



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 ジャツジ向子

2021年8月



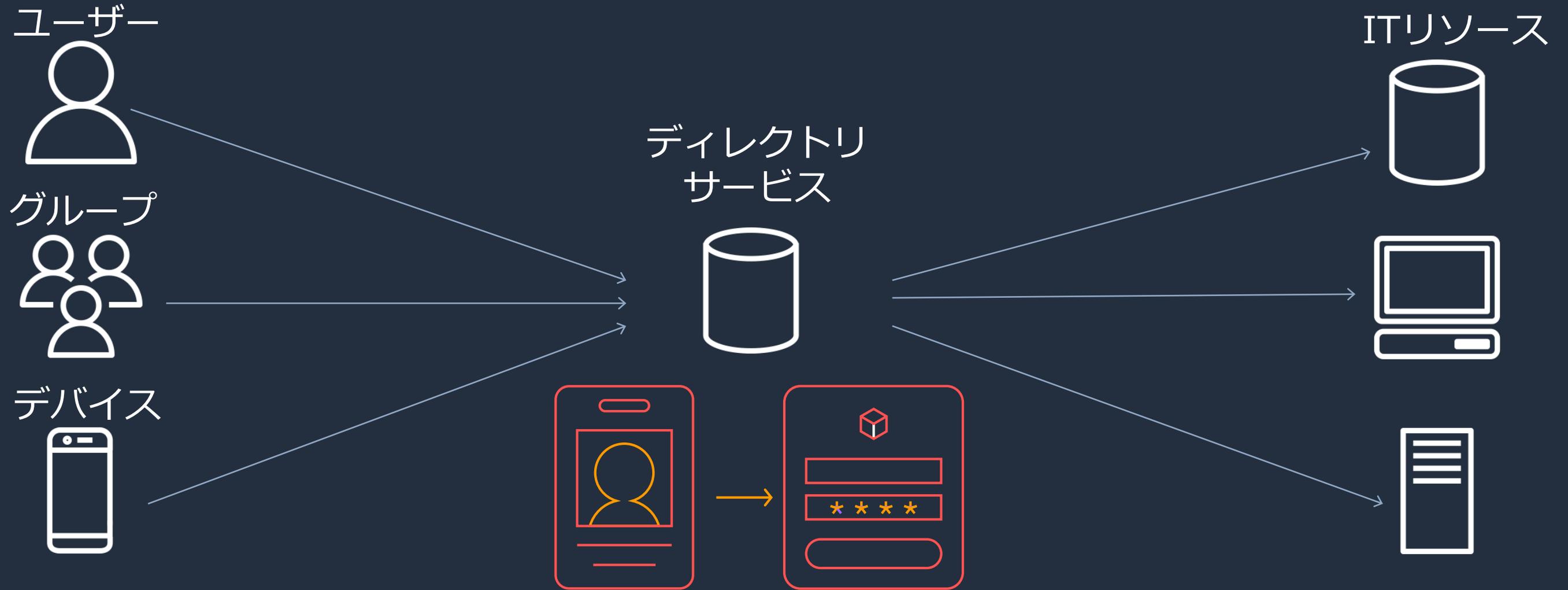
このセッションでお話しすること

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

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

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

Active Directoryの変遷

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



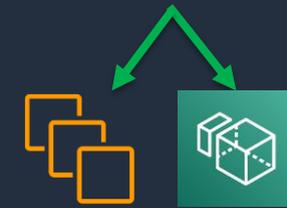
AWS Managed Microsoft AD の特徴



本物のMicrosoft AD



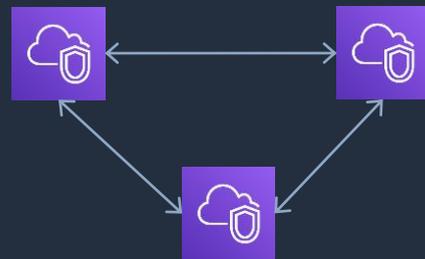
信頼関係のサポート



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

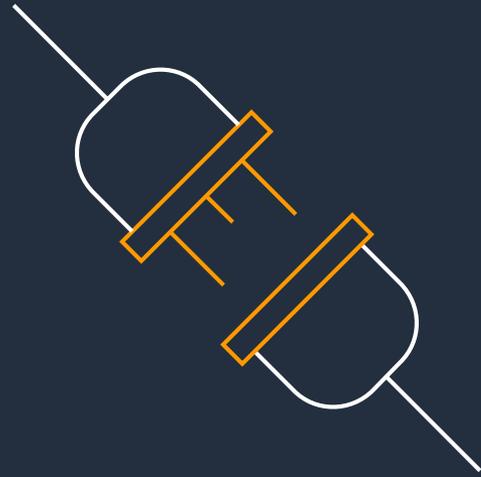


日次の
スナップショット

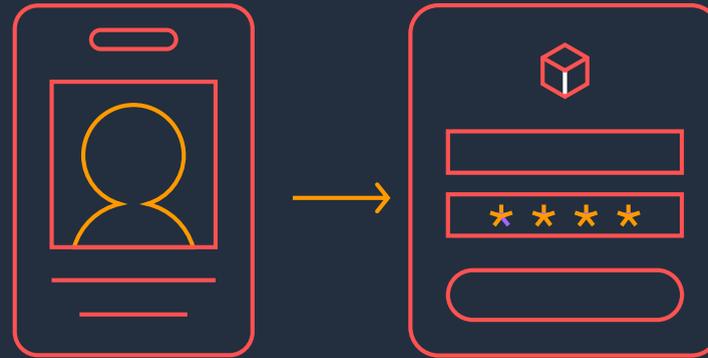


AWSが管理する
インフラストラクチャ

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/>

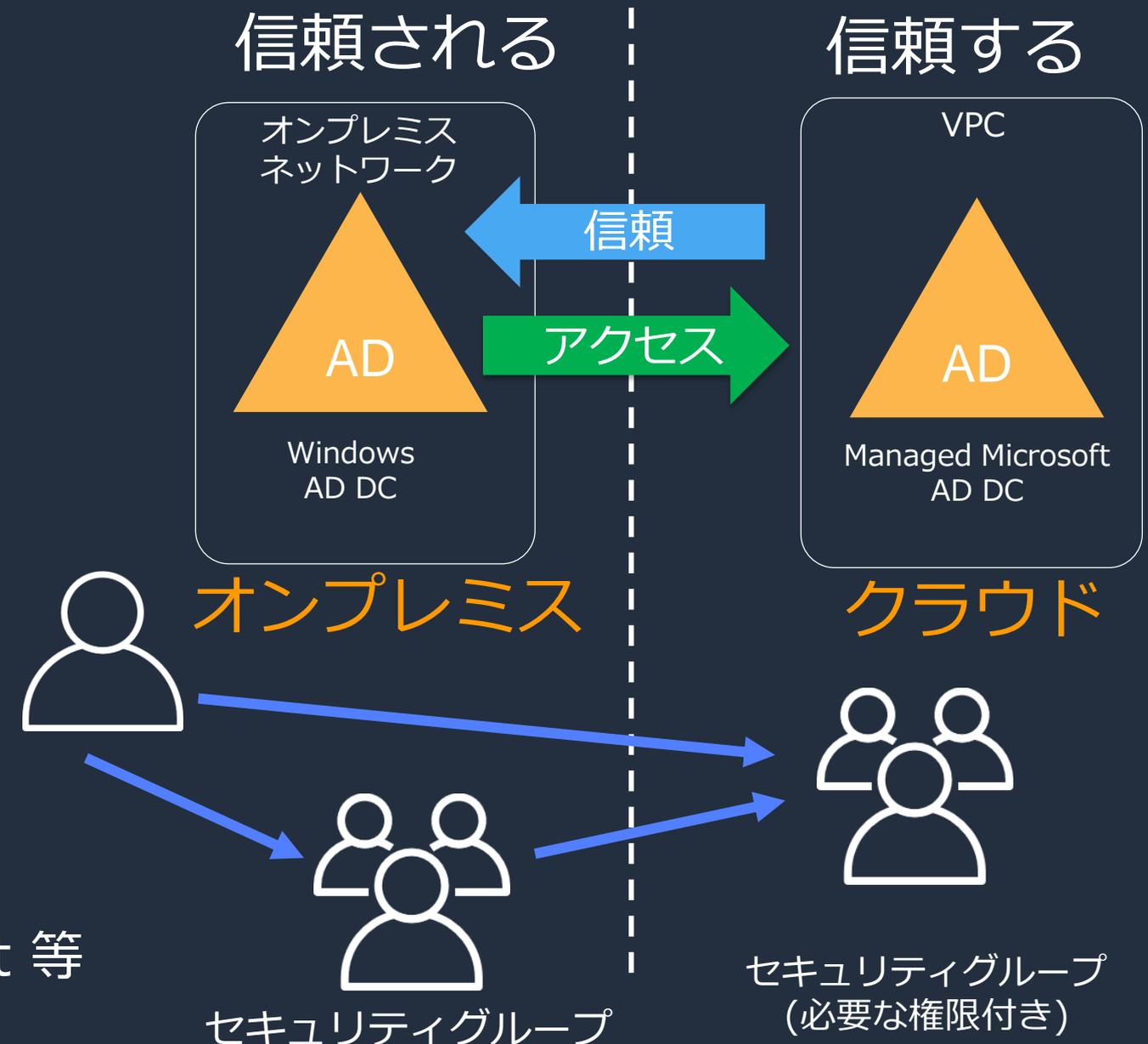
信頼関係とは



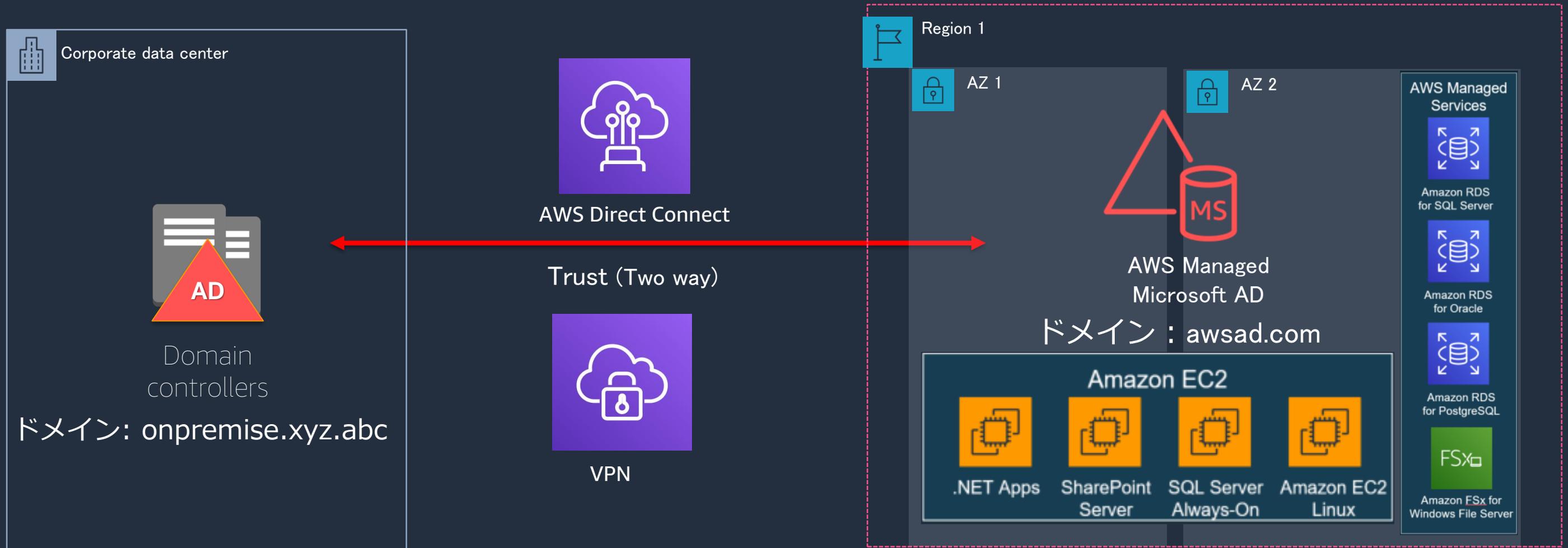
フォレストの信頼関係

- 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

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 Managed Microsoft AD ディレクトリを作成する

1.

ディレクトリのセットアップ

ビジネスニーズに最適なディレクトリを選択すると、そのセットアップ方法が案内されます。

AWS Managed Microsoft AD

ディレクトリのセットアップ

必要なタイプのディレクトリがわからない場合は、当社が選択をサポートいたします。 [詳細はこちら](#)

2.

Directory Service > ディレクトリ > ディレクトリのセットアップ

ステップ 1: ディレクトリタイプの選択

ディレクトリタイプの選択

ステップ 2: ディレクトリ情報の入力

ステップ 3: VPC とサブネットの選択

ステップ 4: 確認と作成

ディレクトリタイプ

- AWS Managed Microsoft AD
- Simple AD
- AD Connector
- Amazon Cognito ユーザープール

AWS Managed Microsoft AD

AWS Managed Microsoft AD クラウドおよびマネージド型 Microsoft Active Directory のサーバー、カスタム IT アプリケーション、およびユーザーを管理するためのソリューションです。

[詳細はこちら](#)

3.

ディレクトリ情報の入力

Windows Server 2012 R2 に基づくマネージド型の Microsoft Active Directory ドメイン。 [情報](#)

ディレクトリのタイプ
Microsoft AD

エディション [情報](#)
Microsoft AD は次の 2 つのエディションで使用できます。

- Standard Edition**
中小企業に最適です。
 - ディレクトリオブジェクト用の 1 GB のストレージ
 - 最大 30,000 個のオブジェクトに最適化
~USD 86.4000/月 (USD 0.1200/時間)*

* 2 つのドメインコントローラーを含む。追加の 1 つのドメインコントローラーごとに USD 43.2000/月 がかかります。
- Enterprise Edition**
大企業に最適です。
 - ディレクトリオブジェクト用の 17 GB のストレージ
 - 最大 500,000 個のオブジェクトに最適化
~USD 288.0000/月 (USD 0.4000/時間)*

* 2 つのドメインコントローラーを含む。追加の 1 つのドメインコントローラーごとに USD 144.0000/月 がかかります。

ディレクトリの DNS 名
完全修飾ドメイン名。この名前は、VPC 内でのみ解決されます。パブリックに解決可能である必要はありません。

ディレクトリの NetBIOS 名 - 任意
ドメインの短い識別子。NetBIOS 名を指定しない場合、デフォルトで、ディレクトリ DNS の最初の部分が名前になります。

最大 15 文字で、次の文字は使用できません: ` / : * ? " < > | `。先頭を ` ` で始めることはできません。

ディレクトリの説明 - 任意
ディレクトリの作成後に詳細ページに表示される説明のテキスト。

最大 128 文字で、英数字と次の文字を使用できます: ` _ @ # % * + = : ? / ! - `。先頭を特殊文字にすることはできません。

Admin パスワード
Admin という名前のデフォルト管理ユーザーのパスワード。

パスワードは 8~64 文字で指定し、「admin」という語は含めず、英小文字、英大文字、数字、特殊文字の 4 つのカテゴリのうちの 3 つを含める必要があります。

パスワードの確認

このパスワードは、上の Admin パスワードと一致する必要があります。

キャンセル 戻る 次へ

4.

Directory Service > ディレクトリ > ディレクトリのセットアップ

ステップ 1: ディレクトリタイプの選択

VPC とサブネットの選択

ステップ 2: ディレクトリ情報の入力

ステップ 3: VPC とサブネットの選択

ステップ 4: 確認と作成

ネットワーク
ディレクトリを含む VPC。最低 2 つのサブネットを持つ VPC がない場合は、VPC を作成する

VPC 情報

[新しい VPC の作成](#)

サブネット 情報

[新しいサブネットの作成](#)

[新しいサブネットの作成](#)

このディレクトリの初期 AD サイト名 [情報](#)
Default-First-Site-Name

5.

ディレクトリの DNS 名
awsad.com

ディレクトリの NetBIOS 名
awsad

ディレクトリ ID
d-

説明 - [編集](#)

アベイラビリティゾーン
us-east-1a, us-east-1b

[0218c27dfd9be4944](#)

DNS アドレス
10.0.6.159,
10.0.5.64

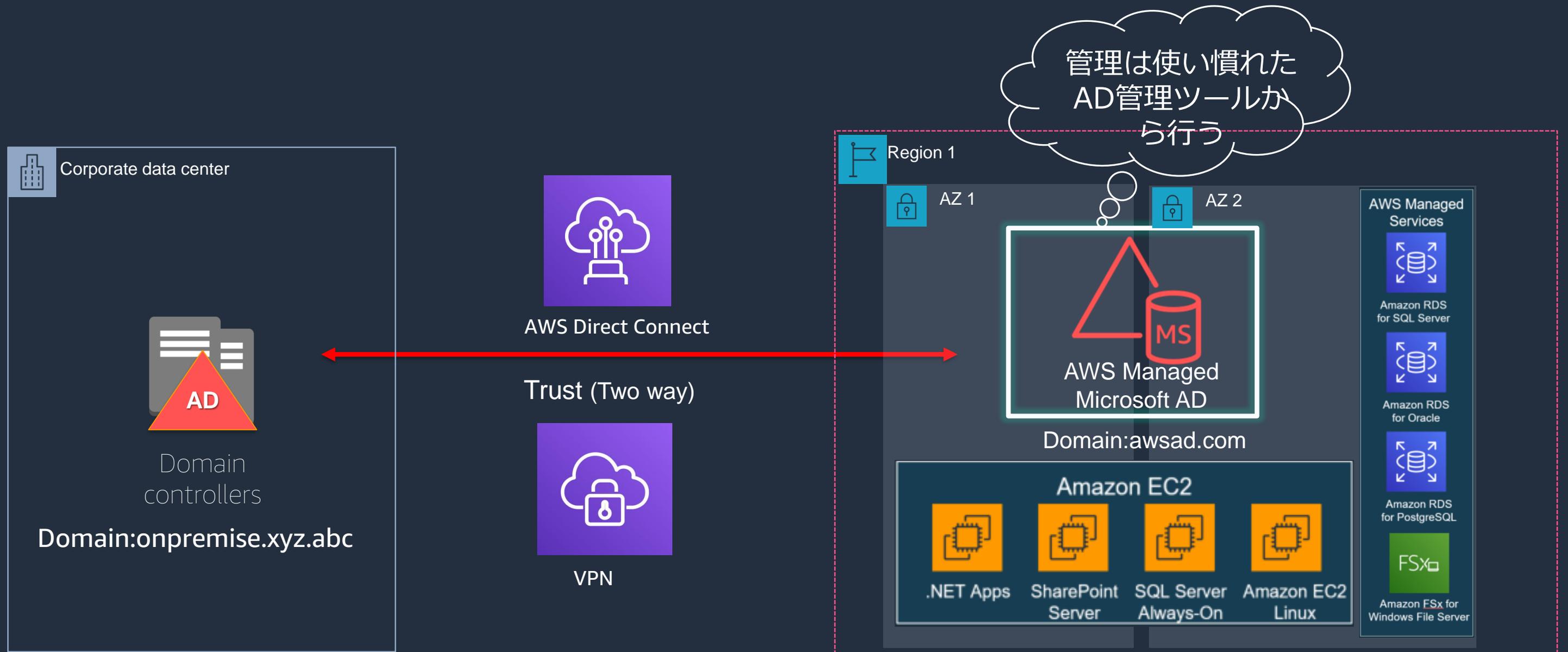
https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/ms_ad_getting_started_create_directory.html



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



Instances to start button and AMI details for Microsoft Windows Server 2019 Base. The AMI is Microsoft Windows 2019 Datacenter edition. [E] with root device type ebs and virtualization type hvm. A label indicates it is eligible for free usage.

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



Domain and IAM role configuration. The domain is awsad.com (d-...). The IAM role is AmazonSSMRoleForInstances. A note states that for successful domain joining, the IAM role must be attached with the AmazonSSMManagedInstanceCore and AmazonSSMDirectoryServiceAccess policies. A link for details is provided.

3. RDP接続を許可する



Security group rule configuration. The rule is named launch-wizard-4 and is for RDP over TCP on port 3389. The source is set to My IP. The rule is being added to a new security group.

IAM ロールに以下の二つのポリシーをアタッチします

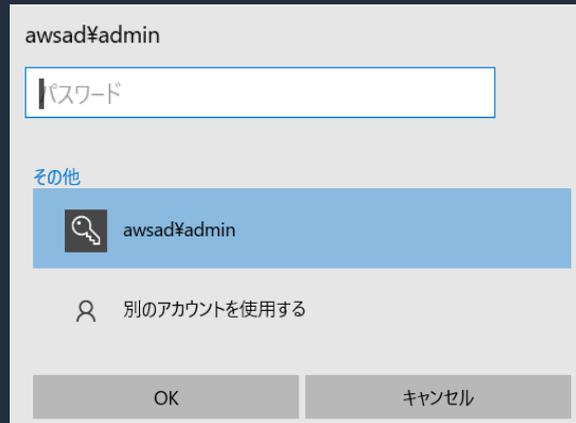
- AmazonSSMManagedInstanceCore
- AmazonSSMDirectoryServiceAccess

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

管理用サーバーにツールをインストール

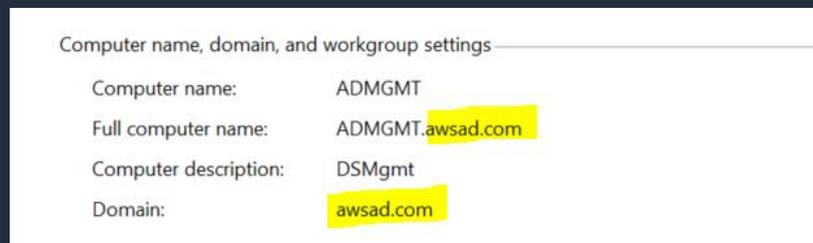
1. Windows インスタンスにドメインユーザで接続する



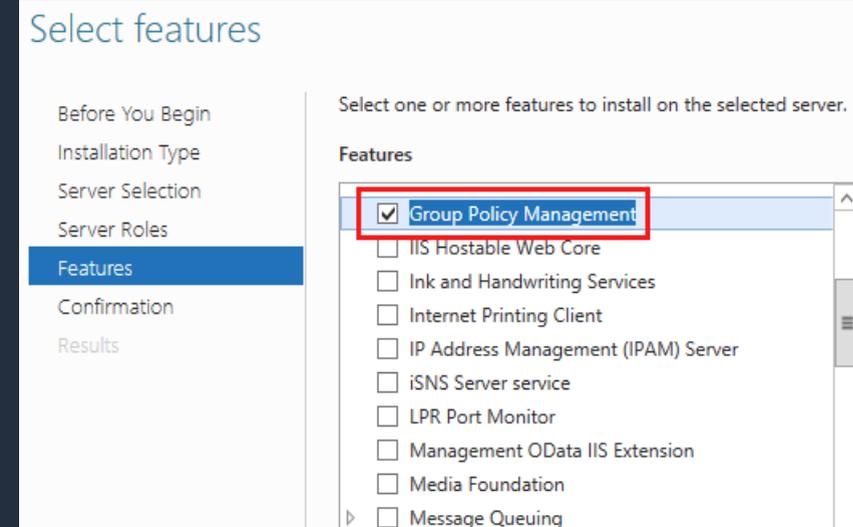
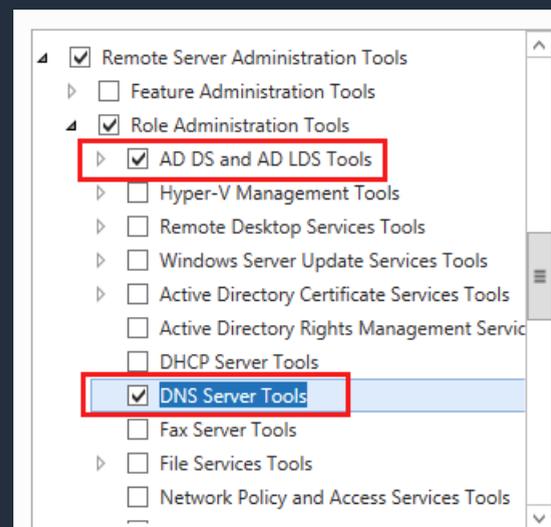
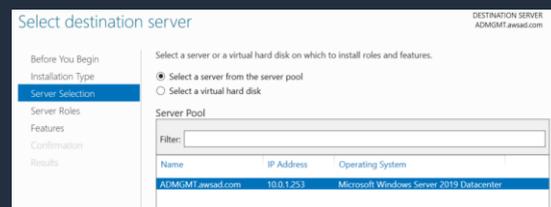
AD管理者
(もしくは権限のあるユーザー)

- 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

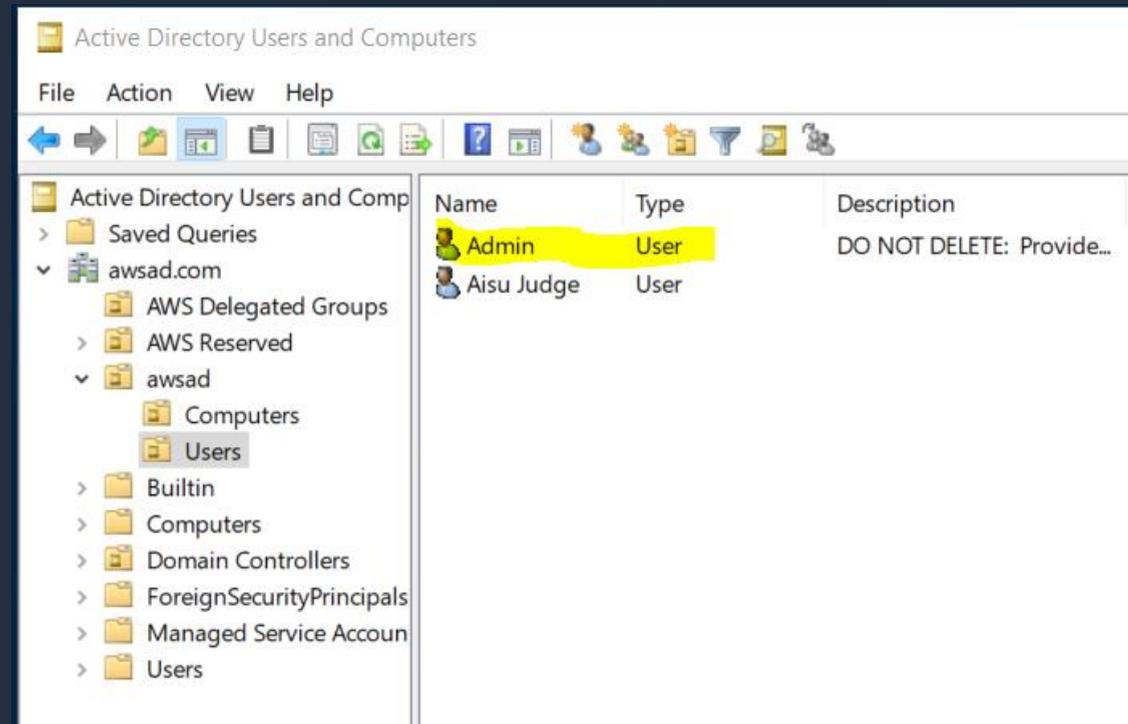
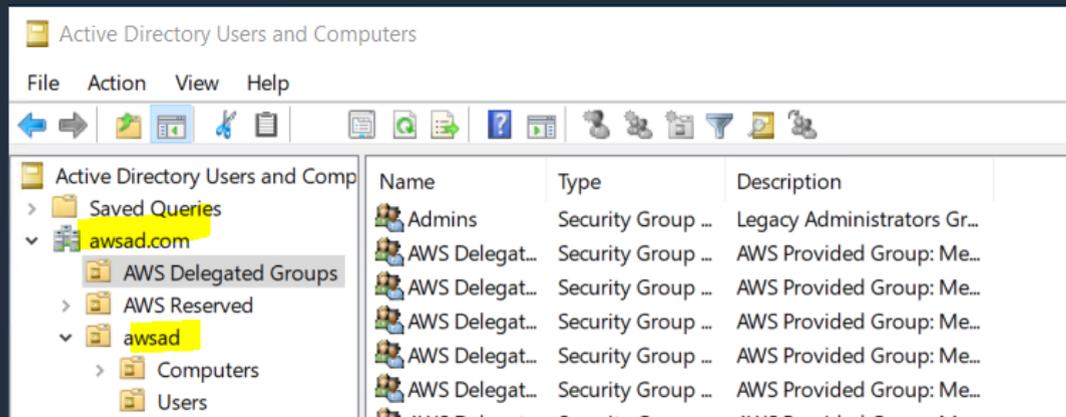
2. ドメインに参加しているか確認する



3. サーバ マネージャーからツールをインストールする



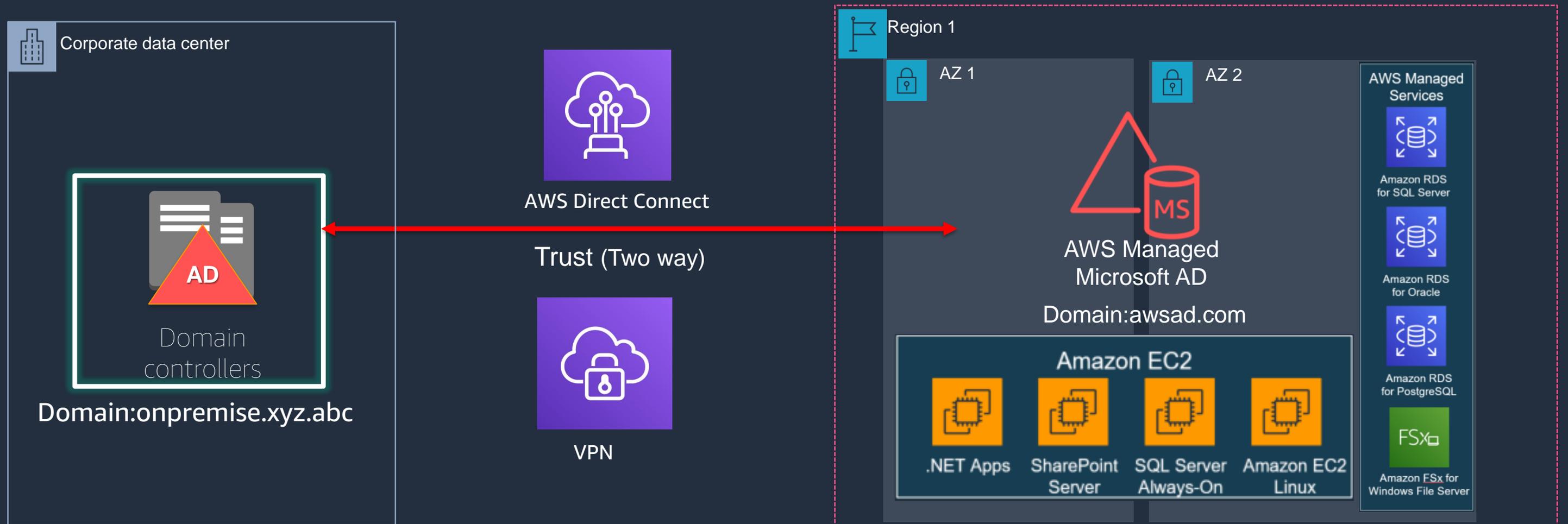
MSADを管理するサーバーで確認



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

オンプレミス側のADを設定する

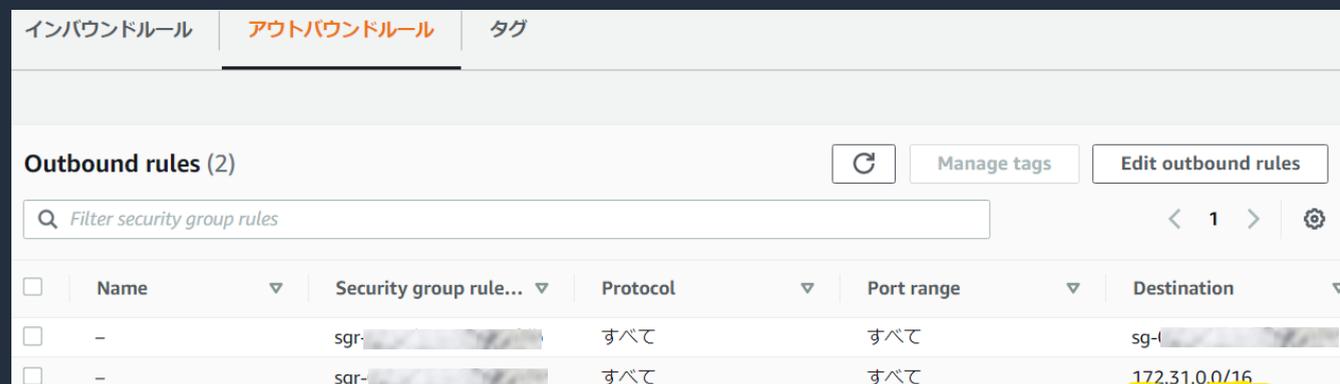


AWS – オンプレミス間の通信

- 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



Name	Security group rule...	Protocol	Port range	Destination
-	sgr-...	すべて	すべて	sg-l...
-	sgr-...	すべて	すべて	172.31.0.0/16

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

The screenshot shows the AWS DNS Manager interface. In the left-hand navigation pane, the 'Conditional Forwarders' folder is expanded, and the 'awsad.com' entry is selected, marked with a red '1.'. The main pane displays a table with the following information:

Name	Type
awsad.com	Conditional F...

Below this, the 'awsad.com Properties' dialog box is open, with the 'Security' tab selected. It shows the following configuration:

- Type: Conditional Forwarder
- Replication: All DNS servers in this domain
- Conditional forwarders are DNS servers that this server can use to resolve DNS queries for records in a specific domain. The domain is the name of the conditional forwarder.
- Master Servers:

IP Address	Server FQDN
10.0.5.64	ip-10-0-5-64.ec2.internal
10.0.6.159	ip-10-0-6-159.ec2.internal

The 'Edit' button is visible at the bottom right of the properties dialog. A red '2.' is placed next to the 'awsad.com Properties' dialog box.

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

The 'Edit Conditional Forwarder' dialog box is shown, with the following configuration:

- DNS Domain: awsad.com
- IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add an...>		
10.0.5.64	ip-10-0-5-64.ec2.internal	OK
10.0.6.159	ip-10-0-6-159.ec2.internal	OK

Additional settings include:

- Store this conditional forwarder in Active Directory, and replicate it as follows:
- All DNS servers in this domain
- Number of seconds before forward queries time out: 5

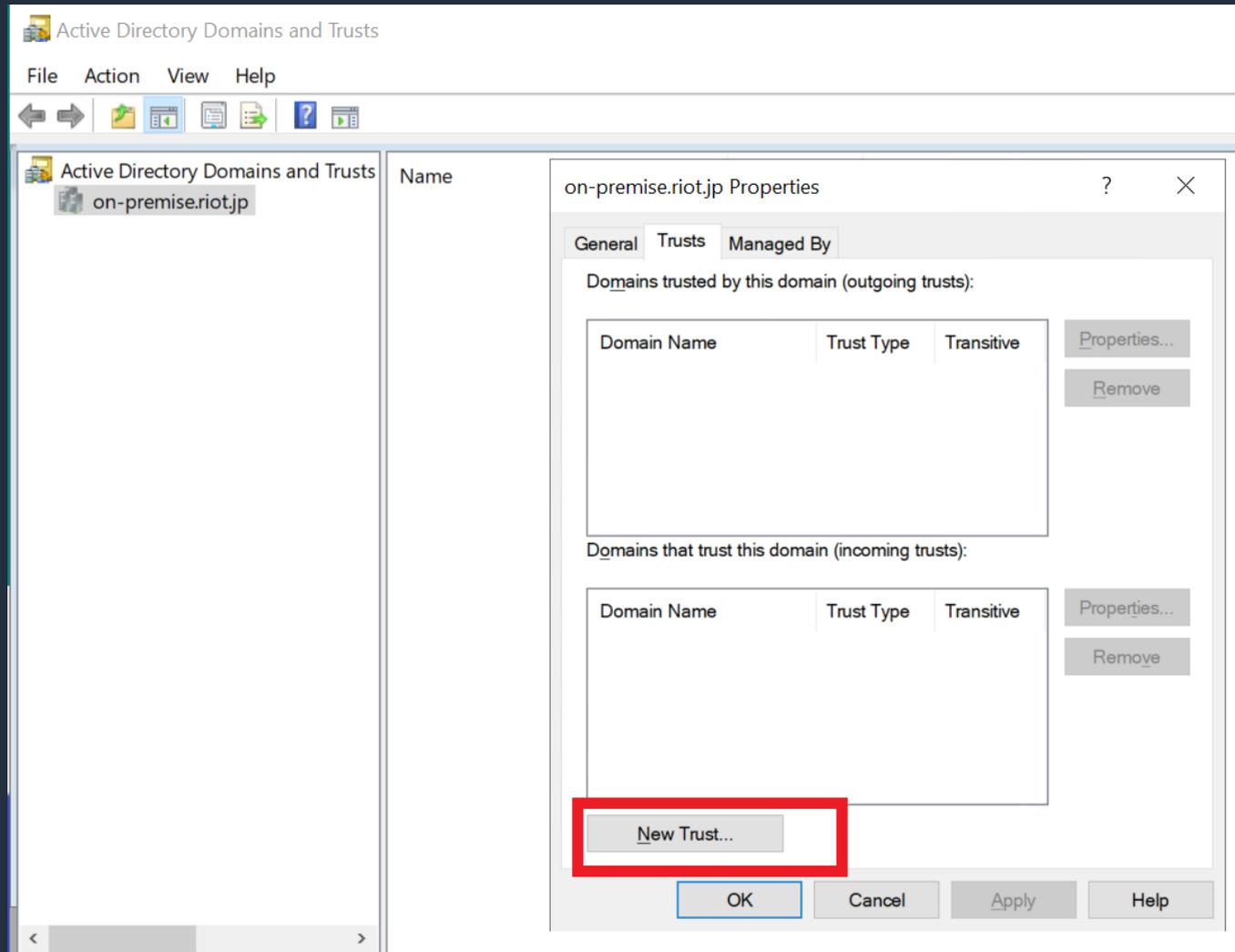
The 'OK' button is highlighted at the bottom right.

信頼関係の設定（双方向）

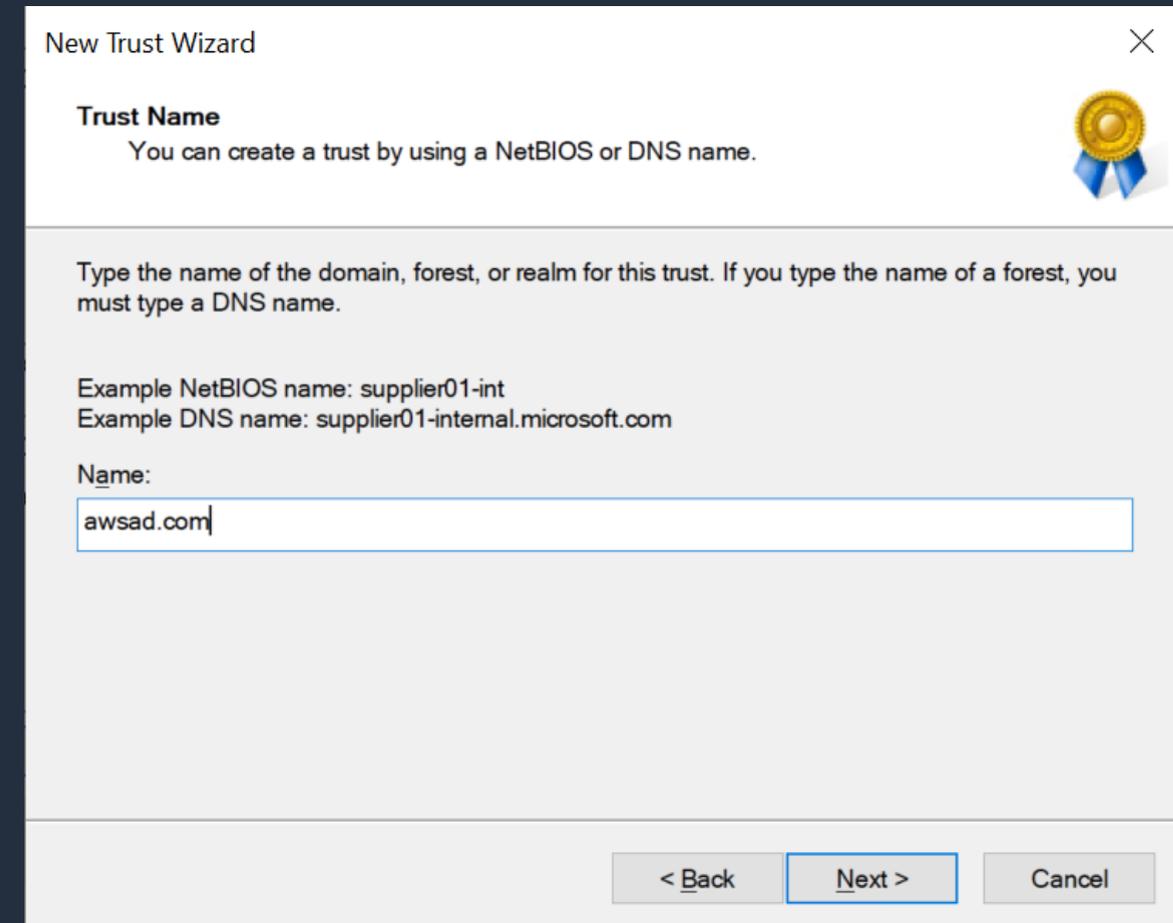
1. AWS Managed Microsoft AD ディレクトリを作成する
2. AWS側のMSADを管理するサーバーを立てる
 1. MSADを管理するサーバーにツールをインストール
3. オンプレミス側のADを設定する
 1. DNS設定
 2. 信頼関係の検証
4. Microsoft Managed ADで信頼関係の確立
5. アプリケーションの管理
 1. AWSマネジメントコンソール使用ユーザーの設定

オンプレミスの信頼関係の検証

1.



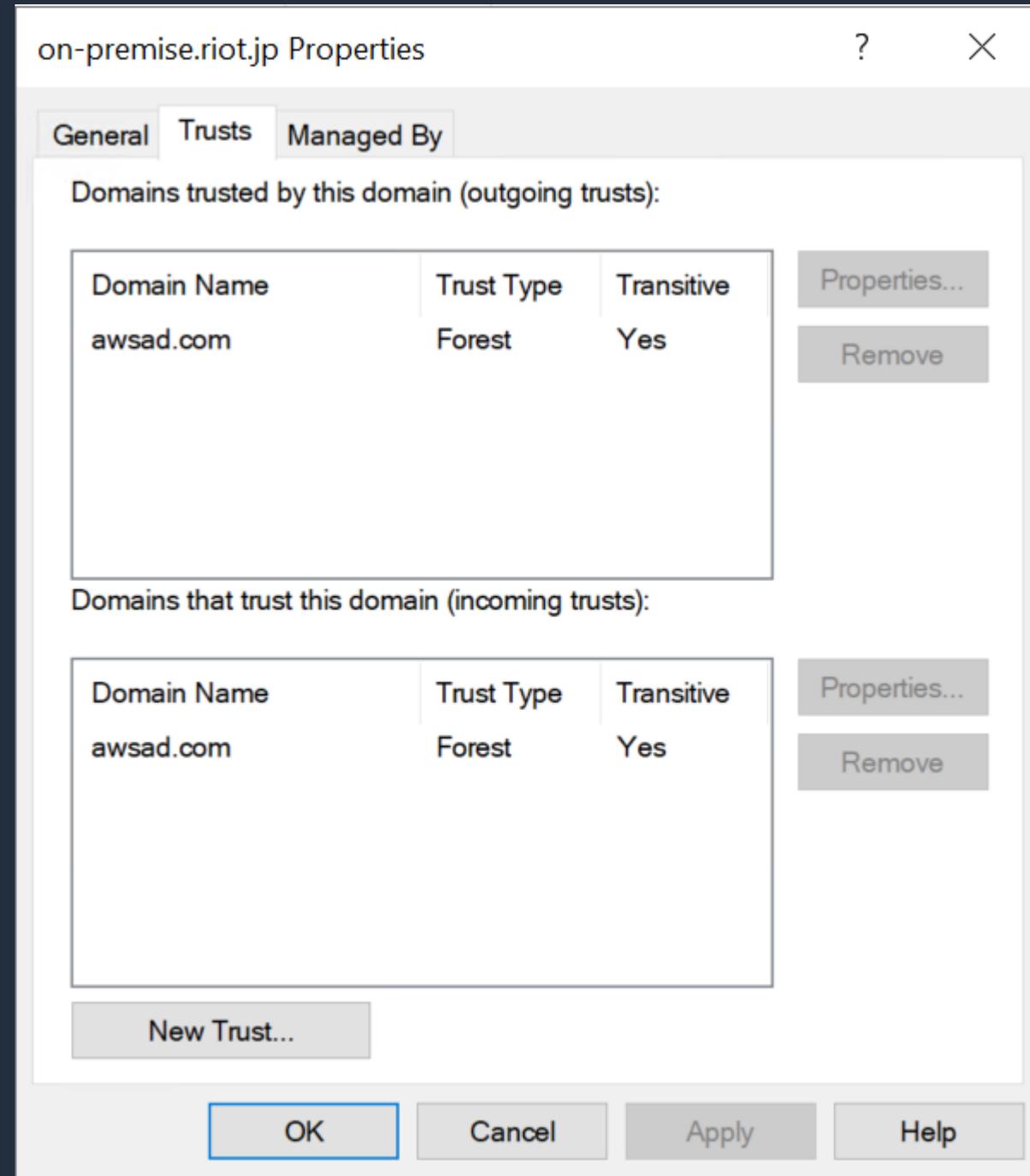
2.



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

セットアップ手順 AWS Microsoft Managed AD

2.

信頼関係 (0) 情報

信頼関係により、このドメインのリソースと既存のドメインのユーザーの間で相互のアクセスが許可されます。

1.	ドメイン名 ▲	タイプ ▼	ステータス ▼	方向 ▼	選択的認証 ▼	条件付きフォワーダーの IP ▼
----	---------	-------	---------	------	---------	------------------

信頼関係が見えません

信頼関係の追加

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 (1) 情報

信頼関係により、このドメインのリソースと既存のドメインのユーザーの間で相互のアクセスが許可されます。

	ドメイン名 ▲	タイプ ▼	ステータス ▼	方向 ▼	選択的認証 ▼	条件付きフォワーダーの IP ▼	最終確認日 ▼
<input type="radio"/>	on-premise. .jp	Forest	<input checked="" type="checkbox"/> 検証済み	Two-Way	Disabled	172.31.63.153	Jun 19, 2021

信頼関係の追加

既存またはリモートの Active Directory とこの信頼に最適なオプションを指定します。 [詳細はこちら](#)

信頼のタイプ

作成する信頼のタイプを選択します。

- 外部の信頼
既存またはリモートのフォレストのドメインと、AWS Directory Service のこのドメインの間の信頼を作成します。
- フォレストの信頼
既存またはリモートのフォレストのフォレストルートドメインと、AWS Directory Service のこのフォレストの間の信頼を作成します。

既存または新しいリモートドメイン

既存またはリモートのドメインの完全修飾ドメイン名。

on-premise. .jp

必須の有効なドメイン名。

信頼パスワード

既存またはリモートのドメインで信頼関係を設定するときは、この同じパスワードを使用する必要があります。

.....

最大 128 文字。

信頼の方向

既存またはリモートのドメインのユーザー間の接続で、このドメインとやり取りする方法を選択します。

- 一方: 出力方向
既存またはリモートのドメインのユーザーは、このドメインのリソースにアクセスできます。
- 一方: 入力方向
このドメインのユーザーは、既存またはリモートのドメインのリソースにアクセスできます。
- 双方向
各ドメインのユーザーは、両方のドメインのリソースにアクセスできます。

選択的認証

特定のユーザーやグループに対する信頼関係を介してリソースへのアクセスを制限します。

条件付きフォワーダー

このドメインおよび既存またはリモートのドメインに条件付きフォワーダーが必要です。FQDN を入力して、このディレクトリの既存の条件付きフォワーダー IP アドレスを見つけます。

172.31.63.153

[別の IP アドレスの追加](#)

キャンセル

追加

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.

AWS マネジメントコンソール 情報

有効

上記のアプリケーションアクセス URL を使用してログインする、このディレクトリおよび共有ディレクトリの委任ユーザーに、AWS マネジメントコンソールでのリソースへのアクセス権を付与します。

この機能は現在無効になっています。AWS マネジメントコンソールでさまざまなリソースを制御する IAM ロールに、委任されたユーザーのアクセス権を割り当てるには、この機能を有効にします。

ユーザーログインセッションの長さ 情報
コンソールがセッションからユーザーをログアウトする前に、ユーザーがログインできる時間の長さ。
現在のセッションの長さ: 8 時間 編集

2.

ロール > ManagedADUser 概要

ロール ARN	arn:aws:iam::417632231328:role/ManagedADUser
ロールの説明	Allows Directory Service to manage AWS service access
インスタンスプロファイル ARN	
パス	/
作成時刻	2021-06-19 11:38 UTC+0900
最後のアクティビティ	追跡期間中はアクセスされません
最大セッション時間	1 時間 編集

アクセス権限 信頼関係 タグ アクセスアドバイザー セッションの無効化

信頼関係の編集

信頼されたエンティティ	条件
ID プロバイダー ds.amazonaws.com	以下の条件では、信頼とタイミングを定義し、このロールに関連付け

3.

コンソールアクセスの委任 (1) 情報

次の該当する IAM ロールに追加することで、コンソールの特定の領域にアクセスできるユーザーとグループを委任できます。開始するには、ロールを選択します。

Q ロールで検索

IAM ロール	▲	コンソールのアクセス許可	委任ユーザー	▼	委任グループ	▼
ManagedADUser		IAM でポリシーを表示	0		0	

※ 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.

Directory Service > ディレクトリ > d-906768d349 > AWS マネジメントコンソール

選択されたロール: ManagedADUser

IAM ロール	ARN	アクセス許可	委任ユーザー	委任グループ
ManagedADUser	arn:aws:iam::417632231328:role/ManagedADUser	IAM でポリシーを表示	2	0

このロールのユーザーとグループの管理 (2) 情報 削除 追加

ここに一覧で示されたドメインユーザーとグループは、この IAM ロールに割り当てられたアクセス許可を継承します。

Q ユーザーまたはグループで検索 < 1 >

<input type="checkbox"/>	名前 ▲	フルネーム ▼	ドメイン名 ▼	タイプ ▼	セキュリティ識別子 (SID) ▼
<input type="checkbox"/>	aisu	Aisu Judge	awsad.com	User	S-1-5-21-...
<input type="checkbox"/>	tomoe	TOMOIE JUDGE	on-premise.riot.jp	User	S-1-5-21-...

2.

ネットワークとセキュリティ | スケール & 共有 | **アプリケーション管理** | メンテナンス

アプリケーションアクセス URL 情報

このディレクトリのユーザーが AWS アプリケーションと AWS マネジメントコンソールにアクセスできるパブリックエンドポイント URL。

アクセス URL:
sakikito20210521.awsapps.com

Amazon WorkDocs のシングルサインオン 情報 無効化

AWS アプリおよびサービス 情報 🔄

このディレクトリのユーザー、および上記のアプリケーションアクセス URL を使用してログインする共有ディレクトリのユーザーが利用できるすべての AWS のアプリケーションとサービスを一覧表示します。

アプリケーション	ステータス	アプリケーションの URL
AWS Client VPN	無効	-
AWS Management Console	有効	sakikito20210521.awsapps.com/console
AWS Single Sign-On	無効	sakikito20210521.awsapps.com/start

3.



Please log in with your sakikito20210521 credentials

Username
on-premise\tomoe

Remember username

Password
.....

Sign In

文字列 .awsapps.com/console

ManagedADUser/tomoe @ sakikito ▲

フェデレーションログイン:
ManagedADUser/tomoe

マイアカウント 417632231328

マイ組織

マイ Service Quotas

マイ請求ダッシュボード

ロールの切り替え

サインアウト

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 Managed Microsoft ADでの制限事項

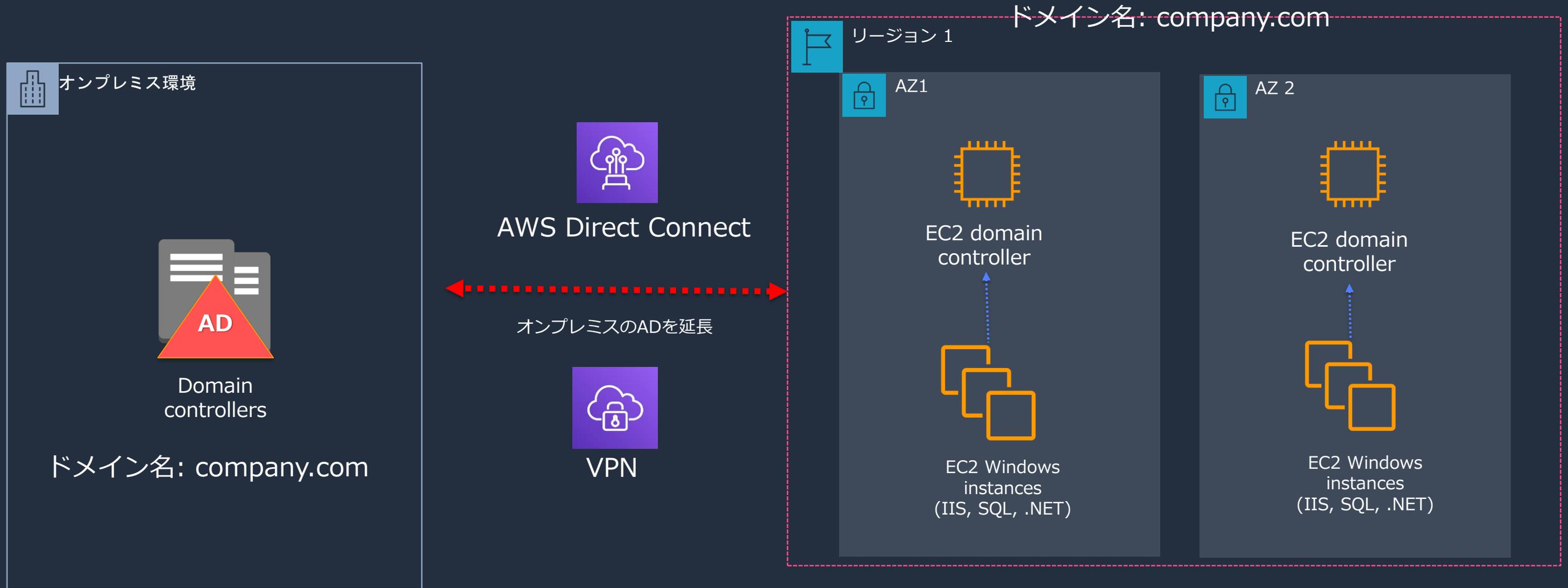
- ドメイン管理者としての権限の制限
- オンプレミスのドメインと同一のドメインの延長 [1]
- サービスクォータ（上限緩和可） [2]
 - デフォルトでは20ディレクトリ
 - 手動でのスナップショットは5つまで
 - ディレクトリごとのドメインコントローラーは20まで
 - ディレクトリごとのCA(Certification Authority)登録は5つまで



[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

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

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
```



通知の作成

通知タイプ
新しい通知の作成を選択します。これにより、新しい SNS トピックが作成されるか、既存の SNS トピックが関連付けられます。

新しい通知の作成

受信タイプ
 E メール
 SMS

受取人
E メールアドレスを入力します

通知を有効にするために、新しい SNS トピックが作成されて、このディレクトリと関連付けられます。トピック名をカスタマイズする場合は、以下のオプションを編集できます。

SNS トピック名
これは、作成する SNS トピックの名前です。
DirectoryMonitoring_d-906768d349
残り 224 文字です。ハイフン (-) と下線 (_) を使用できます。

SNS 表示名
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です。
AWSDIRSvc
残り 0 文字です。SMS 受取人のタイプを使用する場合、表示名は必須です。

キャンセル 作成

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

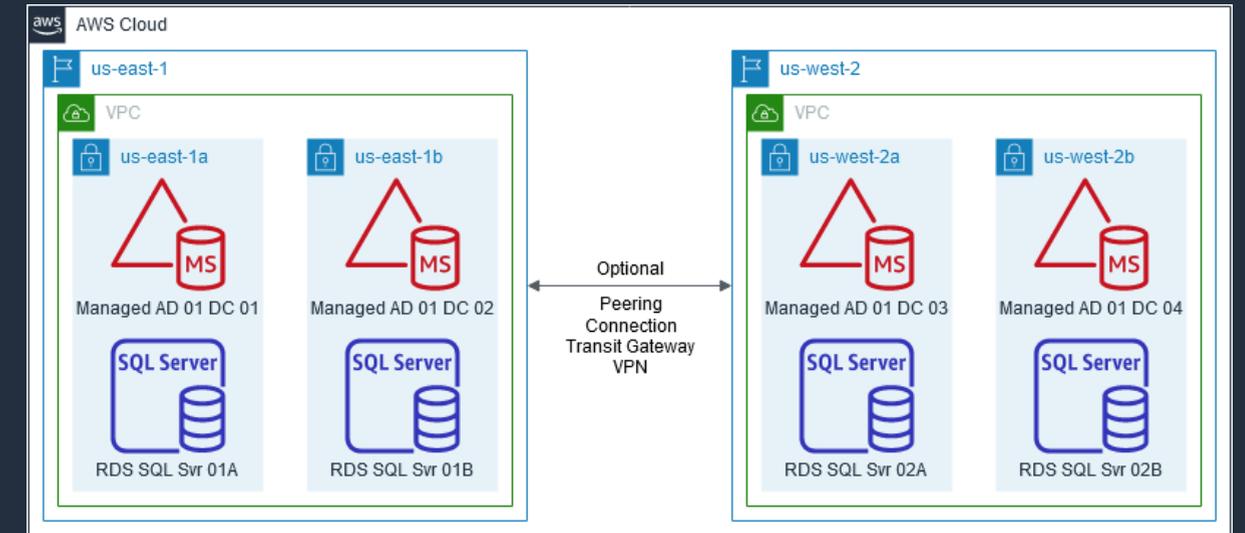
The screenshot displays the Active Directory Administrative Center interface. The top navigation bar shows the path: awsad (local) > System > Password Settings Container. The main content area shows a list of Password Settings Objects (PSOs) with columns for Name, Precedence, Type, and Description. The selected PSO is CustomerPSO-01, which is a Provisioned Password Policy with a precedence of 10. Below the list, the configuration details for CustomerPSO-01 are shown. The Password Settings section includes fields for Name (CustomerPSO-01), Precedence (10), and checkboxes for Enforce minimum password length (7 characters), Enforce password history (24 passwords remembered), Password must meet complexity requirements, and Protect from accidental deletion. The Password age options section includes checkboxes for Enforce minimum password age (1 day), Enforce maximum password age (42 days), and Enforce account lockout policy (Number of failed logon attempts allowed, Reset failed logon attempts count after, and Account will be locked out for a duration of mins).

<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



Microsoft SQL Server Windows 認証

Windows 認証を使用して、この SQL サーバーインスタンスでアクセス権限を付与されたドメインユーザーによる認証を許可するディレクトリを選択します。

Microsoft SQL Server Windows 認証を有効化
ディレクトリを選択して、データベースのインスタンス作成を続行することで、Windows 認証の使用に必要な IAM ロールを作成する権限を Amazon RDS に付与することになります。

ディレクトリ

enterprise.com (d-)

ディレクトリを参照

マルチリージョンレプリケーション (2) 情報

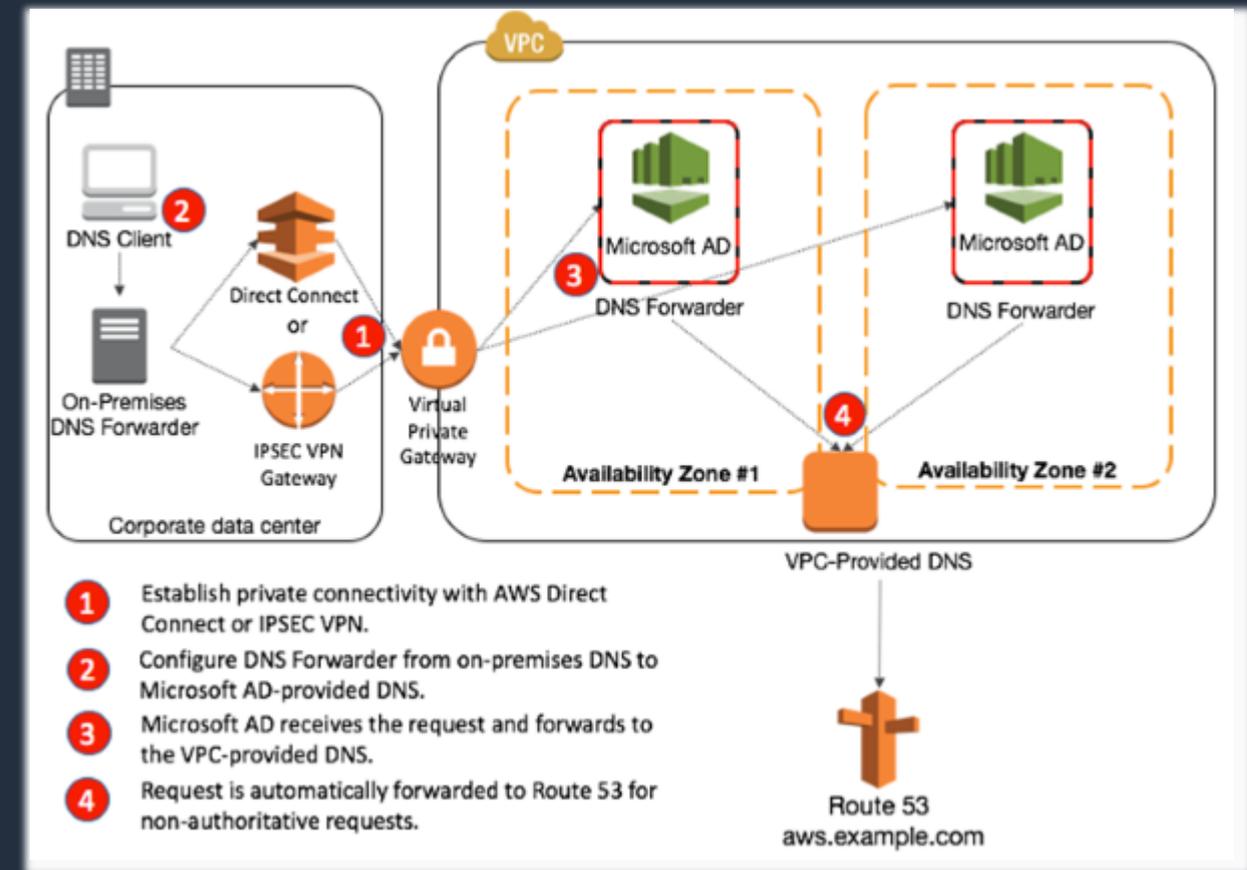
ディレクトリレプリケーションの目的でドメインコントローラーがデプロイされている AWS リージョンを一覧表示します。プライマリリージョンから、リージョンを追加することだけ可能です。

リージョン	VPC	ドメインコントローラー	ステータス
US East (N. Virginia) - プライマリ	vpc-	2	アクティブ
US East (Ohio)	vpc-	2	作成中

<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？

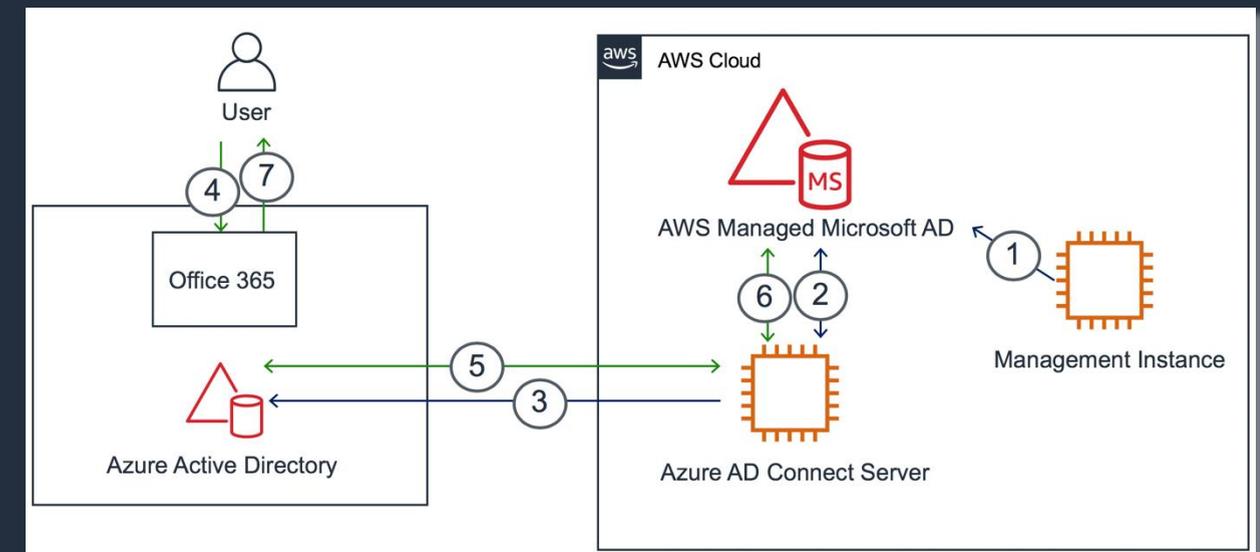
- 転送ルールの設定
 - DNS管理ツールでDirectory ServiceのDNSのIPアドレスに接続 -> 条件付きフォワーダー
 - プライベートドメインのDNSクエリをVPCのAmazonが提供するDNSサーバーのIPアドレスに転送
 - 例) 192.168.0.0/24のネットワークなら192.168.0.2



<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

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

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/>

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 ジャツジ向子 (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!

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おります。
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



お問い合わせ サポート▼ 日本語▼ アカウント▼

今すぐ無料サインアップ »

製品 ソリューション 料金 ドキュメント 学ぶ パートナーネットワーク AWS Marketplace イベント さらに詳しく見る 🔍

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

[AWS Webinar お申込 »](#)

[AWS 初心者向け »](#)

[サービス別資料 »](#)

[ハンズオン資料 »](#)

<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