第 5 章

Windows 10 のサインインと ID の管理

目次

概要

ID の管理は、特に複数のディレクトリ サービスが存在する環境で、複雑なタスクになる可能性があります。Windows 10 には、サインインのために複数の ID 管理方法があり、Microsoft アカウント、Active Directory アカウント、ローカル アカウント、または Azure Active Directory (Azure AD) アカウントを使用できます。この章では、Windows 10 によるエンタープライズ ID の管理について説明します。

目的

この章により、次のことを習得できます。

- エンタープライズ ID の概念について説明することができます。
- クラウド ID の統合を計画することができます。

レッスン 1
エンタープライズ ID の概要

エンタープライズ環境での ID 管理は、コンシューマー シナリオでの ID 管理とは異なります。これは、コンシューマー環境のユーザーのほとんどは、Windows 10 コンピューターのメイン ID として Microsoft アカウントを選択するためです。一方、エンタープライズ環境には、多くの場合、より多くの選択肢があります。さらに、ID を管理する際は、ID をセキュリティで保護する必要もあります。このレッスンでは、基本的な ID の概念と ID 管理について説明します。

目的

このレッスンにより、次のことを習得できます。

- ID を定義することができます。
- ID の種類と認証シナリオについて説明することができます。
- ID を認証するために使用する方法について説明することができます。
- 多要素認証を使用することで、ID のセキュリティを強化する方法について説明することができます。
- Microsoft アカウントとドメインベース アカウントを統合することができます。
- グループ ポリシーを使用して、Microsoft アカウントとドメイン アカウントの統合を管理することができます。

ID とは

サブジェクトまたはエンティティとも呼ばれ、一意に人物またはオブジェクトを記述し、そのサブジェクトと他のエンティティとの関係についての情報を含む一連のデータである

- ディレクトリ データベースとも呼ばれる ID ストアに保存される
- AD DS では、ID は通常、セキュリティ プリンシパルで表現される
- AD DS では、ID は SID によって一意に識別される
- ID は主にユーザーがリソースにアクセスするために使用される

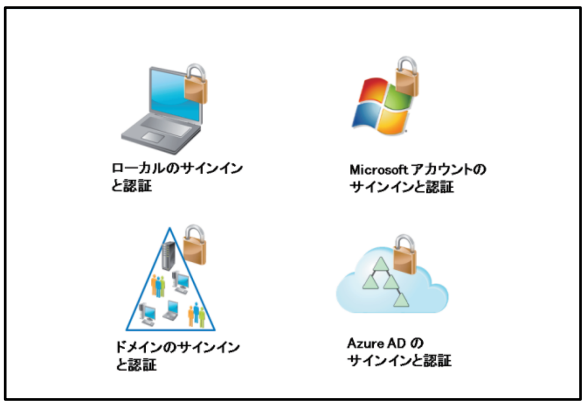
情報の保護と ID 管理の中核において、ID の重要な概念の 1 つが ID の信頼性です。セキュリティで保護されたシステムでは、ID は各ユーザーを表します。コンピューター業界における ID とは、一意に人物またはオブジェクトを記述し、そのサブジェクトと他のエンティティとの関係についての情報を含む一連のデータです。また、ID は、サブジェクトまたはエンティティと呼ばれることもあります。Windows オペレーティング システムでは、ユーザー アカウントは人物またはサービスの ID を表します。ID ストアは 1 人以上のユーザーのアカウントを保持し、ディレクトリ データベースとも呼ばれます。Active Directory ドメイン サービス (AD DS) は、ディレクトリ データベースの一例です。AD DS では、ID は通常、セキュリティ プリンシパルで表現されます。セキュリティ プリンシパルは、セキュリティ識別子 (SID) と呼ばれる属性によって一意に識別されます。同様に、Azure AD では、各 ID はユーザー アカウントと SID で表現されます。

グローバルなデジタル コミュニケーションにおける最大の問題の 1 つは、ID の信頼性です。個人のデジタル ID をグローバルに信頼および信用できる方法で確認することはできません。属性は個人のデジタル ID と関連付けられていますが、これらの属性は (ID でさえも) 変更、マスク、または削除が可能であり、新しい属性や ID を作成することもできます。デジタル表現をエンティティに割り当てるには、属性の利用者が、名前、場所、役職、年齢などの属性の申告が正しく、それらが属性を提示する個人やものに関連付けられていることを信頼する必要があります。また、2 つのディレクトリ サービス間で信頼を確立することもでき、そうすることで、2 つ以上の組織間で ID の信頼性を実現することができます。

一方、システムには、ユーザーがアクセスを要求するリソースという面もあります。リソースはアクセス許可によりセキュリティで保護され、各アクセス許可は、特定レベルのアクセスと ID のペアリングを指定します。多くの Windows ベースのリソースは (NTFS ファイル システム ボリュームのファイルとフォルダーを含む)、セキュリティ記述子により保護されています。このセキュリティ記述子には、随意アクセス制御リスト (DACL) が含まれます。DACL の中で各アクセス許可は、アクセス制御エントリ (ACE) の形式で表されます。ACE は、リソースに対して何らかのアクセス許可を持つユーザー アカウントの SID を指定します。ディレクトリ サービスとリソースが同じ組織に属し、同じディレクトリ データベースを使用する場合、認証タスクと承認タスクの管理はシンプルになります。ただし、現在の IT 環境では、多くの組織が、1 つの組織で 1 つのディレクトリ サービスを使用して ID を管理しながら、別のシステム (通常はクラウドベース サービス) にリソースを保有しています。

ID の種類と認証シナリオ

認証は、ユーザー、コンピューター、グループ、デバイス、サービス、またはプロセスの ID を検証するプロセスです。現実の生活では、認証プロセスは頻繁に実施されます。例えば、外国に旅行に行く際は、空港に着いたらパスポートを空港の税関職員に提示します。こうすることで、認証プロセスを実行しています。税関職員はパスポートを発行したエンティティを信頼しているので、パスポートを提示することにより、信頼できる方法で ID が検証されます。ただし、パスポートを提示しただけでは、飛行機に搭乗 (アクセス) できません (飛行機はリソースの一例です)。



コンピューター環境で、通常、認証は資格情報のセットを提供することで実施されます。ユーザーは、少なくとも 2 つのコンポーネントを含む資格情報を入力します。それは、サインイン名と、ユーザーおよびシステムのみが知っている秘密情報 (パスワードなど) です。システムは、ID の一部として格納された情報と比較して、資格情報の正確性を検証します。この種類の認証に加えて、ユーザーは、スマート カード、PIN、トークンを使用したり、指紋や網膜をスキャンしたりすることで、ID を立証することもできます。

通常、認証はリソースへのアクセスを可能にするために実行されます。リソースへのアクセスには承認が必要であり、承認は正常に認証された後で実施されます。ただし、承認が成功するには、アクセスされるリソースが認証サービスを信頼する必要があります。

例えば、コンピューターが Active Directory ドメインに参加すると、コンピューターは AD DS を信頼するようになります。その結果、ユーザーはドメインの資格情報を使用してコンピューターにサインインし、ローカルのリソースにアクセスできます。

ローカルのサインインと認証

コンピューターの認証には、次の 2 種類があります。

- **ローカルまたは対話型のサインイン :** ユーザーがコンピューターに直接サインインする際に実行されます (自分のコンピューターにサインインする場合など)。
- **リモートまたはネットワークのサインイン :** 別のコンピューターに接続する際に実行されます (ファイル サーバーやメール サーバーからファイルやその他のリソースを取得する場合など)。

スタンドアロン構成の Windows ベース システムでは (ワークグループとも呼ばれる)、各コンピューターは信頼できる ID ストアを 1 つのみ保持します。このストアは、Security Accounts Manager (SAM) データベースと呼ばれるレジストリに格納されたユーザーとグループのローカル リストです。ドメインでの一元化された認証とは異なり、ワークグループでは各コンピューターが固有の SAM を保有しているので、分散された認証システムはありません。

ユーザーは、SAM 内の ID と比較して検証される資格情報を提示する必要があります。ローカルのサインインでユーザーが認証され承認された後、エクスプローラーが起動され、使い慣れた Windows デスクトップが生成されます。

ただし、ユーザーがリモート サーバーの共有フォルダーにアクセスしようとすると、そのサーバーが提示された ID を信頼していない場合、すぐに問題が発生します。これは、その ID が、知らないシステムや信頼関係のないシステムで認証されているためです。サーバーは、自身の ID ストアつまり自身の SAM のみを信頼します。したがって、ユーザーがサーバーにリモートでサインインする場合は、サーバーの SAM に、ユーザーの ID (ユーザー アカウント) が必要です。ID のサインイン名とパスワードが、ワークステーションの ID の資格情報と一致している場合、認証プロセスはユーザーにとって透過的になります。この種類の認証のことを「パススルー認証」と呼びます。ただし、サインイン名またはパスワードが一致しない場合は、共有リソースへの接続を試みる際、サーバーから有効な資格情報を入力するように求められます。

サーバーのセキュリティで保護されたリソースのアクセス制御リスト (ACL) に、信頼関係のないの ID を参照するアクセス許可を含めることはできません。したがって、リソースにアクセスする必要があるすべてのユーザーは、匿名認証によるアクセスが許可されていない限り、アクセスしようとするサーバーにアカウントを保有している必要があります。

これは、管理上の課題になる可能性があります。ユーザーがデスクトップでパスワードを変更した場合、2 つのアカウントは同期しなくなり、サーバーに接続する際、資格情報が求められます。時間が経つほどユーザー、リソース、および Windows ベース システムを環境に追加されるので、問題がさらに大きくなります。各ユーザーが複数の ID を維持するという課題は、即座に複雑化する可能性があります。

ドメインのサインインと認証

Windows Server 2012 オペレーティング システムを使用するビジネス環境では、ユーザーとコンピューターはほとんど Kerberos バージョン 5 (V5) プロトコル認証を使用して、AD DS に対する認証をおこないます。Kerberos 認証はチケットに基づいて動作し、このチケットにより、コンピューターはネットワーク経由で通信して、安全な方法で互いに ID を証明することができます。Kerberos 認証は主に、クライアント/サーバー アーキテクチャ向けに設計されており、相互認証を提供するので、ユーザーとサーバーの両方が互いの ID を検証できます。Kerberos 認証に加えて、Windows オペレーティング システムでは NTLM 認証プロトコルを使用することも、場合によっては基本認証を使用することもできます。NTLM は安全な認証方法と見なされていますが、基本認証はユーザー名とパスワードをクリア テキストで送信することで機能します。したがって、Secure Sockets Layer (SSL) でさらに保護されない限り、運用環境で基本認証を使用することは推奨しません。

コンピューターがドメインに参加するプロセスを理解すると同時に、認証プロセスに留意することが重要です。ユーザーは、ローカル アカウントを使用してコンピューターにサインインした後、そのコンピューターのローカル リソースにアクセスできます。このシナリオでは、ユーザーはローカル SAM またはドメイン アカウントのいずれかを使用して認証されます。ドメイン アカウントの場合、ユーザーは AD DS により認証されます。ユーザーは、サインインするコンピューターが Active Directory ドメインに参加している場合のみ、ドメイン アカウントを使用してサインインできます。この参加により、コンピューターは信頼できる認証サービスとして AD DS を信頼するようになります。AD DS を使用して認証される各ユーザーは、そのコンピューターのローカル リソースにアクセスできます。コンピューターがドメインに参加することで、実際に Active Directory ドメインとコンピューターの間で信頼を確立するプロセスが実行されます。これは、ドメイン間で信頼を確立するプロセスと非常に似ています。2 つのドメイン間で信頼を確立すると、ユーザーは一方のドメインで認証されることで、他方のドメインのリソースにアクセスできるようになります。

コンピューターがドメインに参加することで、そのドメインのユーザーはそのコンピューターにサインインして、そのコンピューターのリソースにアクセスできるようになります。

Microsoft アカウントのサインインと認証

Windows 8 以降、ユーザーは Microsoft アカウントを使用して Windows オペレーティング システムにサインインできます。Windows 8 の前は、ユーザーはローカル アカウントまたはドメイン アカウントを使用してのみ、サインインすることができました。

Microsoft アカウント (以前は Windows LiveID および Microsoft Passport とも呼ばれた) は、ほとんどの場合、Hotmail.com、msn.com、または Outlook.com のサービスで使用するメール アドレスとして知られています。Microsoft アカウントは無料で使用でき、Windows 8 の前は、Microsoft OneDrive (以前の SkyDrive)、Microsoft Office Online などのサービスや、MSDN、Microsoft TechNet などのサービスに加えて、無料メールにアクセスするために使用されていました。一般的に、コンシューマーベースのユーザーは、ほとんどすべての Microsoft Web ベース サービスで Microsoft アカウントを使用して認証されます。

Windows 8 以降の Windows オペレーティング システムでは、Microsoft アカウントを使用して Windows オペレーティング システムにサインインできます。Microsoft アカウントを使用してサインインすると、OneDrive、Outlook.com メール、Skype などのサービスに加えて、Microsoft Windows ストアに直接アクセスできます。
また、Microsoft アカウントにより、同じ Microsoft アカウントを使用してサインインするすべてのデバイスの間で、ファイル、データ、および設定を同期することもできます。例えば、同じ Microsoft アカウントを使用してサインインする場合、Windows コンピューターと Windows Phone の間で保存された Wi-Fi ネットワークのパスワードを同期できます。

Windows マシンで Microsoft アカウントを使用することで、単一コンピューターの ID 管理がよりシンプルになります。Windows にサインインするために、ある資格情報セットを使用し、Skype、OneDrive、または Outlook.com などのサービスにアクセスするために別の資格情報セットを使用する代わりに、ユーザーは Microsoft アカウントを使用して、これらすべてのリソースにアクセスできます。

また、Microsoft アカウントを使用して Windows コンピューターにローカルにサインインすることも、信頼の一例です。これは、コンピューターが Active Directory ドメインに参加する場合と同じプロセスです。Microsoft アカウントのシナリオでは、コンピューターは Microsoft アカウントの ID サービスを信頼しているので、ユーザーは Microsoft アカウントの Web ベース認証サービスで認証されることにより、そのコンピューターのローカル リソースにアクセスできます。

ただし、Microsoft アカウントを使用して、Active Directory ドメインのリソースにアクセスすることはできません。

Microsoft Azure Active Directory のサインインと認証

Windows 10 以降、Azure AD の資格情報を使用しても、Windows 10 コンピューターにサインインできるようになりました。Windows 8 と同様に、Windows 10 でもユーザーは Microsoft アカウントを使用してサインインできますが、認証方法がさらにもう 1 つ提供されました。

Microsoft アカウントとは異なり、Azure AD アカウントは無料ではありません。ただし、Office 365 や Azure Rights Management サービス (Azure RMS) などのサービスを既に使用している場合は、利用可能な Azure AD アカウントが用意されています。また、Azure AD アカウントは、ローカルの AD DS から作成することも、クラウドで作成することもできます。これについては、以降の章で説明します。

Windows 10 では、AD DS ではなく Azure AD に、コンピューターを参加させることもできます。Azure AD アカウントを使用して Windows 10 にサインインすると、Office 365 メールボックス、OneDrive for Business ファイル、SharePoint Online ライブラリなど、その他のリソースにアクセスできます。

ID の認証に使用される方法

コンピューター システムで使用されるすべての ID は、何らかの方法で認証される必要があります。現在では、認証を実行するさまざまな方法があります。認証プロセスは重要なセキュリティ プロセスなので、認証方法は常に改善されています。

パスワードベースの認証

ほとんどの組織では、ネットワークにサインインするユーザーは、Active Directory ドメイン コントローラーにより認証されます。正しい資格情報をドメイン コントローラーに提供するユーザーに、セキュリティ トークンが与えられます。同じ Active Directory 環境内のサーバーは、ユーザーを認証する同じドメイン コントローラーと通信できるので、これらのサーバーで稼働するアプリケーションは、Active Directory ドメイン コントローラーにより提供されるセキュリティ トークンを信頼しています。ただし、この種類の認証は、Active Directory フォレスト境界の外部には拡張されないので、問題が発生します。2 つの Active Directory フォレスト間で、Kerberos プロトコルまたは NTLM に基づいて信頼を実装した場合、その信頼の両側にあるクライアント コンピューターとドメイン コントローラーは、別のフォレストのドメイン コントローラーと通信して、認証と承認に関する意思決定をおこなう必要があります。この通信では、ネットワーク トラフィックが複数のポートで送信される必要があるので、これらのポートは、ドメイン コントローラーとその他のコンピューターの間にあるすべてのファイアウォールでオープンになっている必要があります。ユーザーが、Azure や Office 365 などのクラウドベース システムのリソースにアクセスする必要がある場合、問題はさらに複雑になります。これらの課題を解決するために、Microsoft は Windows 10 に Azure AD 認証を実装しました。

クレームベース認証

クレームベース認証は、ユーザーの認証と承認を個々のアプリケーションから分離するメカニズムを提供します。クレームベース認証を使用することで、ユーザーは組織内に配置されているディレクトリ サービスで認証され、その認証に基づいたクレームを受け取ることができます。そのクレームは、異なる組織で稼働しているアプリケーションに提示することができ、アプリケーションは提示されたクレームに基づいて、ユーザーが情報または機能にアクセスできるようにします。すべての通信は、HTTPS を通じて実行されます。

クレームベース認証のクレームは、ある組織またはテクノロジで定義されたユーザーに関するステートメントです。このクレームは、別の組織またはテクノロジからも信頼されています。クレームには、さまざまな情報を含めることができます。例えば、クレームには、ユーザーのメール アドレス、ユーザー プリンシパル名 (UPN)、およびユーザーが属する特定のグループに関する情報を定義できます。これらの情報は、ユーザーが認証に成功した際、認証メカニズムから収集されます。

アプリケーションを管理する組織は、アプリケーションが許可するクレームの種類を定義します。例えば、アプリケーションは ID を検証するためにユーザーのメール アドレスを要求し、次にクレーム内のグループ メンバーシップを使用して、ユーザーがアプリケーション内で保有するアクセス レベルを決定する場合があります。

Windows Hello と Passport 認証

Windows Hello は、Windows 10 の新しい認証メカニズムであり、認証プロセスの簡略化とセキュリティの向上に役立つように設計されています。Windows Hello は生体認証に基づいているので、ユーザーは顔または指を使用して、Windows 10 コンピューターに認識され、認証されることができます。

注 : 特に強調すべきことは、指紋認証は Windows 10 の前でも Microsoft 以外のアプリケーションを使用して利用可能だったことです。ただし、これらのアプリケーションは、指紋による認証をおこなうためにパスワードも必要としていました。基本的に、これらのアプリケーションのほとんどは、指紋を認識した後でパスワードを入力するように作られていました。

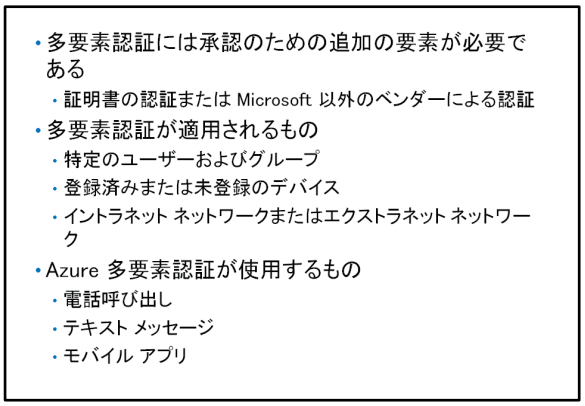
Windows Hello は、ネイティブに生体認証をサポートする新しいオペレーティング システム機能です。生体認証属性 (顔、指紋、または虹彩) を使用することで機能し、ユーザーがシステムに認証されます。エンタープライズ認証およびアプリケーション認証に使用できます。

Windows Hello を使用するには、生体認証をサポートするハードウェアを備えたデバイスを用意する必要があります。
指紋リーダーを備えたコンピューターを既に保有していれば、ほとんどの場合、Windows Hello による指紋認証を使用できます。顔認識では、このテクノロジの要件を満たすカメラが、コンピューターに必要になります。現在、これらの要件を満たすカメラ チップは、Intel RealSense 3D カメラ (F200) だけです。

パスワードによる認証 (特にオンライン サービスでは最も安全性が低い認証方法の 1 つ) を避けるために、Microsoft はアプリケーション、Web サイト、およびネットワーク リソースに対してパスワードを送信することなく安全な認証を可能にする認証システム (現在のコード ネームは「Passport」) を提供しています。Passport は代わりに、PIN 認証または Hello ベースの生体認証を使用します。Passport ベースの認証は、多くの Web サービスにより急速に採用されており、多数の Azure AD ベース サービスで使用されます。

Windows Hello と Passport は、ユーザーを識別するためにバイオメトリック署名による認証サービスを提供する新しい 2 つのテクノロジの例です。Windows Hello は、生体認証データをデバイスのローカルに格納し、だれともこのデータを共有しません。ただし、このデータを使用して Passport がロック解除され、Passport がアプリケーションとサービスでの認証に使用できるようになります。

多要素認証による ID セキュリティの強化



多要素認証により、ユーザー認証のセキュリティが強化されます。標準認証は、ユーザー名とパスワードに基づいています。認証に第 2 の要素を追加することで、承認されていない者がユーザーの資格情報を使用することがより困難になります。認証の第 2 の要素は、ユーザーが知っているだけではなく所有しているものである必要があります。

多要素認証は、いくつかの方法で実装することができます。その 1 つは、追加の認証方法として、Active Directory フェデレーション サービス (AD FS) と AD DS の証明書認証を使用することです。多要素認証に証明書認証を使用することは、既定でサポートされています。多要素認証のもう 1 つの方法は、スマート カードを使用することです。つまり、スマート カードを PIN と一緒に使用し、その PIN でスマート カードをロック解除します。

これにより、ユーザーは、所有しているもの (スマート カード) と知っているもの (PIN) を使用して、コンピューターまたはリソースに認証されることになります。ただし、スマート カードの使用は、Active Directory ドメイン環境に限定されます。さらに、スマート カードでは、Microsoft Identity Manager (以前の Microsoft Forefront Identity Manager) や同様の Microsoft 以外のアプリケーションなど、スマート カード管理ソフトウェアが必要になります。

その他に、AD FS および AD DS と統合できる Microsoft 以外のベンダーによる多要素認証方法があります。多要素認証の一般的な 1 つの方法では、ユーザーは定期的に変化する番号を表示するデバイス (通常はトークン デバイスと呼ばれる) を携帯する必要があります。ユーザーが認証されるには、そのトークン デバイスに表示される番号を入力します。

次のものを、多要素認証の対象にすることができます。

- 特定のユーザーおよびグループ
- 登録済みまたは未登録のデバイス
- イントラネット ネットワークまたはエクストラネット ネットワーク

Azure 多要素認証

Microsoft は Azure 多要素認証も提供しており、第 2 の認証要素として携帯電話またはスマートフォンを使用します。Azure 多要素認証を AD FS と統合すると、追加の認証として次の方法を実装できます。

- **電話呼び出し :** ユーザーは電話に着信を受け、認証を確認します。着信後、ユーザーは番号記号 (#) を押すことで確認をおこないます。
- **テキスト メッセージ :** ユーザーは、パスコードを含むテキスト メッセージを受信し、テキスト メッセージに対してパスコードを入力して応答します。
- **モバイル アプリ :** 認証プロンプトがモバイル アプリに表示された後、ユーザーは受信確認をおこなう必要があります。

Azure 多要素認証は AD FS 認証以外のシナリオで使用でき、セキュリティの強化が必要な状況で組み込むことができます。例えば、次を対象とした認証で使用できます。

- 仮想プライベート ネットワーク (VPN)
- Azure でホストされているクラウドベース アプリケーション
- RADIUS サーバー
- AD DS

Microsoft アカウントとドメインベース アカウントの統合

Windows 8 以降の Windows オペレーティング システムでは、初期セットアップで Microsoft アカウント情報の入力が求められるので、各サービスに個別にサインインする必要なく、Windows ストア、OneDrive、Outlook などのリソースにアクセスできます。さらに、Microsoft アカウントを使用して、コンピューターまたはデバイスにサインインできます。

- Microsoft アカウントを Active Directory ドメイン ユーザー アカウントにリンクできる
- 統合している間、Active Directory ドメイン アカウントでコンピューターにサインインするが、バックグラウンドでは Microsoft アカウントでサインインする
- オンライン リソースと Windows ストアにアクセスするために Microsoft アカウントを使用できる
- データと設定を同期するために Microsoft アカウントを使用できる

ただし、コンピューターが Active Directory ドメインに追加された後は、サインインの資格情報が変わります。コンピューターにサインインするために Microsoft アカウントを使用する代わりに、ユーザーは Active Directory アカウントを使用するようになります。これは、コンピューターと Active Directory ドメインの間で新しい信頼が確立されているからです。

ユーザーが、Microsoft アカウントに関連するオンライン サービスへのアクセスを維持したいが、コンピューターへのサインインに Active Directory ドメインの資格情報を使用する場合、これら 2 つのアカウントを統合するオプションがあります。

この場合、Active Directory ドメイン アカウントはコンピューターにサインインするためのメインのアカウントになりますが、バックグラウンドで、Microsoft アカウントを使用して、アクセスするリソースにサインインします。このアプローチでは、ドメインベースのリソースとプライベートのオンライン リソースの両方に対して、アクセスを維持できます。

Microsoft アカウントを Active Directory アカウントに追加するには、Windows 10 のスタート メニューで [設定] を開き、[アカウント] を選択します。ここに、Microsoft アカウントを既存の Active Directory アカウントに追加するオプションがあります。このオプションを選択すると、使用する Microsoft アカウントの資格情報を入力するように求められます。入力後、Windows 10 はこれらの資格情報を記録し、Windows 10 に構成された内容に従って、これらの資格情報を使用します。

同じ [設定] ページで、設定を同期するオプションを使用することもできます。Windows 10 コンピューターで Microsoft アカウントを使用すると、いくつかの設定 (テーマ、Wi-Fi パスワード、Web ブラウザー設定、言語設定など) を同期できるので、Microsoft アカウント記憶域と同期する設定を手動で選択できます。そうすることで、同じ Microsoft アカウントを持つ別のデバイスで、これらの同じ設定を自動的に使用できます。

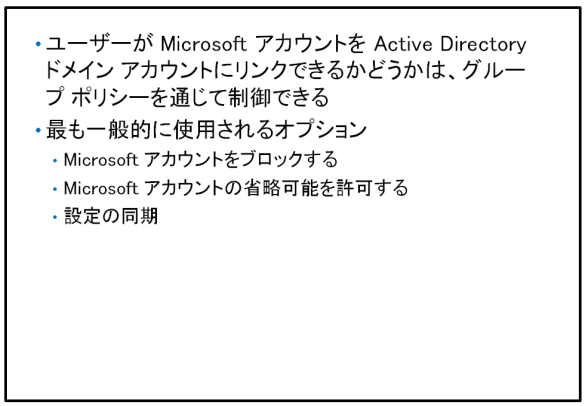
ただし、一部のビジネス環境においては、Microsoft アカウントとドメイン アカウントの統合により、特定のセキュリティ問題が発生することがあります。例えば、企業における次のシナリオについて検討してみます。

- 管理されたチャネルのみを経由するアプリケーションのインストールを制御したい
- ユーザーが Windows ストアを使用できないようにしたい
- Office 365 が展開されている場合、個人用の OneDrive ではなくビジネス向けの OneDrive for Business にデータを保存したい

このようなシナリオで、企業は、Microsoft アカウントとドメイン アカウントの統合をブロックすることを選択できます。

Microsoft アカウントとドメインの統合の管理

Microsoft アカウントを使用して、コンピューターの設定とデータを同期することは、コンシューマーベースのシナリオでは役立ちます。ただし、エンタープライズ環境では、この機能によりセキュリティ リスクが発生する可能性があります。エンタープライズ環境のユーザーがプライベートの Microsoft アカウントを Active Directory ドメイン アカウントに追加できる場合、一部の設定とデータが、企業の管理されたコンピューターと管理されていないプライベート コンピューターの間で同期される可能性があります。
そのため、これらの機能を管理できることが重要です。



ユーザーが Microsoft アカウントを Active Directory ドメイン アカウントにリンクできるかどうかは、グループ ポリシーを通じて制御できます。ユーザーが Microsoft アカウントをドメイン アカウントに追加できないようにするには、次の手順を実行します。

1. 新しいグループ ポリシー オブジェクト (GPO) を作成します (または既存の GPO を編集します)。
2. [コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に展開します。
3. [ローカル ポリシー]、[セキュリティ オプション] の順に展開します。
4. オプションのリストで、[Microsoft アカウントをブロックする] をクリックします。
5. [ユーザーは Microsoft アカウントを追加または Microsoft アカウントでログオンできない] をクリックします。

この設定の GPO をドメインまたは組織単位 (OU) に適用すると、ユーザーは Microsoft アカウントを追加できなくなり、構成を同期するオプションが使用できなくなります。

会社のデバイスで Microsoft アカウントを使用できないようにすることに加えて、Microsoft アカウントを使用せずに一部のアプリケーションを使用したいことがあります。例えば、Windows メール アプリケーションでは、既定で Microsoft アカウントと Windows ストア アプリが必要になります。代わりに職場アカウントを使用する場合、これらのアプリでは Microsoft アカウントを省略可能にする必要があります。このオプションを構成するには、次の手順を実行します。

1. グループ ポリシー エディターを開きます。
2. [コンピューターの構成]、[管理用テンプレート]、[Windows コンポーネント]、[アプリ実行時] の順に展開します。
3. [Microsoft アカウントの省略可能を許可する] を [有効] に構成します。

Windows 8 以降のシステムの同期設定を制御するには、次の手順を実行します。

1. グループ ポリシー エディターで、[コンピューターの構成]、[管理用テンプレート]、[Windows コンポーネント]、[PC 設定の同期] の順に展開します。
2. このセクションには、構成可能なオプションのグループがあります。例えば、ブラウザーの設定は同期するが、パスワードは同期しないことを選択できます。データと設定を同期するためにコンピューターで使用できる各オプションは、グループ ポリシーでも使用できます。

記述が正しい場合は、右側の列にチェック マークを入れます。

記述	解答
Microsoft アカウントを使用して Windows 10 コンピューターにサインインすると、ドメイン アカウントを使用した場合と同様に、企業ネットワークのドメイン リソースにアクセスできます。	
Windows Hello は、生体認証をネイティブにサポートします。	

演習 A : Microsoft アカウントとドメイン アカウントの統合

シナリオ

あなたは、ドメインベースのアカウントを使用して Microsoft アカウントを統合する効果を決定する必要があります。新しい Microsoft アカウントにサインインし、Windows 10 デスクトップ上のドメイン サインイン資格情報に接続します。

目的

この演習により、次のことを習得できます。

- Microsoft アカウントへサインインすることができます。
- Microsoft アカウントをドメイン アカウントに接続することができます。

演習のセットアップ

予定所要時間 : 30 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 MSL-TMG1
ユーザー名	Adatum¥Administrator Adatum¥Aidan
パスワード	Pa$$w0rd

この演習では、用意された仮想マシン環境を使用します。演習を開始する前に、次の手順を実行する必要があります。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. Hyper-V マネージャーで [23697-2B-LON-DC1] をクリックし、操作ウィンドウで [起動] をクリックします。
3. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
4. 次の資格情報を使用してサインインします。
    - ユーザー名 : Adatum¥Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。
6. ユーザー名「Adatum¥Aidan」、パスワード「Pa$$w0rd」を使用してサインインします。
7. インターネットへのアクセスのために、MSL-TMG1 を起動します。

練習 1 : Microsoft アカウントへのサインアップ

シナリオ

評価の一環として、新しい Microsoft アカウントにサインインする必要があります。

主な作業は次のとおりです。

1. Microsoft アカウントへサインアップする

▶ 作業 : Microsoft アカウントへサインアップする

1. LON-CL1 で、ユーザー名「Adatum¥Aidan」を使用してサインインします。
2. Microsoft Edge を起動し、www.live.com を参照します。
3. [作成] リンクをクリックし、ウィザードを使用して新しい Microsoft アカウントを作成します。

注 : 選択したユーザー名を必ず書き留めてください。例えば、次の形式のユーザー名を選択することができます。
<名前の頭文字>-<日付>@outlook.jp (例 : DJ-060815@outlook.jp)
パスワードとして、「Pa$$w0rd!」を使用します。[連絡用メール アドレス] ボックスにあなたが使用しているメール アドレスを入力することを推奨します。

結果 : この練習により、新しい Microsoft アカウントを作成することができました。

練習 2 : Microsoft アカウントのドメイン アカウントへの接続

シナリオ

あなたは、新しい Microsoft アカウントを作成した後で、既存のドメインの資格情報に接続したいと考えています。Windows 10 の組み込みツールやグループ ポリシーを使用して同期設定を管理します。

主な作業は次のとおりです。

1. Microsoft アカウントを Windows 10 に接続する
2. 同期の設定を管理し、Microsoft アカウントでサインインする
3. グループ ポリシー設定との統合を管理する

▶ 作業 1 : Microsoft アカウントを Windows 10 に接続する

1. LON-CL1 で [設定] を開きます。
2. [アカウント設定] ページに移動し、同期の設定を確認します。同期の設定は、関連付けられた Microsoft アカウントを持っていないため、無効です。
3. Microsoft アカウントを追加のアカウントとして追加することを選択します。
4. 前の作業で作成したアカウントを使用します。
5. Windows ストアを開くことで Microsoft アカウントをテストします。

▶ 作業 2 : 同期の設定を管理し、Microsoft アカウントでサインインする

1. LON-CL1 で、[設定] を開き、[アカウント] をクリックします。
2. [同期の設定] が無効化され、変更できないことを確認します。
3. LON-CL1 からサインアウトします。
4. LON-CL1 で、ユーザー名「Adatum¥Administrator」を使用して再度サインインします。
5. コンピューターの管理コンソールを使用して、LON-CL1 上のローカル管理者グループに Adatum¥Aidan を追加します。
6. LON-CL1 からサインアウトし、ユーザー名「Adatum¥Aidan」を使用して再度サインインします。
7. アカウント ウィンドウを使用して、Microsoft アカウントを別のユーザー セクションに追加します。
8. LON-CL1 からサインアウトします。
9. Microsoft アカウントを使用して再度サインインし、正常にサインインできることを確認します。
10. PIN として「111222」と設定します。
11. LON-CL1 からサインアウトします。

▶ 作業 3 : グループ ポリシー設定との統合を管理する

1. LON-DC1 のサーバー マネージャーで、[グループ ポリシーの管理] を開き「Sync Settings」という新しい GPO を作成します。
2. 新しい GPO を編集します。
3. [コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[ローカル ポリシー]、[セキュリティ オプション] の順に展開します。
4. Microsoft アカウントで追加またはサインインできないよう [アカウント : Microsoft アカウントをブロックする] を構成します。
5. [コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[PC 設定の同期] の順に展開します。
6. グループ ポリシー管理エディターで使用可能なオプションを確認して有効化し、Web ブラウザーの設定の同期を防ぎます。
7. LON-CL1 を再起動し、Microsoft アカウントでサインインを試みます。
8. Microsoft アカウントでサインインできないことを確認します。
9. Adatum¥Aidan としてサインインし、[Web ブラウザーの設定] が無効化されていることを確認します。

結果 : この練習により、ドメイン アカウントと Microsoft アカウントを統合することができました。

▶ 次の演習の準備をする

次の演習のために、仮想マシンを起動したままにします。

レッスン 2
クラウド ID 統合の計画

オンラインとクラウドで使用可能なサービスが増えるのに従い、組織ではクラウド ID を定義および管理することが必要になっています。オンプレミスの ID と同様に、ユーザーはリソースにアクセスする際、クラウド ID を使用して認証と承認の手続きをおこなえます。このレッスンでは、クラウド ID を計画し実装する方法について説明します。

目的

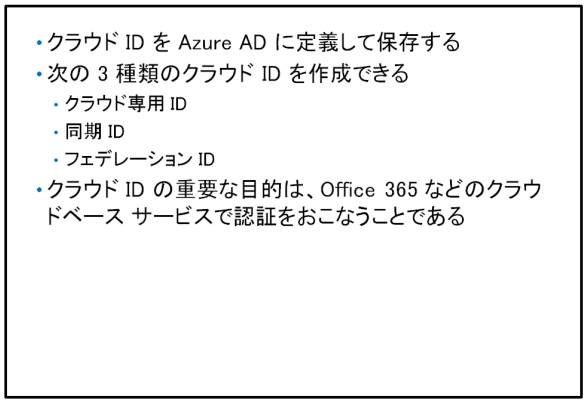
このレッスンにより、次のことを習得できます。

- クラウド ID の概念について説明することができます。
- ローカル ID とクラウド ID の維持に関する課題について説明することができます。
- AD FS でクラウド ID が認証されるしくみについて説明することができます。
- Azure AD の使用について説明することができます。
- Windows 10 で Azure AD に参加するシナリオについて説明することができます。

クラウド ID の概要

既に説明したように、AD DS などのディレクトリ サービスに基づいたコンピューター システムでは、ID は通常ユーザーを表しますが、コンピューターやサービスを表す場合もあります。ID は、ユーザーがリソースにアクセスするための認証と承認に使用されます。

Microsoft では、Azure AD を構築することにより、クラウドベース ID (クラウド ID) が定義されます。ユーザー アカウント (ID) を Active Directory データベースにローカルに格納する代わりに、Azure AD データベースに ID を格納できるようになりました。



クラウド ID には次の 3 つのバージョンがあります。

- **クラウド専用 ID :** これらの ID は、手動で、または Azure AD でスクリプトを使用して作成されます。Azure AD で ID のすべての属性を定義します。これらの ID は、Windows 10 コンピューターにサインインする以外は、ローカルでは使用できません。一方、これらの ID では、クラウドベースのリソースとアプリケーションに完全にアクセスできます。
- **同期 ID :** これらの ID は、ローカルに展開された AD DS と Azure AD との間で同期をおこなうことで、Azure AD に作成されます。AD DS の ID は Azure AD にコピーされ、定期的に同期されるので、AD DS でローカルに実行されたすべての変更は、Azure AD の対応する ID に反映されます。これらの種類の ID では、パスワード ハッシュを Azure AD と同期するか、またはパスワードを AD DS でのみ保持するかを選択できます。同期 ID を使用することで、ローカルのリソース (認証と承認に AD DS を使用) と Azure AD ベースのリソースの両方にアクセスできます。
- **フェデレーション ID :** これらの種類の ID を使用するには AD FS を展開する必要があります。ローカルの AD DS ドメインと Azure AD 間でフェデレーションを確立する際、クラウド リソースにアクセスするために作成した認証要求はすべてローカルに展開された AD FS にリダイレクトされ、さらに検証のために AD DS にリダイレクトされます。ローカルに認証した後、Azure AD を使用中のクラウド リソースを認証することができます。

クラウド ID の重要な目的は、クラウドベース サービスで認証をおこなうことです。Office 365 や Microsoft Intune などの Software as a Service (SaaS) では、ディレクトリ サービスが必要になります。Exchange Server がローカルに AD DS を使用するのと同様に、Office 365 と Microsoft Intune は Azure AD を使用します。認証で使用するユーザー アカウントが、Office 365 が使用する Azure AD インスタンスに存在しない場合、Office 365 サービスは使用できません。これは、Microsoft Intune や Azure RMS のサービスでも同様です。

また、Microsoft アカウントは、Outlook.com のメール、OneDrive、その他のコンシューマーベースのサービスなど、クラウドベース リソースに対する認証とアクセスに使用されるので、クラウド ID として扱うこともできます。ただし、Microsoft アカウントの ID をローカルのディレクトリ サービスと同期することはできません。

ローカル ID とクラウドベース ID の維持に関する課題

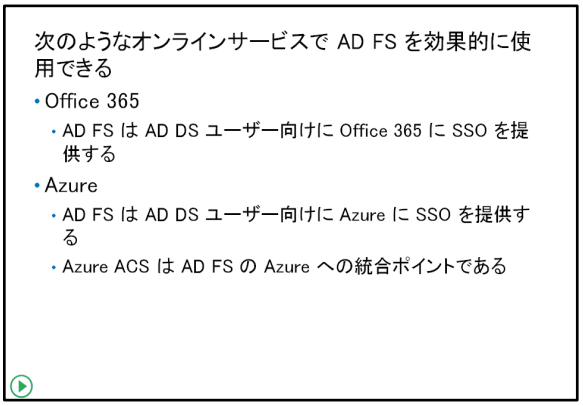
- クラウド専用 ID の課題
  - すべてのユーザー アカウントを手動で作成する必要がある
  - ユーザーはクラウドベース リソースに対して異なる UPN を保有する
  - ユーザーは 2 セットの資格情報を覚えている必要がある
  - シングル サインオン (SSO) を使用できない
  - ID の複雑な管理が必要になる
- 同期 ID とフェデレーション ID の課題
  - 同期サービスを維持する必要がある
  - AD FS を実装する必要がある
  - AD FS (または AD DS) にアクセスできず、Azure AD がパスワード ハッシュを同期していない場合、ユーザーはクラウドベース リソースにアクセスできない

クラウドベース サービスを組織に導入することを決定した場合、クラウドベース ID について検討する必要があります。ローカル ユーザーはクラウドベース リソースにアクセスできる必要があり、アクセスする前に何らかの方法で認証される必要があります。このシナリオでは、組織で使用することを選択したクラウド ID に応じて、いくつかの共通的な課題が発生します。

クラウドベース リソースに対してクラウド専用 ID の使用を決定した場合、Azure AD などのクラウドベース ディレクトリ サービスで、クラウド リソースにアクセスする必要があるすべてのユーザー アカウントを手動で作成する必要があります。これらのユーザー アカウントは、AD DS で使用されるローカル アカウントとは異なる UPN を保有しています。このことにより、ユーザーは、AD DS での認証用とクラウドベース リソースに対する認証用の、2 セットの資格情報を覚えている必要があります。さらにこのシナリオでは、シングル サインオン (SSO) を使用できません。それは、ユーザーが Active Directory アカウントを使用してコンピューターにサインインした後で、クラウドベース リソースにアクセスするたびに認証情報の入力を求められるためです。クラウド専用 ID を使用する場合、ユーザーはローカルの AD DS の可用性とは無関係に、クラウドベース リソースにアクセスできます。ローカル インフラストラクチャがオフラインの場合でも、ユーザーはインターネットを通じてクラウドベース リソースにアクセスし、認証と承認の手続きをおこなうことができます。ただし、このアプローチでは、ユーザーと管理者の両方で ID の複雑な管理が必要になります。

同期 ID モデルの使用を決定した場合、AD DS のローカル アカウントが同期され、ユーザーは同じ資格情報セットを使用して、ローカル リソースとクラウドベース リソースの両方にアクセスできます。このソリューションのメリットは、ユーザーが複数の資格情報を覚える必要がなく、ローカルのユーザー アカウントに対するすべての変更が Azure AD に同期されることです。ただし、このアプローチでは、AD DS と Azure AD が常に同期されるように、同期サービスを維持する必要があります。さらに、パスワード ハッシュを Azure AD と同期しないこと、またはフェデレーション ID を使用することを選択した場合、クラウドベース リソースにアクセスする際にユーザーが認証を受けられるように、AD FS を実装する必要があります。このシナリオでは、AD FS (または AD DS) にアクセスできない場合、クラウドベース リソースがオンラインで使用可能でも、クラウドベース リソースにアクセスできません。

AD FS によるクラウド ID の認証



ユーザーがローカル リソースとクラウドベース リソースの両方にアクセスする際、ローカルのディレクトリ サービス リソースを使用してユーザーを認証することを決定した場合、セキュリティ トークン サービス (STS) を展開する必要があります。Microsoft は、独自の STS 実装である AD FS を提供しています。ユーザーがネットワーク外のリソースにアクセスする際、AD FS を使用してローカル ユーザーを認証できます。リソースは、パートナー組織に配置するか (2 つの Active Directory フォレスト間でフェデレーションの信頼を確立する場合)、または Office 365 や Azure のクラウド サービスに配置できます。ユーザー アカウントを保持する組織は、通常、アカウント フェデレーション パートナーと呼ばれ、アクセスされるリソースを保持する組織は、通常、リソース フェデレーション パートナーと呼ばれます。

アカウントおよびリソースのパートナー組織の各フェデレーション サーバーは、互いに直接通信することはありません。代わりに、次のような Web ベースの通信のみをおこないます。

- アカウント パートナーとリソース パートナーの組織にあるクライアント コンピューターとフェデレーション サーバーの間での通信
- クライアント コンピューターと Web アプリケーションの間での通信

さらに、プロキシが展開されている場合、クライアント コンピューターと Web アプリケーション プロキシ サーバーの間で通信がおこなわれることがあります。

フェデレーション サーバーでクラウド同期 ID を使用すると、AD FS は内部ユーザーに SSO 機能を提供します。この機能によりユーザーは、認証はローカルに実行されつつ、Office 365 などのオンライン サービスにアクセスできます。

Office 365 で使用するために AD FS を展開して構成するには、リソース パートナーが Office 365 であり、他の組織ではなく Office 365 との間に、証明書利用者信頼を構成する必要があります。Office 365 とフェデレーションを確立する際は、フェデレーション サービス プロキシ サーバーまたは Web アプリケーション プロキシ サーバーを展開することをお勧めします。さらに、フェデレーション サーバー ファームとプロキシ ファームの両方を展開して、各ファームに 2 つ以上のメンバーを配置し、Office 365 に対する認証の可用性を高めることもお勧めします。

Office 365 で使用するために AD FS を構成する前に、フェデレーション サーバー ファームの各フェデレーション サーバーに、Microsoft Online Services サインイン アシスタントと Microsoft Online Services Module for PowerShell をインストールする必要があります。Microsoft Online Services Module をインストールした後、Office 365 との間に証明書利用者信頼を作成できます。

プライマリ ドメインを SSO ドメインに変換すると、すべてのユーザーがフェデレーション状態になります。現在は、Office 365 に対して SSO の段階的なロールアウトを実行することはできません。

フェデレーションが構成されると、次のステップの流れで通信が実行されます。

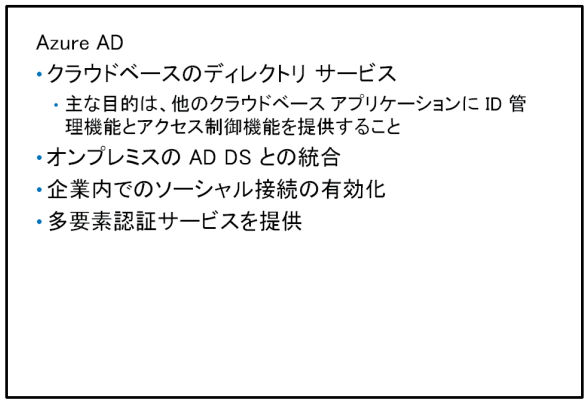
1. ネットワークの外部に配置されたクライアント コンピューターが、Office 365 (または他のクラウド ベース リソース) にアクセスしようとします。クライアント コンピューターは、HTTPS 要求を Office 365 サーバーの Web サービスに送信します。

2. Web サーバーは要求を受信し、クライアント コンピューターがクレームを保有していないことを確認します。ユーザーが提供する UPN に基づいて、Office 365 サービスはフェデレーション ドメインを認識し、Web サーバーはクライアント コンピューターを、ローカル ネットワークに展開されたフェデレーション サービス プロキシにリダイレクトします。クライアントは、HTTPS 要求をフェデレーション サービス プロキシに送信します。シナリオに応じて、フェデレーション サービス プロキシは、ユーザーに認証を求めるか、またはユーザーの資格情報を収集するために統合 Windows 認証を使用します。
3. フェデレーション サービス プロキシは、要求と資格情報をフェデレーション サーバーに渡します。
4. フェデレーション サーバーは、AD DS を使用してユーザーを認証します。
5. 認証が成功すると、フェデレーション サーバーはユーザーに関する Active Directory 情報を収集します。次に、その情報を使用してユーザーのクレームを生成し、そのクレームをクライアントに返送します。
6. クライアントは、トークンを Office 365 の Web サーバーに提示します。Web リソースは要求を受信して、署名されたトークンを検証し、ユーザーのトークン内のクレームを使用してアプリケーションへのアクセスを可能にします。

Azure AD では、Access Control Service (ACS) を使用し、AD FS を ID プロバイダーとして構成できます。これにより、Azure でホストされた ASP.NET アプリケーションは、Active Directory の資格情報を使用してユーザーを認証できるようになります。

Azure Active Directory の概要

Azure AD は、Representational State Transfer (REST) の原則に基づいて構築されたクラウド ベース サービスです。REST は、分散されたハイパーメディア システム向けのアーキテクチャであり、クラウド内でドメイン コントローラーの独立したインスタンスを実行する必要がありません。また、独立した Active Directory 環境を構築する必要もありません。Azure AD はクラウド ベース サービスであり、主な目的は、他のクラウドベース アプリケーションに ID 管理機能とアクセス制御機能を提供することです。これにより、Office 365、Azure、Microsoft Dynamics CRM Online、Microsoft Intune などのすべての Microsoft クラウドベース サービスに、1 つの ID サービスで対応できるようになりました。



クラウドベース アプリケーションにサービスを提供することに加えて、Azure AD はオンプレミスに展開された Active Directory と統合することもできます。Azure AD は、サブスクリプションベースのサービスとして Microsoft から直接購入します。

Azure AD の使用方法としては、次のものがあります。

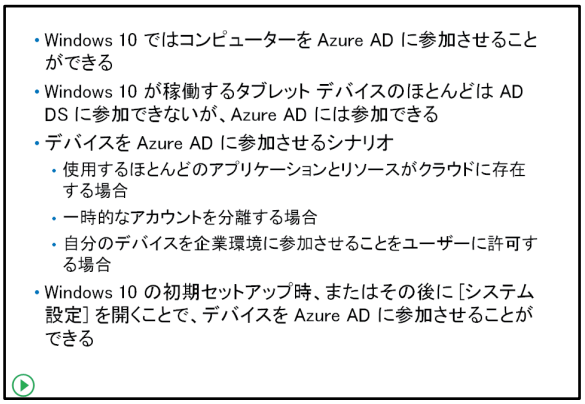
- **アプリケーションのアクセス制御 :** Azure AD は他の ID プロバイダーまたはオンプレミスの AD DS を使用することにより、開発者がアプリケーションの認証と承認を Azure で一元的に受けられるようにします。
- **オンプレミスの AD DS との統合 :** オンプレミスの AD DS と統合することにより、ユーザーはローカルにインストールされた AD DS の資格情報を使用して、Azure および他のクラウド サービスの認証を受けることができます。

- **クラウドベース アプリケーションの SSO :** Azure AD は、ユーザーが Facebook、Google サービス、Yahoo、Microsoft クラウド サービスなどのアプリケーションを使用する際、SSO エクスペリエンスを提供できます。
- **企業内でのソーシャル接続の有効化 :** Azure AD を使用することで、ユーザーは、情報とリレーションシップを容易に検出するために、ユーザー、グループ、役割などのオブジェクトにアクセスするシンプルなインターフェイスを使用できます。

Azure AD は多要素認証を使用して、クラウド アプリケーションへのアクセスをセキュリティで保護することもできます。この認証は、電話呼び出し、テキスト メッセージ、または Windows Phone の Microsoft 認証アプリなどのモバイル アプリケーションを使用して、ユーザーにサインインの確認を求めることにより機能します。これについては、以降の章で詳細に説明します。

AD DS と Azure AD では、目的はだいたい同じですが、サポートするアプリケーションはかなり異なることに留意してください。AD DS は、オンプレミスに展開された複雑な多層アプリケーションをサポートしますが、一方 Azure AD は、ほとんどの場合、Web ベース サービスをサポートします。さらに、AD DS の方が、ユーザーとグループの管理、および管理の委任に関して、非常に強力かつ柔軟です。

Windows 10 の Azure Active Directory への参加



Windows 10 では、コンピューターを AD DS ドメインだけでなく、Azure AD にも参加させることができます。Azure AD でユーザー アカウントを作成できることに加えて、Azure AD でコンピューター アカウントを保有し、Azure AD に参加したデバイスをクラウドから管理することもできます。

Active Directory ドメインと Azure AD のどちらにデバイスを参加させるかを決定する前に、これら 2 つの概念の違いを理解することが重要です。Active Directory ドメインに参加したデバイスでは、サポート対象のオペレーティング システムのバージョンを実行する必要があります (例えば、Windows と Windows RT オペレーティング システムの Home バージョンは、ドメインへの参加をサポートしていません)。さらに、デバイスはほとんどの場合、グループ ポリシーまたは Microsoft System Center アプリケーションを使用して管理されます。Active Directory ドメインに参加できるデバイスは、通常、オンプレミスのアプリケーションとサービスにアクセスします。また、既に説明したように、ドメイン アカウントと Microsoft アカウントを統合した場合は、クラウド リソースにアクセスすることもできます。

Azure AD の方が、参加できるデバイスの範囲が少し広くなっています。Windows 10 が稼働するタブレット デバイスのほとんどは、Active Directory ドメインに参加できませんが、Azure AD には参加できます。ノート PC やデスクトップ コンピューターなどのデバイスも、Azure AD に参加できます。デバイスが Azure AD に参加すると、SSO を使用することで、クラウドベース リソースと Azure ベース リソースに完全にアクセスできるようになります。管理の観点では、これらのデバイスはグループ ポリシーを使用して管理することはできませんが、Microsoft Intune を使用してこれらのデバイスを管理および準備することはできます。

デバイスを Azure AD に参加させる際の一般的なシナリオとしては、次のものがあります。

- **使用するほとんどのアプリケーションとリソースがクラウドに存在する場合 :** Office 365 などのクラウド サービスを既に使用しており、他のワークロードをクラウドに移行する計画がある場合は、クライアント デバイスを Azure AD に参加させ、クラウドベース サービスの簡単操作と SSO を利用できるようにすることをお勧めします。

- **一時的なアカウントを分離する場合 :** 一時的なアカウント (契約社員用や期間従業員用など) を通常のアカウントとは別に管理する必要があるが、一時的なアカウントにも限定的なクラウドベースサービスを提供する場合、これらのアカウントを Azure AD に作成できます。
- **自分のデバイスを企業環境に参加させることをユーザーに許可する場合 :** Bring Your Own Device (BYOD) という概念をサポートし、自分のデバイスをビジネス環境に参加させることをユーザーに許可する場合、Azure AD が適切なソリューションになることがあります。このことは特に、ユーザーが Microsoft 以外のデバイス (iPad や Android タブレットなど) を使用し、これらのデバイスが Azure AD ドメインに参加できないが、Microsoft Intune と Azure AD には登録できるという状況で有効になります。

ユーザーは、Windows 10 の初期セットアップ時、またはその後に [システム設定] を開くことで、Windows 10 コンピューターを Azure AD に参加させることができます。どちらの場合でも、必要な操作は Azure AD の資格情報を入力し、管理ポリシーを許可するだけです。

また、デバイスが参加できるように、Azure AD を準備する必要があることにも留意してください。そのためには、Azure クラシック管理ポータルを開き、Azure AD インスタンスに移動して、[構成] タブを開きます。[デバイス] セクションで、デバイスが参加するためのオプションを構成できます。

知識の確認

質問	
次のサービスで、Azure AD を使用するものはどれですか。	
正しい解答を選択してください。	
	Office 365
	Intune
	AD FS
	Azure RMS
	AD DS

記述が正しい場合は、右側の列にチェック マークを入れます。

記述	解答
AD FS はクラウドベースの認証メカニズムです。	

演習 B : Windows 10 の Azure Active Directory への参加

シナリオ

あなたは、Windows 10 を Azure AD などのクラウドベース サービスに参加させる方法を評価する必要があります。評価版アカウントにサインインしてから、Windows 10 を Azure AD インスタンスに参加させる必要があります。

目的

この演習により、次のことを習得できます。

- Office 365 と Azure AD の両方の評価版サブスクリプションにサインインすることができます。
- Windows 10 を Azure AD に参加させることができます。

演習のセットアップ

予定所要時間 : 40 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 23697-2B-LON-CL4 MSL-TMG1
ユーザー名	Adatum¥Administrator Adatum¥Aidan
パスワード	Pa$$w0rd

この演習では、用意された仮想マシン環境を使用します。演習を開始する前に、次の手順を実行する必要があります。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. Hyper-V マネージャーで [23697-2B-LON-DC1] をクリックし、操作ウィンドウで [起動] をクリックします。
3. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
4. 次の資格情報を使用してサインインします。
    - ユーザー名 : Adatum¥Administrator
    - パスワード : Pa$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 4 を繰り返します。ユーザー名「Adatum¥Aidan」、パスワード「Pa$$w0rd」を使用してサインインします。
6. 23697-2B-LON-CL4 に対して、手順 2 ～ 4 を繰り返します。指示されるまで、サインインしないでください。
7. インターネットへのアクセスのために、MSL-TMG1 を起動します。

練習 1 : Office 365 と Azure の評価版サブスクリプションへのサインアップ

シナリオ

あなたは、Azure AD のインスタンスを確立し、クラウドベースのディレクトリの使用を評価したいと考えています。また、他の機能性についても評価できるようにするために、Office 365 E3 評価版サブスクリプション テナントを構成することに決めました。

主な作業は次のとおりです。

1. Office 365 評価版サブスクリプションにサインアップする
2. Microsoft Azure 評価版サービスにサインインして Azure Active Directory を構成する

▶ 作業 1 : Office 365 評価版サブスクリプションにサインアップする

注 : Intune (第 8 章で使用) など、Microsoft Online Services の一部には、世界中のすべての地域で使用できない場合があります。Microsoft では、Intune やその他のオンライン サービスを世界中で使用可能にすることを目標としています。しかし、現時点では、すべてのサービスがすべての国や地域で使用可能ではありません。http://aka.ms/p5vyl7 で、Office 製品が利用できる国と地域の一覧を確認してください。あなたの国や地域が Office 365、Azure、および Intune の一覧に含まれない場合、この演習およびオンライン アカウントの作成を含む以降の演習では、国や地域として United States を選択してください。

1. LON-CL1 で「Adatum¥Aidan」としてサインインします。
2. Microsoft Edge を使用して、Office 365 Enterprise E3 Business ソフトウェアへのリンク (http://aka.ms/jsn2ec) を参照します。
3. [無料試用版] を選択します。
4. 国/地域を選択し、あなたの情報を入力します。あなたの国/地域が表示されない場合、[United States] を選択します。電子メールアドレスには、前の演習で作成した Microsoft アカウントを使用し、会社名として A. Datum Corporation を使用します。組織の規模には [51-150] を選択します。
5. [ユーザー ID の作成] ページで、ユーザー名 (例えば、姓と名の最初の 1 文字) を入力し、会社のドメイン名を選択します。次の形式の会社のドメイン名を入力します。
   Adatum<日付><頭文字>.onmicrosoft.com. (例えば、Adatum2008DJ.onmicrosoft.com)

注 : 後でこのユーザー ID を使用してサインインするため、必ず書き留めます。

6. 「Pa$$w0rd!」をパスワードとして構成します。
7. 確認のために、使用している携帯電話番号を入力します。

注 : 使用している携帯電話番号を入力する必要があります。携帯電話を持っていない場合、講師に相談してください。

8. サインインを完了させ、Office 365 のダッシュボードで、使用可能なオプションを確認します。
9. 開いているウィンドウをすべて閉じます。

▶ 作業 2 : Microsoft Azure 評価版サービスにサインインして Azure Active Directory を構成する

1. LON-CL1 で、Microsoft Edge を使用し、Azure Pass へのリンク (http://aka.ms/cu92vo) を参照します。
2. あなたの国を選択し、講師から受け取った Azure のプロモーション コードを入力して Azure の評価版サブスクリプションを起動します。
3. [サインイン] ページで、前の作業で構成したユーザー ID を使用します。
4. Azure フル管理ポータルで、ディレクトリ サービス インスタンスを開き、[構成] タブに移動します。
5. 自分のデバイスを Azure AD に参加させることをすべてのユーザーに許可するよう Azure AD を構成します。
6. Azure AD のユーザー オブジェクトとして、Aidan Delaney を追加します。
7. Aidan の一時パスワードを書き留めます。
8. Aidan@<あなたのドメイン名>.onmicrosoft.com と、portal.office.com の一時パスワードを使用して、サインインします。
9. メッセージが表示されたら、パスワードの「Pa$$w0rd!」へ変更します。

結果 : この練習により、Office 365 と Azure の評価版サブスクリプションを構成することができました。

練習 2 : Windows 10 の Azure Active Directory への参加

シナリオ

Azure AD の評価版テナントを構成した後、Azure AD に Windows 10 コンピューターを追加したいと考えています。

主な作業は次のとおりです。

1. Windows 10 を Azure Active Directory に参加させる

▶ 作業 : Windows 10 を Azure Active Directory に参加させる

1. LON-CL4 で、ローカルの管理者としてサインインします。
2. [設定] ウィンドウのシステム ウィンドウを使用して、LON-CL4 マシンを Azure AD に参加させます。
3. Azure AD にマシンを参加させるには次の資格情報を使用します。
   - ユーザー名 : Aidan@<あなたのドメイン名>.onmicrosoft.com
   - パスワード : Pa$$w0rd!
4. Microsoft Edge で、manage.windowsazure.com を参照し、管理資格情報を入力してサインインします。
5. Azure AD で、ユーザー オブジェクトとして Aidan Delaney を開きます。
6. [デバイス] タブを開きし、[LON-CL4] が一覧に表示されることを確認します。
7. LON-CL4 からサインアウトします。
8. LON-CL4 に再度サインインするには次の資格情報を使用します。
   - ユーザー名 : Aidan@<あなたのドメイン名>.onmicrosoft.com
   - パスワード : Pa$$w0rd!

9. [設定]、[アカウント]、[お使いのアカウント] の順に開き、[アカウントの管理] をクリックします。
10. Azure が開いていることを確認します。

結果 : この練習により、Windows 10 コンピューターを Azure AD に追加することができました。

▶ 次の章の準備をする

演習が完了したら、仮想マシンを初期状態に戻します。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. [仮想マシン] リストで、[23697-2B-LON-DC1] を右クリックし、[戻す] をクリックします。
3. [仮想マシンを戻す] ダイアログ ボックスで、[戻す] をクリックします。
4. 23697-2B-LON-CL1 と 23697-2B-LON-CL4 に対して、手順 2 ～ 3 を繰り返します。

復習とまとめ

ベスト プラクティス

- 可能な場合は、クラウドで同期 ID を使用することにより、SSO エクスペリエンスを活用することができます。
- グループ ポリシーを使用して Microsoft アカウントとの同期設定を管理します。
- クラウド内に複数のリソースがある場合は、Windows 10 の Azure AD 参加機能を使用します。
- Azure AD に参加しているコンピューターに使用可能な管理メカニズムが存在していることを確認します。

一般的な問題とトラブルシューティングのヒント

一般的な問題	トラブルシューティングのヒント
ドメインに参加しているコンピューターに Microsoft アカウントを追加することができない。	
Windows 8 で Azure AD 参加オプションを見つけることができない。	
Office 365 のダッシュボードから Azure AD にアクセスすることができない。	

復習問題

質問 : オンプレミス アカウントを使用してクラウド サービスにアクセスしたいが、ローカルで認証を実行する場合、どのようなサービスを使用する必要がありますか。