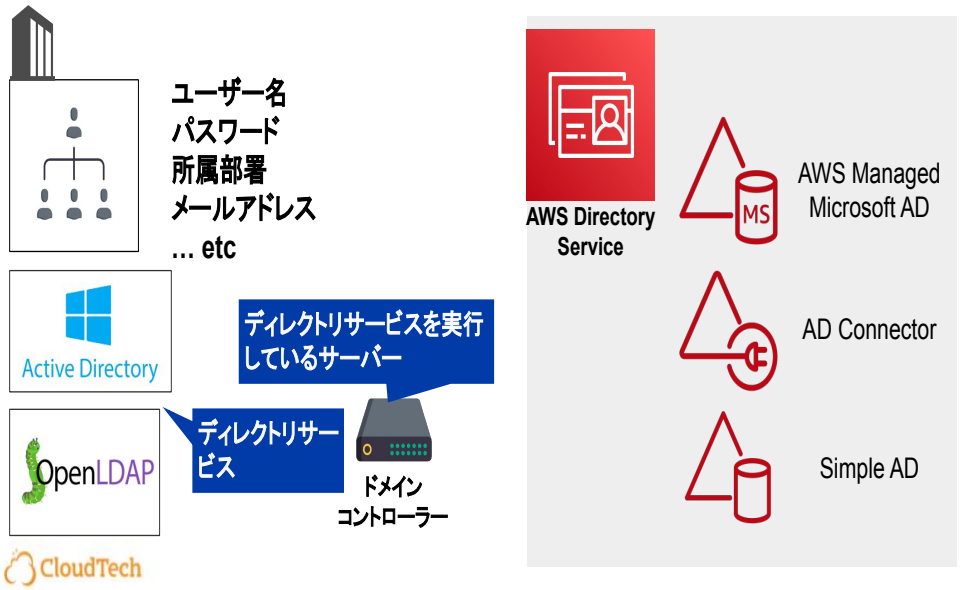
- Directory Service
  - AWSでActive Directory を使用できる、または既に使用しているオンプレのADをAWSに接続するためのサービスです。

AWS Directory Service（そもそもADとは？）



- 前提知識として、そもそもADとは、ユーザーと認証情報を一元管理しているデータベースとイメージしてください。
  - 企業では多くの従業員の情報を管理する必要があります。
    - ユーザー名やパスワード、そしてユーザーに紐付くメールアドレスのような属性情報を管理するために利用されるのがディレクトリサービスです。
  - ディレクトリサービスの代表例として、Microsoft社のActiveDirectoryや、オープンソースのOpenLDAP等があります。
    - これら、サービスを実行しているサーバーを「ドメインコントローラー」と呼びます。

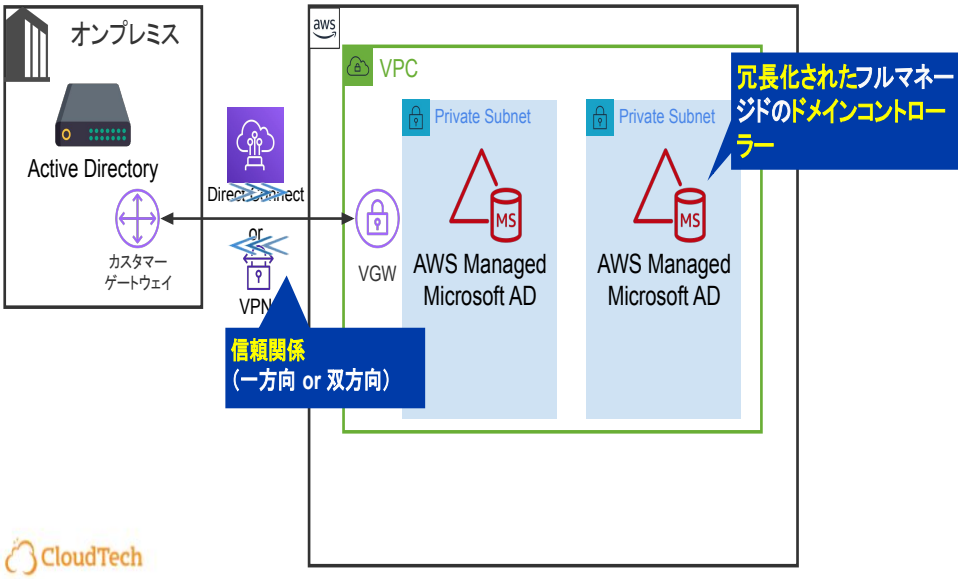
  - AWSDirectoryServiceは、AWS上でディレクトリサービスの利用を可能にするサービスです。
    - 複数のディレクトリタイプが提供されていま

- す。
  - AWS ManagedMicrosoftAD
  - ADConnector
  - SimpleAD
- ひとつずつ見ていきましょう。

AWS Managed Microsoft AD

CloudTech

AWS Managed Microsoft AD



- まず、AWS上でActive Directory（AD）を稼働させる方法として、自力で構築することもできます。
  - Windowsタイプの EC2 インスタンスを立ち上げ、ドメインコントローラーとしてセットアップする方法です。
    - AWSの責任共有モデルを考えると、この EC2 は利用者側が保守する責任を持ちます。
      - 例えば（セキュリティ対策、パッチ、バックアップ）など、管理に手間がかかりますよね。

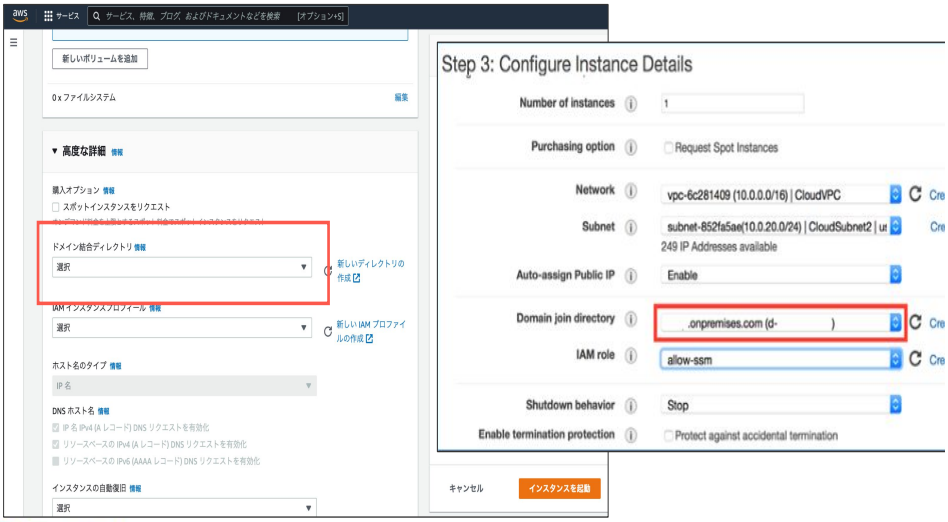
- そこで、AWS Managed Microsoft ADを導入する方法があります。
  - Active Directoryのフルマネージドサービスなので、先ほどのドメインコントローラーに対するパッチやバックアップなどの管理の負担が軽減されます。
    - VPC内に冗長化されたプライベートサブネットがあるとします。

- AWSのマネージメントコンソールの操作だけで、ここに、Windowsサーバーで実行される、冗長化されたドメインコントローラーがフルマネージドで作成されます。
    - そして、これをDXまたはVPNでオンプレのADと接続し、信頼関係を構築できます。
        - 信頼関係は、複数のドメインを併用している場合に用いる標準機能です。
            - この機能を利用すると、異なるドメインのユーザーやグループに対してアクセス権を設定できる利点があります。
        - 補足ですが、信頼関係には片方、もしくは双方向という「方向」の考え方があります。
            - 双方向はイメージが着くかと思いますが、片方の信頼関係の例をとると
                - 「『aws.com』ドメインが『onpre.com』ドメインを信頼する」という信頼関係を設定した場合

        - 信頼された（onpre.com）は、信頼する側のドメイン（aws.com）にユーザー名／パスワードを入力することなくアクセスできるようになります。
        - 逆はできません。
- そして、EC2構築時に出てくるこちらの[Domain join directory] (ドメイン結合ディレクトリ) の指定などで、AWS Managed Microsoft ADに参加させることで、
- オンプレミスのユーザーは EC2にログオンすることができます。
    - 概要欄に参考記事も載せておきます。
        - 他、Managed Microsoft AD はさまざまなAWSサービスへの認証をサポートしてい

        - ■ ます。
            - AWS マネジメントコンソール
            - AWS RDS for SQL Server、Oracle、PostgreSQL、MySQL
            - Amazon FSx
            - workspaces
            - QuickSightなど
- 補足ですが、メンテナンス不要となるメリットがある一方、マネージドサービスのためRDP接続ができません。
    - なので、ドメインにユーザを追加するには、クライアントを用意し、[Remote Server Administration Tools] (リモートサーバー管理ツール)をpowershellでインストールするなど、ちょっとしたセットアップをしなければならない等の不便な点はあります。
    - とは言え、オンプレのグループ、もしくはユーザーはシングルサインオンで対象のAWSリソースを操作できるなど、オンプレのADと信頼関係がむすべるので便利です。
- 他情報として、
    - 5000ユーザーを超える組織に有用です。
    - スタンドアロンのADとしてAWS内で使用できる

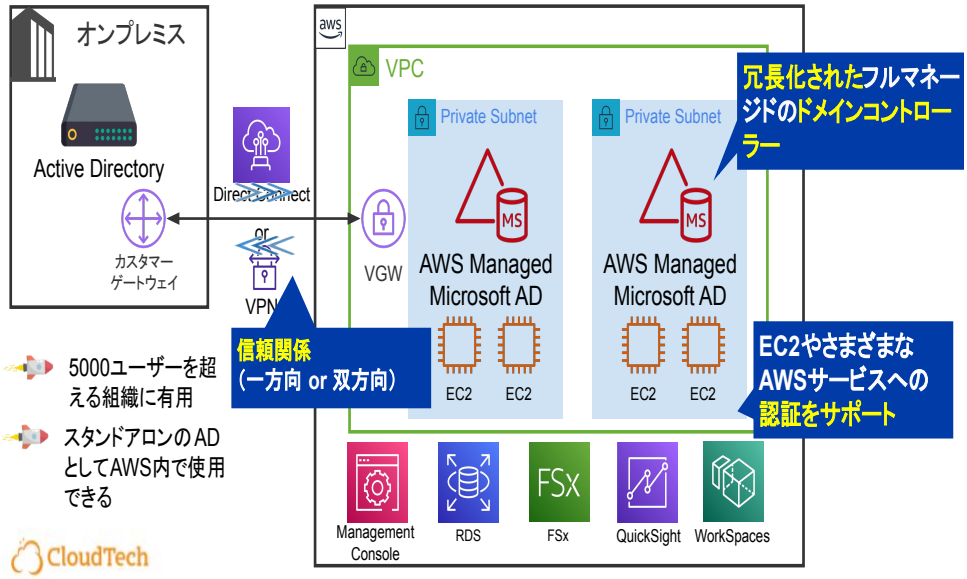
AWS Managed Microsoft AD



CloudTech

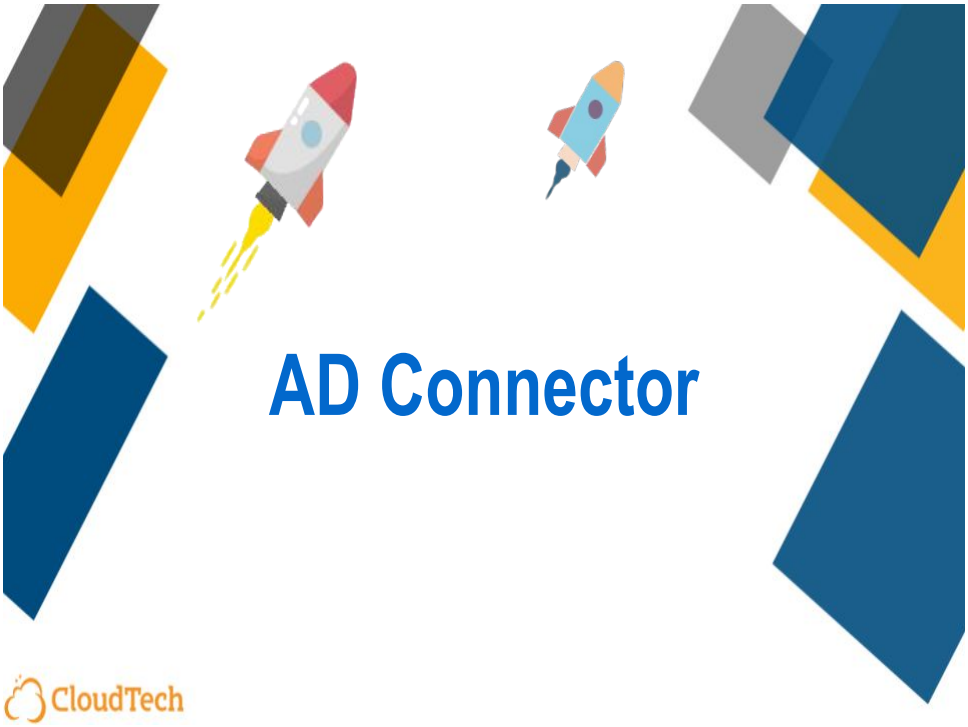
-

AWS Managed Microsoft AD



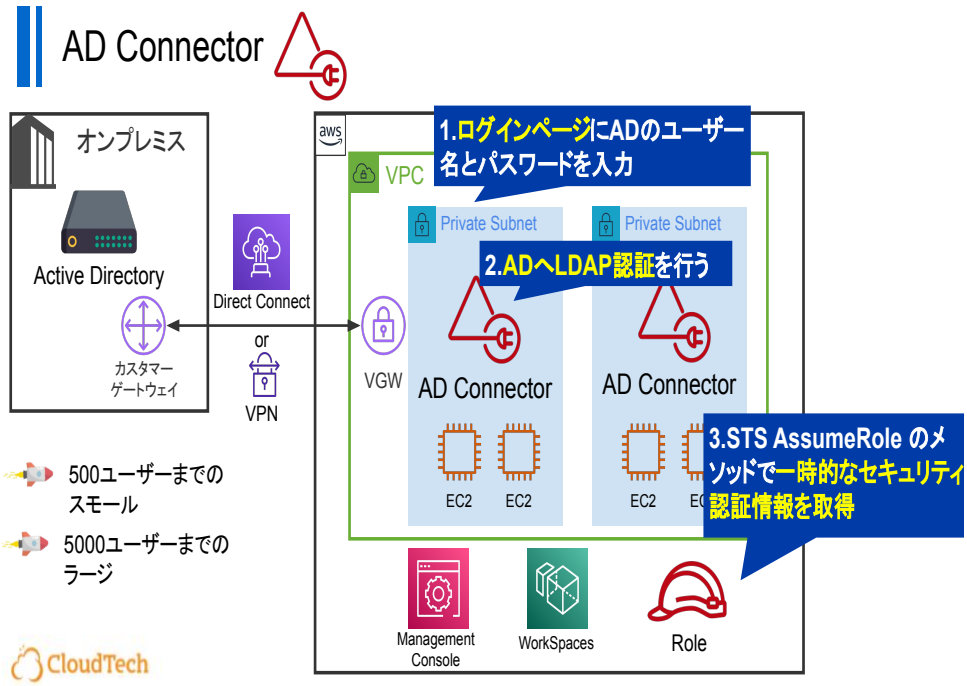
- 5000ユーザーを超える組織に有用
- スタンドアロンのADとしてAWS内で使用できる

CloudTech



AD Connector

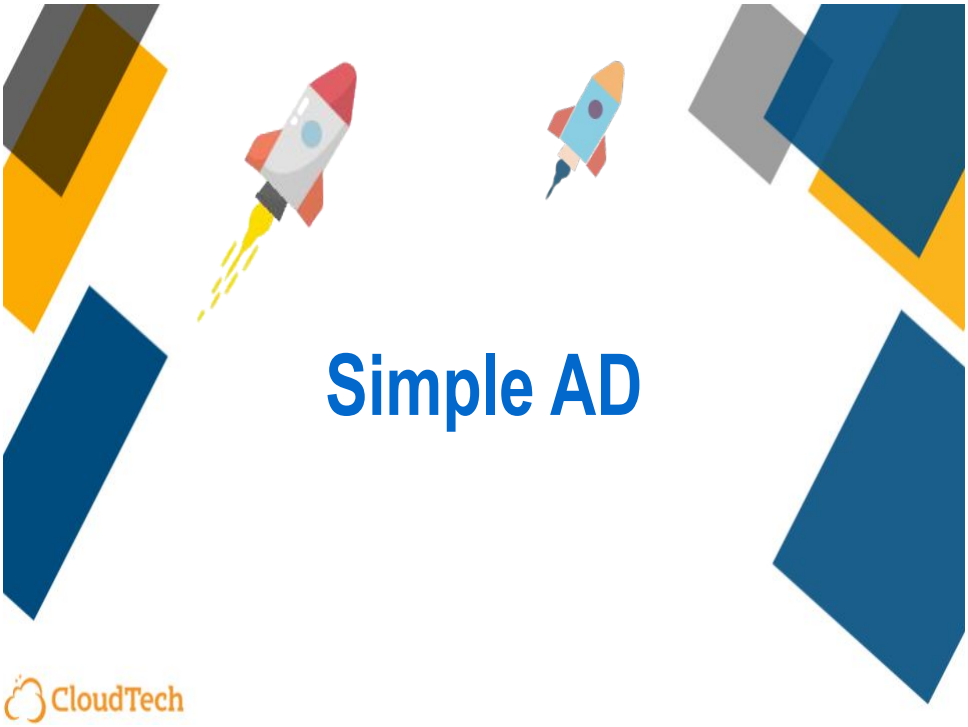
CloudTech



- AD Connectorはオンプレミス環境にある既存のディレクトリサービスと接続するプロキシのような役割を果たします。
    - コネクターという名前からもわかる通り、ユーザー情報等を保持するわけではありません。
        - オンプレでADを運用しているとします。
            - オンプレとDXもしくはVPNを通じて、AWSにあるAD Connectorと連携します。
        - そうすると、オンプレのユーザーは ADの認証を使用し、シングルサインオンでworkspacesなどのリソースへアクセスできます。
            - 詳細に説明すると、
                - AD Connectorを有効にするとログインページが生成されるので、これにActive Directoryのユーザー名とパ

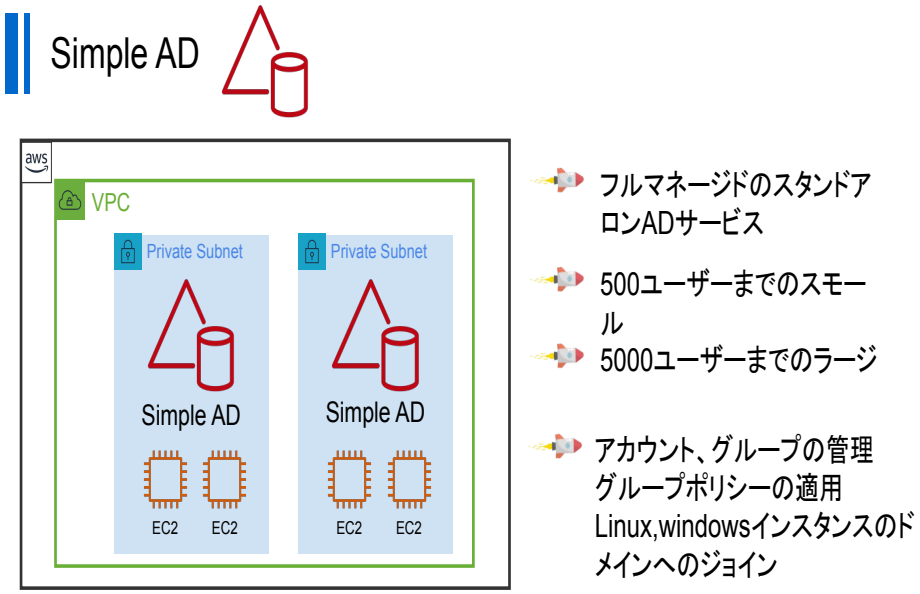
        - スワードを入力します。
            - AD Connectorは認証リクエストを受け取り、これをActive Directoryへ、LDAP認証を行います。
        - ユーザが認証された後、AD ConnectorはSTS AssumeRoleのメソッドを呼び出して、そのユーザの一時的なセキュリティ認証情報を取得します。
        - この一時的なセキュリティ認証情報を使用して、ユーザはAWSにアクセスできるというわけです。
            - ユーザーが複数のロールにマッピングされている場合、サインイン時にどのロールにマッピングするか選択するよう表示されます。
                - なお、ユーザーセッションの有効期限は1時間です。
- つまり、AD ConnectorはオンプレのADの認証情報を使用して、IAM Roleを紐づけているわけですね。
    - また、AD Conectorを使い、EC2をオンプレのドメインに参加させた

        - りもできます。
    - オンプレのADをそのまま使用してAWSを運用したい場合に有用ですね。
- その他
    - サイズは2つあります。
        - 500ユーザーまでのスモール
        - 5000ユーザーまでのラージ



Simple AD

CloudTech



CloudTech

- 最後に、SimpleADを簡単に解説します。
- Simple ADは、AWS上で稼働する、フルマネージドのスタンドアロンADサービスです。
  - ADの代替機能として使用でき、
  - サイズは2つあります。
    - 500ユーザーまでのスモール、5000ユーザーまでのラージ
  - ADの応用機能が利用できませんが、安価に利用できます。
    - 機能としては
      - アカウント、グループの管理
      - グループポリシーの適用
      - Linux,windowsインスタンスのドメインへのジョイン

■EC2のドメイン参加方法
Windows EC2 インスタンスをシームレスに結合する

https://docs.aws.amazon.com/ja_jp/directoryservice/latest/admin-guide/launching_instance.html
[Domain join directory] (ドメイン結合ディレクトリ) で、リストからドメインを選択します。

AWS Managed Microsoft AD へ EC2 インスタンス構築時にシームレスに参加する
https://blog.serverworks.co.jp/seamlessly-joining-an-ec2-instance-to-a-domain