第 6 章

Windows ベースのデバイスによるデータ アクセスの管理

目次

概要

ビジネス用途または個人用途に関係なく、使用するすべてのデバイスで、ある種のデータ アクセスが必要になります。このことから、ビジネス環境では、データ アクセスを管理することが重要になります。データ アクセスでは、認証と承認を必要とします。Windows オペレーティング システムが動作しているコンピューターへの認証では、最初に、サインインが必要になります。コンピューターにサインインすることは、必須の手順です。コンピューターのメンバーシップに基づいて、ユーザーはローカル アカウント、ドメイン アカウント、または Microsoft アカウントのいずれかで、サインインできます。Active Directory (AD DS) 環境では、このサービスが提供するメリットを活用するために、通常、ドメイン アカウントを使用します。

現在では、ユーザーが使用するのは、企業所有のコンピューターのみに制限されません。ユーザーは、通常、自分が所有しているデバイスを使用して、企業データにアクセスします。Windows 10、Windows 8、および Windows Server 2012 R2 の各オペレーティング システムには、Bring Your Own Device (BYOD) シナリオなどで役立つデバイス登録やワーク フォルダーなどの新しい機能が追加されています。また、データ記憶域は、オンサイト サーバーなど従来の記憶域の場所からクラウド記憶域ソリューションに移行しつつあります。

この章では、ドメイン アカウントのメリットやドメイン メンバーではないデバイスからのリソース アクセスを制御するのに役立つ Windows 10 の機能について説明します。また、デバイス登録、ワーク フォルダー、およびクラウドベースの記憶域ソリューションを構成し使用する方法についても説明します。

目的

この章により、次のことを習得できます。

- データ アクセス ソリューションを説明することができます。
- デバイス登録を実装することができます。
- ワーク フォルダーを実装することができます。
- クラウドベースの記憶域ソリューションを使用して、オンライン データを管理することができます。

レッスン 1
データ アクセス ソリューションの概要

Windows 10 のデバイスはさまざまなフォーム ファクターで提供されており、必ずしもドメインに参加しているとは限りません。このため、ローカルに格納されているデータをセキュリティで確実に保護し、デバイスの紛失または盗難が起きた際は、企業データをリモートから確実に管理したりワイプしたりできる必要があります。さらに、これらのデバイスがビジネス用途で使用されているシナリオでは、デバイスから企業データにアクセスできるようにする必要があります。ドメインに参加しているデバイスは、Active Directory ドメインを信頼します。そのようなデバイスには、ドメイン資格情報を使用してサインインでき、その後、資格情報を再入力することなく、ドメイン リソースにアクセスできます。

ドメイン コントローラーは、ドメイン メンバーではないデバイスを信頼しません。ドメインに参加していないこれらのデバイスからドメイン リソースにアクセスする場合、シングル サインオン (SSO) のメリットを活用できません。このレッスンでは、ドメインに参加しているデバイスおよび参加していないデバイスの両方に対して提供されているさまざまなデータ アクセス ソリューションについて説明します。

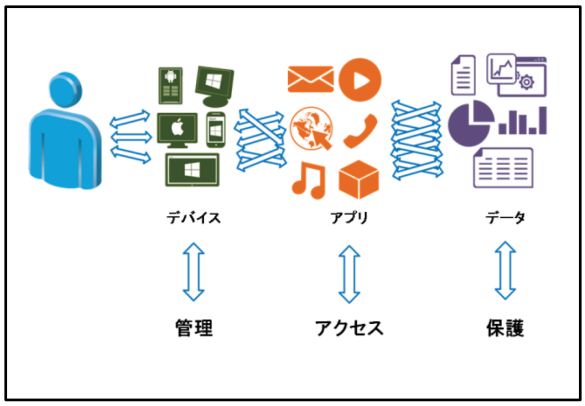
目的

このレッスンにより、次のことを習得できます。

- さまざまな種類のデバイスからデータにアクセスできるようにする場合の課題について説明することができます。
- ドメインに参加していないデバイスからデータにアクセスできるようにする場合の課題について説明することができます。
- データ アクセスに関するソリューションについて説明することができます。

さまざまな種類のデバイスからのデータ アクセスの課題

過去において、企業は企業のアプリやデータに対するアクセスを、ドメイン アカウントを使用し、企業所有かつドメイン メンバーであるデバイスでログオンまたはサインインしているユーザーに対してのみ許可していました。しかし、状況は変化しており、企業はデバイス中心のアプローチから、よりユーザーフレンドリで人中心のアプローチに切り替えつつあります。今日の世界では、ユーザーは、どこにいても、自分が所有するデバイスで企業アプリを実行したり企業データにアクセスしたりして勤務できることを期待しています。このユーザー行動の進化は、企業の情報テクノロジ (IT) 部門に新たな課題をもたらします。



現在、ユーザーは、従来型のデスクトップ コンピューターを使用せず、代わりにデバイスに依存することがますます一般的になってきています。デバイスは、スマートフォンやタブレットなど数年前には存在しなかったさまざまなフォーム ファクターで提供され、通常、ドメイン メンバーではありません。ドメイン メンバーではない理由としては、企業がそれらを所有していない場合や、Windows RT や Microsoft 以外 (Windows 以外) のオペレーティング システムなど、デバイスのオペレーティング システムがドメインに参加できない場合などが挙げられます。しかし、パーソナル デバイスを使い慣れているユーザーは、それらのデバイスを業務で使用することを望んでいます。これは、BYOD シナリオと呼ばれています。

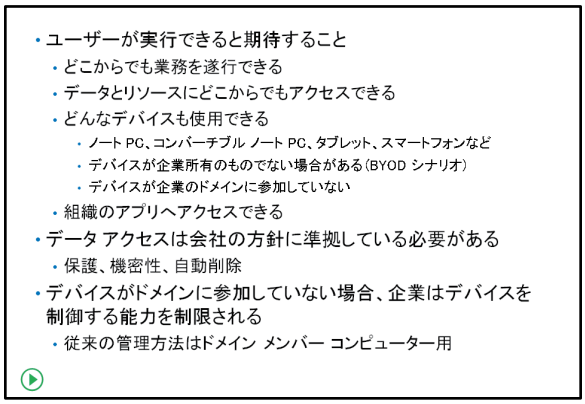
以前は、ドメイン メンバーのコンピューターとドメイン アカウントのみが、アプリやデータにアクセスできました。現在、これは、あてはまらなくなっています。ユーザーは自身の資格を証明するためにドメイン アカウントを引き続き所有しますが、さまざまなハードウェア アーキテクチャ上で動作し、さまざまな種類のディスプレイが搭載されているさまざまなデバイスから、企業の同じアプリやデータにアクセスすることを要求するようになっています。さらに、これらにユーザーは、アクセスが必要になるごとに資格情報を提供することを望んでいません。つまり、ユーザーは、ドメイン環境で働く場合と同じエクスペリエンスを、彼らのパーソナル デバイス上でも持ちたいと思っています。

企業は、通常、データをサーバー上に格納し、ユーザーはどこからでも、あらゆるデバイスから安全にアクセスできることを期待します。これは、ユーザーがパーソナル デバイス上にデータをローカルにコピーし、それらにアクセスすることを意味するため、企業にとって新しい課題となります。管理者は、ユーザーがアクセスできるデータ、ローカルにキャッシュできるデータを、制御できる必要があります。また、ユーザーが退職した場合やデバイスを紛失した場合に企業データをリモートからワイプする方法を理解しておく必要があります。また、管理者は、ユーザーのパーソナル デバイスから企業データをワイプする際は、パーソナル データに影響を及ぼさないようにする必要があります。

IT 部門への新しい課題には、次のものがあります。

- ユーザーが好みのデバイスを使用して働くことを可能にし、また、企業リソースへの一貫したアクセスを提供する。
- 環境を統一し、企業所有かつドメイン所有のデバイスと BYOD デバイスに対して統一されたアプリケーションとデバイスの管理を提供する。
- 企業データの保護、企業ポリシーとコンプライアンス要件の強制、およびアクセス元となる場所やデバイスに関係しないリスクの管理をおこなう。

ドメインに参加していないデバイスからのデータ アクセスの課題



過去においては、ユーザーは企業データにアクセスする場合、企業のローカル エリア ネットワーク (LAN) に接続されているコンピューターを使用する必要がありました。しかし、モバイル テクノロジの進化とビジネス デマンドの変化により、今日のユーザーは、どこからでも、業務を遂行でき、すべての業務リソースにアクセスできることを期待しています。ワイヤレス アクセスがほとんどすべての場所で利用でき、ユーザーは従来型のデスクトップ コンピューターやノート PC の使用を避け、代わりに、コンバーチブル ノート PC、タブレット、スマートフォンなどの新しいデバイスを使用しつつあります。ユーザーは自身が所有するデバイスを使用して企業データにアクセスすることが多くなり、BYOD シナリオが一般的になっています。このため、ユーザーは、自身のデバイス上でも、企業のアプリを使用したり、データにアクセスしたりすることを期待します。企業データのローカル コピーをユーザー デバイスに持つことは、IT 部門にとって対応が必要な課題となります。なぜなら、IT 担当者は、利用可能なデータと、それらのデータへのデバイスからのアクセスが、企業のポリシーとセキュリティ プラクティスに確実に準拠するようにしなければならないためです。

新しい種類のデバイスが急速に採用されるのに従い、企業のインフラストラクチャを管理するための標準ベースのアプローチに変化が起きています。デバイスがドメインに参加している場合、そのデバイスは Active Directory ドメイン サービス (AD DS) にアカウントを持つので、企業はそのデバイスを制御できます。これにより、次の項目が確実に実践されます。

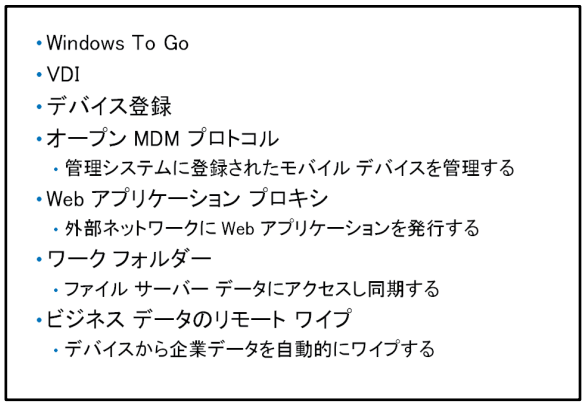
- ドメイン コントローラーが認証を実行します。

- グループ ポリシーを使用して企業ポリシーを強制できます。
- Microsoft System Center Configuration Manager (Configuration Manager) などの製品を使用して、デバイス インベントリを収集したり、デバイスを管理したりすることができます。

デバイスがドメインに参加していない場合、企業はデバイスを制御する能力を制限されるか、またはまったく制御できません。これは、認証がローカルでおこなわれ、ドメインはデバイスの使用者を把握できないためです。デバイスへのサインイン、デバイスの管理、またはアプリの展開にドメイン アカウントは使用できません。また、ドメインに参加していないデバイスにドメイン グループ ポリシーを適用することもできません。

データ アクセスに対するソリューション

IT のコンシューマライゼーションに伴い、ユーザーは、多くの場合、自身が所有しているデバイスを使用して企業リソースにアクセスします。そのような BYOD イニシアティブを奨励する企業も、数多くあります。Windows 8.1、Windows 10 以降、および Windows Server 2012 R2 以降の各オペレーティング システムには、企業所有ではないデバイスの使用をより簡単で安全にするための機能がいくつか含まれています。次に、それらの機能を示します。



- **Windows To Go :** Windows To Go は、Windows 8.1 以降の Enterprise エディションの機能で、Windows オペレーティング システムを USB フラッシュ ドライブにインストールし、その後、デバイスを USB フラッシュ ドライブから起動できるようにします。Windows To Go をカスタマイズしたり、ドメインに参加させたりして、Windows オペレーティング システムがローカルにインストールされている場合と同じ環境を提供できます。ユーザーは、デバイス上のパーソナル データが影響を受けることなく、Windows To Go を使用してデバイスを起動し、企業が承認している環境から業務をおこなうことができます。
- **仮想デスクトップ インフラストラクチャ :** Windows Server 2012 R2 リモート デスクトップ サービスの役割は、複数の仮想デスクトップをホストする仮想デスクトップ インフラストラクチャ (VDI) を実装します。これらの仮想デスクトップは、あらゆるデバイスから接続できる Windows 8.1 以降の仮想マシンを含むことができます。仮想デスクトップでは、ローカルにインストールされている Windows 8.1 以降を使用する場合と同じエクスペリエンスを得ることができます。仮想デスクトップから企業アプリを使用したり企業データにアクセスしたりできますが、ネットワークを介してデバイスから仮想デスクトップに接続できる必要があります。
- **デバイス登録 :** 従来の方法では、デバイスをドメインに参加させるか、ワークグループのメンバーにすることができました。ユーザーは、ドメインに参加しているデバイスから企業リソースにアクセスできましたが、ワークグループのメンバーからアクセスするには、ドメイン資格情報を最初に入力する必要がありました。デバイス登録は、Windows 8.1 で社内参加 (Workplace join) という名前で導入されたもので、これを利用するには、ドメイン内に 1 つ以上の Windows Server 2012 R2 メンバー サーバーが必要になります。デバイスを社内参加させると、ユーザーは、内部 Web サイトやビジネス アプリなどの企業リソースにアクセスすることができる証明書を受け取ります。また、デバイス登録機能を使用する IT 管理者は、ユーザーのデバイス上でアプリやサービスを有効化することができます。

- **オープン モバイル デバイス管理 (MDM) プロトコル :** このプロトコルを使用すると、管理システムに登録されたモバイル デバイスを管理できます。Microsoft は、オープン モバイル デバイス管理 (MDM) プロトコルのサポートを Windows 10 と Windows 8.1 で実装しています。IT 管理者はこのプロトコルを使用することにより、Microsoft 以外のモバイル デバイス管理製品でタブレットやその他の BYOD デバイスを管理できます。オープン MDM プロトコルは、インベントリ収集、設定管理、アプリケーション管理、証明書の提供、Wi-Fi、仮想プライベート ネットワーク (VPN) プロファイル管理、データ保護などの機能をサポートします。
- **Web アプリケーション プロキシ :** Web アプリケーション プロキシ機能を使用すると、企業ネットワークから外部ネットワークに Web アプリケーションを発行できます。この機能により、外部ネットワークに接続しているユーザーは、任意のデバイスから企業の Web アプリケーションにアクセスしたり、それらを使用したりできます。また、Web アプリケーション プロキシを使用すると、企業ネットワークに接続されていないデバイスに対してデバイス登録を有効にすることができます。
- **ワーク フォルダー :** ワーク フォルダー機能を使用すると、企業の Windows Server 2012 R2 ファイル サーバーからユーザー所有のデバイスにデータを同期できます。ワーク フォルダー機能はオフライン ファイル機能に似ており、ネットワーク接続が利用できなくてもワーク フォルダーの内容にアクセスしたり、それらを変更したりできます。また、変更内容はネットワーク接続が回復したときにファイル サーバーに反映されます。次の条件がすべて満たされている場合、ワーク フォルダーは外部ネットワークからアクセスできます。
  - Web アプリケーション プロキシが実装されている。
  - ドメイン メンバーシップが必要ない。
  - デバイスで、デバイス登録が有効になっている。
- **ビジネス データのリモート ワイプ :** BYOD シナリオでは、ユーザーはパーソナル データも含むデバイスから企業データにアクセスします。ビジネス データのリモート ワイプ機能の 1 つでは、企業データとパーソナル データを区別して扱います。管理者は、企業データがデバイス上では暗号化されるように構成できます。これにより、ユーザーが退職したり、デバイスを紛失したりすると、デバイス上の企業データは自動的にアクセス不能になるか、完全に削除されます。しかし、ユーザーのパーソナル データが影響を受けることはありません。

  質問 : 企業でクライアント/サーバー アーキテクチャに基づく会計アプリが使用されています。このアプリは、ユーザーのデバイスで実行している他社のオペレーティング システム上にインストールできません。企業の会計アプリをデバイスでも使用できるようにするにはどのようにしますか。

レッスン 2
デバイス登録の実装

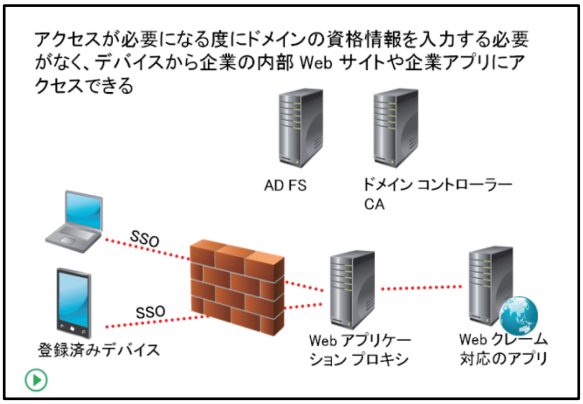
デバイスをドメインに参加させると、企業リソースにアクセスするごとに資格情報を入力する必要なしに、ユーザーは企業リソースにアクセスできますが、デバイス登録を有効にすると、デバイスをドメイン メンバーにする必要なしに、ユーザーは同様のエクスペリエンスを得ることができます。デバイス登録を有効にすると、企業の内部 Web サイトや企業アプリにアクセスする際、SSO エクスペリエンスが可能になります。企業が適切なインフラストラクチャを備えている場合、ドメイン アカウントを持つユーザーは、デバイス登録を自身が所有しているデバイスに実装できます。

目的

このレッスンにより、次のことを習得できます。

- デバイス登録とその使用方法を説明することができます。
- デバイス登録のしくみを説明することができます。
- デバイス登録を使用するためのインフラストラクチャ要件を説明することができます。
- デバイス登録する方法を説明することができます。

デバイス登録の概要



従来の方法では、ユーザーがデバイスから透過的にデータにアクセスする必要がある場合、デバイスをドメインに参加させる必要があります。デバイスがドメインに参加していない場合でもユーザーはそのデバイスから企業データにアクセスできますが、この場合、アクセスが必要になる度にドメインの資格情報を入力する必要があります。Windows 8.1 では、デバイス登録機能が導入されています。この機能を使用すると、ユーザーは、アクセスが必要になる度にドメインの資格情報を入力する必要がなく、デバイスから企業の内部 Web サイトや企業アプリにアクセスできます。また、管理者は、デバイス登録が有効にされているデバイスからどの Web アプリにアクセスできるかを制御するなど、デバイスに関してある程度の管理をおこなうことができます。

Windows 8.1 では社内参加と呼ばれていたデバイス登録は、ユーザーが自身で所有しているデバイスを使用して企業データにアクセスする際に特に役立ちます。デバイス登録を有効にすると、ユーザーは自身で所有しているデバイスを企業ネットワークに登録できます。登録されたデバイスは、企業ディレクトリのユーザー アカウントに関連付けられ、デバイス オブジェクトが AD DS に作成されて、ユーザー証明書がデバイスにインストールされます。AD DS のデバイス オブジェクトは、ユーザーとデバイスとの間の関連付けを確立します。デバイス登録が有効なデバイスからクレームベース認証をサポートする企業リソースとの以降の通信には、デバイスとユーザーに関する情報が含まれます。クレームベース認証をサポートするように適切にアプリを構成すると、ユーザーは資格情報の再入力を求められません。

デバイスでデバイス登録を有効にすると、デバイスは 2 番目の認証として使用されます。同じデバイスを複数のユーザーが使用する場合、各ユーザーは個別に、デバイス登録を有効にすることができます。管理者は、ユーザーが資格情報を再入力することなくデバイスからどのアプリにアクセスできるかを制御することができます。また、デバイス ポリシーを構成して、企業のポリシーとセキュリティがそれらのデバイスに確実に適用されるようにすることができます。企業のグループ ポリシーは、ドメインに参加しているデバイスに対してのみ適用され、デバイス登録が有効にされているデバイスに対しては適用されないことに注意する必要があります。デバイス登録が有効にされているデバイスが危険にさらされている場合、またはデバイスの所有者が退職した場合、管理者はデバイス オブジェクトをドメインから削除できます。これにより、管理者は、SSO を通してドメイン リソースにアクセスするデバイスの能力を失効することができます。

デバイス登録を使用するためのシナリオ

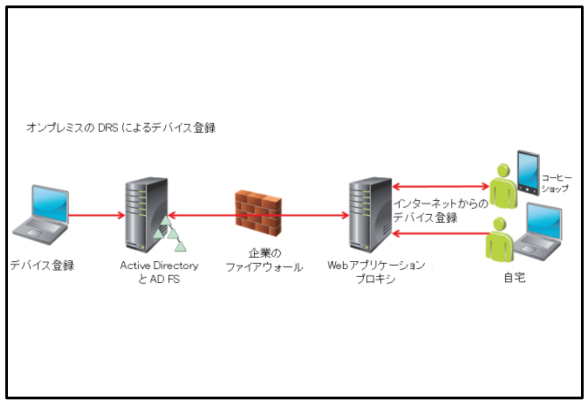
従業員が企業データにアクセスするために使用するデバイスは、企業所有であり、それらのデバイスは、通常、ドメインに参加します。また、ユーザーは、自身が所有しているデバイスを使用して、企業ネットワーク内またはインターネット経由で企業データにアクセスすることもあります。企業の IT 部門はドメインに参加しているデバイスを注意深く監視および管理できますが、ドメイン メンバーではないデバイスについては、そのようなことができない可能性があります。ユーザーは、通常、仮想デスクトップへのアクセス、企業アプリの実行、およびその他の企業リソースへのアクセスをおこなうために、デバイスを使用します。BYOD シナリオが可能な環境には特に、デバイス登録機能が適しています。この機能を使用すると、ユーザーは、デバイス登録が有効なデバイスから SSO を使用して企業リソースにアクセスできます。また、管理者は、デバイスがドメインに参加していない場合でも、そのようなデバイスからリソースへのアクセスや、企業データのローカル コピーのコンプライアンスを制御できます。

デバイス登録機能が有効なデバイスは、クレームベースの企業アプリにアクセスする際、第 2 の認証要素として使用されます。そのようなアプリに対して、管理者は、アクセス可能なユーザー、アクセス元として使用できるデバイス、アクセスが企業ネットワーク内からのみ許可されるのかインターネットからも許可されるのかを制御できます。デバイス登録機能が有効なデバイスは、企業の証明機関 (CA) を信頼します。これにより、ワーク フォルダーなどの追加機能を容易に構成できます。

デバイス登録のしくみ

デバイス登録機能の主な目的は、次の機能を可能にすることです。

- ドメインに参加していないデバイスの AD DS への登録
- 企業の内部ネットワーク内の限定されたアプリケーションやリソースへの SSO



デバイス登録は、デバイス登録サービスと、デバイス認証が有効な Active Directory フェデレーション サービス (AD FS) を使用することによって機能します。ユーザーが登録プロセスを通してデバイス登録すると、デバイス登録サービスがそのデバイスに証明書を割り当てます。この証明書は、デバイスが内部リソースにアクセスする際、デバイスを認証するために使用されます。さらに、デバイスは AD DS 内の特定のユーザーに関連付けられるので、管理者はユーザーと登録されたデバイスに適用されるアクセス ポリシーを構成できます。

Web アプリケーション プロキシ コンポーネントを実装することによって、登録されたデバイスから、インターネットなどの外部ネットワークを介して企業リソースにアクセスできるようにすることもできます。ユーザーは、自身が所有しているデバイスが登録されていると、コーヒー ショップや自宅からでも、Web アプリケーション プロキシおよび AD FS を介して、内部アプリケーションにアクセスできます。ユーザーが登録されているデバイスを内部ネットワークで使用する場合、デバイスは AD FS および AD DS と直接通信して認証されます。登録されているデバイスに対して、限定されたアプリケーションでの SSO を有効にすることもできます。これにより、ユーザーは、リソースにアクセスするごとに資格情報を入力する必要がなくなります。

デバイス登録をサポートするためのインフラストラクチャ要件

デバイス登録機能を使用する前に、まず、企業のインフラストラクチャを構成して、デバイス登録を可能にする必要があります。デバイス上でデバイス登録を有効にする前に、次の前提条件が満たされている必要があります。

- Active Directory 環境
- PKI は重要である
  - デバイスは CA を信頼する必要がある
  - デバイスは CDP や AIA にアクセスできる必要がある
- AD FS サーバー
  - 信頼された証明書を必要な属性を使用して構成する必要がある
- デバイス登録サービス
- Enterpriseregistration という名前のホスト用の DNS レコード
- 外部デバイスの Web アプリケーション プロキシ
- デバイスでサポートされるオペレーティング システム
  - Windows 10、Windows RT 8.1、Windows 8.1、iOS、および Android

- **Active Directory 環境 :** デバイス登録では、ドメイン環境の実装が必要になります。1 つ以上のドメイン コントローラーで Windows Server 2012 以降が動作しており、スキーマは Windows Server 2012 R2 レベルに拡張されている必要があります。
- **公開キー インフラストラクチャ :** デバイス登録機能を使用するには、公開キー インフラストラクチャ (PKI) が展開されており、適切に構成されている必要があります。デバイスは、CA を信頼する必要があります。これは、ドメインに参加しているデバイスでは既定として設定されますが、ドメイン メンバーではないデバイスでは手動で構成する必要があります。証明書には、次の 2 つの情報が両方とも含まれている必要があります。
  - 失効された証明書のリスト (証明書失効リスト (CRL) や CRL 配布ポイント (CDP) など) が利用できるかどうか。
  - CA の最新の証明書 (機関情報アクセス (AIA) など) が利用できるかどうか。

  デバイスがデバイス登録を使用するには、CRL、Delta CRL、および AIA にアクセスできる必要があります。Delta CRL はファイルで発行され、既定では、ファイル名にプラス記号 (+) が含まれます。インターネット インフォメーション サービス (IIS) Web サーバー (および既定) では、名前に特殊文字を含むファイルへのアクセスはできないので、ダブル エスケープを有効にして、特殊文字を使用できるようにする必要があります。Active Directory 証明書サービス (AD CS) がインストールされているサーバーで Pkiview.msc を実行することによって、CRL、Delta CRL、および AIA にアクセスできることを確認できます。
- **AD FS :** デバイスでデバイス登録機能を使用するには、企業は事前に AD FS をセットアップする必要があります。AD FS は、信頼される CA からの SSL (Secure Sockets Layer) 証明書を使用して構成する必要があります。また、SSL 証明書には適切に構成されたサブジェクト名属性とサブジェクトの別名属性が含まれている必要があります。
- **デバイス登録サービス :** デバイス登録を実行すると、デバイス登録サービスがデバイスを AD DS に登録します。このサービスはまた、デバイスでデバイス登録を有効にするユーザーに証明書を提供します。

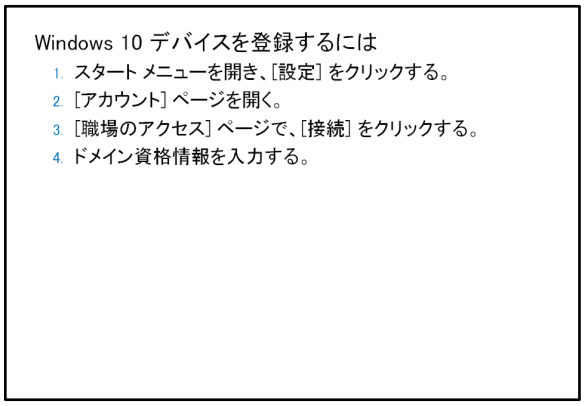
- **Enterpriseregistration という名前のホスト用の DNS レコード :** Enterpriseregistration という名前は必須で、変更できません。DNS サーバーはこの名前を AD FS サーバーの IP アドレスに解決する必要があります。また、AD FS サーバーはその名前を SSL 証明書内のサブジェクトの別名属性の 1 つとして使用する必要があります。
- **Web アプリケーション プロキシ :** これはオプション コンポーネントで、企業ネットワークに接続されているデバイスでデバイス登録を有効にする場合は必要ありません。企業ネットワークに接続されていないデバイスでデバイス登録を有効にする必要があり、デバイスがインターネットに接続されている場合は、Web アプリケーション プロキシをセットアップする必要があります。
- **デバイスでサポートされるオペレーティング システム :** デバイス登録を有効にする必要のあるデバイスでは、サポートされるオペレーティング システムが動作している必要があります。現在、デバイス登録を有効にできるのは、Windows 10、Windows RT 8.1、Windows 8.1、iOS および Android のオペレーティング システムが動作しているデバイスのみです。

ユーザーは、自身が所有しているデバイスでデバイス登録を有効にすると、資格情報を再入力することなく、企業の内部 Web アプリケーションや企業アプリにアクセスできます。SSO を使用するには、管理者はクレームベースの Web アプリケーションを構成し、AD FS サーバーと Web アプリケーションが動作している Web サーバーとの間で証明書利用者信頼を作成する必要があります。

参考資料 : デバイス登録については、次のサイトを参照してください。
任意のデバイスからの職場への参加による業務用アプリケーション間の SSO とシームレスな 2 要素認証
https://technet.microsoft.com/ja-jp/library/dn280945.aspx

デバイス登録

すべての前提条件が満たされたら、デバイスでデバイス登録を有効にすることができます。ドメイン資格情報を持つすべてのユーザーがデバイス登録できます。また、各デバイスは、そのデバイスを複数回 (使用するユーザーごとに 1 回ずつ) 登録できます。デバイス登録するには、次の処理を実行します。



1. スタート メニューを開き、[設定]、[アカウント] の順にクリックします。
2. [アカウント] ページで、[職場のアクセス] をクリックします。
3. [職場のアクセス] ページで、[接続] をクリックします。
4. デバイス登録する際に使用するユーザー ID を入力します。ユーザー ID はユーザーの電子メール アドレスに類似しており、ユーザーのサインイン名、アット マーク (@)、およびドメイン サフィックスの形式を持ちます。ドメイン管理者は、ユーザー ID をユーザー プリンシパル名 (UPN) と呼びます。デバイス登録の実行時には、コンピューターにより Enterpriseregistration.<ドメイン サフィックス> 名の解決が試行されます。その後、SSL 証明書が信頼されていることと、依然として有効であることが検証されます。
5. ユーザーのドメイン資格情報を入力します。デバイスはワークグループ メンバーでも構いませんが、デバイスでデバイス登録を有効にするには、ユーザーはドメイン アカウントを所有している必要があります。

6. デバイスでデバイス登録を有効にすると、デバイス登録サービスによって、参加したデバイスのドメイン オブジェクトが RegisteredDevices AD DS コンテナーに作成され、ユーザーにクライアント認証用の証明書が提供されます。

デバイス登録を有効にするデバイスでは、企業サーバー名を解決するためのネットワーク設定を構成する必要があります。また、企業 CA を信頼するようにデバイスを構成する必要もあります。あなたの会社が、Enterpriseregistration というアドレスを持つサーバー上でパブリックに信頼された証明書を使用する場合、デバイスを構成する必要はありません。あなたの会社が、プライベート CA によって発行された証明書を使用する場合は、証明書をルート CA からエクスポートし、それをデバイス上の信頼されたルート ストアにインポートする必要があります。

知識の確認

質問	
デバイスでデバイス登録機能を有効にする必要がある場合、どの情報を入力する必要がありますか。	
正しい解答を選択してください。	
	UPN
	電子メール アドレス
	パスワード
	Microsoft アカウント
	セキュリティ ID (SID)

レッスン 3
ワーク フォルダーの実装

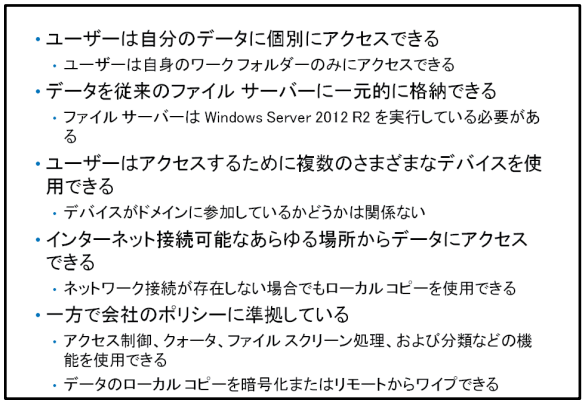
ワーク フォルダーは Windows 8.1 で導入された機能で、ファイルのローカル コピーを Windows Server 2012 R2 ファイル サーバー上のファイルと同期させる機能を提供します。Windows デバイスがドメインに参加していない場合でも、ユーザーはワーク フォルダーを使用できます。また、管理者は、ファイルのローカル コピーに対するポリシーを構成できます。例えば、ローカル コピーを暗号化できます。デバイスの紛失が発生したり、従業員が退職したりした場合は、デバイス上のユーザー データに影響を与えることなく、ワーク フォルダー内のデータのローカル コピーをリモートからワイプできます。このレッスンでは、ワーク フォルダーを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。

- ワーク フォルダーと使用シナリオを説明することができます。
- ワーク フォルダーのコンポーネントを説明することができます。
- ワーク フォルダーを構成するためのプロセスを説明することができます。
- グループ ポリシーを使用してワーク フォルダーを構成することができます。

ワーク フォルダーの概要



従来の方法では、企業ファイルはファイル サーバーに格納されます。このアプローチは、一元的なアクセス制御、監査、一元的なバックアップ、クォータ、レポート処理、ドメインに参加しているネットワーク接続のデバイスからの可用性など、多くのメリットをもたらします。しかし、ユーザーは、企業ネットワークに接続していないときや、ドメイン メンバーではないデバイスから、企業データにアクセスしたり、それらを変更したりすることが必要になります。そのようなシナリオでは、フォルダー リダイレクトやオフライン ファイルなどのソリューションを使用できます。または、Microsoft OneDrive か Microsoft OneDrive for Business を使用することもできました。Windows 10 および Windows 8.1 では、別のソリューションであるワーク フォルダーも使用できます。このソリューションは、次のシナリオで役立ちます。

- ユーザーは、さまざまなデバイスを使用して企業データにアクセスする。
- ユーザーは、デバイス間でデータを同期する必要があるが、一部のデバイスはドメインに参加していない。

ワーク フォルダーは、ユーザーの個人のファイルのみを格納し、ユーザーは自身のワーク フォルダーのみにアクセスできます。ワーク フォルダーのデータは従来型のファイル サーバーに格納されますが、デバイスにも同期共有のユーザーのサブフォルダー、つまりユーザー ワーク フォルダーのローカル コピーが維持されます。ユーザーはネットワーク接続が利用できない場合でも、ワーク フォルダーのローカル コピーにアクセスできます。実行されたすべての変更はファイル サーバー上のワーク フォルダーにすぐに、またはファイル サーバーとの接続が復旧した後に同期されます。ユーザーは、ドメイン メンバーであるかどうかに関係なく、さまざまなデバイスからワーク フォルダーを使用できます。

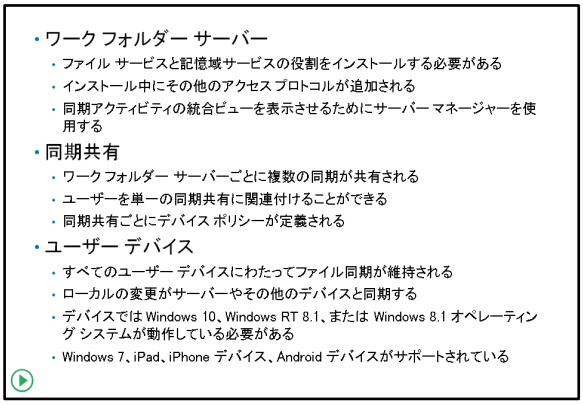
Windows 10、Windows RT 8.1、Windows 8.1、および Windows 7 のオペレーティング システムが動作しているデバイスは、ワーク フォルダーをサポートします。また、iOS や Android のデバイスからもワーク フォルダー機能を使用できます。

ワーク フォルダーが構成されている複数のデバイスをユーザーが使用している場合、あるデバイスでおこなった変更は他のデバイスに自動的に同期されます。ワーク フォルダーのコンテンツはファイル サーバーに保管されるので、ユーザーはファイル サーバーで利用できるすべての機能を使用できます。これらの機能には、ダイナミック アクセス制御、監査、クォータ、ファイル分類インフラストラクチャ、Rights Management サービス (RMS) によるコンテンツ保護などがあります。

ワーク フォルダーにアクセスするデバイスのポリシーを定義することもできます。例えば、ワーク フォルダー データのローカル コピーがデバイス上では暗号化されることを要求するポリシーを作成できます。また、ビジネス データのリモート ワイプ機能を使用して、デバイスの紛失が発生したり、従業員が退職したりした場合、ワーク フォルダー データのローカル コピーにアクセスできなくしたり、それらをワイプしたりすることもできます。

ワーク フォルダーのコンポーネント

ワーク フォルダーを使用するためには、お使いの環境で次のようないくつかのコンポーネントが利用できる必要があります。



- **ワーク フォルダー サーバー :** ワーク フォルダーをホストするために、Windows Server 2012 R2 が動作しているファイル サーバーが必要です。これは、以前のバージョンの Windows Server がワーク フォルダー機能をサポートしていないためです。ファイル サーバーは Active Directory ドメインに参加し、ファイル サービスと記憶域サービスの役割の一部であるワーク フォルダーの役割サービスがインストールされている必要があります。役割サービスをインストールすると、その他のアクセス プロトコルが追加され、サーバー マネージャーが拡張されます。サーバー マネージャーを使用して、次のことをおこなうことができます。
  - ユーザーのワーク フォルダーを含む同期共有を作成および管理する。
  - 同期共有にアクセス可能なユーザー、同期共有がアクセスされた日時、およびアクセス元となったデバイスを確認する。
  - クォータの設定やボリュームの管理など、他のタスクを実行する。

  ユーザーは、HTTPS でカプセル化されたアクセス プロトコルを使用して、ワーク フォルダーにアクセスし、同期することができます。同期では HTTPS 暗号化が使用されるため、ファイル サーバーに SSL 証明書をインストールし、ワーク フォルダーにアクセスするためのデバイスは、証明書を信頼する必要があります。
- **同期共有 :** 同期共有は、ワーク フォルダー サーバーとクライアント デバイスとの間の同期の単位です。ワーク フォルダー サーバー上に複数の同期共有を作成することができます。同期フォルダーはファイル サーバー上の物理フォルダーにそれぞれマッピングされます。ワーク フォルダーを使用するユーザーは、同期共有内に個人用サブフォルダーが作成され、ユーザーは、サブフォルダーのコンテンツにのみアクセスして同期することができます。同期共有にアクセスできるユーザーを構成したり、デバイス ポリシーを指定したりできます。デバイス ポリシーでは、クライアント デバイスに存在するワーク フォルダー データのローカル コピーは暗号化される必要があることなどを指定できます。

ユーザーは、複数の同期共有にアクセスするためのアクセス許可を所有することはできますが、パートナーシップは単一の同期共有に制限されます。既定で、ユーザーは、ワーク フォルダー機能を使用してのみ同期共有にアクセスできますが、管理者は、同期共有と同じフォルダーを使用するサーバー メッセージ ブロック (SMB) 共有を作成することもできます。ユーザーが SMB アクセスを使用して同期共有のコンテンツにアクセスできる場合、ワーク フォルダーを使用しないデバイスから同期されたコンテンツを表示できます。同期共有はファイル サーバーに格納されるので、コンテンツを管理する際、ダイナミック アクセス制御、クォータ、ファイル スクリーン処理などの機能を使用できます。

- **ユーザー デバイス :** ユーザーが、ワーク フォルダーに格納されたコンテンツにアクセスし、変更して同期するデバイスです。ユーザーは、ワークグループのデバイス、登録されているデバイス、またはドメイン メンバーのデバイスからワーク フォルダーにアクセスできます。デバイスでは、サポートされているオペレーティング システムが動作している必要があります。現在サポートされているオペレーティング システムは、Windows 10、Windows RT 8.1、および Windows 8.1 です。Apple iPad などの iOS ベースのデバイスや Android デバイス、Windows 7 クライアントもサポートされています。また、デバイスは、ワーク フォルダー サーバーが使用している SSL 証明書を信頼する必要があります。ワーク フォルダーを使用するようにデバイスを構成すると、データのローカル コピーに対する変更はリアルタイムに検知され、サーバーに反映されます。既定では、デバイスはワーク フォルダー サーバーを 10 分ごとにチェックし、変更をワーク フォルダーのデータのローカル コピーに反映します。

ワーク フォルダーでの同期プロセス

デバイス上にワーク フォルダーを構成する場合は、デバイスとファイル サーバーの間にワーク フォルダーの同期パートナーシップを確立します。初期化を実行中に、データ ディレクトリ、バージョン データベース、およびダウンロードステージング ディレクトリがデバイス上に作成されます。バージョン データベースは、データのローカル コピーとファイル サーバーのデータの同期を維持するのに役立ちます。サーバー側のワーク フォルダーは、ユーザーごとに一度のみ割り当てられます。クライアント側のワーク フォルダーは、ユーザーがワーク フォルダーを使用しているデバイスごとに割り当てられます。ユーザーがワーク フォルダーのコンテンツを変更すると、次のプロセスが実行されます。

1. ユーザーがローカル ワーク フォルダーのコンテンツを変更すると、変更はクライアント側でリアルタイムに検知されます。クライアント デバイスはワーク フォルダー サーバーとの同期セッションを開始し、変更をアップロードします。

2. アップロードが完了すると、ワーク フォルダー サーバーは、アップロードされた変更をユーザーのワーク フォルダーのコンテンツに適用します。既定では、サーバーは、すべての変更をユーザーのデータに対して実行できるように構成されます。例えば、サーバーのアクセス許可が変更され、サーバーが変更を適用できないなどのエラーが発生すると、その問題がユーザーに通知されます。同じ同期サイクルの同じタイミングで、ファイルが複数のユーザー デバイスで変更されると、タイムスタンプに基づいて、ファイルの最新バージョンが元のファイル名を保持します。ファイルの他のコピーは同じフォルダー内に保持されますが、それらの名前には、競合が起きたデバイスの名前が付加されます。さらに、同じファイルに対して複数の競合が存在するときは数値が付加されます。ワーク フォルダー サーバーには、100 の競合ファイルが維持されます。その後、ユーザーが問題を手動で解決するまで、そのユーザーに対するワーク フォルダーの同期は停止します。

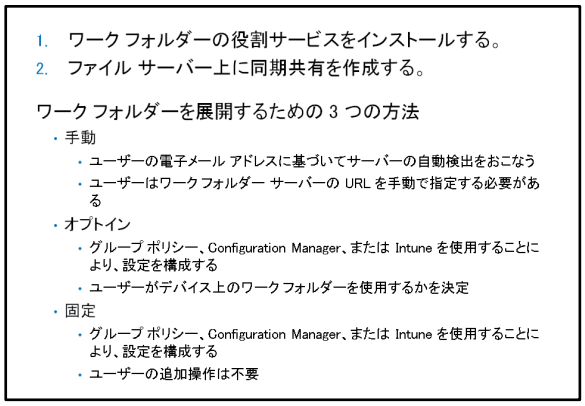
3. 同期が、2 番目のクライアント デバイスによって開始されます。この処理は次の 2 つの理由により発生する可能性があります。まず、データが 2 番目のクライアント デバイスでも変更されており、2 番目のクライアント デバイスがそれらの変更について同期を開始します。もう 1 つの理由として、ローカルの変更がない場合、2 番目のデバイスはプーリング間隔 (既定で 10 分) に基づいて同期を開始します。2 番目のクライアントはワーク フォルダー サーバーから変更をダウンロードし、それらをデータのローカル コピーに適用します。

ワーク フォルダーを使用する際は、次の点に注意する必要があります。

- 同期は、ユーザーごと、デバイスごとに 1 つのパートナーシップに制限されます。複数のユーザーが同じデバイスを使用する場合、すべてのユーザーは、同じまたは異なるワーク フォルダー サーバー上の同期フォルダーとの間でそれぞれ独自のパートナーシップを持つことができます。ただし、同一のユーザーが、同じまたは異なるワーク フォルダー サーバー上の 2 番目の同期共有との間でパートナーシップを作成することはできません。
- 常にクライアントが同期を開始します。ワーク フォルダー サーバーは受動的であり、同期要求に応答するのみです。
- クライアントは、ワーク フォルダー サーバーとの間でのみ同期します。ユーザーが複数のデバイスを使用しており、それらのすべてのデバイスがワーク フォルダーを使用するように構成されている場合、デバイス間で変更が同期されることはありません。同期がおこなわれるのは、サーバーとの間のみです。あるデバイスの変更がサーバーに反映されると、他のデバイスはその変更をサーバーから受信します。
- 変更を適用するシステム (ユーザー デバイスまたはワーク フォルダー サーバーのいずれか) は、競合を解決するための対応をおこなう必要があります。競合は、古いタイム スタンプを持つ競合ファイルの名前を変更することによって、自動的に解決されます。

ワーク フォルダーを構成するプロセス

サーバー管理者は、ユーザーがワーク フォルダーを Windows 10 または Windows 8.1 のコンピューター上で構成して使用できるようにするために、事前に、Windows Server 2012 R2 ファイル サーバー上にワーク フォルダーを作成する必要があります。Windows Server 2012 R2 ファイル サーバー上にワーク フォルダーを作成するには、サーバー管理者は次の 2 つの手順を実行する必要があります。



1. ワーク フォルダーの役割サービスをインストールします。ワーク フォルダーをホストするためにファイル サーバーを構成する前に、まず、ワーク フォルダーの役割サービスをインストールする必要があります。これは、Windows Server 2012 R2 の新しい役割サービスで、サーバー マネージャーから、または次のコマンドレットを実行することによってインストールできます。

```
Install-WindowsFeature FS-SyncShareService
```

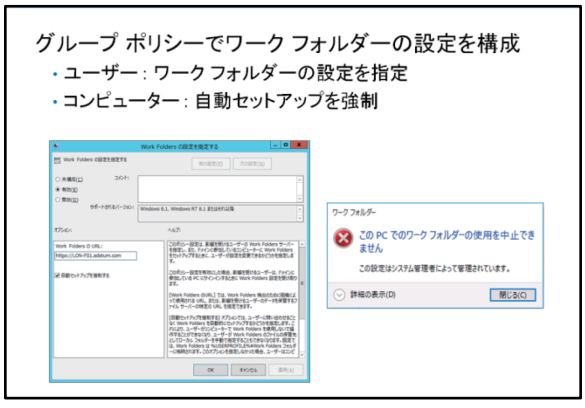
2. ワーク フォルダーの同期共有を作成します。同期共有は、ユーザー デバイスとの間で同期できる、同期の単位です。サーバー マネージャーを使用するか、New-SyncShare コマンドレットを使用して、同期共有を作成することができます。同期共有は既存の SMB 共有にすることも、新しいフォルダーを指すこともできます。複数のユーザーが同一の同期共有にアクセスできるので、ユーザーのサブフォルダーの命名構文を指定する必要があります。名前は、ユーザーのエイリアスまたはユーザー エイリアスのドメインのいずれかの形式で指定できます。最初の構文は、名前にエイリアスを使用する既存のユーザー フォルダーとの互換性を維持し、2 つ目の構文は同一の Active Directory フォレスト内での複数ドメインにおける同じユーザー エイリアスの競合をなくします。既定では、ユーザーはワーク フォルダー構造全体を同期しますが、特定のサブフォルダーに同期を制限することもできます。また、同期フォルダーとデバイス ポリシーにアクセスするためのアクセス許可を所有するユーザーを構成することもできます。デバイス ポリシーでは、同期共有にアクセスするために使用されるデバイスで満たされる必要のある要件を定義します。

インターネットなどの外部ネットワークからワーク フォルダーにアクセスできるようにしたい場合は、追加のコンポーネントを展開する必要があります。Windows Server 2012 R2 の Web アプリケーション プロキシ機能を使用して、内部ネットワークの外にワーク フォルダーを公開することができます。リバース プロキシ システムのサード パーティ製ファイアウォールを使用して、ワーク フォルダーを公開することもできます。インターネット上のワーク フォルダーを公開する場合は、信頼済み証明書を使用して接続のセキュリティを保護するようにしてください。

ワーク フォルダーを Windows Server 2012 R2 ファイル サーバーで構成した後、ワーク フォルダーをクライアント デバイスに展開することができます。クライアント デバイスの種類やドメインに参加しているどうかに応じて、次に示す異なるオプションを使用して、ワーク フォルダーを展開できます。

- **手動 :** コントロール パネルの [ワーク フォルダーの管理] を使用し、ワーク フォルダーを構成することができます。デバイスがドメイン メンバーであるか、登録されたデバイスである場合、ユーザーの UPN を入力できます。この値は、ユーザーの同期共有が配置されているワーク フォルダー サーバーを自動的に検出するために使用されます。デバイスがワークグループのメンバーである場合、ユーザーの電子メール アドレスは解決できないので、代わりにワーク フォルダー URL を入力する必要があります。ワーク フォルダー サーバーの自動検出を有効にするには、DNS に workfolders ホスト レコードを作成する必要があります。
- **オプトイン :** ワーク フォルダー設定は、Microsoft Intune、Configuration Manager、またはドメイン ベースのグループ ポリシーを使用して構成できます。ただし、これらの設定は必須ではありません。ユーザーは、それらの設定を使用してデバイス上にワーク フォルダーを構成するかどうかを決定できます。
- **固定 :** 同じ 3 つの方法 (Microsoft Intune、System Center Configuration Manager、またはドメインベースのグループ ポリシー) を使用してデバイスにワーク フォルダーの設定を配布できます。ただし、これらの設定は必須であるので、ユーザーはそれらを変更できません。この方法を使用すると、ワーク フォルダーは、ユーザーの操作を必要とせずに、デバイス上で透過的に構成されます。

グループ ポリシーによるワーク フォルダーの構成



ワーク フォルダーは、グループ ポリシーを使用して構成できます。グループ ポリシーを使用すると、ワーク フォルダー構成を指定できるだけでなく、ユーザーはデバイス上でワーク フォルダーを使用するかどうかを決定できます。例えば、オプトイン シナリオで、ユーザーは、コントロール パネルの [ワーク フォルダー] 項目を使用して、ワーク フォルダーを構成する必要があります。グループ ポリシーを使用して、ワーク フォルダー構成を必須にすることもできます。これにより、透過的かつユーザーの操作を必要とせずに、デバイスはワーク フォルダーを使用するように構成されますが、ユーザーはワーク フォルダー構成を変更することも、同期フォルダー データのローカル コピーが格納される場所を指定することもできません。

ワーク フォルダー関連の設定は、グループ ポリシーのユーザー ノードとコンピューター ノードに配置されます。グループ ポリシーのユーザー ノードでは、ワーク フォルダーの有効化およびワーク フォルダー URL の指定をおこなうことができ、ワーク フォルダーの自動セットアップを強制することもできます。グループ ポリシーのコンピューター ノードでは、グループ ポリシーの適用対象となるデバイスのすべてのユーザーがワーク フォルダーを自動的に使用するように強制できます。

ドメインベースのグループ ポリシーでワーク フォルダーの設定を構成すると、それらの設定はドメインに参加しているデバイスとドメイン アカウントを使用してサインインしているユーザーに対してのみ適用できます。それらの設定は、ワークグループのメンバーであるデバイスや、デバイス登録を有効にしているデバイスに対しては適用されません。ドメイン メンバーではないデバイス上でワーク フォルダーを自動的に構成する必要がある場合は、Intune を使用する必要があります。

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
ワーク フォルダーの内容は、同僚と共有できます。	

演習 A : ドメインに参加していないデバイスのデータ アクセスの構成

シナリオ

A. Datum 社のユーザーは、会社所有の、ドメインに参加しているコンピューターを使用して企業データにアクセスしています。ユーザーの多くが、職場に自分のデバイスを持ってきて、それを使用して企業データにアクセスしています。自分のタブレットを持っているユーザーは、データをローカルにコピーする際、会社のファイル サーバー上のファイルとの同期を維持することが難しいと苦情を述べています。IT 管理者は、ユーザーが企業データにアクセスするために使用するデバイスの概要を持っておらず、そのようなデバイスにローカルに保存されたデータ上で会社のセキュリティ ポリシーを強制することができないと苦情を述べています。これらの問題に対処するために、ワーク フォルダー機能を実装することを決定しました。

目的

この演習により、次のことを習得できます。

- ワーク フォルダーを構成することができます。

演習のセットアップ

予定所要時間 : 45 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¥Adam Admin 第 5 章で作成した Microsoft アカウント
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$$w0rd
5. 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。ユーザー名「Adatum¥Adam」、パスワード「Pa$$w0rd」を使用してサインインします。
6. 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。
7. 23697-2B-LON-CL4 を起動し、ユーザー名「Admin」、パスワード「Pa$$w0rd」を使用してサインインします。ネットワーク ウィンドウが表示されたら、[はい] をクリックします。
8. [スタート] をクリックし、[設定] をクリックします。

9. 設定ウィンドウで、[アカウント] をクリックします。
10. アカウント ウィンドウの左側のナビゲーション ウィンドウで、[家族とその他のユーザー] をクリックします。
11. 右側のウィンドウの [他のユーザー] セクションで、[その他のユーザーをこの PC に追加] をクリックします。
12. [このユーザーはどのようにサインインしますか?] ページで、第 5 章で作成した Microsoft アカウントの電子メール アドレスを入力し、[次へ] をクリックします。
13. [準備が整いました] ページで、[完了] をクリックします。
14. [スタート] をクリックし、スタート メニューの最上部の人のアイコンをクリックします。
15. ドロップダウン リストで、追加した Microsoft アカウントを選択します。
16. [サインイン] ページで、パスワードとして「Pa$$w0rd!」と入力し、Enter キーを押します。数分待ちます。
17. [PIN のセットアップ] ページで、[この手順をスキップする] をクリックし、PIN の作成ウィザードをスキップし、[次へ] をクリックします。

練習 1 : ワーク フォルダーの構成

シナリオ

現在、ユーザーは、ファイル サーバーのデータと同期しているデータのローカル コピーを保持するために、オフライン ファイルを使用しています。しかし、多くのユーザーが、ドメイン メンバーではないデバイスを使用しているため、オフライン ファイルを使用できないと苦情を述べています。IT 部門は、ワーク フォルダーの実装を検討しており、ドメイン メンバーでないデバイスを持つユーザーでも使用できることを確認する必要があります。また、そのワーク フォルダーがドメイン メンバーであるデバイス上で自動的に構成されることを確認する必要があります。あなたは、ワーク フォルダーの概念実証の展開を実装するよう依頼されました。その結果に基づいて、ワーク フォルダーが会社のニーズを満たすかどうかを IT 部門が決定します。

主な作業は次のとおりです。

1. インフラストラクチャの要件を構成する
2. グループ ポリシー設定を構成してワーク フォルダーを構成する
3. ワーク フォルダーを展開する
4. ワーク フォルダーの同期を実行する

▶ 作業 1 : インフラストラクチャの要件を構成する

1. LON-DC1 の Windows PowerShell ウィンドウで次のコマンドレットを入力し、Enter キーを押します。

```
Install-WindowsFeature FS-SyncShareService
```

2. サーバー マネージャーで、新しい同期共有を作成します。使用するデータを次に示します。
   - ローカル パス : C:¥syncshare1
   - ユーザー フォルダーの構造 : ユーザーのエイリアス
   - グループへの同期アクセスの許可 : Marketing
   - デバイス ポリシー : 選択されない

3. サーバー マネージャー で、[ワーク フォルダー] セクションに [syncshare1] が、[ユーザー] セクションに [Adam Barr] が表示されることを確認します。
4. LON-DC1 の IIS マネージャーで、[Default Web Site] に https サイト バインドを追加します。LON-DC1.Adatum.com を SSL 証明書として使用します。

▶ 作業 2 : グループ ポリシー設定を構成してワーク フォルダーを構成する

1. LON-DC1 のグループ ポリシーの管理コンソールで「Deploy Work Folders」という名前のグループ ポリシーを作成し、[Marketing] OU にリンクします。
2. [Deploy Work Folders] グループ ポリシーのグループ ポリシー管理エディターで、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Work Folders] の順に参照します。
3. [Work Folders の設定を指定する] 設定を有効にし、[Work Folders の URL] に「https://lon-dc1.adatum.com」と設定し、[自動セットアップを強制する] チェック ボックスをオンにします。
4. LON-CL1 からサインアウトし、ユーザー名「Adatum¥Adam」、パスワード「Pa$$w0rd」を使用して再度サインインします。
5. エクスプローラーで、ワーク フォルダーに「On LON-CL1」という名前の新しいテキスト ドキュメントを作成します。

▶ 作業 3 : ワーク フォルダーを展開する

1. LON-CL4 で、コントロール パネルの [ワーク フォルダー] 項目で、ワーク フォルダーを構成します。使用する設定を次に示します。
   - ワーク フォルダー URL : https://lon-dc1.adatum.com
   - 資格情報 : ユーザー名「Adatum¥Adam」、パスワード「Pa$$w0rd」
2. LON-CL4 で、ワーク フォルダーの On LON-CL1.txt ファイルが使用可能であることを確認します。

▶ 作業 4 : ワーク フォルダーの同期を実行する

1. LON-CL4 で、ワーク フォルダーに「On LON-CL4.txt」という名前の新しいテキスト ドキュメントを作成します。
2. LON-CL1 に切り替え、ワーク フォルダーに、On LON-CL1.txt ファイルのみが表示されることを確認します。

注 : ワーク フォルダーは、10 分ごとに自動的に同期します。ただし、同期を手動で起動するオプションもあります。

3. エクスプローラーで、LON-CL1 上でワーク フォルダーを同期します。
4. エクスプローラーで、ワーク フォルダー内に、On LON-CL1.txt ファイルと On LON-CL4.txt ファイルが両方とも表示されることを確認します。
5. 資格情報として、ユーザー名「Administrator」、パスワード「Pa$$w0rd」を使用して、イーサネット ネットワーク接続を無効にします。
6. ワーク フォルダーの On LON-CL1.txt ファイルに「Modified offline」という内容を追加して変更します。
7. ワーク フォルダーに「Offline LON-CL1」という名前の新しいテキスト ドキュメントが作成されます。
8. LON-CL4 で、ワーク フォルダーの On LON-CL1.txt ファイルに「Online modification」という内容を追加して変更します。

9. LON-CL1 で、イーサネット ネットワーク接続を有効にします。資格情報として、ユーザー名「Administrator」、パスワード「Pa$$w0rd」を使用します。
10. LON-CL1 で、On LON-CL1 と On LON-CL1-LON-CL1 を含め、ワーク フォルダーにファイルが表示されることを確認します。

注 : ファイルが 2 つの場所で変更されたため、競合が起き、コピーのうち 1 つのファイル名が変更されました。

結果 : この練習により、ワーク フォルダーを構成することができました。

▶ 次の演習の準備をする

この章の次の演習のために、仮想マシンを起動したままにします。

レッスン 4
クラウドベースの記憶域ソリューションによるオンライン データの管理

この数年において、ますます多くの企業が、オンプレミス記憶域ソリューションの代替策としてオンライン データ記憶域オプションを使用することを検討し始めています。この理由として、オンライン記憶域は一般的により安価で、どこからでもいずれのデバイスからもアクセスでき、とても信頼性が高いことが挙げられます。このレッスンでは、Microsoft が提供するクラウドベースの記憶域ソリューションを使用してオンライン データを管理する方法について説明します。

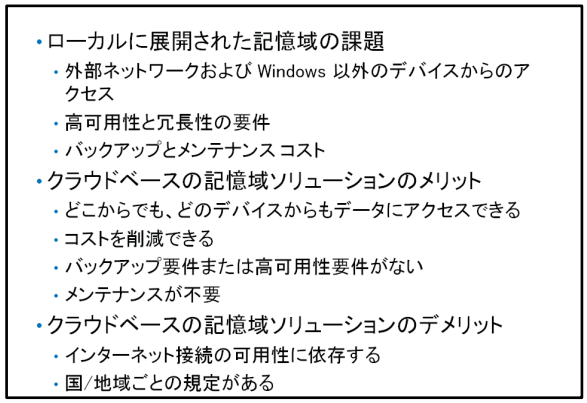
目的

このレッスンにより、次のことを習得できます。

- オンライン データ記憶域の考慮事項を説明することができます。
- 個人向けとビジネス向けの Microsoft OneDrive ソリューションを比較することができます。
- OneDrive を構成するプロセスを説明することができます。
- OneDrive に格納されているデータを共有することができます。
- OneDrive を構成することができます。

データ用オンライン記憶域の考慮事項

ローカルに展開されているデータに対して、適切なアクセス テクノロジを実装し、インターネットなどの外部ネットワークからデータにアクセスできるようにする必要があります。Windows ベースのコンピューターについては、VPN 接続または DirectAccess を展開できますが、モバイル デバイスや Windows 以外のデバイスについては、これらは正しいアプローチではないことがあります。



どこからでも、どのデバイスからもデータにアクセスできる必要があるので、データをローカルに展開された記憶域のみに維持することは、ますます複雑になっています。また、このようにしてデータを維持することは、IT 予算の少ない、または制限されている一部の企業にとってはあまりに高価すぎます。記憶域システムの可用性を高くするには、それぞれに対して、バックアップ システム、冗長なハード ディスク、冗長な電源、および空調設備が必要になります。記憶域システムの可用性を高くしないことを選択すると、データ喪失のリスクが高くなります。これらの理由により、より多くの企業が、データ記憶域ソリューションとしてオンライン記憶域サービスを検討しています。

Microsoft OneDrive for Business などのビジネス クラウド記憶域サービスにデータを格納することには、多くのメリットがあります。次のリストに、これらのメリットの一部を示します。

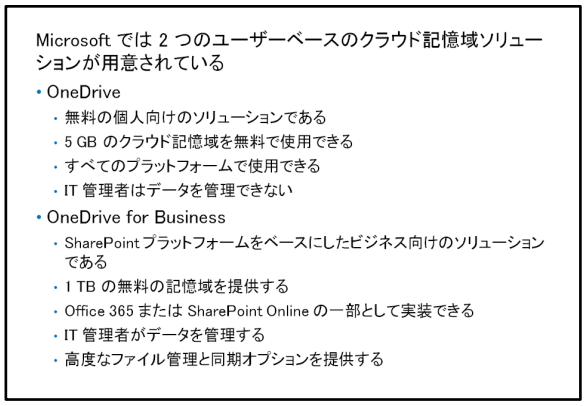
- どのデバイスからも、どこからでも、強力な認証方法を介してデータにアクセスできます。
- 記憶域システムをローカルに展開して維持する必要はありません。これは、展開の対象をローカルに配置する必要のあるデータのみの最小限に抑えられることを意味します。
- データは可用性の高い記憶域システムに格納されます。このシステムには、冗長性が組み込まれているので、バックアップの必要性は、最小限になるか、またはまったく存在しません。

ただし、データをクラウドベースの記憶域システムに格納することには、次に示すようないくつかのデメリットもあります。

- データ アクセスが、お使いのインターネット接続に依存するようになります。インターネット接続が機能しないと、データ アクセスはローカルにキャッシュされているデータのみに制限される可能性があります。
- 一部の企業および/または官公庁は、その国/地域以外の場所にデータを格納することを禁止しています。

Microsoft は、データ記憶域ソリューションとして機能するいくつかのクラウド サービスを提供しています。個人使用の場合、ユーザーは Microsoft アカウントを持つすべてのユーザーに無料で提供されている Microsoft OneDrive を使用できます。ビジネス使用の場合、ユーザーは Office 365 の一部である OneDrive for Business を使用できます。または、Azure サブスクリプションに付随する Azure ベースの記憶域も使用できます。

個人向けとビジネス向けの OneDrive ソリューションの比較



OneDrive は、Microsoft のユーザーベースのクラウド記憶域ソリューションであり、個人とビジネスの両方向けに使用できるクラウド記憶域を提供します。同じ OneDrive ブランドを共有していますが、個人向けの OneDrive と OneDrive for Business を区別する必要があります。これら 2 つのサービスは、異なるプラットフォームに基づいており、異なる環境で使用されます。OneDrive は Microsoft アカウントの一部であり、Microsoft アカウントを持つユーザーすべてに対して無料で提供されていますが、OneDrive for Business は有料サービスで、Office 365 パッケージに組み込まれており、SharePoint Online テクノロジに基づいています。

OneDrive

OneDrive は、個人用のファイルを対象にして設計されたコンシューマー志向のソリューションです。エンタープライズ ソリューションとして使用することは意図されていません。OneDrive では、5 GB のクラウド記憶域を無料で使用できますが、有料オプションを使用して記憶域を増やすこともできます。また、Microsoft や Microsoft パートナーからの特典を利用して記憶域を増やすこともできます。OneDrive を使用すると、自分用のプライベート ストアに個人用のファイルを保存する、またはパブリック ストアに保存して他のユーザーとファイルを共有することができます。

OneDrive には次のようなさまざまな機能が用意されており、ユーザーは自分のニーズを最適に満たすものとして、OneDrive にアクセスし使用できます。

- **Microsoft Office :** Office 2013 で [ファイル] メニュー、[保存] または [名前を付けて保存] の順にクリックし、保存場所として OneDrive を選択することで、Office を使用してドキュメントを OneDrive に保存できます。
- **Microsoft Office Online :** Microsoft Office Online を使用して、OneDrive に保存されているドキュメントを表示および編集できます。
- **PDF と OpenDocument 形式 (ODF) のサポート :** OneDrive に保存されている PDF ドキュメントと ODF ドキュメントを表示できます。

IT 管理者は OneDrive を管理しませんが、ユーザーがドメイン コンピューターで OneDrive アプリケーションを使用しないようにすることができます。

ただし、IT 管理者は個人用の OneDrive フォルダーに格納されているデータを管理できません。また、認証ルールやアクセス制御ポリシーのいずれも構成することはできません。

OneDrive アプリケーションはすべてのモバイル プラットフォームで利用できるので、ユーザーはそれらを自身が所有しているモバイル デバイスで使用することもできます。OneDrive アプリケーションをモバイル アプリとして実装すると、携帯電話のフォト ギャラリーから写真を OneDrive の [写真] フォルダーに自動的にアップロードするように、OneDrive を構成できます。

OneDrive for Business

OneDrive for Business は同期サービスで、ユーザーはドキュメント ライブラリを SharePoint サイトからローカル コンピューターまたはモバイル デバイスに同期できます。OneDrive for Business は、SharePoint Online またはオンプレミス SharePoint 2013 を通して Office 365 の一部として実装できます。Office 365 の一部として、OneDrive for Business はユーザーごとに 1 TB の無料記憶域を提供します。

OneDrive for Business アプリケーションは、Office Professional Plus 2013 および Office 365 プランに含まれますが、スタンドアロン製品として無料でダウンロードすることもできます。ダウンロード ファイルは .msi 形式で提供されているので、グループ ポリシーを使用して展開できます。また、手動でインストールすることもできます。無料のモバイル アプリは、Windows ストア、Google Play、または Apple Store からも入手できます。モバイル アプリケーションは、Office365 サブスクリプションを所有している場合のみ動作し、SharePoint のオンプレミス実装と同期できません。ライブラリへのアクセス、ライブラリの表示、またはライブラリの OneDrive for Business への同期をおこなうには、ユーザーは Office365 アカウントにサインインする必要があります。オンプレミス実装では、SharePoint サイトにサインインする際に入力するのと同じ資格情報が必要になります。

OneDrive for Business のファイル ライブラリをエクスプローラー ウィンドウで操作したい場合は、OneDrive for Business で同期を開始します。SharePoint のドキュメント ライブラリの URL を入力して、[今すぐ同期] をクリックする必要があります。ドキュメント ライブラリを参照している場合は、右上隅の [同期] アイコンをクリックして、現在のライブラリを同期できます。同期されたライブラリが、エクスプローラーの [お気に入り] の下に表示されます。ライブラリを Outlook に同期することもできます。

SharePoint 管理者は、ドキュメント ライブラリのプロパティを構成することによって、ドキュメント ライブラリの同期を無効にすることができます。いずれかのライブラリの同期が停止すると、以前に同期されたすべてのファイルが、ユーザーのコンピューターに残ります。OneDrive ライブラリは、Azure RMS などの RMS サービスを使用するように構成して、保護を強化することができます。

OneDrive for Business のファイル管理は、OneDrive よりもはるかに優れています。OneDrive for Business では、ドキュメントのチェックアウト、バージョン履歴の追跡、およびより高度なオプションが選択可能なファイル共有をおこなうことができます。

OneDrive を構成するプロセス

OneDrive では、エンド ユーザーは自身の OneDrive の内容とモバイルとデスクトップの OneDrive アプリケーションを完全に制御できます。使用しているコンピューターが既定のサインイン シナリオとして Microsoft アカウントを使用していない場合、OneDrive を Microsoft OneDrive タイルから使用するには、ユーザーは Microsoft アカウントをドメイン アカウントまたはローカル アカウントに関連付ける必要があります。OneDrive デスクトップ アプリケーションの場合、ユーザーは、ローカル コンピューターと同期する必要のある OneDrive フォルダーを構成できます。

- OneDrive にサインインするための Microsoft アカウントを持つ必要がある
- OneDrive デスクトップ アプリには、ファイルとフォルダーの同期のためのオプションがある
- オンライン版の OneDrive では、ユーザーは次のことを実行できる
  - 追加の記憶域を購入できる
  - ごみ箱にアクセスできる
  - ファイル バージョンの履歴にアクセスできる
  - 共有を構成できる
- グループ ポリシーを使用する、またはエッジ ファイアウォールで URL ブロック リストを作成することで、アクセスを制限できる

同期対象として構成されているファイルおよびフォルダーは、ユーザーのコンピューターにコピーされ、コンピューターがオフラインの場合にもアクセスできます。その他のファイルは、インターネットが接続されている場合のみ、OneDrive デスクトップ アプリから利用できます。また、ユーザーは OneDrive アプリケーションから同期プロセスを開始したり、同期プロセスを一時停止したりできます。

オンライン版の OneDrive では、ユーザーは次のことを実行できます。

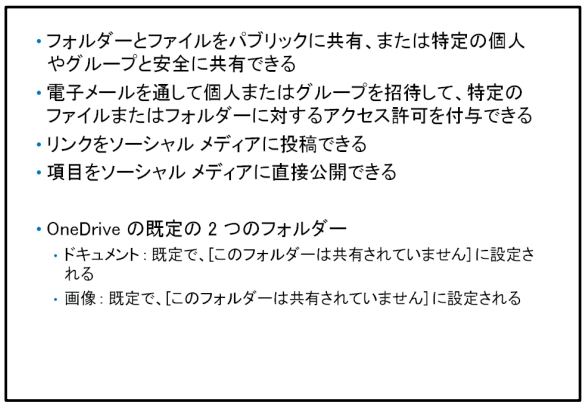
- OneDrive 上の自分のすべてのファイルを管理できます。
- 以前のバージョンのファイルと、OneDrive 記憶域から最近削除されたファイルを含む OneDrive のごみ箱にアクセスできます。
- 追加の記憶域を購入できます。
- ファイルおよびフォルダーの高度な共有オプションを構成できます。

IT 管理者は、ユーザーが組織のシステムから OneDrive にアクセスすることを禁止したい場合があります。グループ ポリシーを使用して、これを実行することができます。適切なグループ ポリシー オブジェクト (GPO) で、[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]、[OneDrive] ノードの順に進み、[OneDrive をファイル記憶域として使用できないようにする] ポリシー設定を有効にします。このグループ ポリシー設定がクライアント システムに適用された場合、ユーザーが OneDrive を起動しようとすると、システム管理者が OneDrive の使用をブロックしたという通知を受け取ります。ユーザーの個人用デバイスを含め、すべてのデバイスに対して、OneDrive へのアクセスをブロックする必要がある場合、組織のファイアウォールで、URL ブロック リストを作成することを検討します。

OneDrive に格納されているデータの共有

OneDrive を、パブリックにアクセスできるフォルダーとして共有できます。または Microsoft アカウントの連絡先である特定のユーザーとの間でのみフォルダーとファイルを安全に共有することもできます。

OneDrive アカウントを初めて作成すると、既定で 2 つのフォルダー (ドキュメントと画像) が作成されます。既定では、ドキュメント フォルダーと画像フォルダーの共有フォルダー設定は、[このフォルダーは共有されていません] に設定されます。これは、所有しているユーザーのみがアクセスできることを意味します。



OneDrive に新しいフォルダーを作成する際は、共有方法を選択できます。ファイルまたはフォルダーを共有すると、それらに「共有」の文字が表示されます。

電子メールを通して個人またはグループを招待して、特定のファイルまたはフォルダーに対するアクセス許可を付与できます。電子メールの受信者に読み取り専用アクセス許可または編集アクセス許可を付与できます。また、受信者が Microsoft アカウントを必要とするかどうかも指定できます。項目へのリンクを共有したり、リンクを Facebook や LinkedIn などのソーシャル メディアに直接公開したりできます。

共有を停止したり、アクセス許可を変更したりするには、共有されている項目を選択し、メニュー バーで [共有] をクリックします。

デモンストレーション : OneDrive の構成

講師は、次のデモンストレーションをおこないます。

- OneDrive を構成する

デモンストレーションの手順

1. LON-CL4 で、Microsoft アカウントを使用して OneDrive オンラインにサインインします。
2. 利用できるオプションを確認し、利用できる記憶域のサイズをチェックします。
3. LON-CL4 で、OneDrive アプリケーションで利用できるオプションを表示します。
4. LON-DC1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
5. グループ ポリシーの管理コンソールで、OneDrive に対して利用できるグループ ポリシー オプションを確認します。
6. 実行中の仮想マシンをすべて戻します。

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
コンピューターがドメインに参加している場合、管理者は、OneDrive および OneDrive for Business の両方について、それらに格納されている内容を管理できます。	

演習 B : OneDrive によるデータ アクセスの管理

シナリオ

あなたは、OneDrive で Windows 10 の統合を構成する必要があります。以前構成した Microsoft アカウントを使用します。

目的

この演習により、次のことを習得できます。

- OneDrive を構成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-CL4 MSL-TMG1
ユーザー名	LON-DC1 には Adatum¥Administrator LON-CL4 には第 5 章で作成した Microsoft アカウント
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。すべての仮想マシンは、前のデモンストレーション後、すでに起動しているものとします。

練習 1 : OneDrive の構成

シナリオ

OneDrive の評価の一環として、フォルダーの同期、およびファイルとフォルダーの共有に使用できるオプションを検査したいと考えています。グループ ポリシーで使用できるオプションも確認します。

主な作業は次のとおりです。

1. OneDrive ストレージを構成する
2. OneDrive の設定を管理する
3. OneDrive 共有をセットアップする
4. OneDrive のグループ ポリシー オプションを確認する

▶ 作業 1 : OneDrive ストレージを構成する

1. LON-CL4 で、第 5 章で作成した Microsoft アカウントを使用して、サインインします。
2. LON-CL4 の Microsoft Edge で、[onedrive.com] を開きます。
3. 既定のフォルダーと使用可能な記憶域を確認します。
4. OneDrive オンラインで、新しいフォルダーを作成し「Projects」という名前を付けます。

注 : フォルダーの作成時にタイムアウト エラー メッセージを受信した場合、Internet Explorer で手順 2 ～ 4 を繰り返します。

5. Microsoft Word Online アプリケーションを使用して、新しい Word 文書を作成します。ドキュメントに「Project1」という名前を付け、Projects フォルダーに保存します。
6. Projects フォルダーにファイルが表示されることを確認します。

▶ 作業 2 : OneDrive の設定を管理する

1. LON-CL4 で、タスク バーの通知領域の [OneDrive] アイコンを使用し、[設定] を開きます。
2. OneDrive のファイルとフォルダーがすべて同期されるよう、[フォルダーの選択] が構成されるようにします。
3. [設定] タブでオプションを表示します。
4. LON-CL4 で、OneDrive の Project フォルダーに「Project2」という名前のテキスト ドキュメントを作成します。
5. ファイルが OneDrive オンラインに同期されていることを確認します。
6. OneDrive オンラインで、テキスト ドキュメントに任意のテキストを追加します。
7. 変更が LON-CL4 上の OneDrive フォルダーと同期していることを確認します。

▶ 作業 3 : OneDrive 共有をセットアップする

1. LON-CL4 で、エクスプローラーを開き、OneDrive フォルダーを展開し、[OneDrive リンクの共有] オプションを使用して Projects フォルダーの URL を生成します。
2. LON-CL4 で、新しい Microsoft Edge に URL を貼り付け、Projects フォルダーにアクセスできることを確認します。
3. OneDrive オンラインの Projects フォルダーで [その他の OneDrive 共有オプション] を探索します。
4. 可能な場合は、教室内の他の受講者を招待して、フォルダーを共有します。

▶ 作業 4 : OneDrive のグループ ポリシー オプションを確認する

1. LON-DC1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. グループ ポリシーの管理コンソールを開きます。
3. 既定のドメイン ポリシーを編集します。
4. [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] の順に展開し、[SkyDrive] をクリックします。

注 : Windows Server 2012 R2 では、以前のブランド名が今も使用されていることに注意してください。

5. OneDrive の構成に使用できるオプションを確認します。

結果 : この練習により、OneDrive を構成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

- 記憶域のコストとメンテナンス コストを削減するために、クラウドベースの記憶域ソリューションの使用を検討します。
- ドメインに参加していないビジネス用途のデバイス登録を構成します。
- オンプレミスのデータ同期を必要とするユーザーに対して、ワーク フォルダーの使用を許可します。
- ユーザーに対して、ビジネス データを OneDrive に保存しないよう説明します。
- Web アプリケーション プロキシを使用して、デバイス登録とワーク フォルダーを公開します。

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
クライアント コンピューター上でワーク フォルダーの同期を構成することはできない。	

復習問題

質問 : ネットワーク接続なしでコンピューター上のワーク フォルダー コンテンツにアクセスすることはできますか。