Q40 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。

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。

[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] [Enter prise] [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。



\equiv \langle \rangle Microsoft Azure	
ホーム > 新規 > Azure AD Domain Services	の作成
Azure AD Domain Services の作	F成
基本* ネットワーク* 管理 同期	確認および作成
Azure AD Domain Services は、ドメイン参加、 します。Azure AD Domain Services は、クラウト 簡単かつシンブルに行えるように、ワンクリックによる	グルーブポリシー、LDAP、Kerberos/NTLM 認証などのマネージドドメインサービスを提供 でドメインコントローラーの管理、パッチ適用、サービスを行わなくてもご利用いただけます。 。展開を提供する既定値が指定されています。 詳細情報
プロジェクトの詳細	
Azure AD Domain Services に必要な基本的な を、作成後に変更できないことに注意してください。	■「情報を選択するときには、サブスクリブション、リソース グループ、 DNS ドメイン名、場所 、
サブスクリプション *	無料試用版 ~
リソース グループ * ①	(新規) adds ✓
	新現作成
サブスクリプションとリソース グループの選択に関す	5ヘルプ
DNS ドメイン名 * ①	lab.yokoyama-planning.com
DNS 名の選択に関するヘルプ	
場所* ①	(アジア太平洋)東日本 🗸
SKU * 🕕	Standard V
SKUの選択に関するヘルプ	
フォレストの種類* ①	(ユーザー) リソース (プレビュー)
フォレストの種類の選択に関するヘルプ	
and the set of the set.	
確認および作成 次へ - ネットワー	
4	

A [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。



Δ 「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。



5 「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。

G
「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。



\equiv \langle \rangle Microsoft Azure	クリソース、サービス、ドキュメントの検索(G+/)	🖗 🗕 🗆 🗙					
市-ム > Microsoft.DomainServices.NSG.VNET.Subnet-20200229124158Z - 概要							
Microsoft.DomainServices.	NSG.VNET.Subnet-20200229124158Z - 概要	\$ ×					
	前 前除 🛇 キャンセル ① 再デブロイ ◯ 最新の情報に更新						
ee wa	デプロイが進行中です						
	デブロイ名: Microsoft.DomainServices.NSG.VNET.Subnet-202002291	開始時刻: 2020/2/29 21:41:59					
(三 出力)	➡■ サブスクリプション: 無料試用版 リソース グループ: adds	相関 ID: d63566ac-23cf-4fa9-b					
◎ テンプレート							
	へ 展開の詳細 (ダウンロード)						
	リソース 種類 状態	操作の詳細					
	lab.yokoyama-planning Microsoft.AAD/DomainS Created	操作の詳細					
	Sadds-vnet Microsoft.Network/virtu OK	操作の詳細					
	aadds-nsg Microsoft.Network/Net OK	操作の詳細					
	~ 次の手順						

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。

1 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。

2 ····· Azure ADDS のドメイン名をクリックする。

 【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。

\equiv $<$ $>$ Microsoft Azure	、P リソース、サービス、ドキュメントの検索 (G+/)
すべてのサービス 🔎 🗈 の検索	
概要	ID (15)
Categories	Azure Active Directory
3~7	Azure AD 82C
	🚸 Azure AD Domain Services
コンビューティング	Azure Information Protection
ネットワーキング	la di si
ストレージ	204 ()N-)
Web	🚨 1-4-
モバイル	🚸 Azure AD Connect Health
コンテナー	職 エンタープライズ アプリケーション
データベース	III アブリハキ45
分析	100 T / 7 / 7 / 7 / 10 E / P
ブロックチェーン	Identity Governance
AI + Machine Learning	New Azure AD 条件付きアクセス
モノのインターネット	◎ マネージド ID
Mixed Reality	
統合	Azure AD Privileged Identity Management
ID	Azure AD のセキュリティ
セキュリティ	a Azure AD Identity Protection

\equiv \langle \rangle Microsoft Azure	アリソース、サービス、ドキュメン	トの検索 (G+/)				
すべてのサービス > Azure AD Domain Services						
Azure AD Domain Services						
+ 追加 ☷ 列の編集 ○ 更新 业 csv	イにエクスポート 🕴 🖉 タグの割り	当て ♡ フィードバック ≓ フ	レビューを終了			
格前でフィルター サブスクリプション	== \$KT UV-2 01-7	*== すべて 💿 (場所 == すべ	て			
1 件中 1 ~ 1 件のレコードを表示しています。						
□ 名前 ↑。	種類 ↑↓	リソース グループ 斗	場所 ↑↓			
🗌 🧄 lab.yokoyama-planning.com 🗲	Azure AD Domain	Services adds	東日本			
	U					



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。

1 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。

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)。

					_	~
Active Directory ユーザーとコンピューター				_		~
ファイル(E) 操作(A) 表示(V) ヘルフ	プ(日)					
◆ → 2 🖬 🖬 🖬 🖓 🗟	2 . 2	' D '&				
Active Directory 1-∜-とコンピュ- Active Directory 1-∜-とコンピュ- Acth/2-TJ Babyokoyama-planning.com AADDC Computers AADDC Computers AADDC SomainConfig Builtin Computers Domain Controllers ForeignSecurityPrincipals ForeignSecurityPrincipals Managed Service Accoun Program Data Sales System Users	AADDC Computers AADDC Users AZURE ADDS Computers Computers Comparing SecurityPrinci Infrastructure LostAndFound Managed Service Acc Infrastructure CostAndFound Managed Service Acc		説明 Default container for up Default container for do Default container for sec J Default container for ma Default container for ma Builtin system settings Default container for up			
< >						

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。

L	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。

lab	のセキュリテ	「イの詳細設定				- D >
所有	诸:	Administ	trators (LAB¥Admin	istrators) 変更(<u>C</u>)		
アクt 詳細	Zス許可 ICついては	有効なアクセ(0Uなどの: フルコント	オブジェクト作成者 (Crea コールのアクセス許可が与	ator Owner) には うえられる	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
アクセ	2ス許可ェ	.ントリ:				
	種類	プリンシバル		アクセス	継承元	適用先
52	許可	Authenticated	d Users	読み取り	なし	このオブジェクトのみ
52	許可	SYSTEM		フルコントロール	なし	このオブジェクトのみ
52	許可	CREATOR OW	/NER	フルコントロール	なし	すべての子オブジェクト
88	許可	SELF			なし	このオブジェクトとすべての子オブジェク
52	許可	SELF		特殊	なし	すべての子オブジェクト
52	許可	Domain Admir	ns (LAB¥Domain A	d 特殊	なし	このオブジェクトのみ
52	許可	Enterprise Adr	mins (LAB¥Enterpri	se フルコントロール	なし	このオブジェクトとすべての子オブジェク
88	許可	Cloneable Dor	main Controllers (L	AB Allow a DC to create a clone of its	なし	このオブジェクトのみ
騦	許可	Enterprise Rea	ad-only Domain Co	ntr ディレクトリの変更のレプリケート	なし	このオブジェクトのみ
騦	許可	Domain Contr	rollers (LAB¥Domaii	n C ディレクトリの変更をすべてにレプリケート	なし	このオブジェクトのみ
88.	許可	AAD DC Admi	inistrators (LAB¥AA	D 組織単位 (OU) オブジェクトの作成	なし	このオブジェクトのみ
88	許可	AAD DC Servic	ce Accounts (L/ 3¥/	AA ディレクトリの変更のレプリケート	なし	このオブジェクトとすべての子オブジェク
騦	許可	ENTERPRISE D	OMAIN CONTE DL	LERS	なし	子 コンピューター オブジェクト
题	許可	ENTERPRISE D	ENTERPRISE DOMAIN CONTI DILERS なし			子 グループ オブジェクト 🗸 🗸
د	AAD DC Administrators グループには OU作成の権限が委任されている					> 既定値に戻す(S)
					ОК	キャンセル 適用(A)

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。

ヒント

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。

ヒント

Azure Active Directory Domain Servicesの価格

https://azure.microsoft.com/ja-jp/pricing/details/active-directory-ds/

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

Azure ADDSが構成されている場合、パスワート 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。 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。