AWS Managed Microsoft AD

AWS Black Belt Online Seminar

アマゾンウェブサービスジャパン株式会社
技術統括本部　ソリューションアーキテクト

伊藤 ジャッジ向子

2021年8月

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

このセッションでお話しすること

1. ディレクトリサービスとは
2. AWS Managed Microsoft Active Directory
3. AWSの他のディレクトリサービス
4. How to…
5. 料金

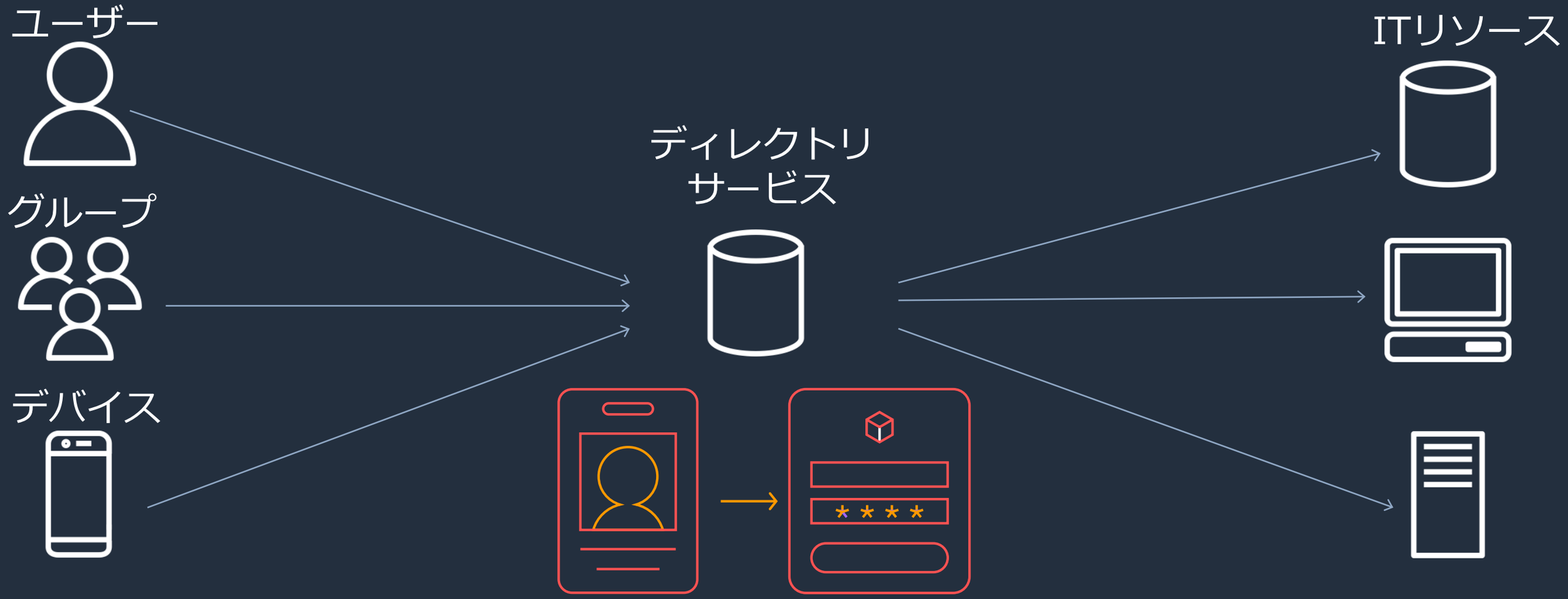
aws

このセッションでお話しすること

1. ディレクトリサービスとは
2. AWS Managed Microsoft Active Directory
3. AWSのディレクトリサービス
4. How to…
5. 料金

aws

ディレクトリサービスとは



このセッションでお話しすること

1. ディレクトリサービスとは
2. AWS Managed Microsoft Active Directory
3. AWSの他のディレクトリサービス
4. How to…
5. 料金

aws

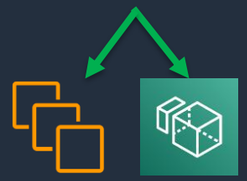
Active Directoryの変遷

AWS Managed Microsoft Active Directory (以降AWS Managed Microsoft AD)

AWS Managed Microsoft AD の特徴

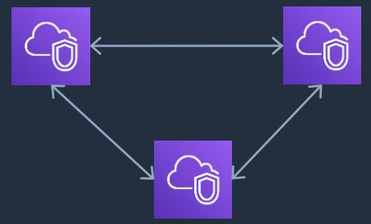
本物のMicrosoft AD

信頼関係のサポート

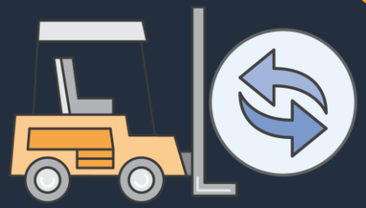


グループポリシー

シームレスなドメイン参加



複数アカウントや複数リージョンでの利用可能



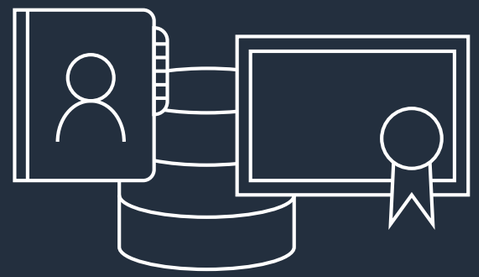
日次の
スナップショット

AWSが管理する
インフラストラクチャ

AWS Managed Microsoft AD の利点

簡単にWindows ワークロードをAWS上に移行して、既存のID管理とつなぐことができる

クラウドとオンプレのユーザー情報を同期は必要なし



Windows Server 2012R2 上で稼働する使い慣れたAD管理ツールの機能

New

2021年7月　AWS Managed Microsoft AD が大阪リージョンでご利用いただけるようになりました
https://aws.amazon.com/jp/blogs/news/aws-directory-service-for-microsoft-active-directory-ad-connector-osaka/

aws

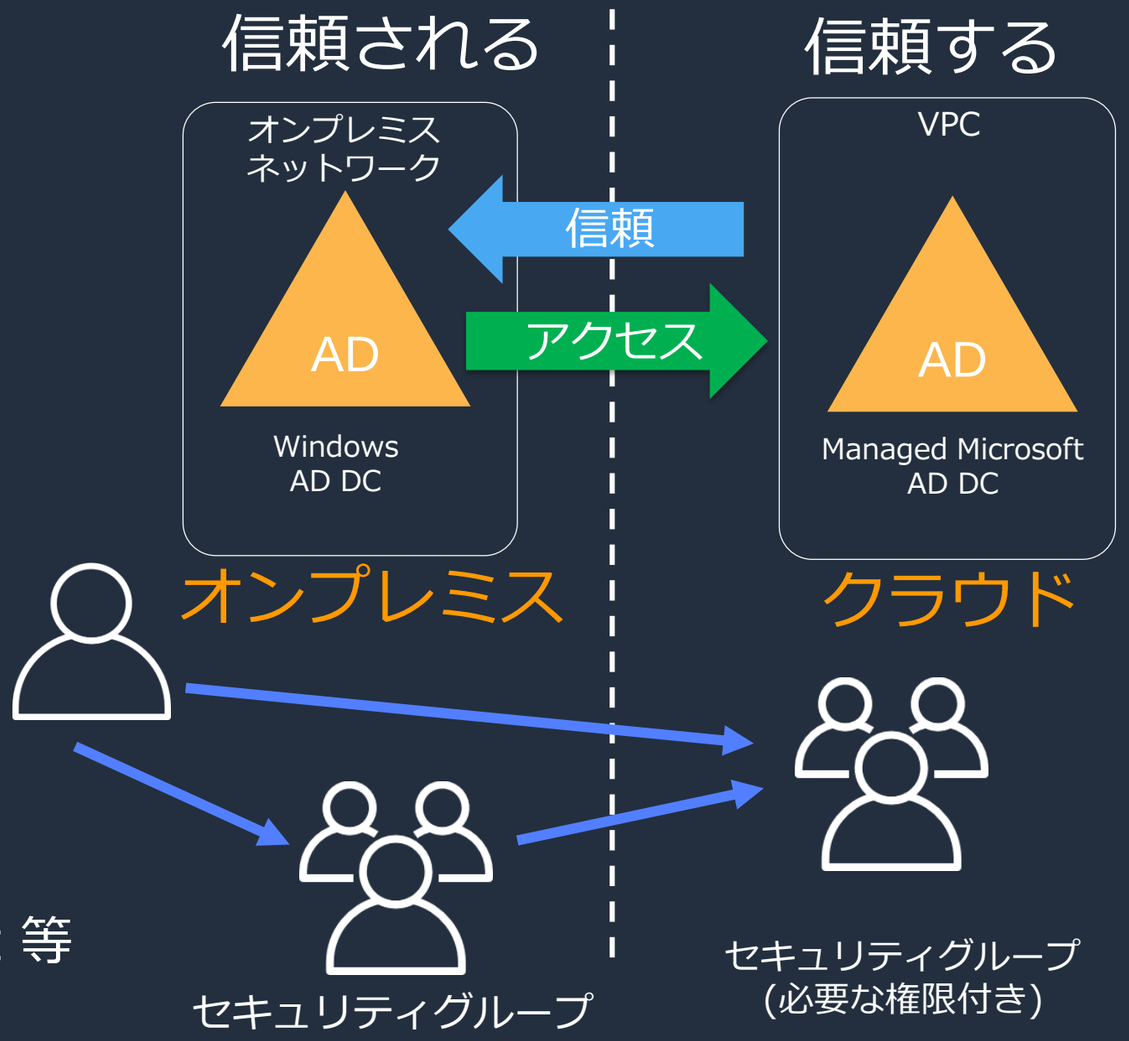
信頼関係とは

フォレストの信頼関係

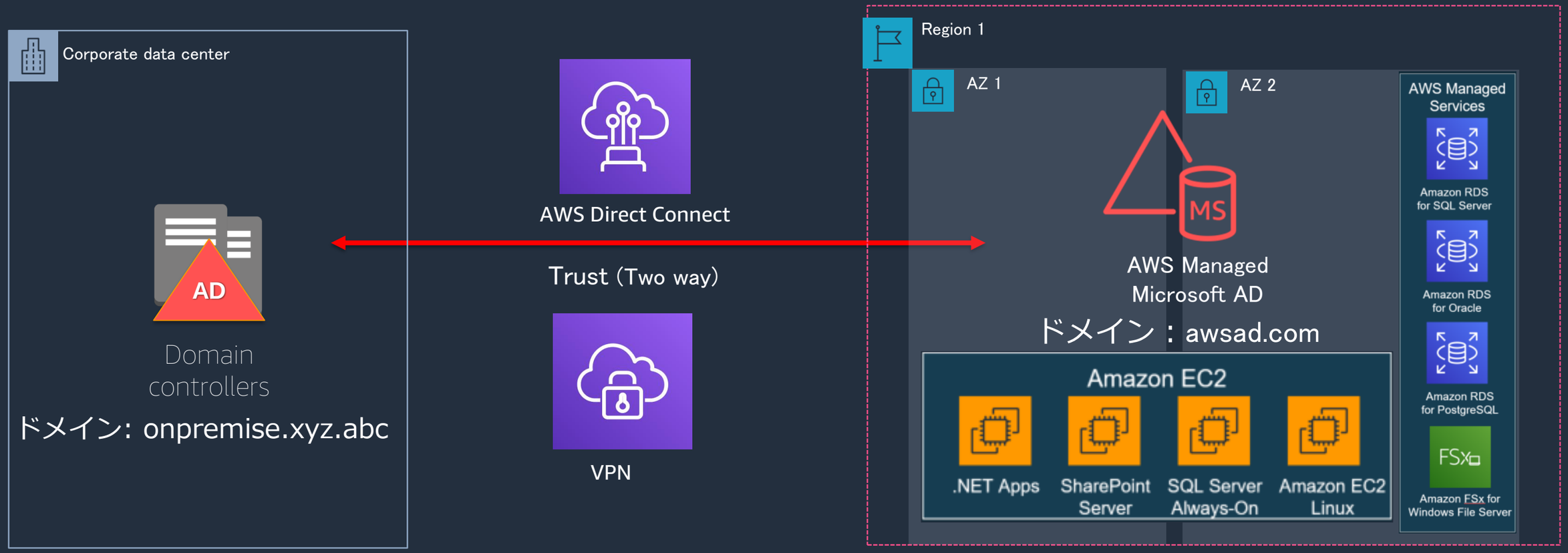
- デフォルトでは互いにアクセスできない
- 信頼関係によりディレクトリ内のオブジェクトを読める

- 一方向、双方向どちらが必要か
  - 一方向：EC2 & RDS SQL Server
  - 双方向：Workspaces, Chime & QuickSight 等企業向けアプリケーションサービス

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_setup_trust.html



使い方の一例



New

2021年8月 Amazon FSx が大阪リージョンでご利用いただけるようになりました
https://aws.amazon.com/jp/blogs/news/amazon-fsx-osaka/

信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

aws

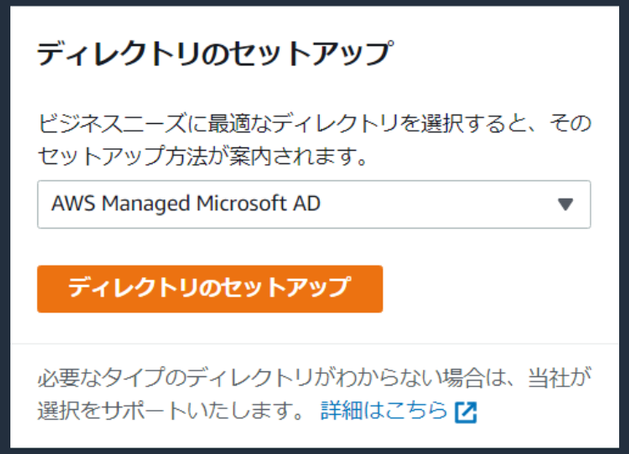
信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

aws

AWS Managed Microsoft AD ディレクトリを作成する

1.



2.

3.

4.

5.

IPアドレスは不変

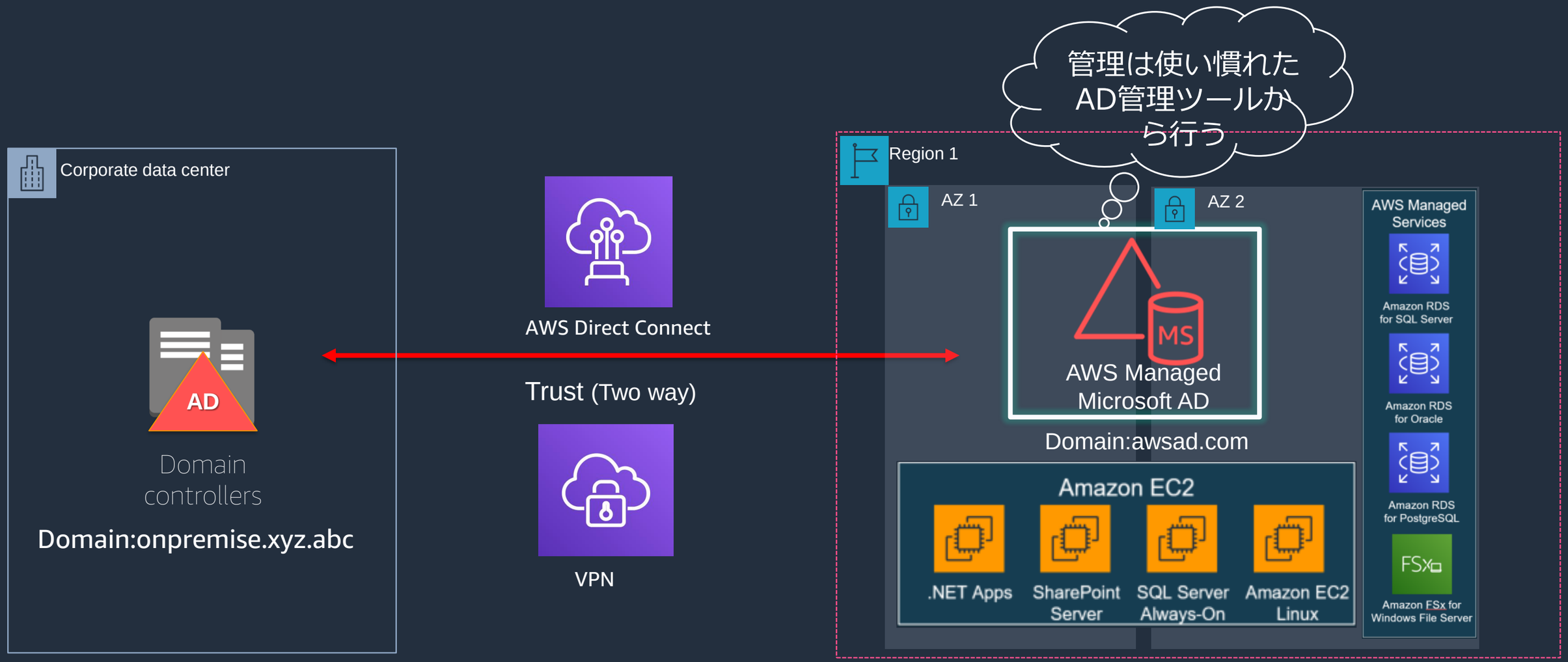
https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/ms_ad_getting_started_create_directory.html

信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

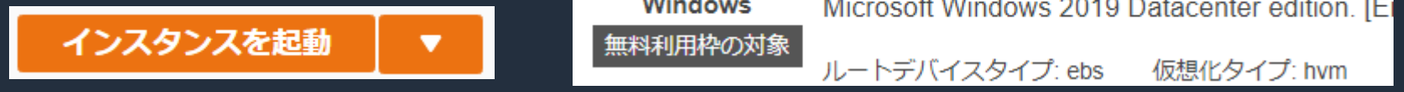
aws

AWS側のMSADを管理するサーバーを立てる



MSADを管理するサーバーを立てる

1. Windows インスタンスを選択する



2. ドメイン 結合ディレクトリ指定することで、Windows インスタンスが自動的にドメインに参加する

3. RDP接続を許可する

IAM ロールに以下の二つのポリシーをアタッチします

- **AmazonSSMManagedInstanceCore**
- **AmazonSSMDirectoryServiceAccess**

信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

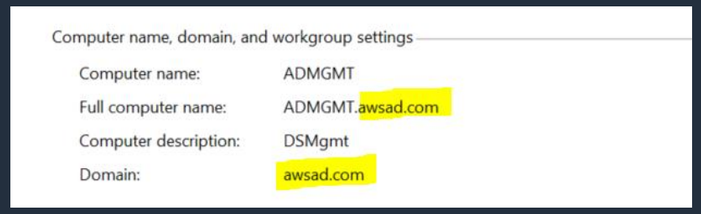
aws

管理用サーバーにツールをインストール

1. Windows インスタンスにドメインユーザで接続する

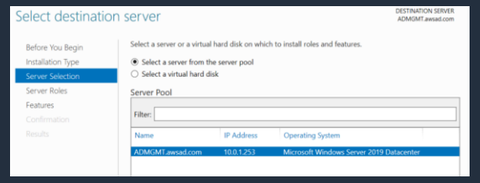
AD管理者
(もしくは権限の
あるユーザー)

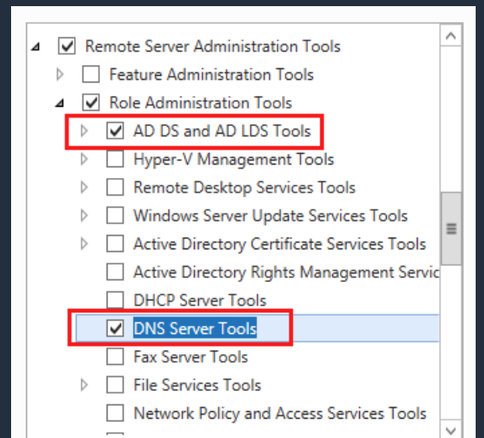
2. ドメインに参加しているか確認する

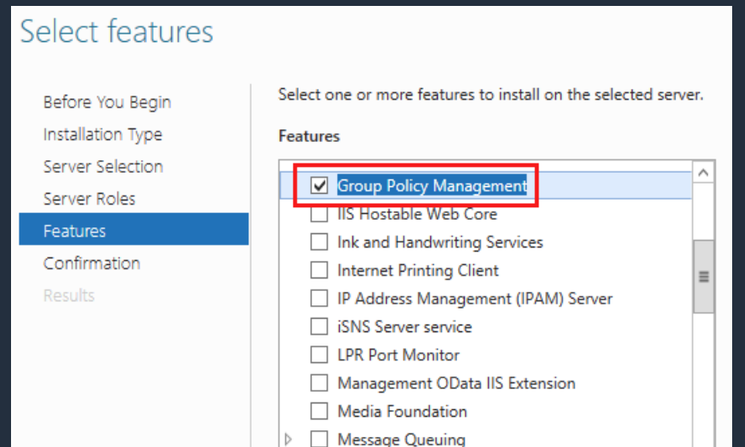


- AD DS および AD LDS ツール
  - アクティブディレクトリの管理
- DNS サーバーツール
  - ドメインコントローラの機能内でDNSを管理
- グループポリシーマネジメントツール（Optional）
  - グループポリシーの管理

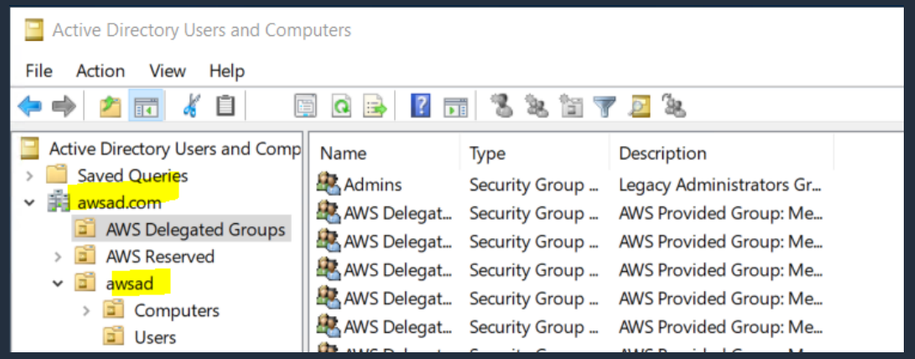
3. サーバ マネージャーからツールをインストールする

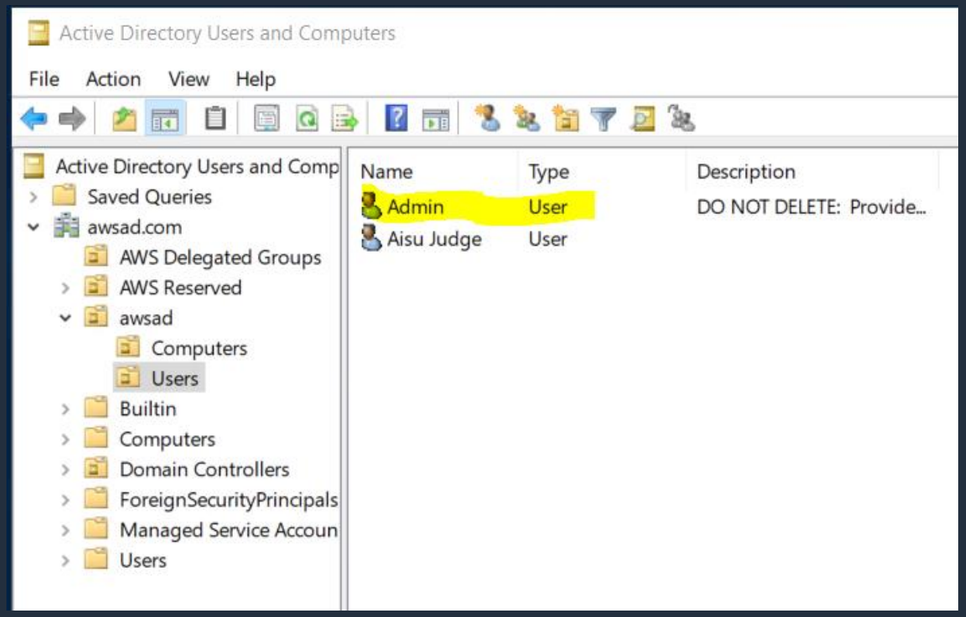






MSADを管理するサーバーで確認



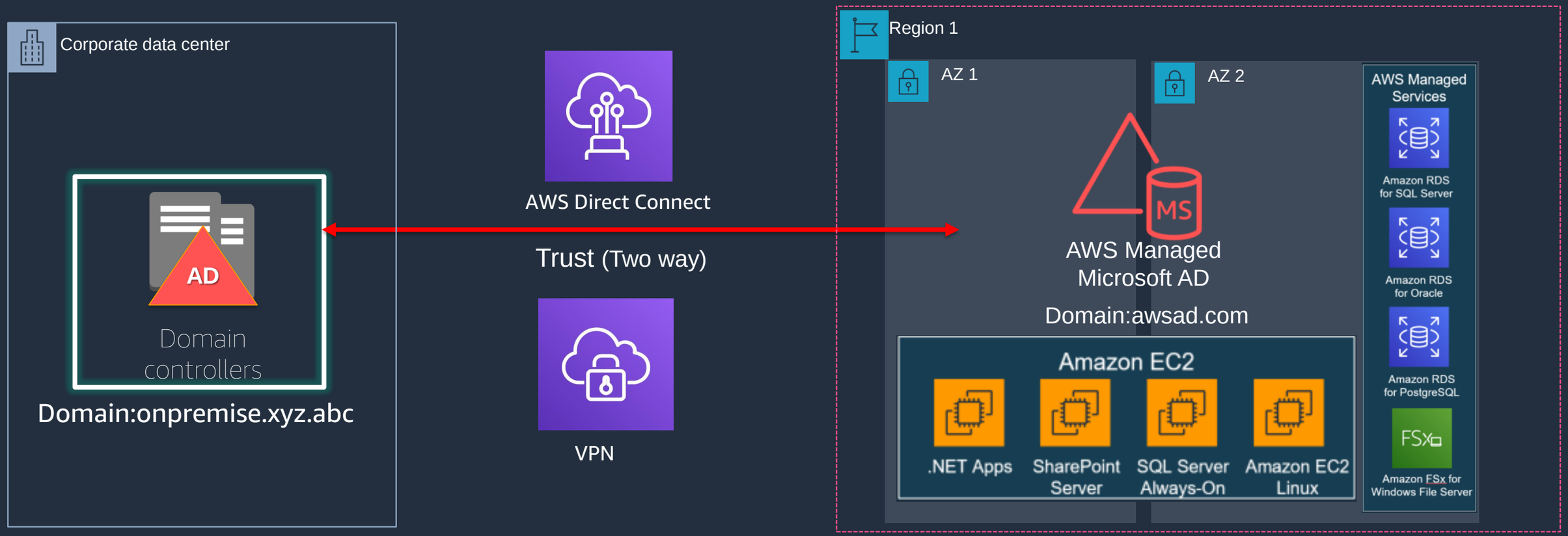


信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

aws

オンプレミス側のADを設定する



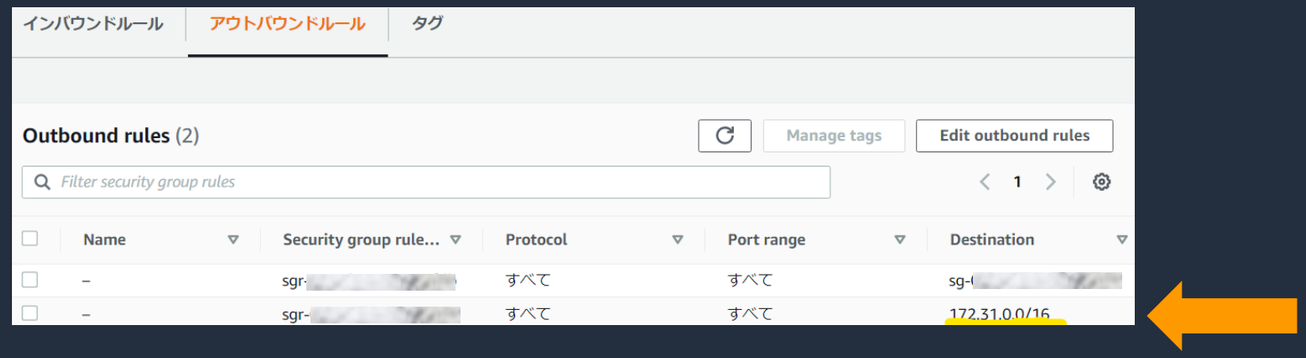
AWS – オンプレミス間の通信

- DNS (TCP & UDP 53)
- Kerberos 認証(TCP & UDP 88)
- LDAP (TCP & UDP 389)
- SMB (TCP & UDP 445)

参照：https://docs.microsoft.com/ja-jp/archive/blogs/jpntsblog/563

AD 側

セキュリティグループ
d-{ディレクトリID}_controller

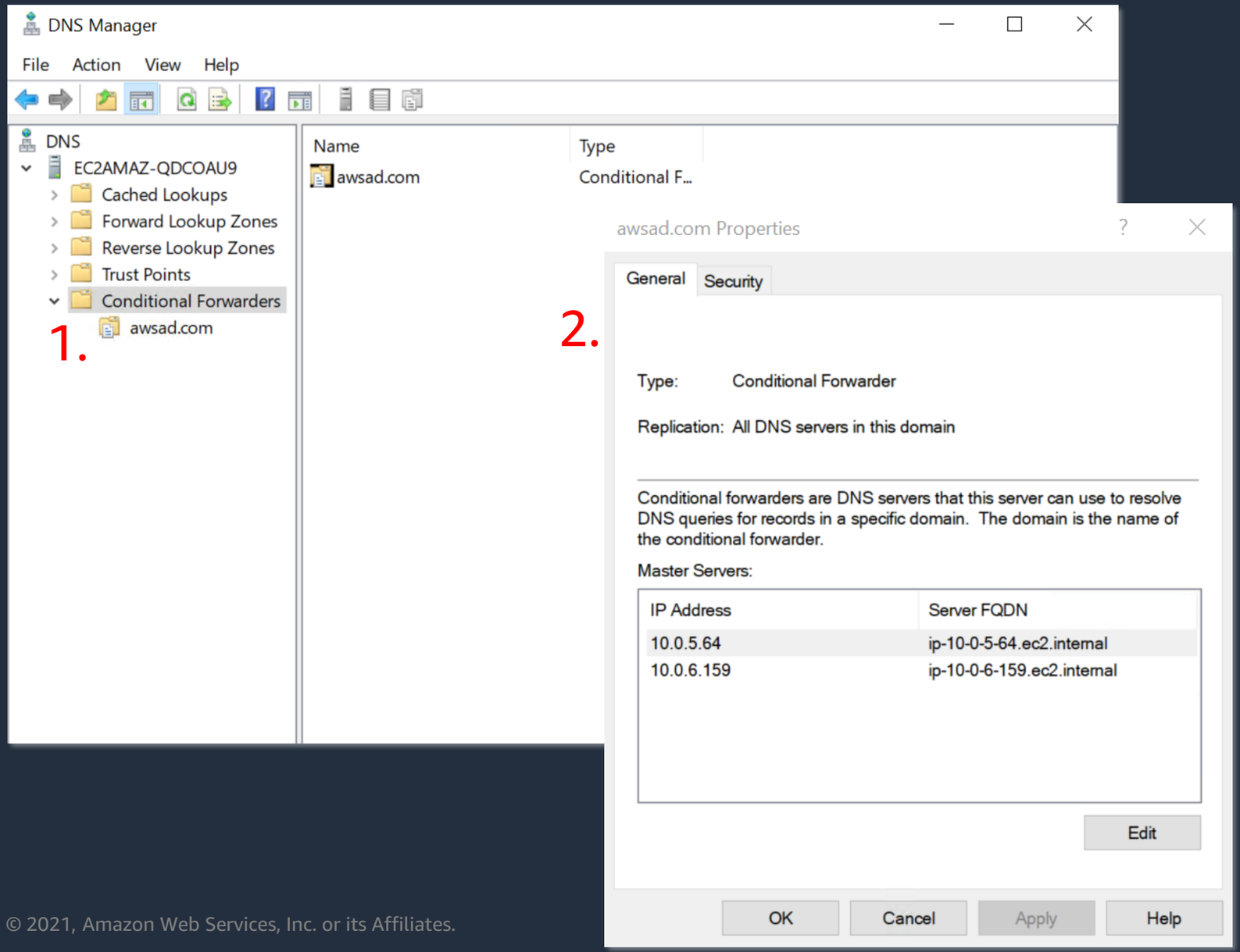


参照：
https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/ms_ad_network_security.html
https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/ms_ad_tutorial_setup_trust.html

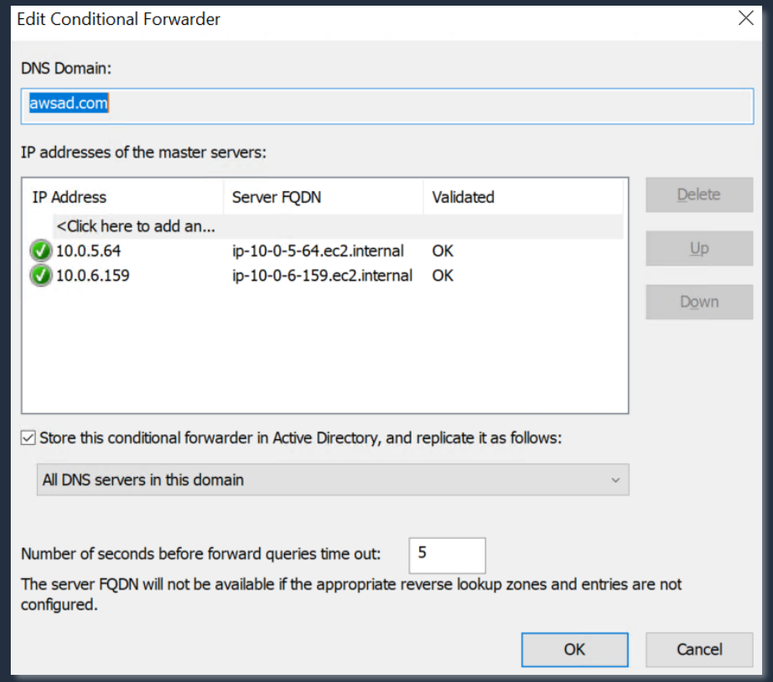
信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

オンプレミスのActive DirectoryのDNSの設定



3. マネジメントコンソールで作成した時払い出された二つのDNSサーバーのIPアドレス



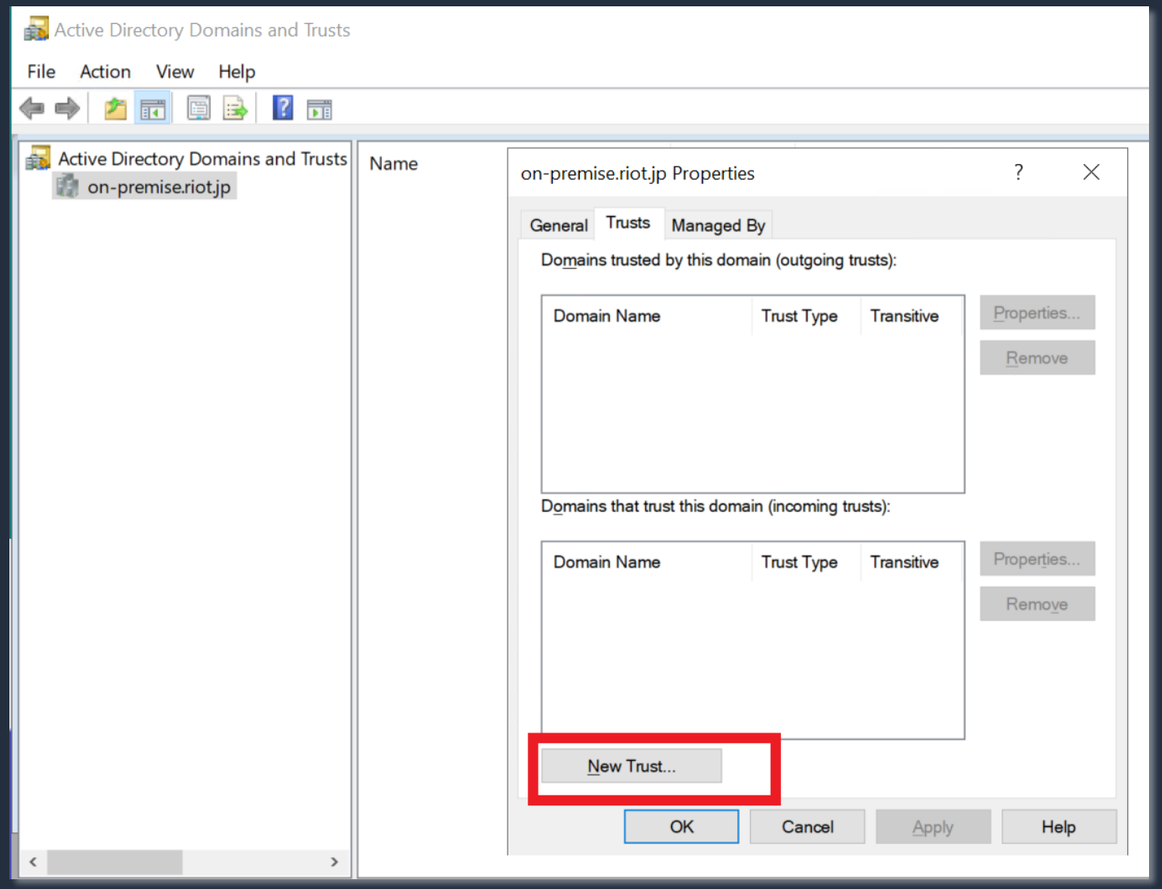
信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

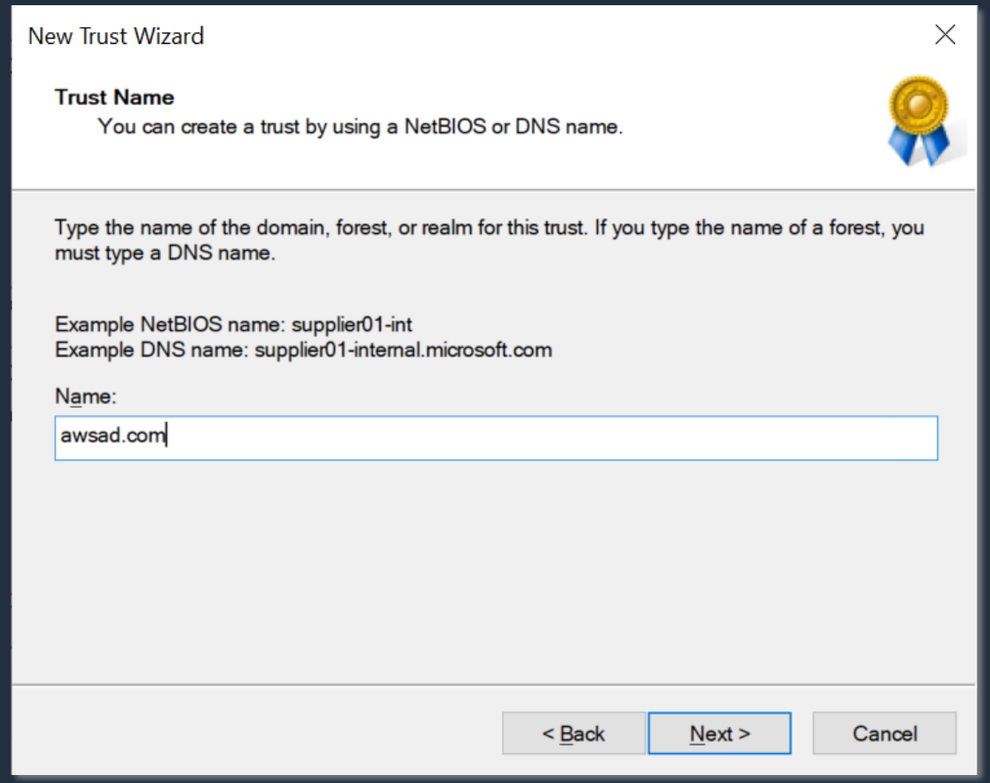
aws

オンプレミスの信頼関係の検証

1.



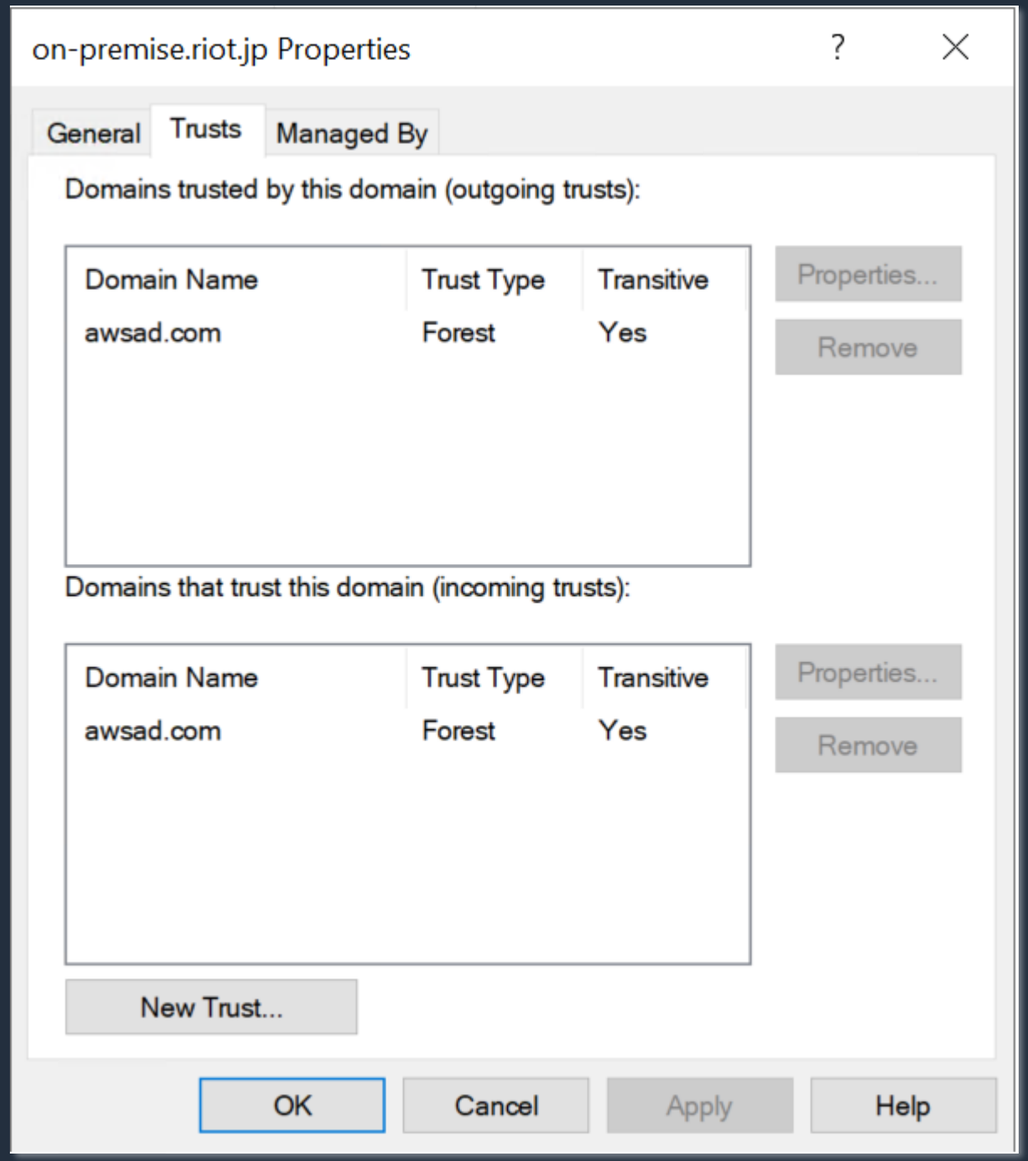
2.



例）

- 信頼のタイプ:フォレストの信頼
- 信頼の方向:双方向
- 信頼を作成する対象:このドメインのみ
- フォレスト全体の認証を指定
  信頼パスワード:
- 新しい信頼
  出力方向＆入力方向:両方とも確認しない

オンプレミスの検証確立



信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

aws

セットアップ手順　AWS Microsoft Managed AD

1.

2.

例）

1. 信頼のタイプ→フォレストの信頼
2. 既存または新しいリモートドメイン
   →オンプレミスのFQDNドメイン
3. 信頼パスワード
   →先ほどオンプレミスで入力したパスワード
4. 信頼の方向→双方向
5. 条件付きフォワーダー
   →オンプレミスで使用しているDNSサーバー

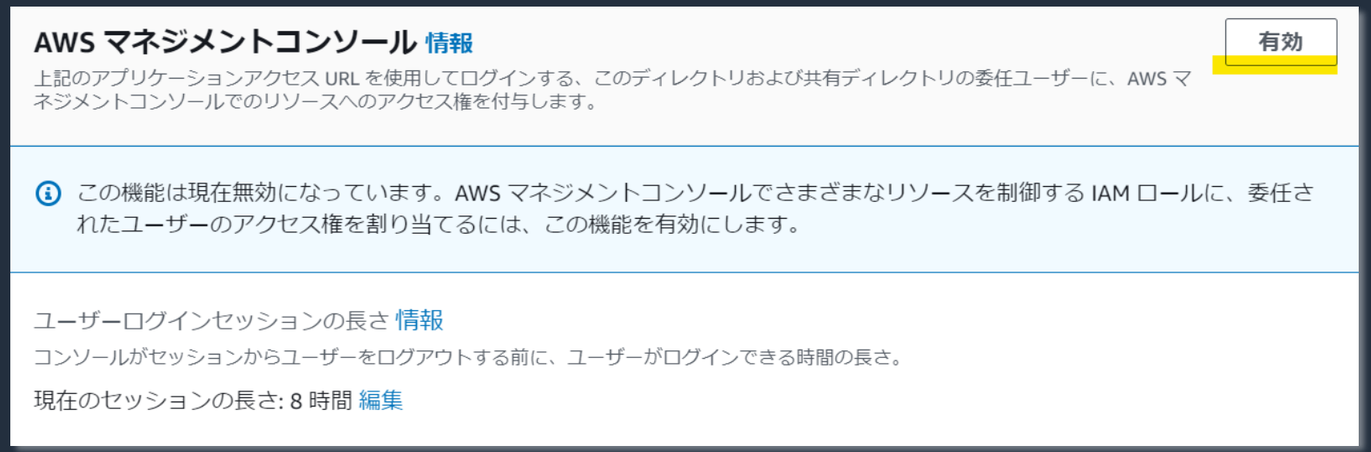
3.

信頼関係の設定（双方向）

1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

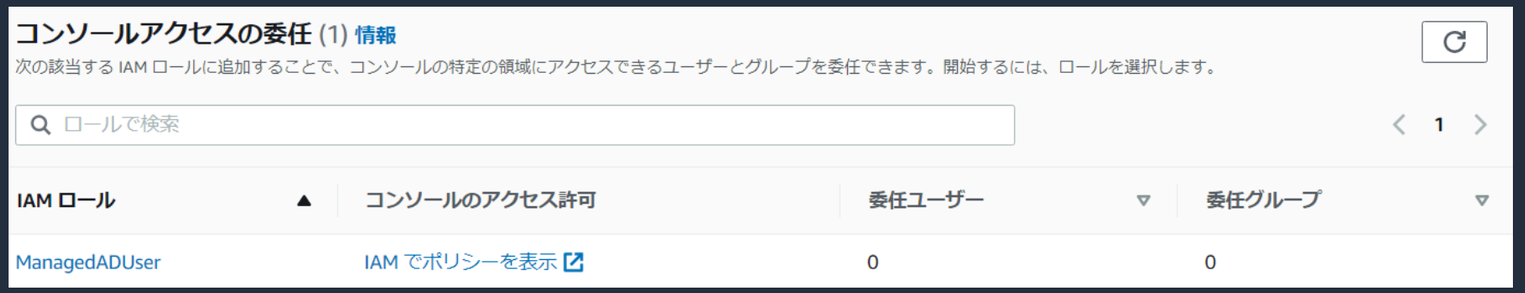
AWSマネジメントコンソール使用ユーザーの設定

1.



2.

3.



※ AWS Single Sign-On：マネジメントコンソールへのログインを可能にする同様のサービスもある
（SSOが使える場合はそちらが推奨）

信頼関係の設定（双方向）

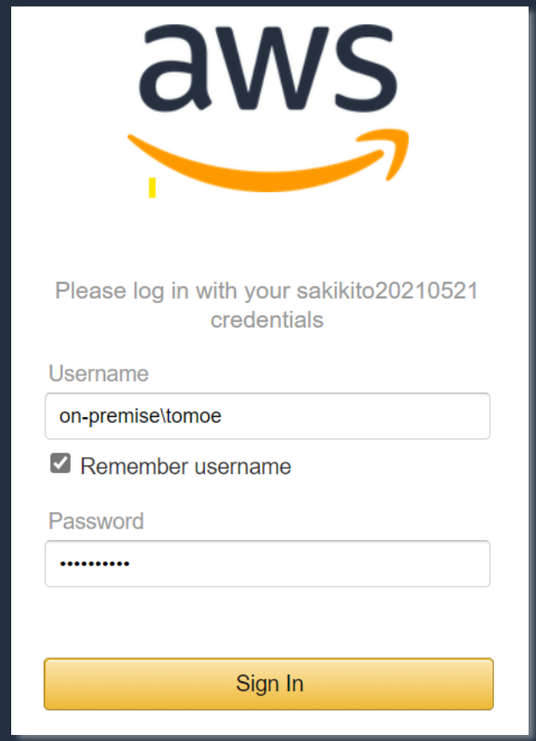
1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
    1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
    1. DNS設定
    2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
    1. AWSマネジメントコンソール使用ユーザーの設定

セットアップ手順　ユーザーログイン

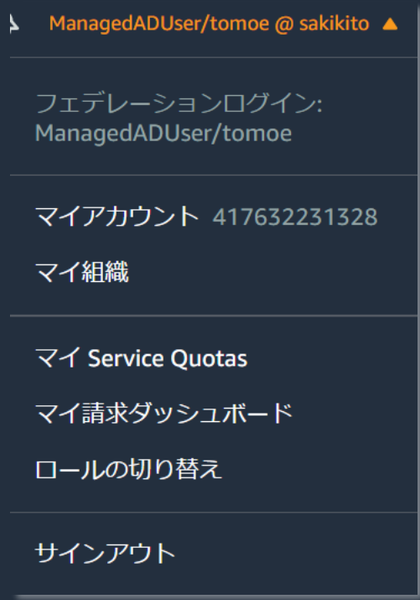
1.

2.

3.



文字列.awsapps.com/console



AWS Managed Microsoft ADで何ができるか

- 実際のMicrosoft Active Directory (2012 R2)
- シングルテナントでマネージドサービス
- デフォルトで2つのドメインコントローラ
- 複数リージョンでレプリケーション可能（Enterprise Edition）
- 権限を委譲されたAdmin Account を使用して OUを管理
- 通常のAD管理ツールを使うことができる
- 管理されたインフラで自動パッチとバックアップ
- 他のAWSサービス群とシームレスな連携
    - AWS SSO, Amazon FSx for Windows File Server, Amazon Workspaces, Amazon WorkDocs, Amazon WorkMail, Amazon RDS for SQL Server, Oracle, PostgreSQL

aws

AWS Managed Microsoft ADでの制限事項

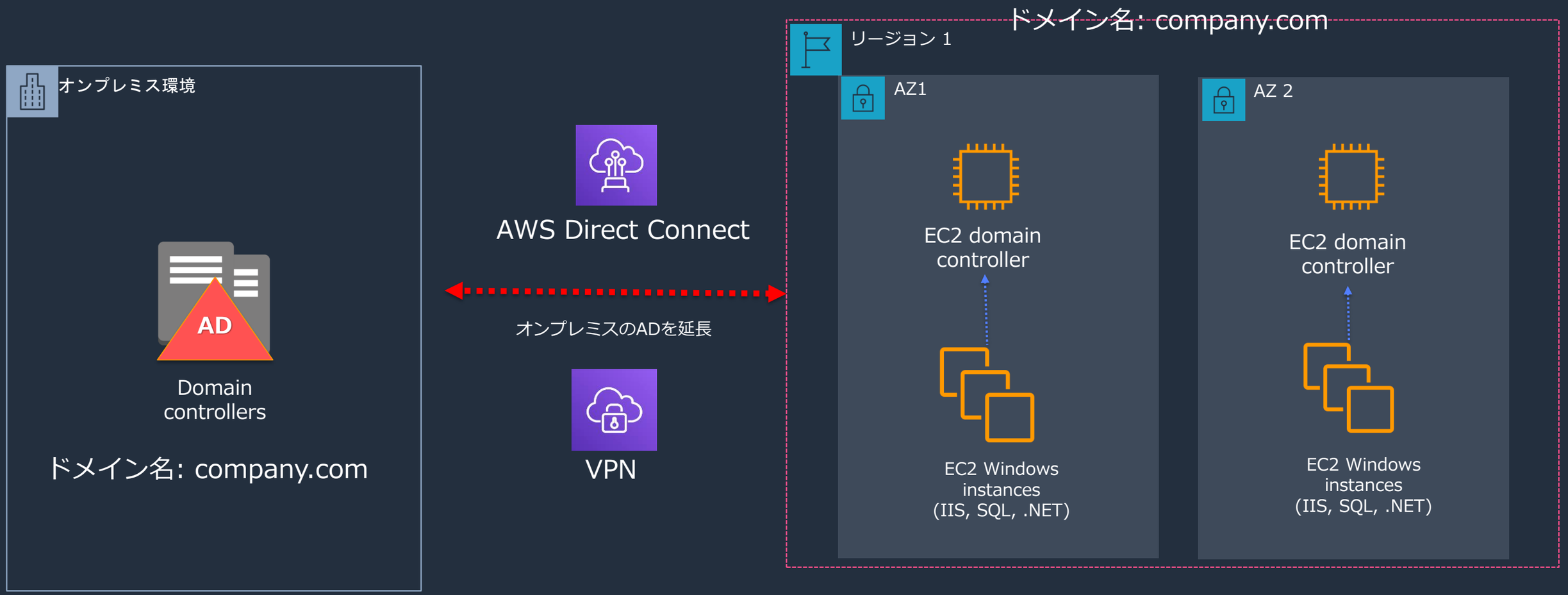
- ドメイン管理者としての権限の制限
- オンプレミスのドメインと同一のドメインの延長 [1]

- サービスクオータ（上限緩和可） [2]
  - デフォルトでは20ディレクトリ
  - 手動でのスナップショットは5つまで
  - ディレクトリごとのドメインコントローラーは20まで
  - ディレクトリごとのCA(Certification Authority)登録は5つまで

[1] https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/ms_ad_getting_started_admin_account.html
[2] https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/ms_ad_limits.html

aws

EC2 インスタンスでActive Directoryを運用



このセッションでお話しすること

1. ディレクトリサービスとは
2. AWS Managed Microsoft AD
3. AWSの他のディレクトリサービス
4. How to …
5. 料金

AWSの他のディレクトリサービス

- **AD Connector**
  - 既存のオンプレミスのActive Directoryユーザー情報でAWSリソース利用
  - クラウド側でのユーザー管理が必要ない場合
  - オンプレミスでユーザー管理のみを行うシンプルな構成が可能
  - オンプレミス側ADへの問い合わせが発生する
- **Simple AD**
  - 低コスト
  - アクティブディレクトリと互換性のあるSamba4のサービスを提供
  - 5000ユーザー以下でユーザー管理
  - ユーザーとグループ管理だけで十分な場合
  - オンプレミスとの信頼関係は使用不可

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/what_is.html

aws

このセッションでお話しすること

1. ディレクトリサービスとは
2. AWS Managed Microsoft AD
3. AWSの他のディレクトリサービス
4. How to…
5. 料金

ディレクトリのモニタリング

- ディレクトリのステータス
  - ステータスの遷移をトリガに SNSによる通知の設定可能

- CloudWatch Logs
  - ログインしたアカウント
  - アクセスしたオブジェクト
  - ポリシーの変更　etc…

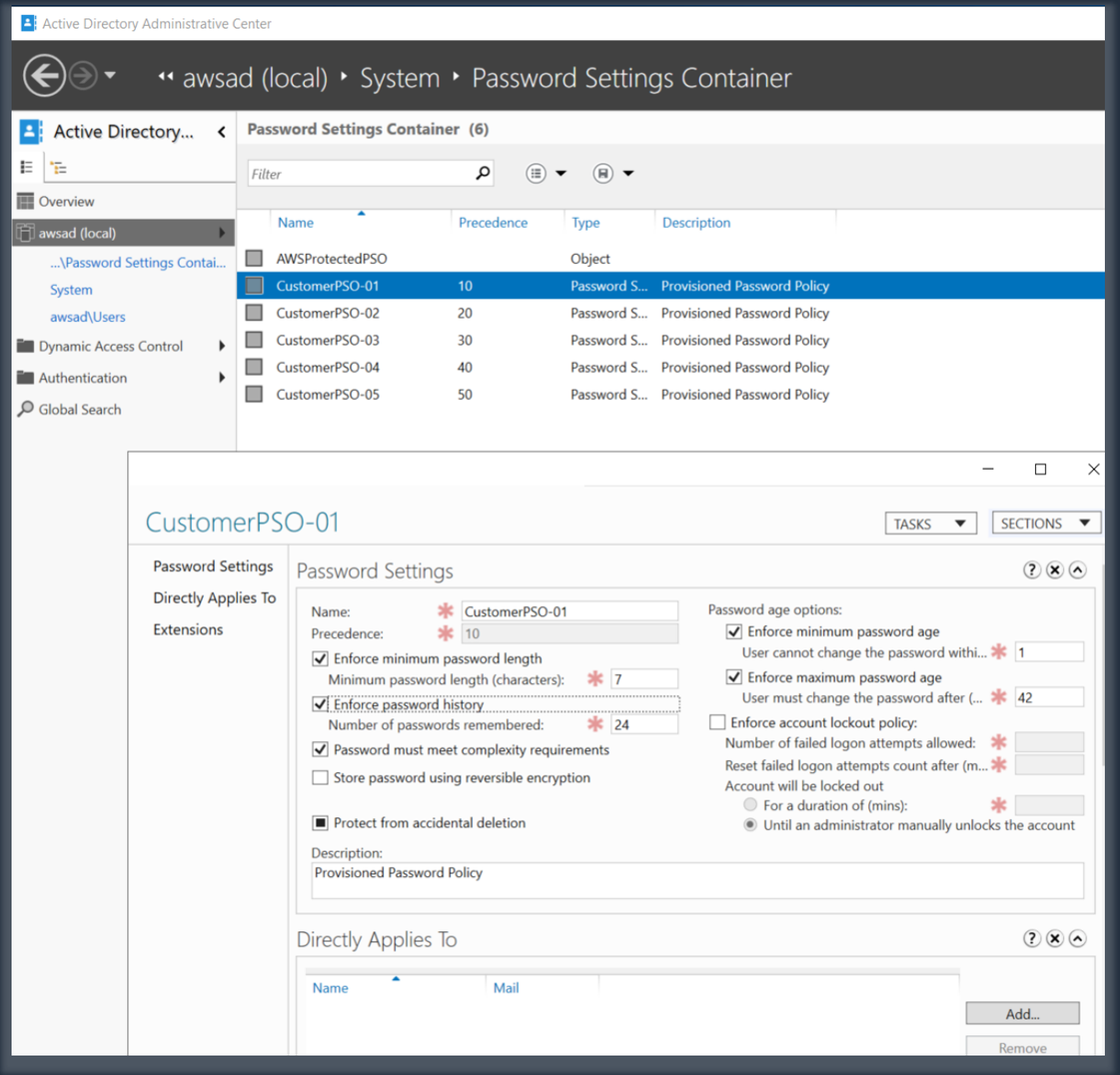
```
Subject:
   Security ID:            S-1-5-18
   Account Name:           WIN-ILO1BA61LUC$
   Account Domain:         awsad
   Logon ID:               0x49B8EF

Privileges:         SeSecurityPrivilege
                    SeBackupPrivilege
                    SeRestorePrivilege
                    SeTakeOwnershipPrivilege
                    SeDebugPrivilege
                    SeSystemEnvironmentPrivilege
                    SeLoadDriverPrivilege
                    SeImpersonatePrivilege
```

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_directory_status.html

https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_directory_logs.html

パスワードルールはどう設定するの？

- デフォルトのパスワードルールがある
  - 7文字以上
  - 過去の24のパスワード履歴を記録
  - 42日間で期限切れ
  - 複雑な文字列
- デフォルトの変更は可能
  - 管理インスタンス
    →Active Directory Administrative Center
  - ドメイン→ System
    →Password Settings Container
  - PSOから始まる5つのポリシーを変更
    → 「Add」からユーザーやグループに適用



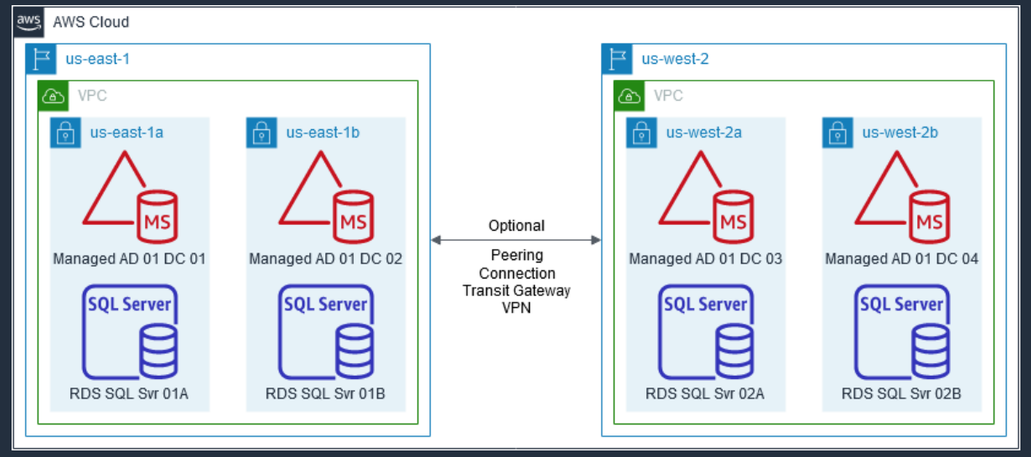
https://aws.amazon.com/blogs/security/how-to-configure-even-stronger-password-policies-to-help-meet-your-security-standards-by-using-aws-directory-service-for-microsoft-active-directory/

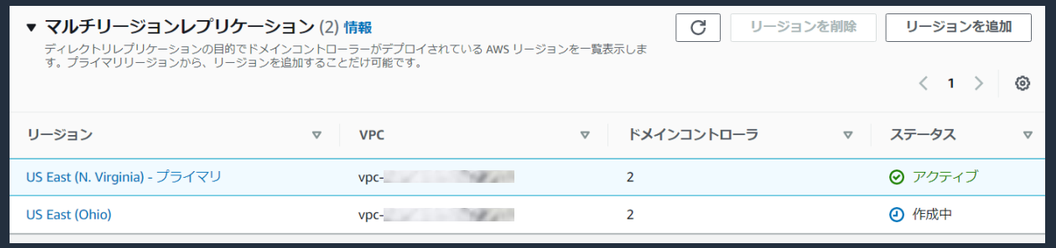
マルチリージョンの設定方法

エンタープライズエディションを使用

例）RDS for SQL Serverの場合

- 双方のリージョンでのDB作成時にディレクトリを指定
  - Microsoft SQL Server Windows 認証を有効化

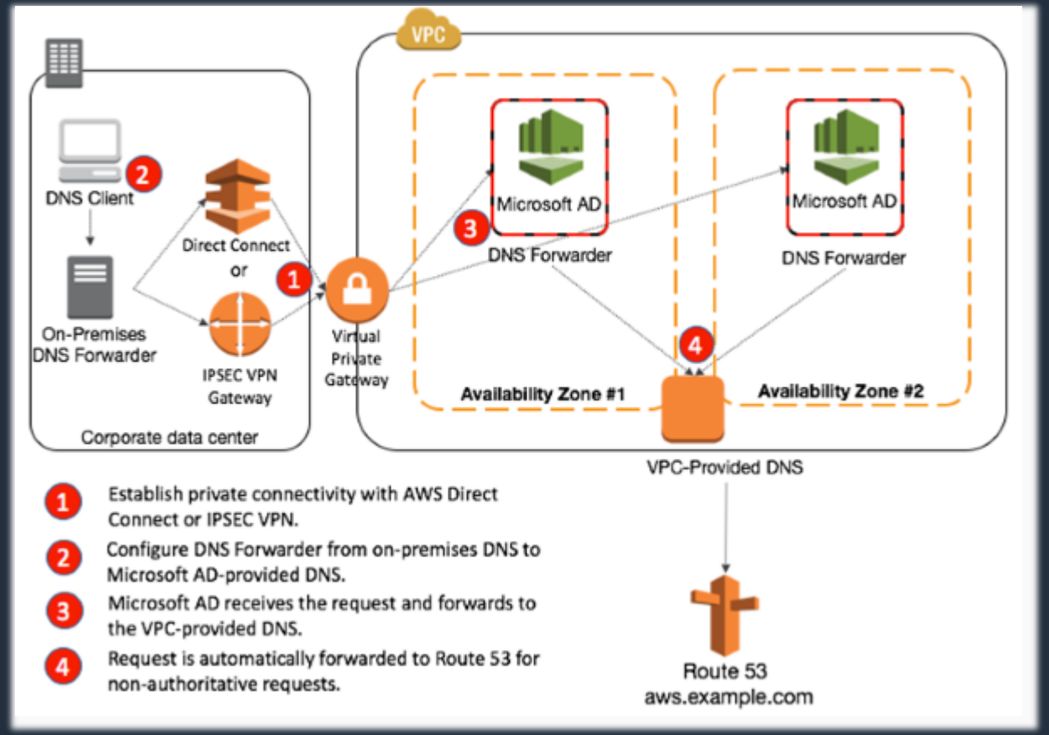




https://aws.amazon.com/blogs/security/use-a-single-aws-managed-microsoft-ad-for-amazon-rds-for-sql-server-instances-in-multiple-regions/

Route53 の Private Hosted Zone の名前解決を行うには？

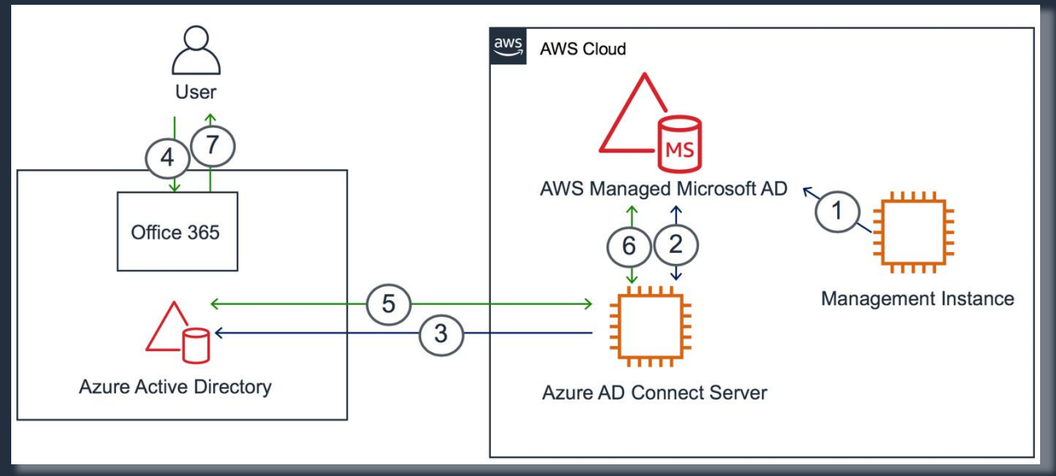
- 転送ルールの設定
  - DNS管理ツールでDirectory ServiceのDNSのIPアドレスに接続　-> 条件付きフォワーダー
  - プライベートドメインの DNS クエリを VPC の Amazon が提供する DNS サーバーの IP アドレスに転送
    - 例）192.168.0.0/24のネットワークなら192.168.0.2



https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-using-aws-directory-service-and-microsoft-active-directory/

Office365をAWS Managed Microsoft ADでパスワード同期を使わずに使用できますか？

- 利点
  - パスワード管理の統一
  - AWS Managed Microsoft ADの強いパスワードポリシーを適用できる
- 手順
  1. Active Directory ドメインサービスにパーミッションを委譲
     1. ADSyncConfigを使用
  2. セキュリティグループの設定
     1. Azure AD Connectを許可
  3. Azure AD Connect パススルー認証の設定
     1. AWS Managed Microsoft ADのユーザー情報でOffice 365 にログイン



https://aws.amazon.com/jp/blogs/security/enable-office-365-with-aws-managed-microsoft-ad-without-user-password-synchronization/

このセッションでお話しすること

1. ディレクトリサービスとは
2. AWS Managed Microsoft AD
3. AWSの他のディレクトリサービス
4. How to …
5. 料金

エディションの違い

- 2つのエディション
  - スタンダードエディション
    - 小～中規模のビジネス（約5000ユーザーくらいまで）
    - 30,000ディレクトリオブジェクト（ユーザー、グループ、コンピュータなど）
    - ストレージ：1GB
  - エンタープライズエディション
    - 500,000　ディレクトリオブジェクト
    - マルチリージョンレプリケーション
    - ストレージ：17GB

aws

料金

- Free Tier
  - 30日間
  - 2つのドメインコントローラなら、2時間の操作時間
  - 各追加のドメインコントローラにつき1時間の操作時間

aws

料金

- 東京リージョン
  （最小で二つのドメインコントローラー）
  - スタンダードエディション
    - $0.146/1時間/1ドメインコントローラー
    - $0.073/1時間/追加ドメインコントローラー
    - 他アカウントとディレクトリを共有につき$0.0219/1時間

  - エンタープライズエディション
    - $0.445/1時間/1ドメインコントローラー
    - $0.2225/1時間/追加ドメインコントローラー
    - 他アカウントとディレクトリを共有につき$0.06675/1時間

- 他のリージョンへのデータ転送　$0.09/GB

https://aws.amazon.com/directoryservice/pricing/

aws

このセッションでお話ししたこと

1. ディレクトリサービスとは
2. AWS Managed Microsoft AD
3. AWSの他のディレクトリサービス
4. How to …
5. 料金

伊藤　ジャッジ向子（いとうじゃっじさきこ）

- **AWS**
  - 2016 年 2月よりAWS
  - Premium Support → Technical Writer
    → Solution Architect（製造業）
  - 好きなサービス
    - AWS IoTサービス群
    - AWS Snowball
    - Premium Support
- **Private**
  - Raspberry Pi
  - 犬、登山、キャンプ

Thank you!

aws

内容についての注意点

- 本資料では2021年8月時点のサービス内容および価格についてご説明しています。
  最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます。
- 価格は税抜表記となっています。
  日本居住者のお客様には別途消費税をご請求させていただきます。

- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at http://aws.amazon.com/agreement/. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.

本資料に関するお問い合わせ・ご感想

- 技術的な内容に関しましては、有料のAWSサポート窓口へお問い合わせください
  - https://aws.amazon.com/jp/premiumsupport/
- 料金面でのお問い合わせに関しましては、カスタマーサポート窓口へお問い合わせください（マネジメントコンソールへのログインが必要です）
  - https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service
- 具体的な案件に対する構成相談は、後述する個別技術相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

AWSの日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected個別技術相談会

- 毎週「W-A個別技術相談会」を実施中
  - AWSのソリューションアーキテクト（SA）に対策などを相談することも可能
- 申込みはイベント告知サイトから
  - https://aws.amazon.com/jp/about-aws/events/

ご視聴ありがとうございました

aws