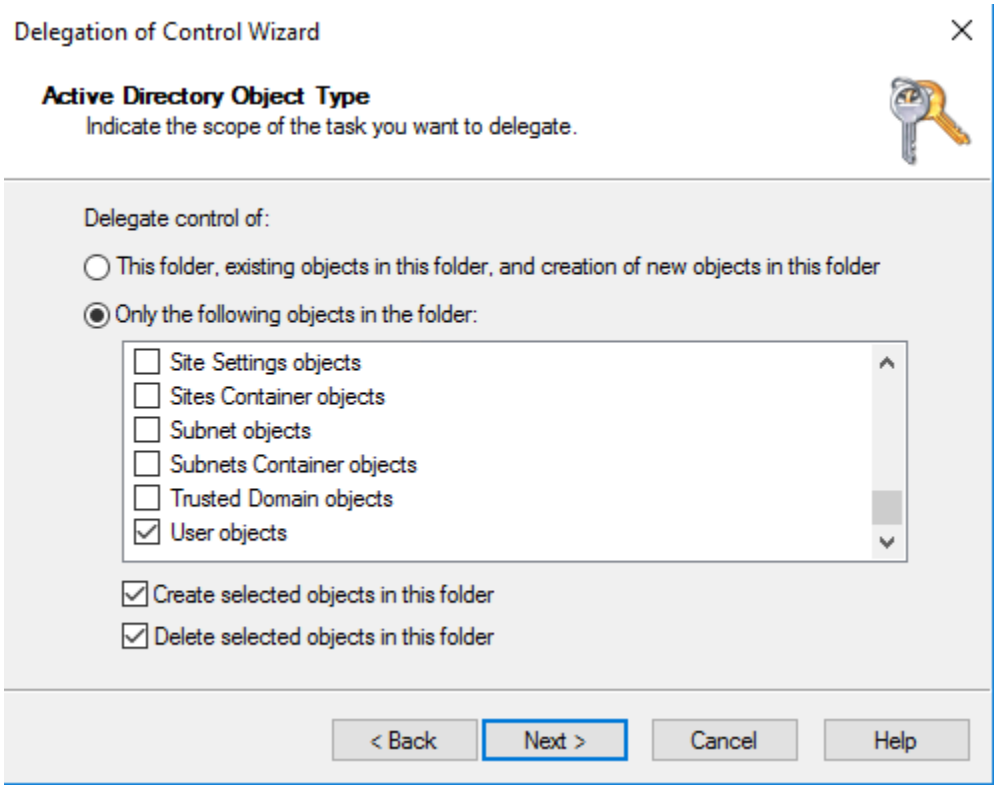
Simple AD での結合の権限を委任するには

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。

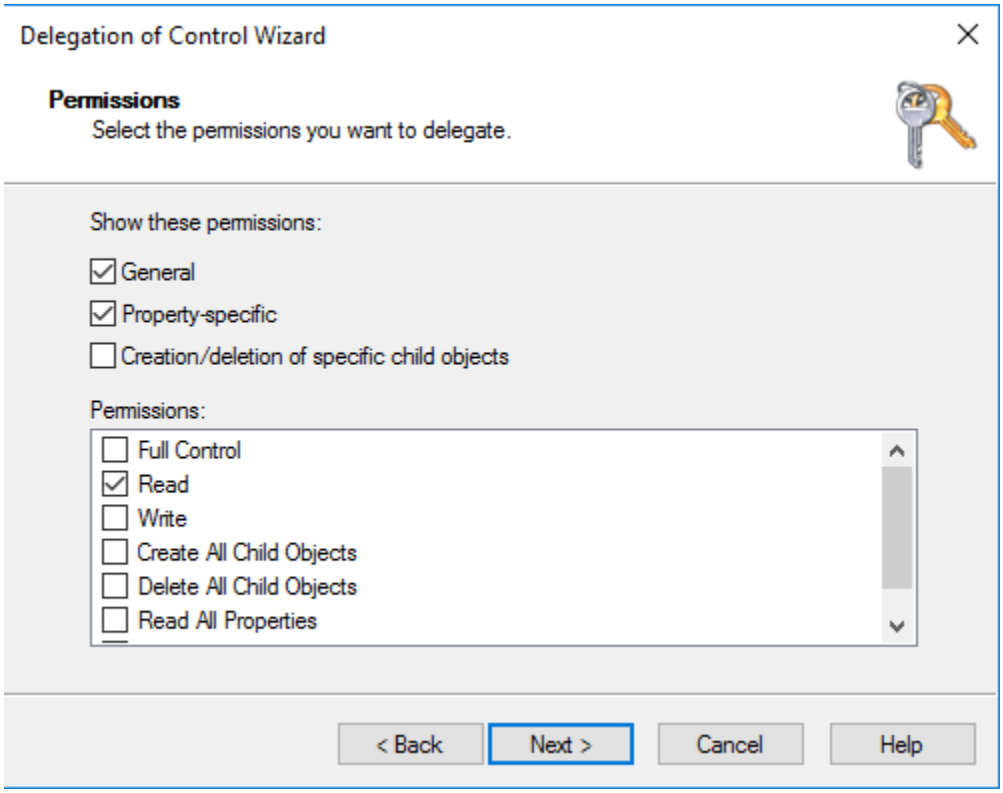
   - [Group name] (グループ名) に「**`Joiners`**」と入力します。

- [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。

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

   が提供するディレクトリの AWS 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、アクション、VPC 設定の編集 を選択します。
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、以下を参照してください。

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

Simple AD ディレクトリの維持

このセクションでは、Simple AD 環境の一般的な管理タスクを維持する方法について説明します。

トピック

- Simple AD を削除する
- ディレクトリをスナップショットまたは復元する
- ディレクトリ情報の表示

Simple AD を削除する

Simple AD を削除すると、ディレクトリデータとスナップショットはすべて削除され、復元することはできません。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。

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。 AWS リージョン Active Directory自分が導入されている場所にいることを確認してください。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. AWS 削除するディレクトリの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 アプリケーションが有効になっていると、 AWS 管理対象の 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 アプリとサービス] セクションには、 AWS ディレクトリで有効になっている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へのアクセスを無効にする」を参照してください。
      - Amazon を無効にするには WorkSpaces、 WorkSpaces コンソールの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「ディレクトリからの登録解除」を参照してください。
      - Amazon を無効にするには WorkDocs、Amazon WorkDocs コンソールで Amazon 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 管理ガイド』の「サイトの削除」を参照してください。
      - Amazon を無効にするには WorkMail、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 管理者ガイド』の「組織の削除」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 ユーザーガイド』の「FSx for Windows File Server 操作」を参照してください。Active Directory
      - 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、Client 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』Active Directoryの「認証」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「Amazon Connect インスタンスの削除」を参照してください。
- アマゾンを無効にするには QuickSight、アマAmazon QuickSight ンの購読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 アカウントの解約」を参照してください。

> **Note**
>
> AWS IAM Identity Center 使用していて、 AWS 削除する予定の管理対象Microsoft ADディレクトリに以前に接続したことがある場合は、削除する前にまずアイデンティティ・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。

ディレクトリをスナップショットまたは復元する

AWS Directory Service 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する機能を提供します。これらのスナップショットは、ディレクトリの point-in-time 復元を実行するために使用できます。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 Support 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。

ディレクトリ情報の表示

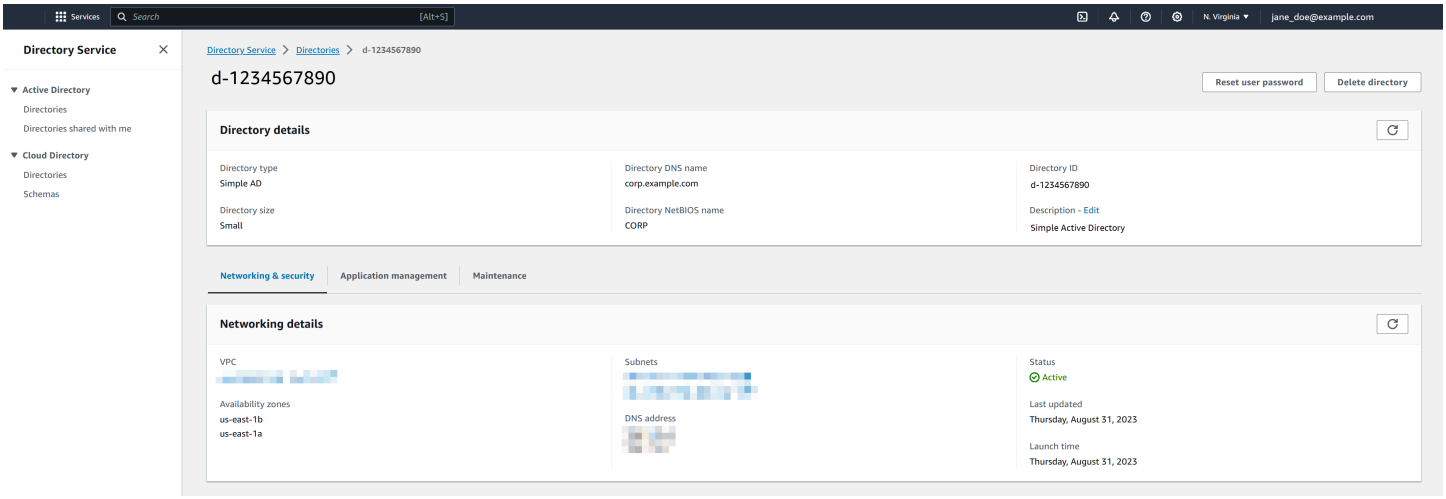
ディレクトリに関する詳細情報を表示できます。

詳細なディレクトリ情報を表示するには

1. AWS Directory Service コンソールナビゲーションペインの でActive Directory、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 リンクをクリックします。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。



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、Simple AD に Amazon などの AWS アプリケーションやサービスに WorkSpacesへのアクセスを許可できますActive Directory。以下の AWS アプリケーションとサービスは、Simple AD と連携するために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、「Amazon Chime 管理ガイド」を参照してください。
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	Simple AD、 AWS Managed Microsoft AD、または AD Connector は、 から直接作成できますWorkSpaces。このためには単純に、Worksp

AWS アプリケーション/サービス	詳細情報
	ace 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、「AD 認証情報による AWS Management Console へのアクセスを有効化する」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検索するには、次のステップを実行します。

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承認または承認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承認 AWS Directory Service。

トピック

- アクセス URL の作成
- シングルサインオン

アクセス URL の作成

Amazon WorkDocs などの AWS アプリケーションとサービスで使用するアクセス URL を使用して、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. [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

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 WorkDocs から Amazon 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がそれ自体でサービスプリンシパル名属性を追加または削除できるようにするアクセス許可を委任できます。AD Connector サービスアカウントのアクセス許可を変更するアクセス許可を持つアカウントを使用して、ドメインに参加しているコンピュータから以下の PowerShell コマンドを実行できます。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"
```

Amazon でシングルサインオンを有効または無効にするには WorkDocs

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、「有効化」を選択して Amazon のシングルサインオンを有効にします WorkDocs。

   [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、「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 Amazon でシングルサインオンを無効にする場合は WorkDocs、 を無効にするを選択し、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、もう一度無効にします。

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ティング () を有効にしますJavaScript。
- 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AuthServerAllowlistを実行して、ポリシーにアクセス URL を追加します。

```
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 ポリシーを使用してドメイン内のコンピュータで Chrome ウェブブラウザを管理する場合は、AuthServerAllowlistポリシーにアクセス URL を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。

AD 認証情報による AWS Management Console へのアクセスを有効化する

AWS Directory Service を使用すると、ディレクトリのメンバーに AWS Management Console へのアクセス権限を付与することができます。デフォルトでは、ディレクトリのメンバーに AWS リソースに対するアクセス権限は付与されません。ディレクトリのメンバーに IAM ロールを割り当てることで、さまざまな AWS サービスやリソースにアクセスできるようにします。IAM ロールでは、ディレクトリメンバーに付与するをサービス、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、「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、「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「ユーザーおよびグループに AWS リソースへのアクセス権限を付与する」を参照してください。

トピック

- AWS Management Console へのアクセスを有効にする
- AWS Management Consoleへのアクセスを無効にする
- 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の記事

- AWS Microsoft ADとオンプレミスの資格情報を使用して AWS Management Console にアクセスする方法

AWS Management Console へのアクセスを有効にする

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。

   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、先に、そのユーザーを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、「ユーザーまたはグループの既存のロールへの割り当て」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へのアクセスを無効にする

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. [Manage Access to AWS Resource] (AWS リソースへのアクセスの管理) ダイアログボックスで、[Continue] (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。

チュートリアル:Simple AD の作成 Active Directory

次のチュートリアルでは、 Simple AD Active Directoryのセットアップに必要なすべての手順を一通り説明します。Simple AD Active Directory を素早く簡単に使い始めることを目的としていますが、大規模な実稼働環境での使用を目的としたものではありません。

チュートリアルの前提条件

このチュートリアルでは、次のことを前提としています。

- アクティブな 1 つがあります AWS アカウント。
- 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。

詳細については、「Simple AD の前提条件」を参照してください。

ステップ 1: Simple AD 用に Amazon VPC を作成して設定する Active Directory

Simple ADで使用するために Amazon VPC を作成し、設定します。この手順を開始する前に、チュートリアルの前提条件 を満たしていることを確認します。

Simple AD 用の VPC を作成する Active Directory

2 つのパブリックサブネットを持つ VPC を作成します。 AWS Directory Service には VPC に 2 つのサブネットが必要で、各サブネットは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。

1. Amazon VPC コンソール (https://console.aws.amazon.com/vpc/) を開きます。
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。

ステップ 2: Simple AD Active Directoryの作成

新しいSimple AD Active Directory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、「ステップ 1: Simple AD 用に Amazon VPC を作成して設定する」チュートリアルの前提条件 に記載されている前提条件を満たしていることを確認してください。Active Directory

Simple AD Active Directory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、 [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、起動時にディレクトリを作成する場合にのみ使用できます。WorkSpaces

   [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。

[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ー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 のベストプラクティス

問題を回避し、Simple 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。

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 Active Directoryに接続するだけです 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互換性を備えた低コストの低スケールディレクトリです。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 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 Active Directory」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 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。セキュリティグループ AWS を設定して、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

に限ります。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、ディレクトリに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**
>
> 技術的には、ディレクトリのセキュリティグループを、ユーザー作成した他の EC2 インスタンスと関連付けることができます。ただし、この方法にはお勧め AWS しません。 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、セキュリティグループを予告なしに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。ディレクトリと別の AWS Directory Service ディレクトリ間の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る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、、Amazon 、 WorkSpacesAmazon 、または Amazon 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 WorkDocs WorkMail QuickSight。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、ドメインコントローラーを追加して高いパフォーマンスを実現できます。詳細については、「追加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 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および Active Directory のその他の機能を使用するには、代わりに AWS Directory Service for Microsoft Active Directory (Standard Edition あるいは 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市販の既製アプリケーションは多数あるため、AWS では、サードパーティー製アプリケーションにおける Simple AD との互換性の公式または広範な検証を行うことが

できません。お客様側でアプリケーションのインストールに関する問題が発生する可能性がある場合、AWS はお客様と協力して問題の解決に努めますが、アプリケーションの Simple AD との現時点および将来における互換性は保証できません。

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

実際の Active Directory に基づいて互換性をより高めるため、お客様は AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) の使用を選択できます。

Simple AD のトラブルシューティング

以下のセクションは、ディレクトリ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

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 または AWS Managed Microsoft AD ディレクトリにサインインできない場合は、 AWS Management Console、Windows PowerShellまたはを使用してパスワードをリセットできます。 AWS CLI

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」 (KDC では要求したオプションを処理できません) というエラーが返される

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 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と、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「ユーザーのログイン失敗」エラーが表示される場合があります。AWS これは既知の問題であり、現在解決に向けて取り組んでいます。

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。

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。この問題が解決しない場合は、AWS Support センターまでお問い合わせください。

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 AWS 年以前に作成されたアカウントの中には、 AWS Directory Service ディレクトリをサポートしない米国東部 (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ーゾーンにアクセスできるものもあります。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ー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。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。この設定について詳しくは、「Microsoft での事前認証」を参照してください TechNet。

追加リソース

次のリソースは、で作業する際のトラブルシューティングに役立ちます。 AWS

- AWS Knowledge Center — 問題のトラブルシューティングに役立つ FAQ や他のリソースへのリンクを検索できます。

- AWS Support センター — テクニカルサポートを受けてください。
- AWS プレミアムSupport センター — プレミアムテクニカルサポートを受けられます。

トピック

- Simple AD ディレクトリのステータスの原因

Simple AD ディレクトリのステータスの原因

ディレクトリが機能または動作しない場合、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が AWS Directory Service コンソールに表示されるか、または `DescribeDirectories` API により `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、「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。

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)
- AWS Directory Service の重要な予約済みユーザーがディレクトリに存在しない
- AWS Directory Service の重要な予約済みユーザーは Domain Admins グループに属している必要がある
- AWS Directory Service の重要な予約済みユーザーが無効化されている
- 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ディレクトリの作成中にユーザーに代わって作成された、重要な Elastic Network Interface (ENI) が、ディレクトリインスタンスにアタッチされていま

せん。このディレクトリでバックアップされた AWS アプリケーションは機能しなくなります。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、AWS Support 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、AWS Support までお問い合わせください。

AWS Directory Service の重要な予約済みユーザーがディレクトリに存在しない

説明

Simple AD が作成されると、AWS Directory Service では、ディレクトリに `AWSAdmin`*`D-xxxxxxxxx`* という名前でサービスアカウントが作成されます。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。

AWS Directory Service の重要な予約済みユーザーは Domain Admins グループに属している必要がある

説明

Simple AD が作成されると、AWS Directory Service では、ディレクトリに `AWSAdminD-xxxxxxxxx` という名前でサービスアカウントが作成されます。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。FSMO ロールの転送、新しいディレクトリコントローラーへのドメインの参加、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操作を実行するために必要な権限を AWS Directory Service に付与するには、このグループのメンバーシップが必要です。

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。

AWS Directory Service の重要な予約済みユーザーが無効化されている

説明

Simple AD が作成されると、AWS Directory Service では、ディレクトリに `AWSAdminD-xxxxxxxxx` という名前でサービスアカウントが作成されます。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。AWS Directory Service でディレクトリのメンテナンスとリカバリの操作を実行できるように、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。問題が解決しない場合は、AWS Support までお問い合わせください。

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 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、AWS Support までお問い合わせください。

のセキュリティ AWS Directory Service

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からメリットを得られます。

セキュリティは、 AWS とユーザーの間で共有される責任です。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 — 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責任 AWS は AWS にあります。 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。に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、「コンプライアンスAWS 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、データの機密性、会社の要件、適用される法律や規制など、その他の要因についても責任を負います。

このドキュメントは、 の使用時に責任共有モデルを適用する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ために AWS Directory Service 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 の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 Identity and Access Management 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

- 管理者アカウントのアクセス権限
- グループ管理サービスアカウント
- 信頼関係の作成
- Kerberos の制約付き委任
- ユーザーおよびグループに AWS リソースへのアクセス権限を付与する
- を使用した AWS アプリケーションとサービスの承認 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 ディレクトリを保護する
- 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 をモニタリングする
- 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 Identity and Access Management AWS Directory Service

へのアクセスには AWS 、 がリクエストの認証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 AWS Directory Service 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 を使用して AWS Directory Service 、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。例えば、 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ための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、リソースを作成またはアクセスするためのアクセス許可はアクセス許可ポリシーによって管理されます。アカウント管理者は、IAM ID (ユーザー、グループ、ロール) にアクセス許可ポリシーをアタッチできます。一部のサービス (など AWS Lambda) では、リソースへのアクセス許可ポリシーのアタッチもサポートされています。

> **Note**
>
> アカウント管理者 (または管理者ユーザー) は、管理者権限を持つユーザーです。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
- 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。 はディレクトリスナップショットリソースも AWS Directory Service サポートしています。ただし、既存のディレクトリのコンテキストでのみスナップショットのみを作成できます。そのため、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: region:account-id :directory/ external-directory-id`
スナップショット	`arn:aws:ds: region:account-id :snapshot/ external-snapshot-id`

AWS Directory Service 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 のアクション」を参照してください。

リソース所有権について

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 AWS 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 AWS アカウントに IAM ロールを作成すると、ロールを引き受けることの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。これは、IAM サービスに関する詳細情報を取得できません。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た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。

```
{
   "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。例えば、S3 バケットにポリシーをアタッチして、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 リソースの場合、IAM ポリシーでは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できます。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) 。リソースベースのポリシー AWS Directory Service はサポートされていません。

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。

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 ID (ユーザー、グループ、ロール) へのアクセス許可ポリシーをアタッチする、ID ベースのポリシーの例を示します。

> **Important**
>
> まず、 AWS Directory Service リソースへのアクセスを管理するための基本概念と使用可能なオプションについて説明する概要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 マネージド (事前定義) ポリシー AWS Directory Service
- お客様管理ポリシーの例
- 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。

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDsEc2IamGetRole",
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ec2:RevokeSecurityGroupIngress",
```

```
                "ec2:CreateNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "iam:GetRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
        },
        {
            "Sid": "AllowPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

ポリシーには次のものが含まれています。

- 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、リソースレベルでこの特定のアクションのアクセス許可をサポートしていません。したがって、ポリシーでは Resource の値としてワイルドカード文字 (*) を指定しています。

- 2 番目のステートメントは、特定の IAM アクションに対するアクセス許可が付与されます。がユーザーに代わって IAM ロール AWS Directory Service を読み取って作成できるようにするには、IAM アクションへのアクセスが必要です。`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、 がそのディレクトリを作成、設定、および破棄するために必要な特定の Amazon EC2 リソースセット AWS Directory Service にアクセス許可を付与します。`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 EC2 リソースおよびサブリソースに対して EC2 アクションを実行するアクセス許可を付与す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 (*) を特定のリソースまたはサブリソースに置き換えます。詳細については、「Amazon EC2 のアクション」を参照してください。

ID ベースのポリシーでアクセス許可を得るプリンシパルを指定していないため、ポリシーでは `Principal` 要素を指定していません。ユーザーに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

ユーザーが AWS Directory Service コンソールを操作するには、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、そのユーザーに必要ですAWS のマネージド (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 マネージド (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スタンドアロン 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、一般的ユースケースに必要な許

可を付与することで、どの許可が必要なのかをユーザーが調査する必要をなくすることができます。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。

アカウントのユーザーにアタッチできる次の AWS マネージドポリシーは、 に固有です AWS Directory Service。

- AWSDirectoryServiceReadOnlyAccess – 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、「AWS Directory Service での AWS 管理ポリシーの使用」を参照してください。
- AWSDirectoryServiceFullAccess – ユーザーまたはグループに以下を付与します。
  - 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

  詳細については、「AWS Directory Service での AWS 管理ポリシーの使用」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管理 AWS ポリシーが他にもあります。これらのポリシーは、 AWS Directory Service ディ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、これらのユーザーが 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、「ユーザーおよびグループに AWS リソースへのアクセス権限を付与する」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。

お客様管理ポリシーの例

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: 任意の AWS Directory Service リソースに対して任意の Describe アクションを実行することをユーザーに許可する
- 例 2: ディレクトリの作成をユーザーに許可する

例 1: 任意の AWS Directory Service リソースに対して任意の Describe アクションを実行することをユーザーに許可する

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。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

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。

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
         "Resource":"*"
         ]
      }
   ]
}
```

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 での 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。

次のタグポリシーの例では、タグとキーのペア "fooKey":"fooValue" が含まれている限り、ds の呼び出しはすべて許可されます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

次のリソースポリシーの例では、リソースにディレクトリ ID 「d-1234567890」が含まれている限り、ds の呼び出しはすべて許可されます。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
      },
      {
         "Effect":"Allow",
         "Action":[
            "ec2:*"
         ],
         "Resource":"*"
      }
   ]
}
```

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。

- AWS Directory Service API オペレーションの名前
- アクションを実行するためのアクセス許可を付与できる、対応するアクション
- 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:GetAuthorizedApplicationDetails`、`ds:UpdateAuthorizedApplications`、`ds:UnauthorizeApplication`、、`ds:CheckAlias`、、`ds:CreateIdentityPoolDirectory`、などの非パブリック AWS Directory Service API オペレーションの使用が必要になる場合があります。

一部の AWS Directory Service APIsは、 を介してのみ呼び出すことができます AWS Management Console。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 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。

関連トピック

- アクセスコントロール

を使用した AWS アプリケーションとサービスの承認 AWS Directory Service

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 アプリケーションが 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、そのユースケースに必要なアクセス許可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を以下に示します。

> **Note**
>
> 新しい AWS アプリケーションに Active Directory を許可するには、 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。

- Managed Microsoft AD、Simple AD、AD Connector ディレクトリのすべての組織単位 (OU) AWS の Active Directory ユーザー、グループ、組織単位、コンピュータ、または認証機関の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証中に 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の有効化の詳細については、「」を参照してください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 AWS アプリケーションとサービスの有効化の詳細については、「」を参照してください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。Simple AD の AWS アプリケーションとサービスの有効化の詳細については、「」を参照してください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。

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アクセス許可を削除するには、 アクセスds:UnauthorizedApplication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無効化します。

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、「ログ転送の有効化」を参照してください。さらに、 メトリクスを使用して CloudWatch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いつ追加するかを決めてください。」を参照してください。
- AWS CloudTrail - すべての AWS Directory Service ディレクトリタイプ CloudTrail で を使用できます。詳細については、「 を使用した AWS Directory Service API コールのログ記録 CloudTrail」を参照してください。

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、コンプライアンスプログラムAWS のサービス による対象範囲内のコンプライアンスプログラムを参照し、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 「コンプライアンスプログラム」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、「 でのレポートのダウンロード AWS Artifact」の」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 を提供しています。

- セキュリティとコンプライアンスのクイックスタートガイド – これらのデプロイガイドでは、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に重点を置いたベースライン環境 AWS を にデプロイする手順について説明します。
- アマゾン ウェブ サービスにおける HIPAA セキュリティとコンプライアンスのアーキテクチャ — このホワイトペーパーでは、企業が AWS を使用して HIPAA 対象アプリケーションを作成する方法について説明します。

  > **Note**
  >
  > すべて AWS のサービス HIPAA の対象となるわけではありません。詳細については、HIPAA 対応サービスのリファレンスを参照してください。

- 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、ガイダンスを保護し AWS のサービス 、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) を含む) のセキュリティコントロールに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、リソース設定が社内プラクティス、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リストについては、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 — これにより AWS アカウント、疑わしい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監視することで、、、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 は、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への対応に役立ちます。
- 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、および高度に冗長な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、 AWS Directory Service では、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できます。詳細については、「ディレクトリをスナップショットまたは復元する」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 は、ホワイトペーパー AWS Directory Service 「Amazon Web Services: セキュリティプロセスの概要」に記載されている AWS グローバルネットワークセキュリティの手順で保護されています。 https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

が AWS 公開している 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 Transport Layer Security (TLS) をサポートしている必要があります。TLS 1.2 以降を推奨しています。また、Ephemeral Diffie-Hellman (DHE) や Elliptic Curve Ephemeral Diffie-Hellman (ECDHE) などの Perfect Forward Secrecy (PFS) を使用した暗号スイートもクライアントでサポートされている必要があります。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。

コマンドラインインターフェイスまたは API AWS を介して にアクセスするときに FIPS 140-2 検証済みの暗号化モジュールが必要な場合は、FIPS エンドポイントを使用します。利用可能な FIPS エンドポイントの詳細については、「Federal information processing standard (FIPS) 140-2」(連邦情報処理規格 (FIPS) 140-2) を参照してください。

また、リクエストは、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、アカウント内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。

AWS Directory 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。そのアカウント内のリソースをクロスサービスの使用に関連付けることを許可する場合は、`aws:SourceAccount` を使用します。

次の例では、 の値は CloudWatch ロググループaws:SourceArn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:*servicename*:*:*123456789012*:* のように指定します。

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回避する方法を示しています。

```
{
  "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、「ap-southeast-1」がリージョン、123456789012」が顧客 ID、DirectoryMonitoring「_d-966739499f」が作成した Amazon SNS トピック名arn:aws:sns:ap-

southeast-1:123456789012:DirectoryMonitoring_d-966739499fであるようなものを使用できます。

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:*servicename*:*:*123456789012*:* のように指定します。

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回避する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:sns: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。

```
{
  "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

インターフェイス VPC エンドポイント を作成することで、Amazon VPC と AWS Directory Service API エンドポイント間のプライベート接続を確立できます。 インターフェイスエンドポイントは を使用しますAWS PrivateLink

AWS PrivateLink を使用すると、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 接続なしで API AWS Directory Service オペレーションにプライベートにアクセスできます。VPC と 間のトラフィック AWS Directory Service は AWS ネットワークを離れません。

各インターフェイスエンドポイントは、サブネット内の 1 つ以上の Elastic Network Interface によって表されます。Elastic Network Interface の詳細については、「Amazon EC2 ユーザーガイド」の「Elastic Network Interface」を参照してください。 Amazon EC2

VPC エンドポイントの詳細については、「Amazon VPC ユーザーガイド AWS のサービス 」の「インターフェイス VPC エンドポイントを使用して にアクセスする」を参照してください。 AWS Directory Service API オペレーションの詳細については、「 API AWS Directory Service リファレンス」を参照してください。

VPC エンドポイントに関する考慮事項

AWS Directory Service API エンドポイントのインターフェイス VPC エンドポイントを設定する前に、「 AWS PrivateLink ガイド」の「インターフェイス 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」を確認してください。

AWS Directory Service リソースの管理に関連するすべての AWS Directory Service API オペレーションは、 を使用して VPC から使用できます AWS PrivateLink。

VPC エンドポイントポリシーは、 Directory Service API エンドポイントでサポートされています。デフォルトでは、エンドポイント経由で Directory Service API オペレーションへのフルアクセスが許可されます。詳細については、「Amazon VPC ユーザーガイド」の「エンドポイントポリシーを使用して VPC エンドポイントへのアクセスを制御する」を参照してください。

可用性

AWS Directory Service は、次の で VPC エンドポイントをサポートします AWS リージョン。

AWS リージョン 可用性

- 米国東部 (バージニア北部)
- 米国東部 (オハイオ)
- 米国西部 (北カリフォルニア)
- 米国西部 (オレゴン)
- アフリカ (ケープタウン)
- アジアパシフィック (香港)
- アジアパシフィック (ハイデラバード)
- アジアパシフィック (ジャカルタ)
- アジアパシフィック (メルボルン)

- 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 (東京)
- カナダ (中部)
- カナダ西部 (カルガリー)
- 中国 (北京および寧夏)
- アジアパシフィック (香港)
- 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 (ミラノ)
- 欧州 (パリ)
- 欧州 (スペイン)
- 欧州 (ストックホルム)
- 欧州 (チューリッヒ)
- イスラエル (テルアビブ)
- 中東 (バーレーン)
- 中東 (アラブ首長国連邦)
- 南米 (サンパウロ)
- AWS GovCloud （ 米国東部 ）
- AWS GovCloud （ 米国西部 ）

API 用の AWS Directory Service インターフェイスエンドポイントの作成

AWS Directory Service API の VPC インターフェイスエンドポイントは、Amazon VPC コンソールまたは AWS Command Line Interface () を使用して作成できますAWS CLI。詳細については、『AWS PrivateLink ガイド』の「Create a VPC endpoint (VPC エンドポイントを作成)を参照してください。

次のサービス名を使用して AWS Directory Service 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`

中国を除き、エンドポイント AWS リージョン のプライベート DNS を有効にすると、 などの のデフォルト DNS 名を使用して AWS リージョン、VPC エンドポイント AWS Directory Service でに API リクエストを実行できますds.us-east-1.amazonaws.com。中国 (北京および寧夏) では AWS リージョン、ds-api.cn-northwest-1.amazonaws.com.cnそれぞれ ds-api.cn-north-1.amazonaws.com.cnと を使用して VPC エンドポイントで API リクエストを行うことができます。

詳細については、「Amazon VPC ユーザーガイド」の「インターフェイス 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 API 用の VPC エンドポイントポリシーの作成

VPC エンドポイントに AWS Directory Service API へのアクセスをコントロールするエンドポイントポリシーをアタッチできます。このポリシーでは、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。
- 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、「Amazon VPC ユーザーガイド」の「エンドポイントポリシーを使用して VPC エンドポイントへのアクセスを制御する」を参照してください。

例: AWS Directory Service API アクションの VPC エンドポイントポリシー

AWS Directory Service API のエンドポイントポリシーの例を次に示します。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、リストされている AWS Directory Service API アクションへのアクセスが許可されます。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeCertificate",
         ],
```

```
         "Resource":"*"
      }
   ]
}
```

例: 指定された からのすべてのアクセスを拒否する VPC エンドポイントポリシー AWS アカウント

次の VPC エンドポイントポリシーは、エンドポイントを使用した リソースへのすべてのアクセスを拒否 AWS アカウント します。*123456789012* このポリシーは、他のアカウントからのすべてのアクションを許可します。

```
{
   "Statement": [
      {
         "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal:" "*"
      },
      {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "*",
        "Principal": {
            "AWS": [
               "123456789012"
            ]
         }
      ]
}
```

AWS Directory Service のサービスレベルアグリーメント

AWS Directory Service は、非常に可用性の高いサービスであり、AWS が管理するインフラストラクチャ上に構築されています。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アグリーメントによってバックアップされています。

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 Connector	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 (北カリフォルニア)	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 (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
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

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 (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
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	 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

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 (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	 いいえ
カナダ西部 (カルガリー)	ca-west-1	ds.ca-west-1.amazonaws.com	HTTPS	 はい	 はい	 いいえ
中国 (北京)	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	 はい	 はい	 いいえ
中国 (寧夏)	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	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
欧州 (フランクフルト)	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	 はい	 はい	 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	 いいえ
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

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
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
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

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
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

（米国西部）リージョンおよび AWS GovCloud（ AWS GovCloud 米国東部）リージョン AWS Directory Service での の使用については、「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 の使用については、「中国 での Amazon Web Services のエンドポイントと ARNs」を参照してください。

ブラウザの互換性

AWS 、Amazon WorkSpaces、Amazon Connect WorkMail、Amazon Chime、Amazon などの アプリケーションおよびサービス AWS IAM Identity Center には WorkDocs、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。 Amazon Connect 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 バージョン	互換性あり
Mozilla Firefox	最新の 3 バージョン	互換性あり
Google Chrome	最新の 3 バージョン	互換性あり
Apple Safari	最新の 3 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、および 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
証明書ベースの認証設定	AWS 管理対象の 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) リージョンでのスマートカードと Amazon WorkSpaces アプリケーションマネージャのサポートに関するコンテンツを追加しました	2020 年 12 月 1 日
パスワードのリセット	AWS Management Console、Windows PowerShell AWS CLI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。	2019 年 1 月 2 日

ディレクトリ共有	AWS 管理対象の 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	AWS オンプレミスユーザーに割り当てることができる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 のディレクトリにドメインコントローラーを追加する方法に関するコンテンツを追加しました。	2017 年 6 月 30 日
チュートリアル	AWS マネージド 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 マネージド型Microsoft AD による MFA	AWS マネージド 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	Microsoft Active Directory AWS 用Directory Service 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	での IAM の使用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 マネージドMicrosoft AD	AWS マネージド 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。