Q 40 Azure Active Directory Domain ServicesでGPOを使うには

Microsoft Azureで、Active Directoryドメインサービスが提供され、グループポリシーが使えるようになりました。ここでは、Azure上でグループポリシーを使う手順について説明します。

Azure Active Directory（Azure AD）

Microsoft Azureは、マイクロソフトが提供するIaaSおよびPaaSベースのパブリッククラウドサービスです。IaaS（Infrastructure as a Service）は仮想マシンとネットワークを提供し、PaaS（Platform as a Service）はアプリケーションの実行環境（プラットフォーム）を提供します。

Microsoft .NETベースのアプリケーション実行環境（PaaS）として登場したAzureは、その後仮想マシンのサービス（IaaS）が追加されたほか、多くのアプリケーションサービスが追加されています。中でも高い評価を受けているのが「Azure Active Directory（Azure AD）」です。Azure ADは、SAML、WS-Federation、OAuthと言った業界標準の認証プロトコルをサポートし、Office 365などマイクロソフトが提供するサービスに加えて、Salesforce.comやDropboxなど、多くのサービスのID基盤として利用できます。

ただしAzure ADは、Active Directoryドメインサービス（AD DS）が利用するKerberos認証をサポートしませんし、グループポリシーに必要なSYSVOL共有も提供しません。同じ「Active Directory」ですが互換性はないので注意してください。

なお、オンプレミスのAD DSからAzure ADに対してパスワードを含むユーザー登録情報を複製することはできます。

Azure Active Directory Domain Servicesについて詳しくは、以下のサイトを参照してください。

Active Directory Domain Servicesのドキュメント
https://docs.microsoft.com/ja-jp/azure/active-directory-domain-services/

Azure Active Directory Domain Services（Azure ADDS）の構築

マイクロソフトは、AzureベースのActive Directoryドメインサービス「Azure ADDS」を提供しています。Azure ADDSは、オンプレミスのActive Directoryドメインサービスと完全な互換性を持ち、Kerberos認証とグループポリシーが利用できます。Azure ADDSは内部的には同名のAzure ADの拡張機能として構成されています。

ヒント

Azure ADDSはオンプレミスで使える？

Azure ADDSはADDSと同様の機能を持ち、Azureの仮想ネットワークとVPN接続を行えば、技術的にはオンプレミスのADDSの代用として使うことができます。しかし本来Azure ADDSはAzure上の仮想マシンから使うために設計されており、オンプレミスからの利用は想定していないということです。

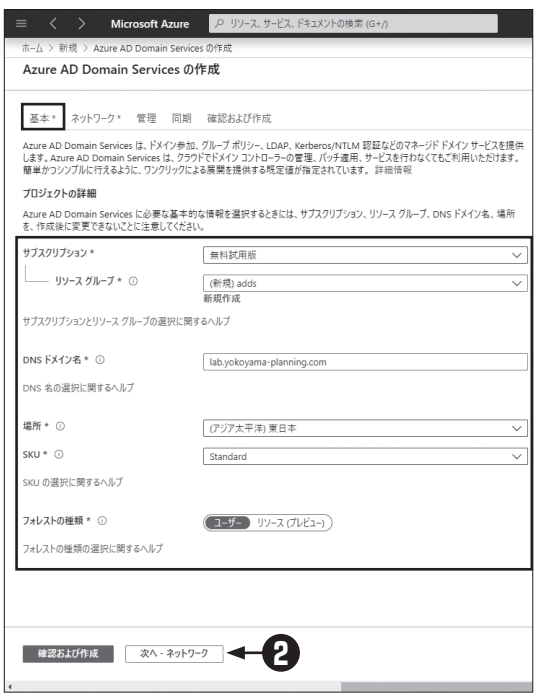
● Azure ADDSの登録

Azure ADDSの構築手順は以下のとおりです。なお、Azureの仮想マシンンと仮想ネットワークの詳細は『ひと目でわかるAzure　基本から学ぶサーバー＆ネットワーク構築　第3版』（日経BP、2019年）などを参照してください。

❶ Azure の管理ポータル（https://portal.azure.com）で、［＋リソースの作成］―［ID］―［Azure AD Domain Services］を選択する。

❷ ［基本］で、以下を指定して［次へ：ネットワーク］をクリックする。

- **サブスクリプション**…Azureの契約名
- **リソースグループ**…Azureの管理グループ（ここでは新規作成している）
- **DNSドメイン名**…Azure ADDSのドメイン名（インターネットに登録されていなくてもよいが、登録されているとインターネットで提供されているSaaSとの連係が容易になる）
- **場所**…Azure ADDSを作成する場所（リージョン）
- **SKU**…規模に応じて［Standard］［Enterprise］［Premium］を選択（［Standard］が最小構成）
- **フォレストの種類**…通常は［ユーザー］を選択する。［リソース］は、サーバーやアプリケーションのみを登録する場合に指定する。



❸

［ネットワーク］で、Azure の仮想ネットワークとサブネットを選択し、［次へ：管理］をクリックする。仮想ネットワークを新規作成する場合は［新規作成］を選択し、以下のパラメーターを指定して［OK］をクリックする。

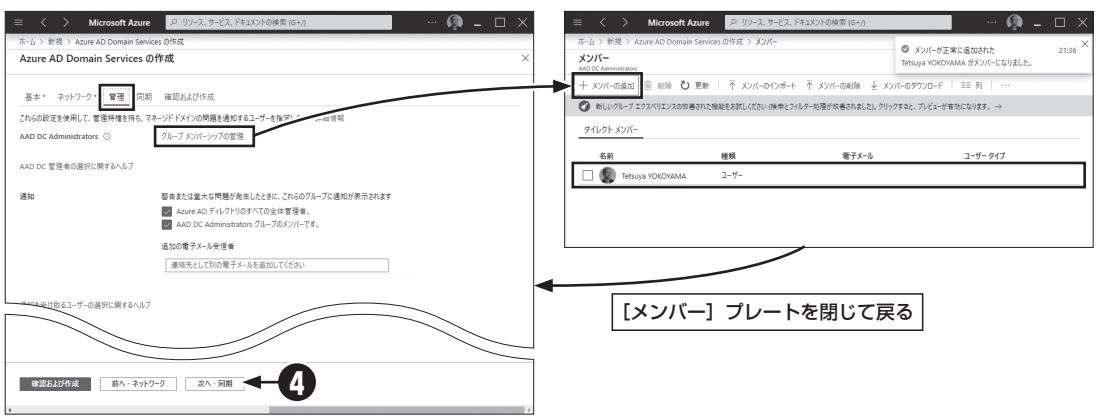
- **名前**…仮想ネットワークの名前
- **アドレス空間**…仮想ネットワークのIPアドレス範囲(わかりやすくするため､多くは16ビットマスク)
- **サブネット名**…アドレス空間内に割り当てたサブネットの名前
- **アドレス範囲**…サブネット範囲（わかりやすくするため、多くは24ビットマスク）

●Azure ADDS を構成した場合、ドメインコントローラー兼 DNS サーバーが 2 台構成されるので、仮想ネットワークの DNS サーバーとして登録する。Azure の仮想マシンの IP アドレスは､サブネット .4 から使われるため、たとえば 172.16.1.0/24 のサブネットであれば、172.16.1.4 および 172.16.1.5 がドメインコントローラー兼 DNS サーバーになる。

❹

［管理］で、［グループメンバーシップの管理］をクリックして［メンバーの追加］をクリックし、管理者を追加する。追加が完了したら［メンバー］ブレードを閉じて［次へ：同期］をクリックする。

●この管理者は、現在管理中の Azure AD のユーザーが指定できる。ユーザーを作成していない場合は、Azure の契約に使った Microsoft アカウントのユーザーを指定する。



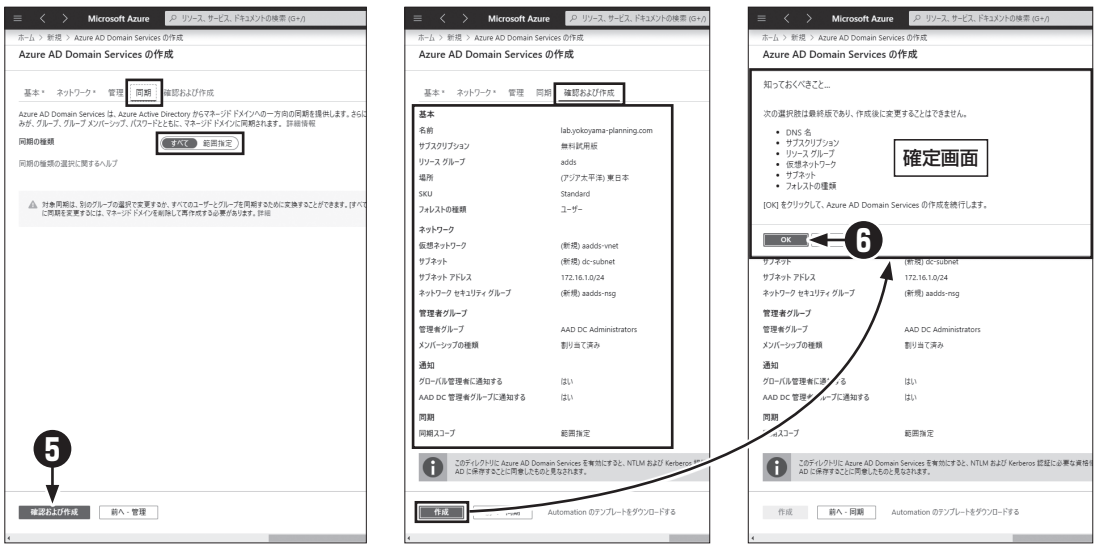
❺

［同期］で、Azure AD から Azure ADDS への同期の種類を選択して［確認および作成］をクリックする。［すべて］は全ユーザーの同期を行い、［範囲指定］は、指定した Azure AD グループのメンバーだけを同期する。

❻

［確認および作成］で設定内容を確認し、［作成］をクリックする。DNS 名などが変更できないなどの注意を確認し［OK］をクリックする。

●Azure ADDS の構築には 60 分以上かかる場合がある。［デプロイが進行中です］の画面になればウィンドウを閉じて構わない。

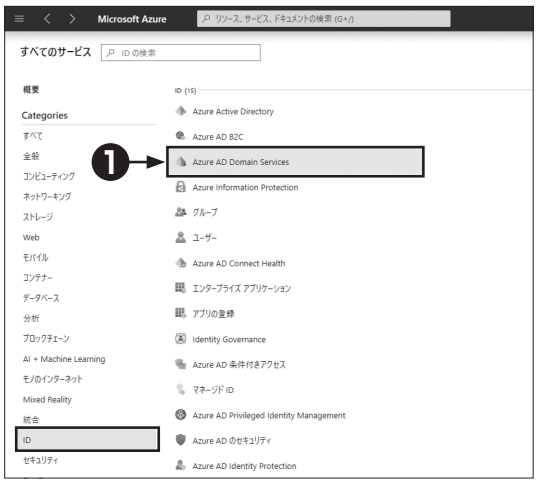


Azure ADDS を構成すると、ドメインコントローラーが 2 台作成されます。

●仮想ネットワークの設定の変更

Azure ADDSのクライアントコンピューターは、Azure ADDSのドメインコントローラーをDNSサーバーとして使用する必要があります。そのため、以下の手順で2台のAzure ADDSドメインコントローラーのIPアドレスを登録してください。

❶ Azure の管理ポータルで［すべてのサービス］―［ID］―［Azure AD Domain Services］を選択する。



❷ Azure ADDS のドメイン名をクリックする。

❸ ［概要］で、仮想ネットワークの DNS 構成を変更するため［仮想ネットワークの DNS サーバー設定の更新］にある［構成］をクリックする。

仮想ネットワークに構成した仮想サーバーは常にDHCPクライアントになります。仮想ネットワークにDNSサーバーを登録すると、その後に起動するAzureの仮想サーバーが正しいDNSサーバーを参照するようになります。

● ドメインへの参加

Azure ADDSを構築した仮想ネットワーク、あるいはこの仮想ネットワークと接続した別の仮想ネットワーク上にメンバーサーバーを作成することで、ドメインに参加させることができます。

開発者向けの機能を除き、Azureではサーバーしか登録できません。クライアントコンピューターをAzure ADDSに参加させるには、Azureの仮想ネットワークと社内ネットワークをサイト間VPNで接続する必要があります。

● Azure ADDSの制約

以上の作業で、ほぼ完全なActive Directoryドメインサービス環境が完成します。ただし、以下の制約があることに注意してください。

- **ドメインコントローラーにログオンする権利は与えられない。**
- **ドメイン全体の管理者権限は与えられない。**

Azure Active Directory Domain Services（Azure ADDS）の運用管理

Azure ADDSのドメインコントローラーにログオンすることはできないため、ユーザー登録などの管理作業は以下の手順で行います。

❶ Azure ADDS にメンバーサーバーを構成する。
これは、Azure ADDS が作成した仮想ネットワーク上に仮想マシンを作成し、Azure ADDS ドメインのメンバーとして構成するのが最も簡単です。

❷ Azure ADDS のメンバーサーバーに、Active Directory ドメインサービスの管理ツールをインストールする。

Windows Serverには［役割管理ツール］として、Active Directoryドメインサービスの管理ツールが標準で含まれます。このツールを使うことで、ドメイン管理が可能です（**図40-1**）。

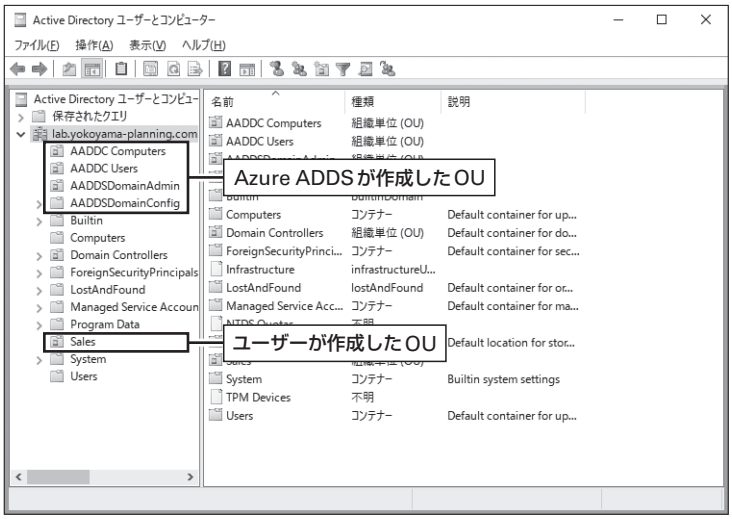


図40-1：Azure ADDSの管理

Azure ADの登録ユーザーをAzure ADDSに複製することもできます。このとき、パスワードも複製されるため、アカウント管理を一元化できます。ただし、Azure ADの登録ユーザーのログオン名（UPN）に使うドメインは「確認された」ものでなければいけません。「確認された」ドメインとして登録するためには、そのドメインに指示されたDNSレコードを作成する必要があります。つまり、インターネットに登録され、管理権限を持つDNSドメインのみが利用できます。

ヒント

UPN

UPN（User Principal Name）は、メールアドレス形式のユーザー名で、既定では「ユーザー名@DNSドメイン名」となります。UPNに使うDNSドメイン名は、AD DSのドメイン名と一致する必要はありません。

● ドメイン管理者

Azure ADDSを構成すると、初期ユーザーが「AAD DC Administrators」グループに登録されます。このグループは、ドメイン管理の権限はありませんが、一般的な管理作業は行えるように管理制御の委任が構成されています（**図40-2**）。そのため、OUを作成し、一般ユーザーを登録することは可能です。

また、グループポリシーの作成や管理も行うことができます。GPOをドメインに直接リンクすることはできませんが、AAD DC Administratorsが作成したOUにリンクすることは可能です。

管理制御の委任については、この章の「1.3 管理制御」を参照してください。

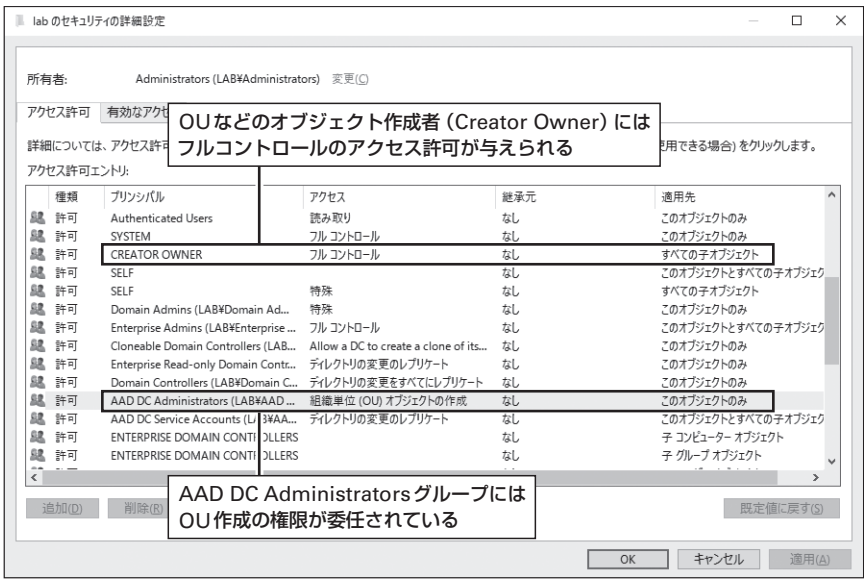


図40-2：Azure ADDSの委任（ドメインのセキュリティ設定）

● グループポリシー管理者

前述のように、AAD DC AdministratorsのメンバーはOUの作成と、作成したOUのフルコントロールのアクセス許可があります。そのため、新規に作成したOUについては、GPOの作成およびリンクが可能です。SYSVOL共有への書き込み権限もあるため、中央ストアの構成も可能です。

ただし、最初から作成されているドメインやDomain Controllersなど一部のOUにGPOをリンクすることはできません。

価格

Azure ADDSは、最も安価なSTANDARD版（2万5,000人以下を想定）で、1時間あたり16.80円になります（2020年2月現在）。1ヶ月にすると1万円を超えます。ディレクトリサービスは、「使わないときに停止する」というわけにいかないため、ほぼ固定料金と考えてよいでしょう。Azure ADDSはドメインコントローラーを2台作成します。 小規模な仮想マシンでも1ヶ月で1万円を超えるので、決して高価ではありません。

しかし、Azure ADは50万オブジェクトまでの無料枠があります。機能が違うので単純な比較はできませんが、Azure ADDSは割高な印象を受けます。

Azure Active Directory Domain Servicesの価格について詳しくは、以下のサイトを参照してください。

Azure Active Directory Domain Servicesの価格
https://azure.microsoft.com/ja-jp/pricing/details/active-directory-ds/

ヒント

Azure ADとAzure ADDSのパスワード

Azure ADのユーザーは、ADDS認証に必要なパスワードハッシュを持っていません。Azure ADのユーザーをAzure ADDSで使うには、Azure ADDS構成後、Azure ADのユーザーアカウントのパスワードをリセットします。

Azure ADDSが構成されている場合、パスワード変更時にAzure ADDSに必要なパスワードハッシュが生成されます。

ヒント

Azure ADDSの管理者アカウント

Azure ADDSの管理者は、Microsoftアカウントまたは Azure ADのユーザーアカウントを使用します。これらのユーザーのDNSドメイン名が、Azure ADDSのドメイン名と異なっている場合でもログオンは問題なくできます。

Active Directoryドメインサービスのドメイン名

Active Directoryドメインサービス（AD DS）のドメイン名は、「～ .local」という名称がよく使われていました。これは、マイクロソフトのドキュメントにサンプルとして使われていたためです。

しかし、現在では.localドメインを使うべきではないとされています。そもそも.localドメインはmDNS（マルチキャストDNS）で予約されています。MacOSはmDNSを使うため、.localドメインを使っていると不都合が生じるようです。また、Windows 10でもmDNSが採用されています。

しかも、Azure ADDSでドメインを使うにはインターネットからドメイン名を識別できる必要があります。.localドメインはインターネットから識別できないため、.localドメインをAzure ADDSで使うことはできません。

本書では、筆者（横山）が取得したドメインyokoyama-planning.comのサブドメインを使って構築したAzure ADDSを利用しています。