第 1 章
エンタープライズ環境でのデスクトップとデバイスの管理

目次

概要

Windows 10 Enterprise Edition は、大規模組織のユーザー用に設計された Microsoft クライアント オペレーティング システムの最新バージョンです。Windows 10 は、Windows 7 および Windows 8.1 の両方のコア機能を基に構築され、さまざまなプロセッサ アーキテクチャやデバイスの種類を通して、安定したクライアント エクスペリエンスを提供します。この章では、エンタープライズ環境でクライアント オペレーティング システムを管理する問題とモバイル ワーカーのデバイスを管理する問題についての情報を紹介します。また、組織の目的達成を支援するクラウド サービスのオプションについても討論します。

目的

この章により、次のことを習得できます。

- エンタープライズ環境での Windows 10 の管理について討論することができます。
- モバイル ワーカーの管理の複雑さを説明することができます。
- エンタープライズでデバイスをサポートする問題を列挙することができます。
- IT 管理とサービスをクラウドに拡張する方法を説明することができます。

レッスン 1
エンタープライズでの Windows 10 の管理

エンタープライズ環境で Windows クライアント オペレーティング システムを管理することは、中小規模のビジネス環境での管理とは異なります。エンタープライズ環境でのクライアント コンピューターの管理を成功させるためには、適正なツールを選択して、効率的に管理タスクを実行できるようにする必要があります。中小規模のビジネスでクライアント コンピューターを管理するために使用される大多数の技術は、エンタープライズ環境にまで拡張することはできません。そこでは、数百から数千のクライアント コンピューターの管理が必要だからです。

目的

このレッスンにより、次のことを習得できます。

- エンタープライズ環境でデスクトップ コンピューターを管理することの問題点を説明することができます。
- Windows 10 オペレーティング システムの特徴と機能を説明することができます。
- エンタープライズ環境で Windows 10 を管理するための技術を説明することができます。

エンタープライズ環境でのデスクトップの管理

デスクトップ コンピューターの管理に関して、エンタープライズ環境は相当な数の問題を抱えています。エンタープライズ環境の規模はさまざまですが、一般的には数百、ときには数千のコンピューターが収容されます。

- エンタープライズ環境には、数百、ときには数千のコンピューターが収容される
- 複数のコンピューターを一度に管理する方が、同じ操作を各コンピューターに手動でおこなうよりも効率的
- SOE により、組織は、コンピューターごとに独自の構成を持たせるのではなく、少数の構成を維持することができる

エンタープライズ環境内には大量のコンピューターが存在するため、コンピューターを一元的に管理する機能が重要となります。例えば、1 つのソリューションを使用して大量のコンピューター全てにソフトウェア更新プログラムをインストールすることは、組織内の各コンピューターに手動でソフトウェア更新プログラムをインストールするよりもはるかに効率的です。

ユーザーに自身のコンピューターの管理をさせることで、次の問題が起きる可能性があります。

- **ソフトウェア更新の問題 :** 多くのユーザーは、セキュリティとオペレーティング システムのパッチで、オペレーティング システムとアプリケーション ソフトウェアを最新に保つ必要性を認識していません。一元化された更新管理なしに、一部のユーザーはソフトウェア更新を維持できません。
- **マルウェア対策の問題 :** 一元的に管理されなければ、多くのユーザーはマルウェア対策のソフトウェアを有効化し、最新に保つことができません。
- **アプリケーション管理 :** 一元的に管理された「ロックダウンされた」構成がない場合、ユーザーが未承認のソフトウェアをインストールする可能性があります。ユーザーは、ソフトウェアを申請するための組織の煩雑なプロセスを実行する代わりに未承認のアプリケーションをインストールする場合があります。

- **ハードウェアのサポート :** エンタープライズでハードウェアを購入する場合、大抵、延長サポートの契約を結びます。ハードウェアで障害が発生した場合、交換部品の入手が比較的容易で、サポート期間中ならばコンピューター全体の交換も可能です。ユーザー自身がハードウェアを購入すると、障害が起きたとき、多くの場合、ハードウェアを修理する最善の方法の決定はユーザーに委ねられます。

大量のコンピューターの管理を効率化するために、エンタープライズでは、多くの場合 1 つ以上の標準オペレーティング環境 (SOE) を採用します。SOE は、オペレーティング システム、アプリケーション、およびハードウェアの構成のセットです。SOE には次のメリットがあります。

- **新規および交換したコンピューターの展開が容易 :** 新しいコンピューターが必要になった場合、SOE の展開は、最初から構成を構築するよりも簡単です。Windows 展開サービスや System Center 2012 R2 Configuration Manager (Configuration Manager) などの製品を使用して、イメージから SOE を展開することができます。
- **組織全体で一貫したアプリケーションとハードウェア :** 障害が起きた場合、IT 部門の従業員は、ユーザーの生産性を維持したまま、コンピューターをより迅速に交換することができます。交換したコンピューターには、元のものと同じアプリケーションがインストールされているため、ユーザーは交換されたシステムに多くの調整をする必要がありません。
- **容易なインベントリ :** 組織は、ハードウェアとソフトウェアの資産を追跡する必要があります。全員が同様に構成されたコンピューターを使用している場合、各人が個別に構成されたコンピューター、オペレーティング システム、およびアプリケーションのスイートを使用している場合よりも、ハードウェアとソフトウェアの資産の追跡がはるかに簡単になります。
- **更新の簡略化 :** SOE は、オペレーティング システムとアプリケーションの更新プログラムを管理するプロセスを簡略化します。更新プログラムを、限られたセットの構成に対してのみテストすればよいからです。
- **容易なソフトウェアの展開 :** Configuration Manager のような製品により、新規または更新されたアプリケーションをコンピューターに展開するプロセスが簡略化されます。

Windows 10 の概要

Windows 10 は、デスクトップ コンピューター、タブレット、コンバーチブルなコンピューターで使用するように設計された Microsoft クライアント オペレーティング システムです。Windows 7 以降の多くの改善と、Windows 8.1 以降の多数の重要な拡張と機能強化が含まれます。Windows 10 のバージョンには、Raspberry Pi などのモノのインターネット (IoT) デバイスで使用できるものもあります。その他に、電話で使用できる Windows 10 のバージョンもあります。

Microsoft は、Windows 7、Windows 8、および Windows 8.1 オペレーティング システムを所有するユーザーに対して、無料のアップグレード版として Windows 10 を提供しました。この無料アップグレードは、公開後の数週間以内に Windows 10 オペレーティング システムへ移行するユーザー用です。

Windows 10 には、エンタープライズ データ保護、Open Mobile Alliance-Device Management (OMA-DM) のサポート、資格情報ガード、デバイス ガードなどの多くのセキュリティと管理ベースの機能が含まれます。

参考資料 : Windows 10 の新機能については、次のサイトを参照してください。
Windows 10 の新機能
https://technet.microsoft.com/ja-jp/library/dn986867(v=vs.85).aspx

エンタープライズ環境での Windows 10 の管理

Windows 10 Enterprise Edition は、IT 部門がデスクトップ コンピューターの構成を管理している、大規模な組織の環境に最も適したエディションです。Windows 10 Enterprise Edition には、Home および Pro Edition のすべての機能が含まれます。さらに、Windows 10 Enterprise Edition には、Home および Pro Edition では使用できない機能が含まれます。

Windows 10 Enterprise がサポートする新機能
- Azure AD に参加する機能
- 組織向けの Windows ストア
- エンタープライズ データ保護
- きめ細かい UX コントロール
- Windows Update for Business
- Current Branch for Business
- 資格情報ガード
- デバイス ガード
- Long Term Servicing Branch

Windows 10 Enterprise Edition で使用可能な機能には、Windows 7、Windows 8、および Windows 8.1 の Enterprise Edition でも使用可能だったものが含まれます。次の機能は、以前のバージョンの Windows クライアントの Enterprise Edition と同様に、Windows 10 Pro および Enterprise Edition の両方で使用できます。ただし、Windows 10 の Home Edition では使用できません。

- **ドメイン参加 :** Active Directory ドメインに参加させることができます。
- **グループ ポリシーの管理 :** Active Directory ドメインに参加している場合、グループ ポリシーを使用して管理することができます。
- **BitLocker :** すべてのボリューム暗号化とブート環境の保護のソリューションとして機能します。
- **Internet Explorer のエンタープライズ モード :** Internet Explorer の互換性モードは、Internet Explorer 11 による Internet Explorer 7 または Internet Explorer 8 のエミュレートを可能にします。
- **割り当てられたアクセス :** 管理者は特定のユーザー アカウントを、特定の単一の Windows ストア アプリの使用に限定することができます。この機能は、コンピューターまたはユーザーに、使用できるすべてのアプリではなく、単一のアプリの使用のみを許可するキオスク シナリオで役立ちます。
- **リモート デスクトップ :** 互換性のあるリモート デスクトップ接続クライアントからのリモート デスクトップ接続を可能にします。
- **クライアント Hyper-V :** 十分なハードウェア リソースを持つクライアント コンピューターで仮想マシンをホストすることができます。

次の機能は、Windows 10 Pro または Home Edition では使用できませんが、Windows 8.1 Enterprise Edition と Windows 10 Enterprise Edition では使用することができます。

- **DirectAccess :** コンピューターにより認証済みの、常にオンの仮想プライベート ネットワーク (VPN) 接続です。これにより、リモート コンピューターは、内部ネットワーク リソースにアクセス可能になります。また、クライアント コンピューターのリモート管理も可能になります。
- **Windows To Go Creator :** サポートされる USB 記憶装置に、起動可能な Windows 10 のインストールを作成することができます。
- **AppLocker :** AppLocker は、特定のバージョンのアプリケーションのみを実行できるようにアクセスを限定することを含め、コンピューター上で実行可能なアプリケーションを管理者が制御できるようにする、Windows 10 の機能です。

- **Windows BranchCache :** BranchCache により、ワイド エリア ネットワーク (WAN) リンクを経由するファイル共有上にあるファイルを、ローカル エリア ネットワークのピアツーピア キャッシュに格納できます。
- **グループ ポリシーによるスタート画面の制御 :** この機能により、グループ ポリシーを使用して、スタート メニューまたはスタート画面の表示や内容をカスタマイズできます。

次の機能は、Windows 10 Pro および Enterprise Edition でのみ使用できます。

- **Azure AD に参加する機能 :** Windows 10 Pro および Enterprise Edition を実行するコンピューターは、Azure AD に参加することができます。この機能により、コンピューターは、クラウドにホストされたアプリへのシングル サインオン (SSO) を実行することができます。
- **組織向けの Windows ストア :** Windows 10 Enterprise では、アプリ用の通常の Windows ストアに加え、組織向けの特別な Windows ストアを使用することができます。
- **エンタープライズ データ保護 :** 組織は、重要なデータにアクセスできるアプリケーションを制御できます。
- **きめ細かい UX コントロール :** 管理者は、ユーザーが特定のタスクのみを実行できるようにユーザー インターフェイスをロックすることができます。この機能は、Windows 10 をキオスクとして展開する場合に役立ちます。
- **Windows Update for Business :** 配布リング、メンテナンス期間、ピアツーピア配信、および System Center などの既存のツールとの統合を構成する機能を含む、クラウド ベースの Windows Update ソリューションです。
- **Current Branch for Business :** 機能の更新が Windows 10 のコンシューマー向けバージョンで使用可能になってから数ヵ月後に、その更新プログラムを展開することができます。Current Branch for Business では、Windows Update、Windows Update for Business、または Windows Server Update Services (WSUS) を更新管理に使用できます。

次の機能は、Windows 10 Enterprise Edition でのみ使用できます。

- **資格情報ガード :** Windows NT LAN Manager (NTLM) ハッシュと Kerberos チケットなどの派生資格情報を、セキュリティ用に Hyper-V を使用して、保護され、分離されたコンテナーに格納します。この機能には、仮想化拡張と Second Layer Address Translation (SLAT) だけでなく、Unified Extensible Firmware Interface (UEFI 2.3.1) 以降が必要です。
- **デバイス ガード :** Windows 10 を実行するコンピューターで信頼されたソフトウェアのみを実行できるようにソフトウェアの実行を制限することができます。このプロセスは、カーネルから実行され、エンタープライズ ポリシーで構成された署名を使用して、信頼できるアプリケーションを指定します。仮想化拡張と SLAT の他に、UEFI 2.3.1 以降が必要です。
- **Long Term Servicing Branch :** Long Term Servicing Branch は、長期のサポートを提供し、セキュリティに関係しないオペレーティング システムの更新プログラムを最大 10 年間、組織が延期できるようにする Windows 10 のバージョンです。

Windows 10 pro および Enterprise Edition では、キー管理サービス (KMS) ライセンスなどのエンタープライズ機能もサポートします。KMS を利用するコンピューターは、各コンピューターで使用する個別のライセンス キーを用いるのではなく、内部ネットワークに展開された KMS サーバーに対して定期的にライセンス認証をおこないます。

デモンストレーション : Windows 10 の機能の探索

講師は、次のデモンストレーションをおこないます。

- 管理タスクを実行する
- Windows PowerShell の出力コピーし、メモ帳に貼り付ける
- 資格情報ガード機能をインストールする

デモンストレーションの手順

1. LON-CL1 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. [スタート] を右クリックし、それぞれのオプションを確認します。
3. [タスク バーのプロパティ] ダイアログ ボックスを開きます。[ナビゲーション] タブで、[左下隅を右クリックするか Windows キー + X キーを押したときに表示されるメニューで、コマンド プロンプトを Windows PowerShell に置き換える] を有効にします。
4. [スタート] を右クリックし、[Windows PowerShell] と [Windows PowerShell (管理者)] が表示されることを確認します。
5. [Windows PowerShell (管理者)] を開きます。
6. [オプション] ページで、[Ctrl キー ショートカットを有効にする] が有効であることを確認します。
7. 管理者 : Windows PowerShell ウィンドウで、次のコマンドレットを実行します。

```
Get-NetIPConfiguration
```

8. コマンドレットの出力をメモ帳にコピーします。
9. [分離ユーザー モード] 機能を追加し、コンピューターを再起動します。
10. デモンストレーションが完了したら、23697-2B-LON-DC1 と 23697-2B-LON-CL1 を戻します。

レッスン 2
モバイル ワーカーの管理

21 世紀に入る前は、ほぼすべての組織の従業員は、オフィス内で仕事をしていました。それらの従業員には、有線ネットワークに接続されたデスクトップ コンピューターが割り当てられました。現在、勤務時間のすべて、または一部を、ホーム オフィスでの業務に費やす従業員が増えています。その他に、仕事の一環で移動し、長時間にわたって内部ネットワークから離れている従業員もいます。それらの従業員には、ノート PC、タブレット、コンバーチブル デバイス (ノート PC とタブレットのフォーム ファクター間での切り替えが可能なデバイス) などのモバイル コンピューターが割り当てられます。Active Directory ドメイン サービス (AD DS) などの従来のテクノロジを使用して、これらのリモート ユーザーの使用するコンピューターを管理することが困難なため、内部ネットワークからの距離は、IT 部門にとって問題となっています。

目的

このレッスンにより、次のことを習得できます。

- モバイル ユーザーを管理する上での問題を説明することができます。
- 外部のクライアント コンピューターを管理するためのソリューションを説明することができます。
- リモート データやアプリケーションへの保護されたアクセスを提供するためのエンタープライズ ソリューションを列挙することができます。

モバイル ワーカーの管理の問題

現在、エンタープライズ環境で使用されている相当な数のコンピューターがノート PC、タブレット、またはノート PC とタブレットのフォーム ファクター間での切り替えができるコンバーチブル デバイスです。これらのモバイル コンピューターは、従来のデスクトップ コンピューターでは起きなかったような、モバイル コンピューター固有の管理の問題をエンタープライズ IT 部門にもたらしています。これらの問題には、次のものがあります。

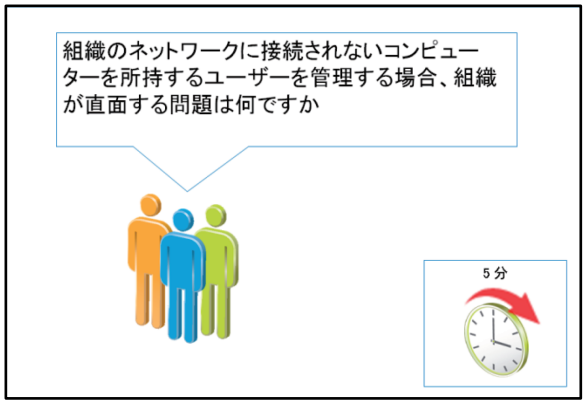
モバイル コンピューターがもたらす管理の問題
- 組織の外で悪意のあるネットワークに接続する
- 常に組織のネットワークに接続しているわけではない
- デスクトップ コンピューターよりも紛失や盗難に遭いやすい
- ほとんどの場合、データがバックアップされず、デバイスが障害や紛失に遭うと、データが失われる可能性がある
- 侵害されたコンピューターが内部ネットワークに接続される

- **悪意のあるネットワークに接続するモバイル コンピューター :** 組織のネットワークは保護され、脅威から守られているでしょうが、モバイル コンピューターは頻繁に組織の外のネットワークに接続します。ある個人のホーム ネットワークは安全かもしれませんが、組織のコンピューターは、空港やカフェなどの公共の場所にある Wi-Fi アクセス ポイントに接続する場合があります。悪意のあるハッカーが運営する Wi-Fi アクセス ポイントは、ネットワーク トラフィックをキャプチャしたり、コンピューターを侵害しようと Web ブラウザーのセッションにマルウェアを挿入したりする場合があります。
- **組織のネットワークに断続的に接続するモバイル コンピューター :** コンピューターが常に組織のネットワークにいるわけではないため、常に組織のネットワークに接続されていることを想定する、グループ ポリシーなどのツールを使用して、管理することは困難です。

- **データのバックアップ**：モバイル コンピューターのデータは、ほとんどの場合、バックアップされません。コンピューターが組織のネットワークに接続されている場合、ユーザーは、ファイル共有や SharePoint サイトなどの一元的な場所にあるドキュメントを使用する傾向があります。しかし、モバイル コンピューター上のデータは、そのモバイル コンピューターにのみ格納される可能性が高くなります。これは、モバイル コンピューターが紛失、盗難、またはハードウェア障害に遭うと、その組織に 1 つだけのデータのコピーが失われる可能性があることを意味します。
- **モバイル コンピューターは簡単に紛失したり、盗まれたりする**：盗まれたコンピューターを交換するための平均的な費用が、コンピューターの購入金額の 15 倍を超える場合があります。紛失または盗難に遭ったコンピューターに格納されていたデータを、組織で判定するために、高額な費用が必要になります。中には、そのデータがモバイル デバイス上にのみ存在し、そのため組織から失われてしまう場合もあります。
- **侵害されたコンピューターが内部ネットワークに接続される**：マルウェアに感染したモバイル コンピューターは、そのマルウェアを組織内に持ち込む可能性があります。組織では、モバイル コンピューターを、マルウェアを媒介する可能性があるものとして扱う必要があります。

討論：モバイル ユーザーを管理する上での問題とは

次の問題を熟考し、講師とクラスで討論できるように解答を準備します。



質問：あなたの組織では、何人のユーザーがノート PC、タブレット、またはコンバーチブル デバイスを使用していますか。

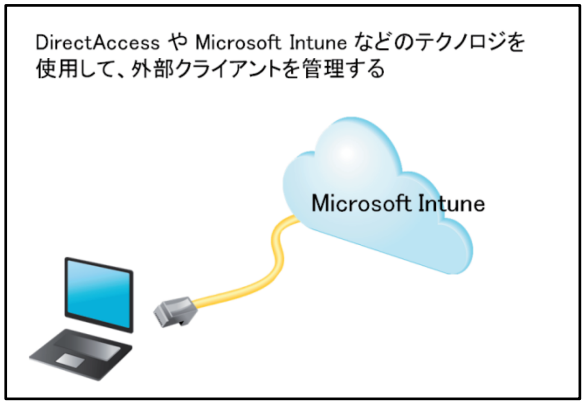
質問：組織内のノート PC、タブレット、またはコンバーチブル デバイスを管理する上で直面した最大の問題は何ですか。

質問：どのくらいの頻度で、リモート ユーザーは自身のコンピューターを組織のネットワークに接続しますか。

質問：リモート ユーザーの管理にどのテクノロジを使用しますか。

外部クライアントを管理するためのソリューション

多くの組織には、組織のネットワークにほとんど接続しないクライアント コンピューターとデバイスがあります。それらは、ホーム オフィスや小規模なブランチ オフィスにあるクライアントであったり、勤務時間のほとんどを外出して過ごしているリモート ワーカーのデバイスであったりします。



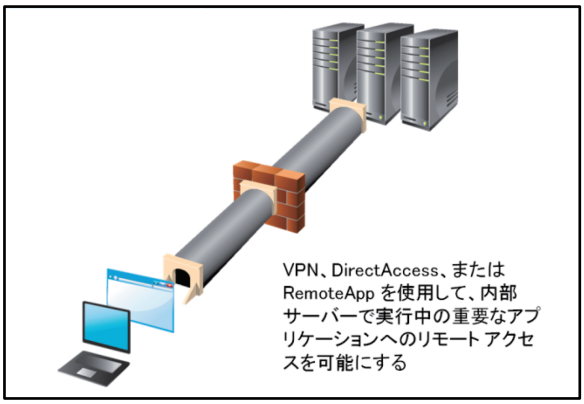
これらのユーザーのコンピューターとデバイスは組織のネットワークに接続しないため、これらを直接管理することは困難です。直接管理には、通常、管理サーバーからクライアント コンピューターへの、断続的ではなく、常時の接続が必要です。クライアント コンピューターが組織のネットワークにいない場合、接続を維持することは困難です。

これらのコンピューターとデバイスを管理することが困難でも、この目的を達成するために使用できる複数のテクノロジがあります。

- **VPN を介した管理 :** VPN テクノロジの一部には、リモート デバイスから内部ネットワークへのアクセスを許可するだけでなく内部ネットワークからリモート デバイスへのアクセスを許可するものもあります。Configuration Manager クライアントなどの一部のクライアント テクノロジでは、VPN 接続を使用して、管理ポリシー、更新プログラム、およびソフトウェアを取得することができます。
- **DirectAccess :** 認証されたコンピューターによる、常にオンの VPN リンクにより、リモート クライアントは、グループ ポリシーやデータを Configuration Manager などの一元的な管理製品から取得することができます。
- **Microsoft Intune :** Microsoft Intune は、組織のネットワークに接続されていないコンピューターを組織が管理できるようにするソリューションを提供します。Configuration Manager を Microsoft Intune に接続し、オンプレミス コンピューター、およびリモート モバイル コンピューターとデバイスの両方の管理を可能にすることもできます。
- **他の MDM ソリューション :** Windows 10 には、モバイル デバイス管理のための公開の規格である、OMA-DM のサポートが含まれます。このプロトコルのサポートにより、Microsoft 以外のモバイル デバイス管理ソリューションによる Windows 10 を実行するコンピューターの管理が可能になります。

リモート データおよびアプリケーションへのアクセスのためのエンタープライズ ソリューション

多くのリモート ワーカーを抱える組織は、エンタープライズ アプリケーションとエンタープライズ データへのアクセスを提供する際に問題に直面します。例えば、組織は、リモート ワーカーに重要なデータへのアクセスや内部サーバーで実行されているアプリケーションへのアクセスを提供しなければならない場合があります。



内部アプリケーションへのリモート アクセスを提供する必要がある組織は、次のテクノロジを活用することができます。

- **VPN または DirectAccess :** 組織は、VPN または DirectAccess を使用して、リモート クライアントにアプリケーションへアクセスを提供します。これには、アプリケーションがリモート コンピューター上で実行されるクライアント コンポーネントを備えており、そのクライアント コンポーネントが VPN または DirectAccess 接続を介してアプリケーションのサーバー コンポーネントに接続できることが必要です。
- **RemoteApp または Azure RemoteApp :** RemoteApp (Windows オペレーティング システムの機能) または Azure RemoteApp により、サーバー上でアプリケーションを安全に実行し、リモート コンピューターでアプリケーションの実行結果のみを表示することができます。RemoteApp は、特別なクライアント ソフトウェアを必要とせず、Windows 10 に組み込みのリモート デスクトップ接続ソフトウェアを使用します。Azure RemoteApp は、インターネットからダウンロードできる特別なクライアント ソフトウェアを必要とします。
- **Web アプリケーション プロキシを介した内部アプリの公開 :** 境界ネットワーク上の Web アプリケーション プロキシを介して、内部の Web アプリケーションを保護された方法でインターネット上のクライアントに公開することができます。

- **Azure Rights Management (RMS) :** 組織は、Azure RMS を使用して、インターネット経由でクライアントに転送される必要がある重要なデータを保護することができます。データが横取りされた場合、データを横取りしたユーザーが、そのデータにアクセスできるように構成された人物のアカウント資格情報を持っていない限り、データへのアクセスは許されません。
- **ワーク フォルダー :** 内部と外部のネットワーク上で、デバイスがドメインに参加しているかどうかに関わらず、ユーザーは自分の作業ファイルにアクセスできます。Web アプリケーション プロキシを介して公開されている場合は、外部のネットワーク上のクライアントもワーク フォルダーを使用することができます。ワーク フォルダーをホストするサーバーに接続すると、ファイルは同期され、オフライン状態のデバイスがサーバーへの接続を再確立すると、変更点がデバイスに同期されます。同じ名前を持つ複数のファイルとの競合がある場合は、競合ファイルのコピーが作成され、名前が追加されます。それらのコピーには、競合している変更がおこなわれたクライアントの名前が含まれます。

レッスン 3
エンタープライズでのデバイスのサポート

業務の遂行に Android や Apple iOS などのモバイル デバイス オペレーティング システムを使用する人々が増えています。これにより、多くの組織で、業務を実行するために、最適なプラットフォームとして、これらのデバイスを使用したいというユーザーの要求とのバランスをとらなければならないという問題が発生します。エンタープライズの IT 部門の観点からは、これは、ユーザーが安全に重要なデータとアプリケーションにアクセスできるようにする方法を開発することを意味します。

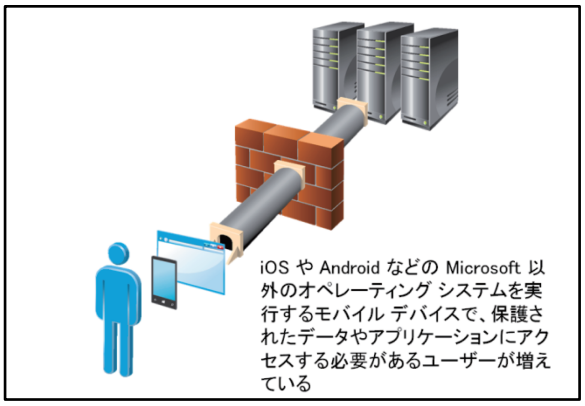
目的

このレッスンにより、次のことを習得できます。

- さまざまなオペレーティング システムを実行するモバイル デバイスをサポートするための考慮事項について、討論することができます。
- さまざまなオペレーティング システムを実行するモバイル デバイスに保護されたデータ アクセスを提供するソリューションを列挙することができます。
- さまざまなオペレーティング システムを実行するモバイル デバイスからエンタープライズ基幹業務 (LOB) アプリケーションへのアクセスを実現するためのソリューションを説明することができます。

デバイスをサポートするための考慮事項

割り当てられたデスクトップやノート PC 以外のデバイスを使用して、業務を遂行するエンタープライズの従業員が増えています。これらのデバイスは、ほとんどの場合、iOS または Android を実行しています。これにより、組織の IT 部門は、最適なプラットフォームを使用したいというユーザーの要求と、承認された人物とデバイスのみが重要なアプリケーションやデータにアクセスできるようにするという組織の要件のバランスをとるという問題に直面します。



モバイル デバイス サポート ポリシーを検討する際、組織は次を考慮する必要があります。

- そのデバイスは、ユーザーが所有していますか、それとも組織が所有していますか。
- ユーザー所有のデバイスによる重要なアプリケーションやデータへのアクセスを許可する必要がありますか。
- デバイスの所有者が IT 部門による管理を同意した場合のみ、ユーザー所有のデバイスで重要なアプリケーションやデータへアクセスすることを許可すべきでしょうか。
- デバイスを紛失したり、ユーザーの雇用が終了したりした場合、デバイスに格納されたデータを保護するために、組織はどのような対処をとることができますか。

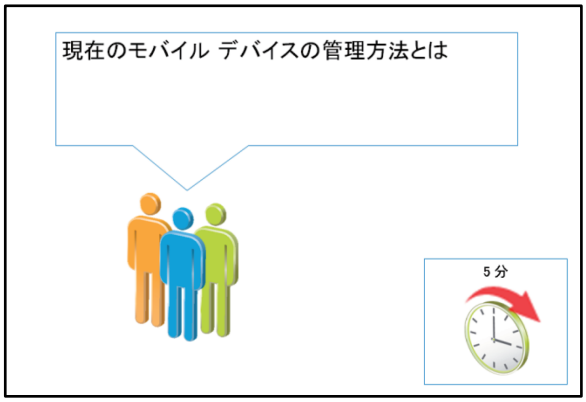
モバイル デバイスは、ノート PC のような大きなデバイスよりも、紛失や盗難に遭う可能性が高くなります。現在のモバイル デバイスは、10 年前に組織のほとんどのファイル サーバーが格納できた量よりも大量のデータを格納できるため、これは問題となります。そのため、モバイル デバイスの損失は、潜在的には、数ギガバイトの組織のデータが公開されたことを意味します。

モバイル デバイスに重要なデータへのアクセスを許可する組織は、次の状況を管理するためのポリシーを用意する必要があります。

- ユーザーがデバイスを紛失、または置き忘れた。
- デバイスの所有者であるユーザーの雇用が終了した。

討論 : 現在のモバイル デバイスの管理方法とは

次の問題を熟考し、講師の指導の下で、クラスで討論できるように解答を準備します。



質問 : あなたの組織では、承認されたモバイル デバイスの承認リストを指定するポリシーが用意されていますか。

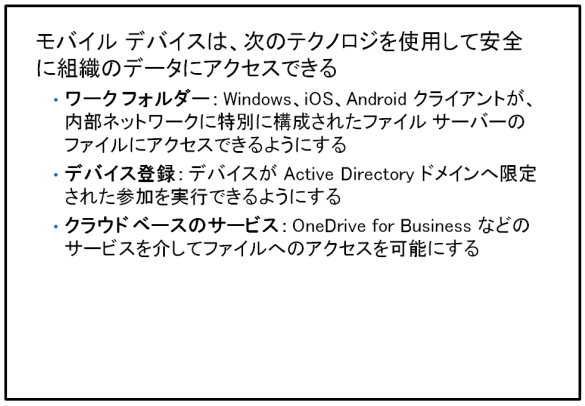
質問 : あなたの組織のモバイル デバイス ユーザーは、どのオペレーティング システムを使用していますか。

質問 : あなたの組織では、モバイル デバイス ユーザーに組織内部の重要なデータとアプリケーションへのアクセスを許可していますか。

質問 : モバイル デバイスにマルウェアが存在しないように、またユーザーがそのデバイスを紛失した場合や、ユーザーが組織を辞めた場合、リモート ワイプを実行できるようにするため、どのようなモバイル デバイス管理テクノロジを使用していますか。

デバイスにデータ アクセスを提供するソリューション

Android および iOS オペレーティング システムを実行するモバイル デバイスに内部の重要なデータへのアクセスを提供する方法は、増えています。次のものがあります。



- **ワーク フォルダー :** さまざまなコンピューターとデバイス間でユーザー データを同期することができます。ワーク フォルダーには、2 つの主要な機能があります。
  - ファイルは、クラウドではなく、内部のファイル サーバーに格納されます。
  - 複数のコンピューターとデバイスが、あらゆる場所からファイルを同期することができます。

ワーク フォルダーは、Windows 7、Windows 8.1、および Windows 10 を実行するコンピューターでサポートされます。ワーク フォルダーは、iOS 8 以降と Android 4.4 以降を実行するデバイスでもサポートされます。

- **デバイス登録 :** Windows 8.1 ではワークプレース参加と呼ばれた、デバイス登録は、ドメイン メンバーになることができないデバイスでも識別できるようにすることで、アプリケーションへのアクセスに対するセキュリティの懸念に対処します。デバイス登録が有効になると、そのデバイスを表すオブジェクトが AD DS に作成されます。デバイス登録が有効なコンピューターにも、認証に使用するための証明書が付与されます。デバイス登録は、iOS および Android デバイス用でもサポートされます。

- **クラウド ベースのサービス :** クラウド ベースのサービスの例としては、Microsoft OneDrive for Business (以前の SkyDrive Pro) があります。OneDrive for Business へのアクセスには、Microsoft Office 365 のアカウントが必要です。
  OneDrive for Business に格納されたファイルも、Azure RMS を使用して保護することができます。
  OneDrive for Business は、Android および iOS デバイス用にもサポートされます。

どちらのテクノロジを使用しても、デバイスが紛失または盗難に遭った場合、アクセスを無効にすることができます。

デバイスにアプリケーション アクセスを提供するソリューション

デバイス登録、RemoteApp、リモート デスクトップなどのさまざまな方法を使用して、モバイル デバイスがアプリケーションに安全にアクセスできるようにします。

次の方法により、モバイル デバイスにアプリケーションへの安全なアクセスを提供
- RemoteApp または Azure RemoteApp
- Remote Desktop
- デバイス登録
- Microsoft Office Online などのクラウド サービス

Azure RemoteApp と RemoteApp

RemoteApp は、表示の仮想化の 1 形態です。RemoteApp では、アプリケーションのユーザー インターフェイスがデバイスに配信され、その間アプリケーション自体は内部ネットワークの RemoteApp サーバー上か、Azure RemoteApp を使用している場合は Azure にホストされる仮想マシンの特別なコレクション上で、実行されます。これは、アプリケーションが保護された環境で実行され、暗号化された接続でアプリケーションの表示がクライアントに配信されることを意味します。RemoteApp クライアントは、Android および iOS デバイスの両方に用意されています。このテクノロジにより、Android や iOS デバイスでは実行できないアプリケーションを、それらのデバイスで表示することができます。

リモート デスクトップ

リモート デスクトップは、単一のアプリケーションではなく、デスクトップ全体をデバイスに配信します。保護されたアプリケーションへのアクセスを提供する方法の 1 つは、組織で仮想デスクトップ インフラストラクチャ (VDI) 環境をプロビジョニングすることです。これにより、iOS および Android を実行するデバイスのユーザーは、Windows 10 オペレーティング システムを実行する仮想マシンにアクセス可能になります。リモート デスクトップ セッション ホスト サーバーにより、適切に構成された Windows Server ホストで実行されるリモート デスクトップ セッションへのアクセスを実現することもできます。

デバイス登録

アプリケーションの認証プロセスの一環として、クレームに対応するアプリケーションでは、デバイス登録が有効化されたデバイスについての情報を使用することができます。クレームに対応するアプリケーションとは、認証に Active Directory Federation Services (AD FS) を使用するアプリケーションです。AD FS によりユーザーが認証されると、AD FS はそのユーザーについての一連の情報を提供します。それらはクレームに含まれます。クレームには、名前、グループ メンバーシップ、その他のユーザーのプロパティが含まれる場合があります。

アプリケーションは、クレームの使用をサポートする必要があります。また、アプリケーションは、AD FS の特定のインスタンスを信頼するように構成される必要があります。アプリケーションは、特別に定義された AD FS サーバーからのクレームのみを信頼します。

クレームに対応するアプリケーションの例としては、Office 365、Windows SharePoint Server、および Microsoft Windows Identity Foundation を使用して開発されたカスタム アプリケーションがあります。これらのアプリケーションのすべてを、AD FS が認証用に提供するクレームを信頼するように、構成することができます。

クラウド サービス

また、クラウド サービス経由でアプリケーションへのアクセスを提供することもできます。その例の 1 つが Microsoft Office Online で、Web ブラウザーを介して、Office アプリの簡易版を提供します。

レッスン 4
IT 管理とサービスのクラウドへの拡張

デバイス管理のインフラストラクチャをオンプレミスからクラウド サービスに移行する組織が増えています。多くの中小規模のエンタープライズでは、Configuration Manager などの複雑な製品を展開して管理するよりも、Microsoft Intune などのクラウド サービスを使用する方が無駄がありません。そうすることで、組織で、管理サーバーのインフラストラクチャの管理だけでなく、それらを所有する必要もなくなります。

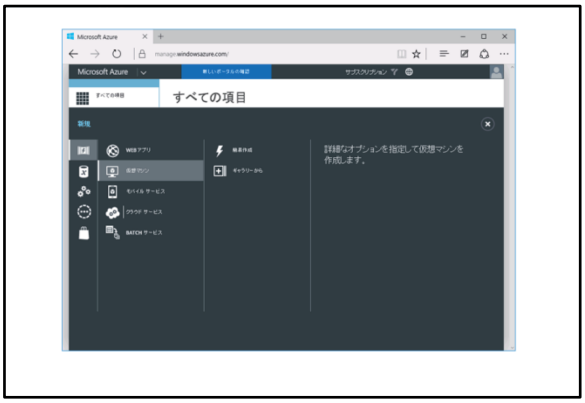
目的

このレッスンにより、次のことを習得できます。

- クラウド サービスで使用可能なアプリケーションとサービスの概要を説明することができます。
- アプリケーション、データ、およびデスクトップの管理用のクラウド ベースのソリューションを説明することができます。
- Enterprise Mobility Suite を説明することができます。
- Windows 10 Enterprise がどのようにクラウド サービスをサポートするかを説明することができます。

クラウド サービスで使用可能なアプリケーションとサービスの概要

今日では、さまざまなクラウド サービスがあり、クラウド サービスは、IaaS、PaaS、および SaaS というカテゴリに分類することができます。



IaaS

Infrastructure as a Service (IaaS) は、組織が仮想マシン、仮想化されたネットワーク、仮想化されたハードウェア デバイスなどの仮想化されたリソースを実行できるようにする、クラウド コンピューティングの 1 形態です。組織における IaaS のメリットは、オンプレミスの仮想化インフラストラクチャを必要とすることなく、組織が仮想マシンを実行できることです。

PaaS

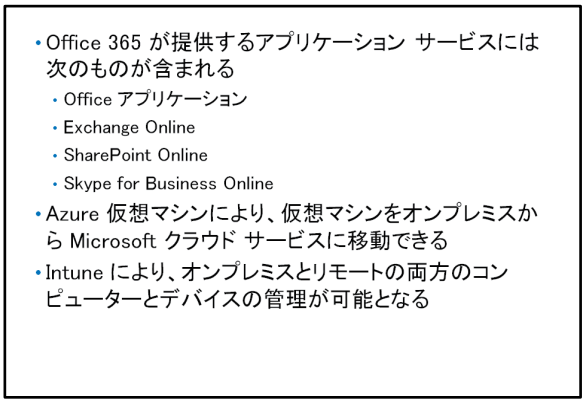
Platform as a Service (PaaS) は、Web アプリケーションやデータベースのホストなどのプラットフォームへのアクセスを提供する、クラウド コンピューティングの 1 形態です。PaaS のメリットは、Web アプリケーションやデータベース サーバー ソフトウェアをホストするオペレーティング システムを管理する必要なしに、組織が Web アプリケーションやデータベースを展開できることです。

SaaS

Software as a Service (SaaS) は、クラウド コンピューティングの 1 形態で、SaaS ではユーザーがクラウドで実行中のソフトウェアにアクセスできます。Office Online は SaaS の一例で、ユーザーは Web ブラウザーを介して Office アプリのさまざまなバージョンにアクセスすることができます。SaaS のメリットは、アプリケーションの維持と更新はクラウド プロバイダーに任せて、ユーザーがそれらのアプリケーションにアクセスできることです。

アプリケーション、データ、およびデスクトップの管理用のクラウド ベースのソリューション

Microsoft では、組織がアプリケーション、データ、およびデスクトップの管理操作に使用できる、多数のさまざまなクラウド ベースのソリューションを提供しています。



Office 365

Office 365 は、組織がオンプレミス インフラストラクチャの拡張や置き換えに使用できる、アプリケーションとサービスのスイートです。Office 365 には次の要素が含まれます。

- **Office アプリケーション :** Office 365 のライセンスが割り当てられたユーザーは、Office 365 ProPlus にアクセスすることができます。これには、Word、Excel、PowerPoint、Outlook などの広く使用されている Office アプリケーションが含まれます。ユーザーは、これらのアプリケーションの Web ベースのバージョンである、Office Online にもアクセスすることができます。
- **Exchange Online :** Exchange Online は、クラウドにホストされた Exchange の機能を提供します。組織は、オンプレミスの Exchange 環境と関連付けて Exchange Online を展開することができます。または、組織のオンプレミスの Exchange メールボックスをすべて、Exchange Online に移行することができます。
- **SharePoint Online :** SharePoint Online は、クラウドのホストされた状態で、オンプレミスの SharePoint 環境のすべての機能を提供します。組織は、オンプレミスの SharePoint 環境全体を SharePoint Online に移行することができます。または、オンプレミスの環境と関連付けて、SharePoint Online を展開することができます。
- **Skype for Business Online :** Skype for Business Online (以前の Lync Online) は、オンプレミスの Skype for Business 環境ではなく、Microsoft クラウド サービス にホストされた、インスタント メッセージ、音声およびビデオ会議の機能を組織が使用できるようにします。

Azure 仮想マシン

Azure 仮想マシン は、仮想マシンを Azure にホストできるようにします。Azure Site Recovery により、組織は、仮想マシンを Azure にレプリケートして Azure を障害回復サイトとして構成します。また、オンプレミスの仮想マシンと物理サーバーを移行し、Azure 仮想マシンとして実行することもできます。

Intune

Intune は、組織がコンピューターとモバイル デバイスの構成の管理に使用できるクラウド サービスです。Intune を使用して、次のことをおこなうことができます。

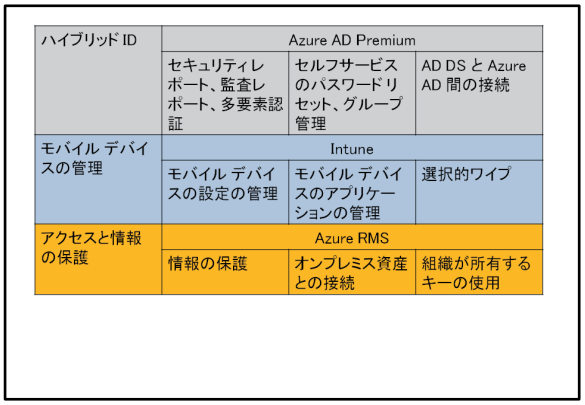
- ソフトウェアの展開
- ソフトウェア更新プログラムの展開
- マルウェア対策ポリシーの管理
- Windows ファイアウォール ポリシーの管理
- ソフトウェアとハードウェアのインベントリの生成
- ソフトウェア ライセンスの管理
- セルフサービスのソフトウェア展開機能の提供
- パスワード ポリシーの適用

- Exchange ActiveSync を使用するデバイス向けの電子メール アクセスの管理
- パスコードのリセット、ロック、またはモバイル デバイスのワイプ

Enterprise Mobility Suite とは

Enterprise Mobility Suite (EMS) は、Microsoft クラウド サービスのコレクションで、次をサポートします。

- ハイブリッド ID
- モバイル デバイスの管理
- アクセスと情報の保護



ハイブリッド ID

ハイブリッド ID 機能は、Azure AD Premium で提供されます。これには、セキュリティ レポートと監査レポートの生成機能が含まれます。ユーザーは、EMS 用に構成されたデバイスにサインインする際、多要素認証を使用できます。ユーザーはセルフサービスのパスワードのリセットを実行することができ、管理者はグループの管理ができます。EMS は、オンプレミス Active Directory 環境と Azure AD 間の接続もサポートします。

モバイル デバイス管理

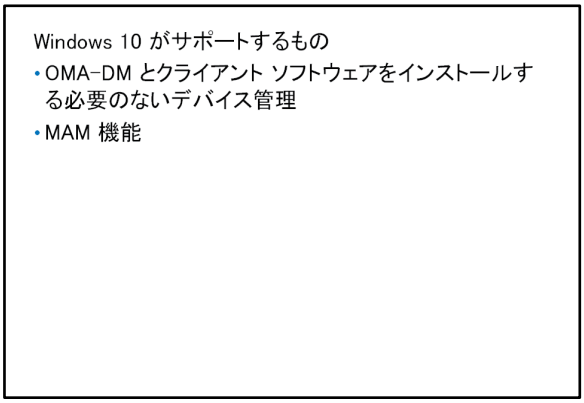
Enterprise Mobility Suite のモバイル デバイス管理には、モバイル デバイスの設定の管理、モバイル デバイスのアプリケーションの管理、データの選択的ワイプの実行など、すべての Intune 機能が含まれます。

アクセスと情報の保護

Enterprise Mobility Suite のアクセスと情報の保護機能は、Azure RMS を使用して、情報の保護を提供します。例えば、組織は、Azure RMS を使用して、ドキュメントが電子メールで組織の外のサード パーティに送信された場合でも、そのドキュメントを開くことができるのは組織のアカウントを持つユーザーのみとすることができます。組織は、Microsoft が提供した RMS キーではなく、組織が所有する RMS キーを使用することもできます。

Windows 10 Enterprise がクラウド サービスをサポートするしくみ

Windows 10 は、Microsoft クラウド サービスと他の組織が提供する管理サービスの両方を統合します。OMA-DM は、クライアント ソフトウェアをインストールする必要なく、デバイス管理ができる、クライアント管理プロトコルです。
Windows 10 は OMA-DM をサポートします。これは、他の組織が提供する管理サービスで OMA-DM を使用して、次のタスクが実行できることを意味します。



- Windows ストアからアプリを直接インストールする。
- オフライン ストア アプリとライセンスを展開する。
- LOB アプリ (ストア以外のアプリ) を展開する。

- デバイスのすべてのアプリの一覧を作る (ストアとストア以外のアプリ)。
- ユーザーのすべてのアプリの一覧を作る (ストアとストア以外のアプリ)。
- ユーザーのすべてのアプリをアンインストールする (ストアとストア以外のアプリ)。
- デバイスのすべてのユーザーに対してアプリをプロビジョニングする。
- デバイスが最新状態を保つように自動更新ポリシーを構成する。
- インストールされていない必須の更新プログラムの一覧を生成する。
- デバイスごとの更新承認の一覧を指定する。
- 更新の展開が自動的におこなわれるように、エンド ユーザーのライセンス契約をエンドユーザーの代わりに承認する。

エンタープライズ データ保護により、組織は、組織のデータを操作できるアプリケーションと、操作がおこなわれるしくみを指定することができます。例えば、特定のアプリケーションでのみデータを開くことができるようにデータにタグ付けしたり、そのアプリケーションから他のアプリケーションにデータをコピーできないようにタグ付けしたりすることができます。エンタープライズ データ保護は、Intune などのサービスを介して使用できるモバイル アプリケーション管理 (MAM) テクノロジに依存します。

演習 : エンタープライズでの Windows 10 とデバイスの管理計画

シナリオ

Windows 10 デスクトップとモバイル デバイスを管理するのに適したテクノロジを決定する必要があります。シナリオは、練習で説明します。

目的

この演習により、次のことを習得できます。

- デスクトップとモバイル デバイスを管理するための最も効率的な方法を決定することができます。

演習のセットアップ

予定所要時間 : 15 分

これは机上の演習であるため、仮想マシンは必要ありません。

練習 1 : シナリオの読み取り

シナリオ

A. Datum 社は、国際営業チーム用に Windows 10 Enterprise Edition を実行する 200 台のノート PC を購入しました。現在、A. Datum 社では、Microsoft 以外の構成管理ソリューションを使用しています。Windows 10 への移行に伴い、管理では、Microsoft 以外の構成管理ソリューションの使用から移行して、Microsoft クラウド サービスで提供される機能を活用したいと考えています。

A. Datum 社は、営業チームのメンバーが使用している、いくつかのブランチ オフィスを閉じる予定です。これらのブランチ オフィスは、クラウドへの移行が必要な、多くの仮想マシンをホストしています。技術者が各ブランチ オフィスにソフトウェアをインストールするのではなく、管理では、クラウドから営業チームが使用するノート PC へソフトウェアを展開することを望んでいます。Microsoft 以外の製品でソフトウェアとハードウェアのインベントリを収集するのではなく、管理では、Microsoft クラウド サービスによりソフトウェアとハードウェアのインベントリ機能が提供されることを希望しています。

マーケティング チームの一部のメンバーは、ノート PC の使用を完全にやめ、メンバー自身の iOS または Android ベースのタブレットを使用することを望んでいます。この移行を阻む要素は、A. Datum 社で使用されている、多くの重要なビジネス アプリケーションが、Windows デスクトップおよび Windows Server のオペレーティング システムでのみ機能することです。

管理の最終的な懸念は、重要なドキュメントが A. Datum 社の社外の人々に誤って電子メールで送信される可能性があることです。管理では、適切な Microsoft クラウド ソリューションを活用して、重要な情報には A. Datum 社の資格情報を持つユーザーのみがアクセスできるように、情報の分散を制限することを望んでいます。

質問 : A. Datum 社のユーザーが作成したドキュメントを、A. Datum 社の他のユーザーのみが開くことができ、組織の外の人には開くことができないようにするためには、どのようなテクノロジを使用する必要がありますか。

質問 : オンプレミスの仮想化環境の使用停止後、組織の仮想マシンをホストするためには、どのような種類のクラウド サービスを使用する必要がありますか。

質問 : どのようなテクノロジを使用して、iOS と Android ベースのタブレットのユーザーに対して、Windows オペレーティング システムを実行するコンピューターでのみ実行されるアプリケーションへのアクセスを可能にすることができますか。

質問 : どのようなクラウド ベースのテクノロジを使用して、Windows 10 を実行する営業チームのノート PC に、アプリケーションを展開することができますか。

質問 : どのようなクラウド ベースのテクノロジを使用して、Windows 10 を実行する営業チームのノート PC で、ソフトウェアとハードウェアのインベントリを実行することができますか。