第 7 章
リモート アクセス ソリューションの管理

目次

概要

この章では、さまざまなリモート アクセス ソリューションと、それらを Windows 10 オペレーティング システムを実行しているコンピューターと同期させる方法について説明します。

Windows 10 と Windows Server 2012 R2 の機能により、企業のリソースにリモート接続する Windows 10 ユーザーに対して、ほぼシームレスなエクスペリエンスが実現します。仮想プライベート ネットワーク (VPN)、DirectAccess、および RemoteApp の機能を利用して、ユーザーがどこから接続しても作業環境にアクセスできるようにすることができます。

目的

この章により、次のことを習得できます。

- リモート アクセス ソリューションを説明することができます。
- Windows 10 で DirectAccess を実装することができます。
- リモート ネットワークへの VPN アクセスを構成することができます。
- Windows 10 で RemoteApp をサポートすることができます。

レッスン 1
リモート アクセス ソリューションの概要

DirectAccess や VPN など、さまざまな形式のリモート アクセスを実装することができます。組織が実装できるリモート アクセス テクノロジの種類は、組織のビジネス要件によって異なります。
複数のリモート アクセス テクノロジを異なるサーバー上で展開する組織もあれば、同じサーバー上で展開する組織もあります。このレッスンでは、このようなさまざまなリモート アクセス テクノロジについて説明します。

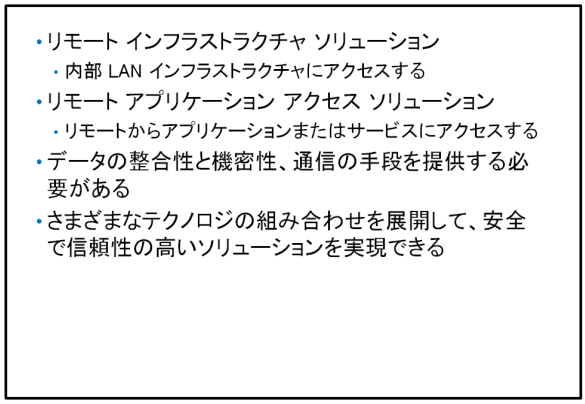
目的

このレッスンにより、次のことを習得できます。

- Windows 10 のリモート アクセス ソリューションの種類を説明することができます。
- リモート インフラストラクチャ アクセスを説明することができます。
- リモート アプリケーション アクセスを説明することができます。

リモート アクセス ソリューションの種類

リモート アクセス テクノロジは、さまざまな場所から組織のインフラストラクチャに安全にアクセスできるようにするためのさまざまなソリューションを提供します。組織は通常、ローカル エリア ネットワーク (LAN) をその組織自体が完全に所有して保護していますが、サーバー、共有、およびアプリへのリモート接続は、多くの場合、インターネットなど、組織から見ると保護や管理がされていないネットワーク インフラストラクチャを介しておこなう必要があります。このようなリモート接続には、データの整合性と機密性および通信手段を保護する方法を含める必要があります。

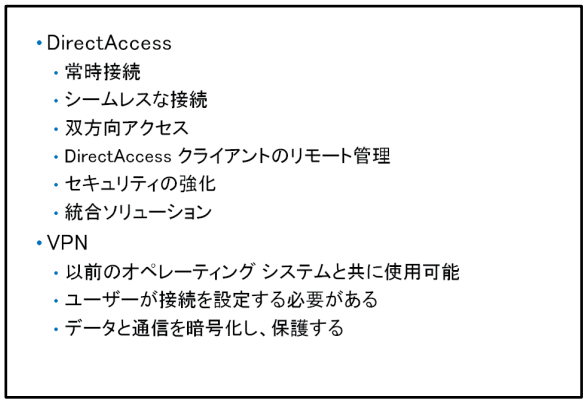


適切な種類のリモート アクセス テクノロジを選択すると、組織のニーズ、インフラストラクチャ、および技術レベルに応じた最適なソリューションを展開できます。例えば、管理者がインターネット経由でサーバーを管理する必要がある組織では DirectAccess を展開し、内部アプリケーションをインターネットに公開する必要がある場合は、同時に Web アプリケーション プロキシを展開します。以前のテクノロジを引き続きサポートする必要がある組織では、今後も VPN ソリューションが最適な選択肢になる場合もあります。Azure などのクラウド サービスを統合した組織では、Azure RemoteApp や Azure App Service の Web Apps 機能を使用して、エンド ユーザーに安全で信頼性の高いアプリ ソリューションを提供できます。最終的に、多くの組織では、リモート アクセス テクノロジを組み合わせて使用して、ニーズに合った総合的で包括的なリモート アクセス ソリューションを提供しています。

このようなテクノロジの開発や成長に伴い、インターネットへのリモート接続が当たり前になってきています。今日では、組織とリモート ユーザーがインターネットに接続している場合、単純にこの相互接続を使用してリモート ユーザーが組織のネットワークにアクセスできるようにすることができます。ただし、このような接続の使用は本質的に安全ではありません。安全な通信を提供するためには、データや制御パケットを暗号化する必要があります。これは、例えば、VPN、DirectAccess、RemoteApp、Web アプリケーション プロキシ、Azure などで実現でき、今日ではほとんどの状況でこれらのテクノロジのすべてが使用されています。

リモート インフラストラクチャ アクセスの概要

次に示す各オプションは、組織がさまざまなシナリオでリモート サイトのオフィスから、またはインターネットから内部リソースにアクセスするために使用できるテクノロジを表しています。



DirectAccess

DirectAccess を使用すると、リモート ユーザーは、電子メール サーバー、共有フォルダー、内部 Web サイトなどの組織のリソースに安全にアクセスができます。また、DirectAccess によってユーザーから見た場合、オフィスの内部からでも外部からでも同じようにコンピューターが組織に接続されるため、モバイル ワーカーの生産性が向上します。ユーザーは、インターネットに接続できればどこからでも、組織のオフィスにある自分のワークステーションにリモート デスクトップ接続することもできます。新しい統合された管理エクスペリエンスにより、DirectAccess と以前の VPN 接続の両方を 1 つの場所で構成できます。DirectAccess のその他の機能拡張として、展開の簡略化やパフォーマンスとスケーラビリティの改善があります。

また、DirectAccess には次のメリットがあります。

- **常時接続 :** ユーザーがクライアント コンピューターをインターネットに接続するときは、必ずクライアント コンピューターはイントラネットにも接続されます。この接続性により、リモート クライアント コンピューターは容易にアプリケーションにアクセスして更新することができます。また、イントラネット リソースが常に使用可能になり、ユーザーは企業のイントラネットにいつでもどこからでも接続できるので、生産性とパフォーマンスが向上します。
- **シームレスな接続 :** DirectAccess により、クライアント コンピューターがローカルかリモートかに関わらず、一貫した接続性を提供します。これにより、煩わしい接続のオプションやプロセスをおこなうことなく、ユーザーは仕事に集中できます。この一貫性により、ユーザーのトレーニングのコストが削減され、サポートが必要なインシデントも減ります。
- **双方向アクセス :** DirectAccess クライアントはイントラネット リソースにアクセスでき、管理者はイントラネットから DirectAccess クライアントにアクセスできるように DirectAccess を構成することができます。つまり、DirectAccess を双方向に構成できます。これにより、クライアント コンピューターでは常に最新のセキュリティ更新がおこなわれ、ドメイン グループ ポリシーが実施されるため、企業のイントラネット ユーザーとパブリック ネットワークのユーザーの差がなくなります。この双方向のアクセスは、次のメリットももたらします。
    - 更新時間の削減
    - セキュリティの強化
    - 更新の失敗率の低下
    - コンプライアンスの監視の向上
- **DirectAccess クライアントのリモート管理 :** DirectAccess クライアントのリモート管理機能のみを有効にすることができます。DirectAccess クライアント構成ウィザードのこの新しいサブオプションは、クライアント コンピューターの管理に使用するポリシーの展開を自動化します。DirectAccess クライアントのリモート管理では、ユーザーがファイルまたはアプリケーションにアクセスするためにネットワークに接続できるようにするポリシー オプションを実装しません。DirectAccess クライアントのリモート管理は片方向で、管理を目的とする着信限定アクセスのみを提供します。

- **セキュリティの強化 :** 従来の VPN とは異なり、DirectAccess では、ネットワーク リソースへのアクセスを制御する複数のレベルを提供します。この厳しい制御により、セキュリティ設計者は、指定されたリソースにアクセスするリモート ユーザーを精密に制御することができます。きめ細かいポリシーを使用して、DirectAccess が使用できるユーザーと、そのユーザーが DirectAccess でアクセスできる場所を定義することができます。インターネット プロトコル セキュリティ (IPsec) 暗号化が DirectAccess の保護に使用されているため、ユーザー間の安全な通信が保証できます。
- **統合ソリューション :** DirectAccess は、サーバーとドメインの分離を統合しました。その結果、イントラネットとリモート コンピューター間のセキュリティ、アクセスおよび正常性の要件のポリシーを統合できます。

VPN

VPN 接続を使用すると、社外 (例えば、自宅や客先、公共無線アクセス ポイント) で仕事をしているユーザーが、インターネットなどのパブリック ネットワークを提供するインフラストラクチャを利用して、組織のプライベート ネットワークのサーバーにアクセスすることができます。ユーザーから見た場合の DirectAccess と VPN の相違点は、DirectAccess を使用する場合、クライアントはインターネットから内部ネットワークに自動的に接続されることです。一方、VPN を使用する場合、クライアントは VPN クライアント ソフトウェアを起動し、VPN 接続を開始し、認証と承認のために VPN サーバーが必要とする資格情報を提供する必要があります。論理的にはデータが専用のプライベート リンクで送信されるかのように見えるため、共有ネットワークかパブリック ネットワークかという実際のインフラストラクチャの区別は必要ありません。

リモート アクセス サーバーを Windows Server 2012 R2 オペレーティング システムに移行し、クライアント コンピューターを Windows 10 に移行すると、組織は VPN テクノロジを DirectAccess に置き換えることができます。ただし、引き続き VPN テクノロジをリモート アクセスに使用する組織のために、Windows 10 にはオプションとして VPN 接続が含まれています。

リモート アプリケーション アクセスの概要

VPN と DirectAccess は、エンド ユーザーが組織のネットワーク インフラストラクチャに安全に接続する方法を提供しますが、全体的にセキュリティで保護された通信が確立された後に接続してソフトウェアを実行するテクノロジもあります。このようなテクノロジの多くは、環境全体を提供するのではなく、単にユーザーにリモートでアプリを提供するだけです。別の選択肢として、Azure による Software as a Service (SaaS) を使用する方法があります。

リモート デスクトップ

リモート デスクトップ サービス (以前のターミナル サービス) は、ユーザーに完全なリモート デスクトップ エクスペリエンスへのアクセスを提供します。このシナリオでは、ユーザーは、ローカルのリモート デスクトップ接続 (RDC) クライアントを介してリモート セッションに安全に接続します。認証されると、まるでローカルでサインインしたかのように完全なデスクトップがユーザーに表示されます。クライアント マシンは、キーボード操作とマウスの動きをサーバーに送信し、画面のイメージがクライアント マシンに返送されます。ユーザーは、リモート デスクトップ セッション ホスト (RD セッション ホスト) サーバー上で実行されているアプリケーションに、ローカルで実行されているかのようにアクセスできます。各ユーザーが独自のプライベート セッションを確立するため、同じ RD セッション ホスト サーバーに接続している他のユーザーに影響を与えることはありません。

リモート デスクトップにアクセスするには、接続しているユーザーのユーザー アカウント (またはドメイン グローバル グループ) を、接続しているコンピューターの Remote Desktop Users グループに追加する必要があります。既定では、このグループにはメンバーがないため、ユーザーのアカウントがローカルの Remote Desktop Users グループに追加されるまで、ユーザーはリモート デスクトップ接続をおこなうことはできません。ただし、最初の RDS 展開時にこれを構成することができます。

注 : 標準ユーザーには、ローカルでもリモートでもドメイン コントローラーにサインインする権限はありません。ドメイン コントローラーで標準ユーザーを Remote Desktop Users グループに追加しても、これは変わりません。標準ユーザーがドメイン コントローラーにリモートで接続するには、標準ユーザーに、ドメイン コントローラーにサインインする権限を付与し、Remote Desktop Users グループに追加する必要があります。

RD セッション ホストの役割をサーバーにインストールすると、ローカル コンピューターへのリモート デスクトップ接続が自動的に有効になり、アクセスを許可されたユーザーがローカルの Remote Desktop Users グループに追加されます。RD セッション ホストの役割をインストールしていない場合でも、リモート接続を許可するようにシステム プロパティを変更することで、Windows ベースのオペレーティング システムへのリモート デスクトップ アクセスを有効にすることができます。既定では、この方法による接続は管理者に制限されており、許可される同時接続は 2 つのみです。コントロール パネルの [システムのプロパティ] 項目を使用してリモート接続を許可し、リモートで接続できるユーザーを選択できます。

リモート デスクトップは、POS 端末などの単一タスクの作業者やデータ入力作業者に最適です。このようなシナリオでは、すべての作業者に一貫性のあるデスクトップ エクスペリエンスを提供することが重要です。また、リモート デスクトップは帯域幅が制限される場合でも十分に実行できるため、IT サポートが制限される可能性のあるブランチ オフィスに最適なソリューションです。リモート デスクトップは通常、シン クライアントで採用されます。リモート デスクトップのもう 1 つの一般的な使用方法は、ユーザーが社内の自分のデスクトップにアクセスできるようにすることです。例えば、ユーザーは自宅から自分のワークステーションに接続して仕事をすることができます。

Web アプリケーション プロキシ

Web アプリケーション プロキシは、Windows Server 2012 R2 で新しく導入された、リモート アクセスの役割サービスです。この役割サービスは、リバース Web プロキシとして機能することで、組織のネットワークにリモートで接続しているユーザーが組織内部の Web アプリケーションにアクセスできるようにします。Web アプリケーション プロキシは、Active Directory フェデレーション サービス (AD FS) を使用してインターネット ユーザーを事前認証し、要求に対応するアプリケーションを発行するための AD FS プロキシとして機能します。

AD FS は、ユーザーにシングル サインオン (SSO) 機能を提供します。SSO により、ユーザーは組織の Web アプリケーションにアクセスするために資格情報を 1 回入力すれば、残りのセッションでは組織の Web アプリケーションにアクセスするときに資格情報の入力を求められません。Web アプリケーション プロキシの構成が完了すると、AD FS 事前認証を使用する要求に対応するアプリケーションと、パススルー事前認証を使用する Web アプリケーションのどちらも発行することができます。

一般的なシナリオでは、Web アプリケーション プロキシ サーバーは、2 台のファイアウォール デバイス間の境界ネットワークに配置されます。AD FS サーバーと発行されるアプリケーションは、ドメイン コントローラーとその他の内部サーバーとともに組織のネットワーク内に配置され、2 番目のファイアウォールで保護されます。このシナリオでは、インターネット上のユーザーが組織のアプリケーションに安全にアクセスすることができます。同時に、このシナリオでは、組織の IT インフラストラクチャをインターネット上のセキュリティの脅威から保護することができます。

RemoteApp

RemoteApp プログラムは RDS を介してリモートにアクセスしますが、エンド ユーザーのローカル コンピューターで実行しているかのように見えます。これらのアプリケーションは、ローカルにインストールされたアプリケーションと同じように、スタート メニューに表示されます。Windows 10 を実行しているコンピューターでは、RemoteApp プログラムはタスク バーにピン留めすることができ、リモート デスクトップ ロゴのアイコン オーバーレイによって識別されます。RemoteApp を構成するには、コントロール パネルの [RemoteApp とデスクトップ接続] で Web フィードの URL を指定します。このアドレスの形式は、https://ServerFQDN/rdweb/feed/webfeed.aspx です。ここで、ServerFQDN は RD Web アクセス サーバーの完全修飾ドメイン名 (FQDN) です。

注 : コントロール パネルの [RemoteApp とデスクトップ接続] にセキュリティで保護された URL を設定するには、Secure Sockets Layer (SSL) 証明書が必要です。

RemoteApp は、従来のデスクトップ コンピューターを使用しているユーザーにとって最適な選択肢です。これにより、ユーザーはローカルにインストールされたアプリケーションと同じようにリモート アプリケーションを操作することができます。サーバーでアプリケーションを実行することで、アプリケーションをローカルにインストールできないという互換性の問題が回避されます。RemoteApp は、一元的に管理する必要があるアプリケーションやユーザーの PC では対応できないコンピューティング要件が高いアプリケーション (例えば、大量の RAM を必要とするアプリケーションや集中的なグラフィック処理を必要とするアプリケーション) に適しています。

Azure RemoteApp

RemoteApp は、モバイル デバイスを使用するユーザーにも最適な選択肢です。現代の従業員の Bring Your Own Device (BYOD) 機能全体の一部として、RemoteApp はデバイス自体にビジネス ソフトウェアを提供することができます。ただし、オンプレミスでない場合や、RemoteApp を提供するサーバーと同じ LAN 上にない場合は、セキュリティだけではなく、可用性においてもさまざまな問題があります。

Azure RemoteApp は、デバイスがインターネットに接続できればどこからでもソフトウェアを使用可能にすることができます。ソフトウェアを社外から使用できるようにするには、多くの場合、手間のかかる高度な作業を要しますが、プロセスをクラウドへ移動することによってこの作業は大幅に削減されます。また、Azure には多くのメリットもあります。Windows 10 では、デバイスを Azure Active Directory (Azure AD) に参加させ、そのデバイス上のさまざまな Azure RemoteApp プログラムに SSO を適用することができます。RemoteApp プログラムごとにサインインする必要はありません。スタート メニューの電子メール アプリがユーザーのアカウント資格情報を保存するのと同様に、Azure AD を最初に使用すると、ユーザーのアカウント資格情報がローカルの資格情報ストアに保存されるためです。

Web Apps

今日では、ユーザー アプリケーションと組織のアプリケーションの間で、多くのビジネス レベルの処理、例えば、データベース サーバーによるデータの追加、変更、削除などが、Web ポータルを介しておこなわれます。そのため、ソフトウェアを使用するには、それが非常に高度なソフトウェアであっても、必要なのはインターネットへの接続と互換性のある Web ブラウザーのみです。処理はクライアント デバイスからサーバーに移動するため、これは組織にとって大きなメリットとなります。クライアントに必要なのはブラウザーのみで、組織は各クライアントにソフトウェアを展開する必要も、クライアントの種類に合わせて異なるバージョンのソフトウェアを用意する必要もありません。

Web アプリケーション プロキシと同様に、組織の Web サーバー インフラストラクチャで Web アプリケーションを開発することができます。ただし、この場合も、Web アプリケーションをリモートで社外に提供するのは高度なタスクであり、厳重なセキュリティと可用性の変更が必要になります。Web Apps により、組織が所有する多くのインフラストラクチャが必要なくなるため、このようなインフラストラクチャを設計、維持するための複雑な処理の多くが不要になります。開発者は、Azure ポータルから新しい Web Apps をすばやく変更または展開できるため、新しいまたは変更した Web アプリをエンド ユーザーに渡すまでにかかる時間が削減されます。さらに、エンド ユーザーは、アプリをローカルにインストールしなくても、インターネット接続を使用してどこでも自分のモバイル デバイスを使用できます。

知識の確認

質問	
VPN よりも DirectAccess を使用する主なメリットは何ですか (2 つ選択します)。	
正しい解答を選択してください。	
	より高速です。
	ユーザーは接続を開始する必要がありません。
	DirectAccess ではより多くのユーザー構成が必要です。
	DirectAccess は内部接続と外部接続を提供します。そのため、ユーザーは内部接続用の接続と外部接続用の接続を個別に覚える必要がありません。
	VPN は内部接続と外部接続を提供します。

レッスン 2
Windows 10 の DirectAccess のサポート

Windows 10 の DirectAccess 機能により、ユーザーが開始した VPN 接続を最初に確立することなく、イントラネット リソースへのシームレスなリモート アクセスが可能になります。DirectAccess 機能は、内部のユーザーとリモート ユーザーに対し、アプリケーション インフラストラクチャへのシームレスな接続も保証します。

イントラネットへの接続を開始するためにユーザーの操作を必要とする従来の VPN とは異なり、DirectAccess では、クライアント コンピューター上の任意のアプリケーションが、イントラネット リソースへのアクセスを確立することができます。DirectAccess では、リモート アクセスが制限されるリソースやクライアント側のアプリケーションを指定することもできます。

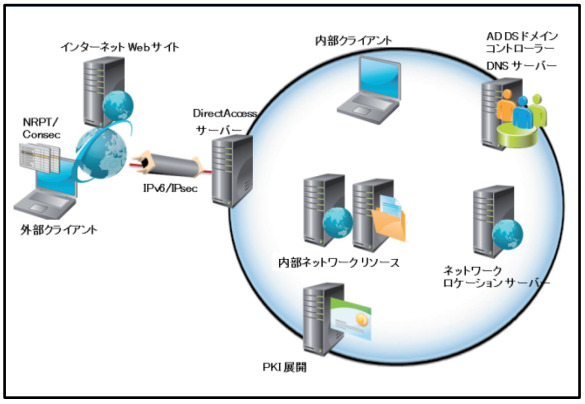
目的

このレッスンにより、次のことを習得できます。

- DirectAccess を実装するために必要なコンポーネントを説明することができます。
- 内部クライアントに対する DirectAccess の動作方法を説明することができます。
- 外部クライアントに対する DirectAccess の動作方法を説明することができます。
- 作業の開始ウィザードを使用して DirectAccess を構成することができます。

DirectAccess コンポーネント

DirectAccess を展開し、構成するには、組織が次のインフラストラクチャ コンポーネントを備えている必要があります。



- DirectAccess サーバー
- DirectAccess クライアント
- ネットワーク ロケーション サーバー
- 内部ネットワーク リソース
- Active Directory ドメイン サービス (AD DS) ドメイン
- グループ ポリシー
- 公開キー基盤 (PKI) (内部ネットワーク用のオプション)
- ドメイン ネーム システム (DNS) サーバー
- 名前解決ポリシー テーブル (NRPT)

DirectAccess サーバー

DirectAccess サーバーは、ドメインに参加し、DirectAccess クライアントの接続を受け付け、イントラネット リソースとの通信を確立している任意の Windows Server 2012 R2 または Windows Server 2012 オペレーティング システムです。このサーバーは、DirectAccess クライアントに対する認証サービスを提供し、外部トラフィックに対する IPsec トンネル モードのエンドポイントとして機能します。Windows Server 2012 R2 リモート アクセス サーバーの役割により、DirectAccess と VPN 接続の両方を一元的に管理、構成、および監視できます。

以前の Windows Server 2008 R2 での実装と比較すると、新しい DirectAccess ウィザード ベースのセットアップでは、中小規模の組織向けの DirectAccess 管理が簡略化されています。このウィザードは、完全な PKI の展開の必要性と、インターネット接続用の物理アダプターに 2 つの連続したパブリック IPv4 (IPv4) アドレスを割り当てる要件を排除しました。Windows Server 2012 R2 では、DirectAccess セットアップ ウィザードが DirectAccess サーバーの実際の実装状態を検出し、最適な展開を自動的に選択します。これにより、インターネット プロトコル バージョン 6 (IPv6) への移行テクノロジを手動で構成する複雑な作業から管理者を解放します。

DirectAccess クライアント

DirectAccess クライアントは、ドメインに参加し、Windows 7、Windows 8、Windows 10 の Education または Enterprise エディションを実行中の任意のコンピューターです。

注 : オフライン ドメイン参加により、クライアント コンピューターを内部ネットワークに接続することなく、ドメインに参加させることができます。

DirectAccess クライアント コンピューターは、DirectAccess サーバーに、IPv6 と IPsec を使用して接続します。ネイティブ IPv6 ネットワークが使用できない場合は、クライアントは、6to4 または Teredo を使用して IPv6-in-IPv4 トンネルを確立します。この手順を完了するために、ユーザーがコンピューターにサインインする必要はありません。

ファイアウォールまたはプロキシ サーバーが、6to4 または Teredo を使用しているクライアント コンピューターによる DirectAccess サーバーへの接続を許可しない場合は、クライアントは自動的に Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) を使用して接続を試行します。IP-HTTPS は、SSL 接続を使用しているため、接続が保証されます。クライアントは、名前解決ポリシー テーブル (NRPT) の規則および接続のセキュリティのトンネル規則でアクセス可能です。

ネットワーク ロケーション サーバー

DirectAccess クライアントは、ネットワーク ロケーション サーバー (NLS) を使用して、クライアント自身の場所を判断します。クライアント コンピューターが HTTPS を使用して安全にネットワーク ロケーション サーバーに接続できる場合、クライアント コンピューターは自身がイントラネット上にいるとみなし、DirectAccess ポリシーは適用されません。クライアント コンピューターがネットワーク ロケーション サーバーと通信できない場合は、クライアント コンピューターはインターネット上にいるとみなします。ネットワーク ロケーション サーバーは、Web サーバーの役割を持つ DirectAccess サーバーにインストールできます。

注 : ネットワーク ロケーション サーバーの URL は、グループ ポリシー オブジェクト (GPO) を使用して配布されます。

内部ネットワーク リソース

内部サーバーまたはクライアント コンピューターで実行されている IPv6 対応のあらゆるアプリケーションを、DirectAccess クライアントに使用できるように構成することができます。古いアプリケーションや Windows Server 2003、その他の Microsoft 以外のオペレーティング システム、IPv6 をサポートしないものを含むサーバーのため、Windows Server 2012 R2 では、プロトコル変換 (NAT64) と名前解決 (DNS64) ゲートウェイがネイティブ サポートされ、DirectAccess クライアントからの IPv6 通信を内部サーバーのために IPv4 に変換します。

Active Directory ドメイン

少なくとも 1 つの AD DS ドメインを展開して、Windows Server 2003 のドメインの機能レベルで実行する必要があります。DirectAccess では、複数ドメインのサポートが組み込まれており、異なるドメインに属するクライアント コンピューターが、別の信頼される側のドメインに配置されているリソースにアクセスできます。

グループ ポリシー

グループ ポリシーは、DirectAccess 設定の管理と展開の一元化のために必要です。作業の開始ウィザードでは、DirectAccess クライアント、DirectAccess サーバー、および選択されたサーバー向けの一連の GPO のセットと設定を作成します。

PKI

構成と管理を簡略化するために、PKI の展開はオプションになっています。DirectAccess では、DirectAccess サーバーで実行されている HTTPS ベースの Kerberos プロキシ サービスを経由して、クライアントの認証要求を送信することができます。これにより、クライアントとドメイン コントローラー間に第 2 の IPsec トンネルを確立する必要がなくなります。Kerberos プロキシは、クライアントに代わって、Kerberos バージョン 5 プロトコル要求をドメイン コントローラーに送信します。ただし、2 要素認証、トンネリングの強制適用が可能な完全な DirectAccess 構成には、DirectAccess 通信に参加する各クライアントの認証のために証明書を実装する必要があります。

DNS サーバー

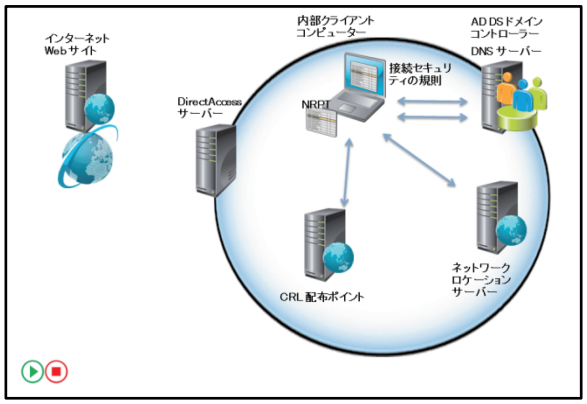
ISATAP を使用する場合は、Windows Server 2008 R2、Windows Server 2008 SP2、またはそれ以降のバージョンの DNS サーバーを使用するか、ISATAP 経由での DNS メッセージ交換をサポートする Windows ベース以外の DNS サーバーを使用する必要があります。

NRPT

DirectAccess GPO は、クライアント コンピューター用の NRPT エントリも作成します。NRPT の構成を確認するには、Windows PowerShell コマンド ライン インターフェイスで Get-DNSClientNrptPolicy コマンドレットを実行します。NRPT は、DirectAccess 用に構成された DNS 名前空間ごとにエントリを持ちます。

参考資料：ネットワークとアクセスのテクノロジについては、次のサイトを参照してください。
ネットワークとアクセスのテクノロジ
https://technet.microsoft.com/ja-jp/network

内部クライアントに対する DirectAccess の働き



ネットワーク ロケーション サーバーは、HTTPS ベースの URL をホストする内部ネットワーク サーバーです。DirectAccess クライアントは、ネットワーク ロケーション サーバーの URL へのアクセスを試みて、自身がイントラネットに存在するのか、またはパブリック ネットワークに存在するのかを判定します。
DirectAccess サーバーをネットワーク ロケーション サーバーにすることもできます。組織によっては、DirectAccess が不可欠なサービスのため、ネットワーク ロケーション サーバーに高可用性が必要な場合があります。一般に、ネットワーク ロケーション サーバー上の Web サーバーは、DirectAccess クライアントのサポート専用である必要はありません。

DirectAccess クライアントの動作はネットワーク ロケーション サーバーからの応答に依存するため、ネットワーク ロケーション サーバーが組織のどこからでも利用できることが重要です。支店間のリンク障害時もネットワーク ロケーション サーバーへのアクセスを保証するためには、支店ごとに別のネットワーク ロケーション サーバーが必要な場合があります。

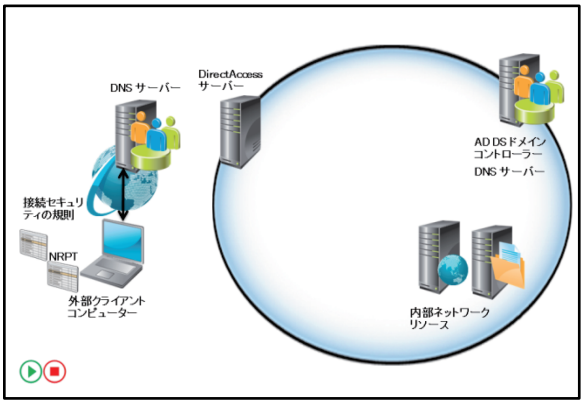
内部クライアントに対する DirectAccess の働き

DirectAccess 接続のプロセスはユーザーの操作を必要とせず、自動的に実行されます。DirectAccess クライアントは、次のプロセスを使用してイントラネット リソースに接続します。

1. DirectAccess クライアントは、ネットワーク ロケーション サーバーの URL の完全修飾ドメイン名 (FQDN) を解決しようとします。
2. ネットワーク ロケーション サーバーの URL の FQDN は NRPT の除外規則に該当するため、DirectAccess クライアントは、ローカルに構成された DNS サーバー (イントラネット ベースの DNS サーバー) に DNS クエリを送信します。イントラネット ベースの DNS サーバーは名前を解決します。
3. DirectAccess クライアントは、HTTPS ベースのネットワーク ロケーション サーバーの URL にアクセスし、そのプロセスでネットワーク ロケーション サーバーの証明書を取得します。
4. ネットワーク ロケーション サーバーの証明書の証明書失効リスト (CRL) 配布ポイントのフィールドに基づき、DirectAccess クライアントは、CRL 配布ポイントの CRL 失効ファイルをチェックして、ネットワーク ロケーション サーバー証明書が失効していないかを判断します。
5. HTTP 応答コード 200 に基づき、DirectAccess クライアントは、ネットワーク ロケーション サーバーの URL の成功 (アクセス、証明書の認証、および失効チェックの成功) を判断します。次に、DirectAccess クライアントはネットワーク位置認識サービスを使用して、ドメインのファイアウォール プロファイルに切り替え、DirectAccess のポリシーを無視し、ネットワークの変更が起きるまでは自身が内部ネットワークにいるものとみなします。
6. DirectAccess クライアント コンピューターは、AD DS ドメインの場所を特定し、コンピューター アカウントを使用してサインインしようとします。クライアントは、セッションが接続されている間、NRPT の DirectAccess の規則を参照しないため、すべての DNS クエリをインターフェイスに構成された (イントラネット ベースの) DNS サーバー経由で送信します。ネットワークの場所の検出とコンピューターのドメインへのサインインの組み合わせにより、DirectAccess クライアントは、自身を通常のイントラネット アクセス用に構成します。
7. コンピューターのドメインへのサインイン成功に基づき、DirectAccess クライアントは、接続したネットワークにドメイン ファイアウォール の ネットワーク プロファイルを割り当てます。設計により、DirectAccess の接続のセキュリティのトンネル規則はパブリックおよびプライベート ファイアウォールのプロファイルをスコープに設定しているため、それらの規則はアクティブな接続のセキュリティの規則のリストで無効化されます。
8. DirectAccess クライアントは、イントラネットに接続されていることを正常に判定し、DirectAccess の設定 (NRPT の規則または接続のセキュリティのトンネル規則) を使用しません。DirectAccess クライアントは、イントラネット リソースに通常どおりアクセスできます。このように、DirectAccess クライアントは、正常にイントラネット リソースにアクセスできるようになります。

外部クライアントに対する DirectAccess の働き

DirectAccess クライアントは、ネットワーク ロケーション サーバー用に指定された URL にアクセスしようとします。NLS と通信できないため、イントラネットに接続されていないとみなします。DirectAccess クライアントは、NRPT と接続セキュリティの規則の使用を開始します。NRPT は名前解決のための DirectAccess ベースの規則を保持し、接続セキュリティ規則はイントラネット リソースとの通信のために DirectAccess の IPsec トンネルを定義します。インターネットに接続された DirectAccess クライアントは、イントラネット リソースとの接続に次の手順で実行します。



1. DirectAccess クライアントはネットワーク ロケーション サーバーへのアクセスを試みます。
2. クライアントはドメイン コントローラーの特定を試みます。
3. クライアントは最初にイントラネット リソース、次にインターネット リソースへのアクセスを試みます。

DirectAccess クライアントによるネットワーク ロケーション サーバーへのアクセスの試行

DirectAccess クライアントは、次のようにネットワーク ロケーション サーバーへのアクセスを試みます。

1. クライアントは、ネットワーク ロケーション サーバー URL の FQDN の名前解決を試みます。ネットワーク ロケーション サーバーの URL の FQDN は NRPT の除外規則に該当するため、DirectAccess クライアントは、ローカルに構成された (インターネットベースの) DNS サーバーに DNS クエリを送信しません。外部のインターネットベースの DNS サーバーは名前を解決できません。
2. DirectAccess クライアントは、NRPT の DirectAccess の除外規則に定義されたとおりに、名前解決要求を処理します。
3. DirectAccess クライアントが存在する現在のネットワークにはネットワーク ロケーション サーバーが見つからないため、DirectAccess クライアントは接続したネットワークにパブリックまたはプライベート ファイアウォールのネットワーク プロファイルを適用します。
4. パブリックおよびプライベート プロファイルをスコープとする DirectAccess の接続のセキュリティのトンネル規則は、パブリックまたはプライベート ファイアウォールのネットワーク プロファイルを提供します。
5. DirectAccess クライアントは、NRPT 規則と接続のセキュリティの規則を組み合わせて使用し、インターネットから DirectAccess サーバー経由でイントラネット リソースの場所を特定し、アクセスします。

DirectAccess クライアントによるドメイン コントローラーを特定するための試行

DirectAccess クライアントは、起動後に自身のネットワークの場所を特定すると、ドメイン コントローラーを検索してサインインを試みます。このプロセスで、DirectAccess サーバーに対して、IPsec トンネル モードとカプセル化セキュリティ ペイロード (ESP) により、IPsec トンネル (インフラストラクチャ トンネル) が作成されますこのプロセスは次のとおりです。

1. ドメイン コントローラーの DNS 名が、NRPT のイントラネット名前空間の規則と一致します。これにより、イントラネット DNS サーバーの IPv6 アドレスが指定されます。DNS クライアント サービスは、イントラネット DNS サーバーの IPv6 アドレスを指定した DNS 名クエリを作成し、DirectAccess クライアントの送信用 TCP/IP スタックに渡します。

2. パケットを送信する前に、TCP/IP スタックは、パケットに対して Windows ファイアウォール通信規則または接続セキュリティ規則があるかどうかチェックします。
3. DNS 名のクエリ内の送信先の IPv6 アドレスが、インフラストラクチャ トンネルに該当する接続のセキュリティの規則と一致するため、DirectAccess クライアントは、認証済み IP (AuthIP) と IPsec を使用して、ネゴシエーションと認証をおこない、DirectAccess サーバーへの暗号化された IPsec トンネルを確立します。DirectAccess クライアント (コンピューターとユーザーの両方) は、インストールされたコンピューターの証明書と Microsoft Windows NT LAN Manager (NTLM) の資格情報をそれぞれ使用して、認証を受けます。

注 : AuthIP は、Kerberos プロトコルまたは SSL 証明書によるユーザーベースの認証のサポートを追加して、IPsec での認証を強化します。また、AuthIP は、効率的なプロトコル ネゴシエーションおよび複数セットの認証用証明書の使用もサポートしています。

4. DirectAccess クライアントは、インフラストラクチャ トンネルを通って DirectAccess サーバーに DNS 名クエリを送信します。
5. DirectAccess サーバーは、DNS 名クエリをイントラネット DNS サーバーに転送します。DNS 名クエリの応答は、DirectAccess サーバーに返信され、IPsec インフラストラクチャ トンネルを通って DirectAccess クライアントに返信されます。

その後のドメイン サインイン トラフィックは、IPsec インフラストラクチャ トンネルを通ります。DirectAccess クライアントでユーザーがサインインすると、ドメイン サインイン トラフィックは IPsec インフラストラクチャ トンネルを通ります。

DirectAccess クライアントによるイントラネット リソースへのアクセス試行

DirectAccess クライアントが、インフラストラクチャ トンネルの接続先のリストに含まれないイントラネットの場所 (内部の Web サイトなど) にトラフィックを初めて送信するときは、次のプロセスが実行されます。

1. 通信を試みているアプリケーションまたはプロセスは、メッセージまたはペイロードを構築し、それを TCP/IP スタックに渡して送信します。
2. パケットを送信する前に、TCP/IP スタックは、パケットに対して Windows ファイアウォール通信規則または接続セキュリティ規則があるかどうかチェックします。
3. 宛先の IPv6 アドレスは、イントラネット トンネルに対応する接続セキュリティ規則と一致するため (この規則でイントラネット全体の IPv6 アドレス空間が指定されます)、DirectAccess クライアントは AuthIP と IPsec を使用して、DirectAccess サーバーへの追加の IPsec トンネルをネゴシエートし、認証します。DirectAccess クライアントは、インストールされたコンピューター証明書とユーザー アカウントの Kerberos 資格情報を使用して自身を認証します。
4. DirectAccess クライアントは、イントラネット トンネル経由でパケットを DirectAccess サーバーに送信します。
5. DirectAccess サーバーは、イントラネット リソースにパケットを転送し、イントラネット リソースがそれに応答します。応答は、DirectAccess サーバーに返送され、イントラネット トンネルを介して DirectAccess クライアントに返送されます。

その後のイントラネット アクセス トラフィックは、インフラストラクチャ トンネルに対応する接続セキュリティ規則内のイントラネットの宛先と一致しない場合、このイントラネット トンネルを通ります。

DirectAccess クライアントによるインターネット リソースへのアクセス試行

DirectAccess クライアント上のユーザーまたはプロセスが、インターネット リソース (インターネット Web サーバーなど) へのアクセスを試みると、次のプロセスが実行されます。

1. DNS クライアント サービスは、NRPT 経由で、インターネット リソース用の DNS 名を伝えます。一致するものがありません。DNS クライアント サービスは、インターフェイスに構成されたインターネット DNS サーバーの IP アドレスを指定した DNS 名のクエリを作成し、送信用 TCP/IP スタックに渡します。
2. パケットを送信する前に、TCP/IP スタックは、パケットに対して Windows ファイアウォール通信規則または接続セキュリティ規則があるかどうかチェックします。
3. DNS 名クエリ内の宛先 IP アドレスは、DirectAccess サーバーへのトンネルの接続セキュリティ規則と一致しないため、DirectAccess クライアントは DNS 名クエリを通常どおり送信します。
4. インターネット DNS サーバーは、インターネット リソースの IP アドレスを返します。
5. ユーザー アプリケーションまたはプロセスは、最初のパケットを作成し、インターネット リソースに送信します。パケットを送信する前に、TCP/IP スタックは、パケットに対して Windows ファイアウォール通信規則または接続セキュリティ規則があるかどうかチェックします。
6. DNS 名のクエリ内の宛先 IP アドレスが、DirectAccess サーバーへのトンネルの接続のセキュリティの規則と一致しないため、DirectAccess クライアントはパケットを通常の方法で送信します。

その後のインターネット リソース トラフィックは、インフラストラクチャ トンネルとイントラネット トンネルのどちらかの接続セキュリティ規則に一致する宛先がない場合、通常どおり送受信されます。

ドメイン コントローラーとイントラネット リソースへのアクセスは、接続プロセスにおいてはほぼ同じで、どちらのプロセスでも、NRPT を使用して適切な DNS サーバーを検索して名前クエリを解決します。ただし、クライアントと DirectAccess サーバーの間で確立される IPsec トンネルには重要な違いがあります。ドメイン コントローラーにアクセスする場合は、すべての DNS クエリが IPsec インフラストラクチャ トンネルを通って送信されますが、イントラネット リソースにアクセスする場合は、2 番目の IPsec トンネルを確立してイントラネット リソースにアクセスします。

デモンストレーション : 作業の開始ウィザードによる DirectAccess 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。

- DirectAccess 作業の開始ウィザードを実行する

デモンストレーションの手順

1. LON-RTR に切り替えます。
2. LON-RTR のサーバー マネージャーで [リモート アクセス管理] を選択します。次の設定を使用して、作業の開始ウィザードを完了します。
    1) [リモート アクセスの構成] ページで、[DirectAccess のみを展開します] をクリックします。
    2) [エッジ] が選択されていることを確認し、[クライアントからリモート アクセス サーバーへの接続に使用するパブリック名または IPv4 アドレスを入力してください] に「131.107.0.2」と入力します。
    3) [リモート アクセスの確認] ページで、Domain Users グループを削除し、DA_Clients グループを追加します。
    4) [リモート アクセスの確認] ページで、[モバイル コンピューターに対してのみ DirectAccess を有効にする] チェック ボックスをオフにします。
    5) [DirectAccess クライアントのセットアップ] ページで、DirectAccess 接続の名前として「Windows 10 職場の接続」と設定します。

知識の確認

質問	
クライアントとサーバーが適切にセットアップされるようにするために、DirectAccess は AD DS に 2 つの GPO を必要とします。これらの GPO をどこで適用しますか。	
正しい解答を選択してください。	
	ドメイン コントローラー上のグループ ポリシーの管理コンソールで適用します。
	Gpedit.msc コンソールで適用します。
	適用しません。作業の開始ウィザードを実行すると、GPO は自動的に作成されます。
	リモート管理コンソールで [Create GPO] から適用します。
	DirectAccess には適用されません。

演習 A : DirectAccess の実装

シナリオ

A. Datum 社の従業員の多くは、自宅や出張先など、社外から作業することが頻繁にあります。そのため、A. Datum 社の従業員に対してリモート アクセス ソリューションを実装し、彼らが社外から企業ネットワークに接続することができるようにする必要があります。あなたは、Windows 10 クライアント コンピューターに DirectAccess を実装することを決定しました。DirectAccess 環境を構成して、リモートでの操作時に内部ネットワークにクライアント コンピューターが接続できることを検証します。

目的

この演習により、次のことを習得できます。

- DirectAccess サーバーを構成することができます。
- リモート接続を検証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-RTR 23697-2B-LON-CL1 23697-2B-INET1
ユーザー名	Adatum¥Administrator Admin
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$$w0rd
5. 23697-2B-LON-RTR と 23697-2B-LON-CL1 に対して、手順 2 ～ 4 を繰り返します。
6. Hyper-V マネージャーで [23697-2B-INET1] をクリックし、操作ウィンドウで [起動] をクリックします。
7. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
8. 次の資格情報を使用してサインインします。
    - ユーザー名 : Administrator
    - パスワード : Pa$$w0rd

練習 1 : DirectAccess サーバーの構成

シナリオ

あなたは、Windows 10 コンピューターの DirectAccess へのアクセスをテストする前に、DirectAccess 通信を許可するようにリモート アクセス サーバーを構成する必要があります。

主な作業は次のとおりです。

1. DirectAccess サーバーを構成する

▶ 作業 1 : DirectAccess サーバーを構成する

1. LON-RTR に切り替えます。
2. LON-RTR で、サーバー マネージャーを開き、[リモート アクセス管理] を選択します。次の設定を使用して、作業の開始ウィザードを完了します。
    1) [リモート アクセスの構成] ページで、[DirectAccess のみを展開します] をクリックします。
    2) [エッジ] が選択されていることを確認し、[クライアントからリモート アクセス サーバーへの接続に使用するパブリック名または IPv4 アドレスを入力してください] に「131.107.0.2」と入力します。
    3) [リモート アクセスの確認] ページで、Domain Users グループを削除し、DA_Clients グループを追加します。
    4) [リモート アクセスの確認] ページで、[モバイル コンピューターに対してのみ DirectAccess を有効にする] チェック ボックスをオフにします。
    5) [DirectAccess クライアントのセットアップ] ページで、DirectAccess 接続の名前として「Windows 10 職場の接続」と設定します。
    6) 他のすべてのページに既定を提供し、[リモート アクセスの構成] ページで、[完了] をクリックして、[作業の開始ウィザードの設定を適用しています] ダイアログ ボックスで、[閉じる] をクリックします。
3. LON-RTR を再起動します。

結果 : この練習により、DirectAccess サーバーを構成することができました。

練習 2 : DirectAccess クライアントの構成

シナリオ

DirectAccess を使用して Windows 10 のテストを完了する前に、DirectAccess GPO が Windows 10 コンピューターに適用されていること、また、DirectAccess が適用される前と同じくらい簡単に Windows 10 コンピューターが内部ネットワーク リソースにアクセスできることを確認します。この時点で IPSec 暗号化はテストされないため、クライアント証明書またはサーバー証明書をチェックする必要はありません。

主な作業は次のとおりです。

1. グループ ポリシー設定を検証する
2. 内部接続を検証する

▶ 作業 1 : グループ ポリシー設定を検証する

1. LON-CL1 に切り替えます。
2. DirectAccess サーバーを構成すると、ウィザードにより、2 つのグループ ポリシーが作成され、ドメインにリンクされます。それらを適用するために、LON-CL1 を再起動し、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。
3. グループ ポリシーを適用するために、LON-CL1 で、コマンド プロンプトを開き、次のコマンドを入力します。

```
gpupdate /force
```

4. コンピューター設定に DirectAccess クライアントの設定 GPO が適用されていることを確認するために、次のコマンドを入力します。

```
gpresult /R
```

注 : DirectAccess クライアントの設定 GPO が適用されていない場合、LON-CL1 を再起動し、LON-CL1 で手順 2 ～ 4 を繰り返します。

5. 次のコマンドを入力します。

```
netsh name show effectivepolicy
```

6. [有効な DNS 名前解決ポリシー テーブルの設定] というメッセージが表示されることを確認します。

注 : このコンピューターが会社のネットワーク内にある場合、DirectAccess の設定は非アクティブとなります。

▶ 作業 2 : 内部接続を検証する

1. LON-CL1 に切り替えます。
2. Internet Explorer を開きます。
3. http://lon-dc1.adatum.com に接続します。LON-DC1 の既定のインターネット インフォメーション サービスサービス (IIS) Web ページが表示されます。
4. エクスプローラーで ¥¥LON-DC1¥labfiles に移動します。フォルダーの内容にアクセスできることを確認します。
5. ISATAP トンネル アダプターのメディアが切断状態であることを確認するために、コマンド プロンプトを開き、次のコマンドを入力します。

```
ipconfig
```

6. 開いているウィンドウをすべて閉じますが、サインアウトしないでください。

結果 : この練習により、DirectAccess クライアントを構成することができました。

練習 3 : リモート接続の検証

シナリオ

DirectAccess の Windows 10 クライアントのセットアップに関連するテストがすべて成功しました。クライアントは、LAN 上の内部リソースに問題なくアクセスすることができます。そこで、あなたは、クライアントをパブリック ネットワーク接続に配置することをシミュレーションし、内部リソースにまだアクセスできることを確認します。サーバーは、LON-RTR のパブリック ネットワーク アドレスを見つけるためにクライアントが使用するパブリック DNS サーバーとして動作するよう設定されています。クライアントが LON-SVR1 に接続できる場合、DirectAccess は LON-RTR 上で正常に動作します。

主な作業は次のとおりです。

1. 外部の場所からリソースへのアクセスを確認する

▶ 作業 1 : 外部の場所からリソースへのアクセスを確認する

クライアントをイントラネットからパブリック ネットワークへ移動する

1. LON-CL1 で、ネットワーク接続を開きます。
2. イーサネットを無効にします。
3. イーサネット 2 を有効にします。
4. イーサネット 2 で [インターネット プロトコル バージョン 4 (TCP/IPv4)] のプロパティを開き、次の設定を確認します。
   - IP アドレス : 131.107.0.20
   - サブネット マスク : 255.255.255.0
   - 優先 DNS サーバー : 131.107.0.100
5. ネットワーク接続を閉じます。

パブリック ネットワークから内部ネットワーク リソースへの接続を確認する

1. LON-CL1 で、Internet Explorer を開き、アドレス バーに「http://lon-dc1.adatum.com」と入力して、Enter キーを押します。LON-DC1 の既定のインターネット インフォメーション サービス (IIS) 8.0 Web ページが表示されます。
2. Internet Explorer を閉じます。
3. エクスプローラーで ¥¥LON-DC1¥labfiles を開きます。フォルダーの内容にアクセスできることを確認します。

DirectAccess サーバーへの接続を確認する

1. コマンド プロンプトで次のように入力し、Enter キーを押します。

```
Netsh name show effectivepolicy
```

2. [有効な DNS 名前解決ポリシー テーブルの設定] に、adatum.com と Directaccess-NLS.Adatum.com の 2 つのエントリがあることを確認します。
3. Windows PowerShell ウィンドウで、次のコマンドレットを入力します。

```
Get-DAClientExperienceConfiguration
```

4. DirectAccess クライアントの設定を確認します。

5. スタート メニューで [設定] アプリを開きます。[ネットワークとインターネット] を参照し、コンソール ツリーで [DirectAccess] を選択します。[Windows 10 職場の接続] 接続オブジェクトが表示されます。これは、練習 1、作業 1 の作業の開始ウィザードで DirectAccess 接続の名前として入力した名前です。
6. 開いているウィンドウをすべて閉じます。

DirectAccess サーバーへのクライアント接続を確認する

1. LON-RTR に切り替え、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. リモート アクセス管理コンソールを開きます。
3. コンソール ツリーの [リモート クライアントの状態] をクリックします。6to4 および IPHttps 経由でクライアントが接続されていることを確認します。接続の詳細ウィンドウの右下隅で、Kerberos プロトコルがマシンとユーザーの認証に使用されていることを確認します。
4. 開いているウィンドウをすべて閉じます。

結果 : この練習により、DirectAccess によるリモート接続を検証することができました。

▶ 次の演習の準備をする

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-RTR、23697-2B-INET1、23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。

質問 : DA_Clients グループに含まれていたアカウントはどれですか。また、DA_Clients グループはどのようなことを実行しましたか。

質問 : DirectAccess を使用するために、Windows 10 クライアント コンピューターの IPv6 アドレスをどのように構成しますか。

レッスン 3
リモート ネットワークへの VPN アクセスの構成

組織内に VPN 環境を正しく実装し、サポートするには、適切なトンネリング プロトコルの選択方法、VPN 認証の構成方法、および、選択した環境をサポートするためのその他の設定の構成方法を理解することが重要です。

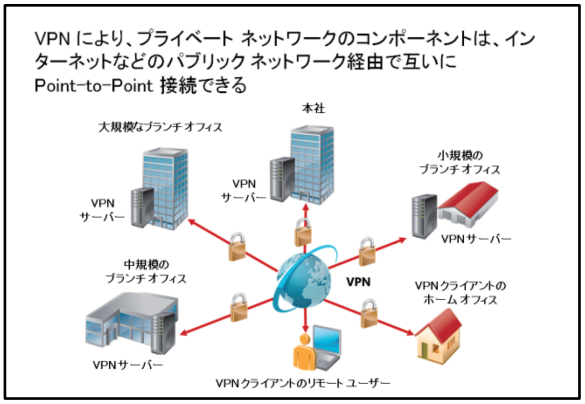
目的

このレッスンにより、次のことを習得できます。

- VPN を説明することができます。
- VPN が使用するトンネリング プロトコルを説明することができます。
- VPN の認証メカニズムを説明することができます。
- Windows 10 で VPN を構成することができます。
- 接続マネージャー管理キット (CMAK) を説明することができます。
- 管理ソリューションを使用して VPN 接続プロファイルを準備する方法を説明することができます。

VPN とは

VPN により、インターネットなどのパブリック ネットワークを経由する、プライベート ネットワークのコンポーネント間の Point-to-Point 接続が可能になります。VPN クライアントは、トンネリング プロトコルを使用して、VPN サーバーの仮想リスニング ポートへの接続を確立し、維持することができます。Point-to-Point リンクをエミュレートするには、データの先頭にヘッダーを付加してカプセル化 (ラップ) します。このヘッダーに、データがパブリック ネットワークを経由してエンドポイントに到達するためのルーティング情報が格納されます。



プライベート リンクをエミュレートするには、データを暗号化して機密性を確保します。パブリック ネットワークでパケットが傍受されても、暗号化キーがなければ解読できません。

リモート アクセス VPN 接続

リモート アクセス VPN 接続は、自宅や顧客サイト、または公衆無線アクセス ポイントから、組織のプライベート ネットワーク上のサーバーへのアクセスを可能にします。これには、インターネットなどのパブリック ネットワークが提供するインフラストラクチャを使用します。

ユーザーの視点から見ると、VPN は、VPN クライアントと組織のサーバーの間をつなぐ Point-to-Point 接続です。論理的には、データは専用のプライベート リンクを経由して送信されているように見えるため、共有ネットワークやパブリック ネットワークのインフラストラクチャそのものは重要ではありません。

VPN 接続のプロパティ

VPN 接続には次のプロパティがあります。

- **カプセル化 :** VPN テクノロジを使用すると、プライベート データは、データが通過ネットワークを通過するためのルーティング情報を含むヘッダーを付けてカプセル化されます。

- **認証 :** VPN 接続の認証には、次の 3 つの形があります。
    - **Point-to-Point プロトコル (PPP) 認証によるユーザーレベルの認証 :** VPN 接続を確立するために、VPN サーバーは PPP ユーザーレベル認証方式を使用して、接続を試行している VPN クライアントを認証し、VPN クライアントが適切な権限を持っていることを確認します。相互認証を使用する場合は、VPN クライアントも VPN サーバーを認証します。これにより、VPN サーバーを偽装するコンピューターから保護できます。
    - **インターネット キー交換 (IKE) によるコンピューターレベルの認証 :** IPsec セキュリティ アソシエーションを確立するため、VPN クライアントと VPN サーバーは IKE プロトコルを使用して、コンピューターの証明書または事前共有キーを交換します。どちらの場合でも、VPN クライアントとサーバーは、コンピューター レベルで互いに認証します。認証方法として非常に強力な、コンピューター証明書での認証をお勧めします。コンピューターレベルの認証は、レイヤー 2 トンネリング プロトコル (L2TP/IPsec) 接続のみ実行されることに注意してください。
    - **データ送信元の認証およびデータの整合性 :** VPN 接続で送信されたデータが、接続の相手側システムから送信されていることと、通過の際に変更されていないことを確認するため、送信側と受信側だけが知っている暗号化キーに基づいた暗号化チェックサムがデータに含まれています。データ送信元の認証とデータの整合性は、L2TP/IPsec 接続の場合のみ使用可能です。
- **データ暗号化 :** 共有またはパブリックの通過ネットワークをスキャンする際のデータの機密性を確保するため、送信側がデータを暗号化し、受信者が暗号化を解除します。暗号化と暗号化解除のプロセスは、共通の暗号化キーを使用して送信側と受信側の両方で処理されます。通過するネットワークの中でパケットが傍受されても、共通の暗号化キーを所有していない第三者には判読できません。

暗号化キーの長さは、重要なセキュリティ パラメーターです。暗号化キーを決定するにあたり、計算を用いる手法を使用することができます。ただし、こうした手法は、暗号化キーが長くなるにつれ、より高いコンピューターの処理能力とやより多くの処理時間が必要となります。このため、データの機密性を確保するために、可能な範囲でのキーの長さを最大にして使用することが重要です。

VPN 接続のトンネリング プロトコル

VPN を展開する際、クライアントがパブリック ネットワークから接続するときに使用するプロトコルを、組織がさまざまなトンネリング プロトコルの中から選択する場合があります。VPN のトンネリング プロトコルには、Point-to-Point トンネリング プロトコル (PPTP)、L2TP、Secure Socket トンネリング プロトコル (SSTP)、インターネット キー交換のバージョン 2 (IKEv2) があります。IKEv2 は、PPTP、L2TP、SSTP とは異なり、Windows Server 2012、Windows Server 2008 R2、および Windows 7 以降 (Windows 10 を含む) を実行しているコンピューターでのみサポートされます。VPN を自動検出に設定している場合、Windows 7 以降では IKEv2 が既定の VPN トンネリング プロトコルになります。その他のプロトコルは、IKEv2 が成功しない場合に試行されます。

トンネリング プロトコル	ファイアウォール アクセス	説明
PPTP	TCP ポート 1723	データの機密性を提供するが、データの認証とデータの整合性は提供しない
L2TP/IPsec	UDP ポート 500、UDP ポート 1701、UDP ポート 4500、IP プロトコル ID 50	認証は、証明書 (推奨) または事前共有キーを使用する
SSTP	TCP ポート 443	SSL を使用して、データの機密性、データの認証、データの整合性を提供する
IKEv2	UDP ポート 500	最新の IPsec 暗号化アルゴリズムを使用して、データの機密性、データの認証、データの整合性を提供する

Windows 10 では、VPN 接続に次のトンネリング プロトコルを使用できます。

PPTP

PPTP は、Microsoft オペレーティング システムがサポートする最も古いトンネリング プロトコルです。PPTP は、トラフィックを暗号化し、IP ヘッダーをカプセル化して、IP ネットワークに送信します。

PPTP は、リモート クライアントとサイト間の VPN 接続に使用することができます。インターネットを使用する場合、VPN サーバーはクライアントに次の機能を提供します。

- **PPTP カプセル化 :** PPTP は、IP データグラムの PPP フレームをカプセル化し、ネットワーク経由の送信をおこないます。PPTP では、トンネル管理には TCP 接続を使用し、トンネル データの PPP フレームのカプセル化には Generic RoutingEncapsulation (GRE) の更新バージョンを使用します。カプセル化した PPP フレームのペイロードは、暗号化と圧縮の両方が可能です。
- **暗号化 :** PPP フレームは、MS-CHAPv2 または EAP-TLS 認証プロセスから生成された暗号化キーを使用し、Microsoft Point-to-Point 暗号化 (MPPE) で暗号化されます。VPN クライアントは、PPP フレームのペイロードが暗号化するために、MS-CHAPv2 または EAP-TLS 認証プロトコルを使用する必要があります。PPTP では、基になる PPP 暗号化と、以前に暗号化された PPP フレームのカプセル化を使用します。

L2TP

L2TP は、マルチプロトコル トラフィックを暗号化し、IP や非同期転送モード (ATM) など、Point-to-Point データグラム配信をサポートする任意のメディアに送信することができます。L2TP は、PPTP と Layer Two Forwarding (L2F) の技術を組み合わせたものです。L2TP は、PPTP と L2F の最も優れた機能を表しています。

L2TP は、暗号化サービスのトランスポート モードで IPsec に依存しています。L2TP と IPsec の組み合わせは、L2TP/IPsec と呼ばれます。

L2TP クライアント サポートは、Windows Vista 以降の Windows オペレーティング システムに組み込まれています。L2TP の VPN サーバー サポートは、Windows Server 2008 およびそれ以降の Windows Server ファミリに組み込まれています。

- **カプセル化 :** L2TP/IPsec パケットのカプセル化は、L2TP カプセル化と IPsec カプセル化の 2 つのレイヤーで構成されています。L2TP は、次の方法でデータのカプセル化と暗号化をおこないます。
  - **第 1 レイヤー :** 第 1 レイヤーは L2TP カプセル化です。PPP フレーム (IP データグラム) は、L2TP ヘッダーとユーザー データグラム プロトコル (UDP) ヘッダーでラップされます。
  - **第 2 レイヤー :** 第 2 レイヤーは IPsec カプセル化です。結果の L2TP メッセージは、IPsec ESP ヘッダーとトレーラー、メッセージの整合性と認証を提供する IPSec 認証のトレーラー、および最終 IP ヘッダーでラップされます。IP ヘッダーには、VPN クライアントとサーバーに対応する発信元 IP アドレスおよび宛先 IP アドレスが含まれています。
- **暗号化 :** L2TP メッセージは、IKE ネゴシエーション プロセスを生成する暗号化キーを使用し、高度暗号化標準 (AES) または Triple Data Encryption Standard (3DES) で暗号化されます。

SSTP

SSTP は、TCP ポート 443 の HTTPS プロトコルを使用するトンネリング プロトコルです。PPTP や L2TP/IPsec のトラフィックは、ファイアウォールなどでブロックされる場合もありますが、SSTP は TCP ポート 443 が使われるため、ファイアウォールや Web プロキシ があっても通過することができます。SSTP は、HTTPS プロトコルの Secure Sockets Layer (SSL) チャネルを通じて PPP をカプセル化するメカニズムを提供します。PPP を使用することで、EAP-TLS などの強力な認証方法をサポートすることができます。SSL は、強化されたキー ネゴシエーション、暗号化、整合性チェックを使用して、トランスポート レベルのセキュリティを提供します。クライアントが SSTP ベースの VPN 接続を確立しようとする場合、SSTP はまず SSTP サーバーに対して双方向の HTTPS レイヤーを確立します。この HTTPS レイヤーを通じ、次のカプセル化と暗号化の方法を使用して、プロトコル パケットがデータペイロードとともに送信されます。

- **カプセル化 :** SSTP は、ネットワークを通じた転送をおこなうため、IP データグラムの PPP フレームをカプセル化します。SSTP は、ポート 443 での TCP 接続を使用してトンネル管理をおこなうほか、PPP データ フレームも使用します。
- **暗号化 :** SSTP メッセージは、HTTPS プロトコルの SSL チャネルで暗号化されます。

IKEv2

IKEv2 は、UDP ポート 500 を通じて IPSec トンネル モード プロトコルを使用します。IKEv2 は、モビリティのサポートにより、他のプロトコルと比べて、ネットワーク接続が変更されても接続を維持する機能が大幅に向上しました。IKEv2 ベースの VPN では、ユーザーはワイヤレス ホットスポット間やワイヤレスとワイヤード (有線) 接続間を容易に移動することができます。IKEv2 と IPsec を使用することで、次のような強力な認証と暗号化の方法のサポートが可能です。

- **カプセル化 :** IKEv2 は、ネットワークを通じた転送をおこなうために、IPsec ESP または 認証ヘッダー (AH) を使用して、データグラムをカプセル化します。
- **暗号化 :** メッセージは、IKEv2 ネゴシエーション プロセスにより生成された暗号化キーを使用して暗号化されます。暗号化には、AES 256、AES 192、AES 128、3DES の各暗号化アルゴリズムのいずれかが使われます。

IKEv2 は、Windows 7 以降のオペレーティング システム (Windows 10 を含む)、Windows Server 2012 R2、Windows Server 2012、および Windows Server 2008 R2 が稼働しているコンピューターでのみサポートされます。

VPN 認証方法の概要

クライアントの認証は、重要なセキュリティ上の関心事です。認証方法は通常、接続の確立プロセス中にネゴシエートされる認証プロトコルを使用します。リモート アクセスの役割は、次の認証方法をサポートしています。

プロトコル	説明	セキュリティレベル
PAP	プレーンテキストのパスワードを使用する。通常、リモート アクセス クライアントとリモート アクセス サーバーが、より安全な検証方法をネゴシエートできない場合に使用される。	最もセキュリティレベルの低い認証プロトコル。再生攻撃、リモート クライアントの偽装、リモート サーバーの偽装に対する保護をおこなわない。
CHAP	業界標準の MD5 メッセージ ダイジェスト アルゴリズムを使用するチャレンジ/レスポンス認証プロトコル。	パスワードが PPP リンク上で送信されないことで、PAP よりも改善されている。 チャレンジ応答を検証するために、プレーンテキスト バージョンのパスワードが必要。リモート サーバーの偽装に対する保護をおこなわない。
MS-CHAPv2	MS-CHAP のアップグレード版。双方向の認証、すなわち相互認証を提供。リモート アクセス クライアントは、ダイヤル先のリモート アクセス サーバーがユーザーのパスワードにアクセスできるという確認の応答を受信する。	CHAP よりも強力なセキュリティを提供。
EAP	EAP の種類と呼ばれる認証スキーマを使用して、任意の認証によるリモート アクセス接続が可能。	認証の種類を選択する上で最も柔軟性が高いため、最強のセキュリティを提供。

PAP

パスワード認証プロトコル (PAP) は、プレーンテキストのパスワードを使用する、最もセキュリティ レベルの低い認証プロトコルです。これは通常、リモート アクセス クライアントとリモート アクセス サーバーが、より安全な検証方法をネゴシエートできない場合に使用されます。PAP は、古い Windows クライアント オペレーティング システムをサポートするために Windows Server 2012 に組み込まれています。

CHAP

チャレンジ ハンドシェイク認証プロトコル (CHAP) は、業界標準の MD5 メッセージ ダイジェスト アルゴリズムを使用してレスポンスを暗号化するチャレンジ/レスポンス認証プロトコルです。CHAP は、ネットワーク アクセス サーバーおよびネットワーク アクセス クライアントのさまざまなベンダーで使用されています。CHAP では可逆的に暗号化されたパスワードを使用する必要があるため、MS-CHAPv2 などの他の認証プロトコルの使用を検討することをお勧めします。

MS-CHAPv2

MS-CHAPv2 は、一方向の暗号化されたパスワードを使用する相互認証プロセスで、次のように機能します。

1. 認証システム、つまりリモート アクセス サーバーが、またはネットワーク ポリシー サーバー (NPS) を実行しているコンピューターが、リモート アクセス クライアントにチャレンジを送信します。チャレンジは、セッション識別子と任意のチャレンジ文字列で構成されます。
2. リモート アクセス クライアントが応答を送信します。これには、受信したチャレンジ文字列、ピア チャレンジ文字列、セッション識別子、およびユーザー パスワードを一方向に暗号化したものが含まれます。

3. 認証システムは、クライアントからの応答をチェックし、応答を返します。これには、接続の試行の成功または失敗を示す情報と、送信されたチャレンジ文字列、ピア チャレンジ文字列、クライアントの暗号化された応答、およびユーザー パスワードに基づいて認証された応答が含まれます。
4. リモート アクセス クライアントが認証の応答を確認し、その応答が正しければ、接続を使用します。認証の応答が正しくない場合、リモート アクセス クライアントは接続を終了します。

EAP

拡張認証プロトコル (EAP) では、任意の認証メカニズムにより、リモート アクセス接続が認証されます。使用される認証方式は、リモート アクセス クライアントおよび認証システム (リモート アクセス サーバーまたはリモート認証ダイヤルイン ユーザー サービス サーバー) によってネゴシエートされます。ルーティングとリモート アクセス サービス (RRAS) には、既定で EAP-TLS のサポートが含まれています。RRAS を実行しているサーバーに他の EAP モジュールを組み込むことで、その他の EAP メソッドを提供できます。

デジタル証明書

証明書は、Active Directory 証明書サービスやベリサイン パブリック認証局などの証明機関 (CA) が発行するデジタルのドキュメントです。証明書は、コード署名や電子メール通信のセキュリティ確保など、さまざまな目的に使用されますが、VPN では、ネットワーク アクセスの認証に使用されます。これが使用される理由は、ユーザーやコンピューターの認証において強力なセキュリティを確保でき、安全性の低いパスワードベースの認証方法が不要になるためです。NPS は、EAP-TLS および PEAP (Protected Extensible Authentication Protocol) を使用して、VPN やワイヤレス接続など、多数のネットワーク アクセスに対して証明書ベースの認証をおこないます。

証明書ベースの認証の種類で認証を構成する場合、証明書を使用する認証方法として、EAP と PEAP の 2 種類があります。EAP では、認証の種類として TLS (EAP-TLS) を構成でき、PEAP では、認証の種類として TLS (PEAP-TLS) および MS-CHAPv2 (PEAP-MS-CHAPv2) を構成できます。どちらの認証方法でも、サーバーの認証には常に証明書が使用されます。これらの認証方法で構成した認証の種類に応じて、ユーザーの認証とクライアント コンピューターの認証にも証明書が使用される場合があります。

Windows 10 では、証明書を使用した VPN 接続の認証が最も強力な認証方法です。L2TP/IPsec に基づく VPN 接続には、IPsec 認証用の証明書を使用する必要があります。PPTP 接続には証明書は必要ありませんが、EAP-TLS を認証方法として使用する場合は、コンピューターの認証に証明書を使用するように PPTP 接続を構成することもできます。ワイヤレス クライアントでは、EAP-TLS と PEAP を組み合わせて、スマート カードまたは証明書を使用する認証方法を使用します。

その他のオプション

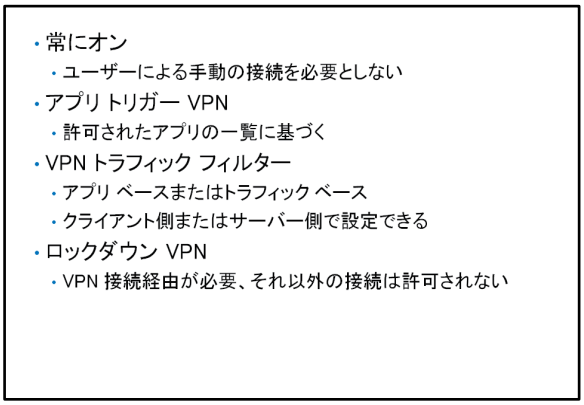
認証方法を選択する場合、既に説明した認証方法のほかに、さらに 2 つのオプションを有効にすることができます。

- **認証されていないアクセス :** これは実際には認証方法ではなく、認証をおこなわないことを意味します。認証されていないアクセスでは、リモート システムは認証なしで接続できます。このオプションは運用環境では絶対に有効にしないでください。ネットワークを危険にさらすことになります。ただし、テスト環境においては、このオプションが認証の問題のトラブルシューティングに役立つ場合があります。
- **IKEv2 のマシン証明書 :** このオプションは、VPN 再接続を使用する場合に選択します。

これらの各認証方法には、セキュリティ、ユーザビリティ、およびサポート範囲の面で、それぞれメリットとデメリットがあります。ただし、パスワードベースの認証方法では強力なセキュリティ機能は提供されないため、推奨されません。また、リモート アクセスで証明書をサポートしているのであれば、証明書ベースの認証方法を使用すべきです。

Windows 10 VPN プロファイル機能

Windows 10 では、ユーザーの VPN のエクスペリエンスを高めるための VPN プロファイル機能が新しく追加されています。これらの機能には、常にオン、アプリ トリガー VPN、トラフィック フィルター、ロックダウン VPN があります。



常にオン

[常にオン] は Windows 10 の新機能で、アクティブな VPN プロファイルを次のイベントによって自動的に接続できます。

- ユーザーのサインイン
- ネットワークの変更

[常にオン] を使用すると、手動による接続を必要とせずに、会社へのアクセスを確立できます。また、Windows 10 デバイスが省電力状態にあっても、デバイスに永続的な接続を提供することができます。Windows 10 のユーザーは、[設定]、[ネットワークとインターネット]、[VPN]、[VPN プロファイル]、[この VPN 接続を自動的に使用する] の順に選択し、アクティブ プロファイルを指定することができます。

アプリ トリガー VPN

アプリ トリガー VPN により、指定された一連のアプリの起動時に自動的に接続できるようになります。VPN の自動接続動作が拡張され、Windows 10 の VPN プロファイルで、アプリ トリガー VPN 接続がサポートされます。アプリ トリガー VPN 接続を自動的に起動するよう構成し、信頼できるアプリがネットワーク リソースを必要としている場合、安全な接続を作成できるようにします。従来のデスクトップ アプリや最新のストア アプリを含むことができる、信頼できるアプリのリストを作成することができます。アプリは、ユニバーサル アプリのパッケージのファミリ名、または従来の Windows デスクトップ アプリのファイル パスを使用して定義できます。

VPN トラフィック フィルター

VPN トラフィック フィルターは、作成したポリシーに基づいて組織ネットワークに進入が許可されるトラフィックを決定するための機能を提供します。組織ネットワーク上のリモートの脅威が増え続ける一方で、ユーザーのデバイス自体の組織的な制御は少なくなっており、デバイスからのトラフィックおよびデバイスへのトラフィックを制御することが必須になっています。ファイアウォール、プロキシ、およびその他のネットワーク関連の制限やサーバー関連の制限は便利ですが、VPN トラフィック フィルターは保護用の別のレイヤーを追加します。フィルター処理の最初のレイヤーをクライアント側に構成し、サーバー側でより高度なフィルター処理を実現できます。トラフィック フィルター規則には次の 2 種類があります。

- **アプリ ベースの規則 :** アプリ ベースの規則では、一覧に含まれるアプリから送信されたトラフィックのみが VPN の通過を許可されるようにします。この規則は、アプリ トリガー VPN によく似ていますが、クライアント側またはサーバー側で設定できます。また、アプリトリガー VPN と VPN トラフィック フィルター を併用することもできます。
- **トラフィック ベースの規則 :** トラフィック ベースの規則は、規則に一致するトラフィックのみが VPN の通過を許可されるように指定できる 5 組のポリシー (発信元 IP アドレス、発信元ポート、宛先 IP アドレス、宛先ポート、および宛先プロトコル) に基づいています。

ロックダウン VPN

ロックダウン VPN は、組織がより高いセキュリティを求めている場合、デバイス通信上の全か無かの制限を提供します。ロックダウン VPN ポリシーをデバイスに適用する場合、動作中の VPN 接続経由以外の通信は許可されません。接続することなく、デバイスは実質的に分離されています。ロックダウン VPN には、次のような特性があります。

- Windows 10 は VPN の常時接続を試みます。
- ユーザーは VPN 接続を切断できません。
- ユーザーは VPN プロファイルを削除または変更できません。
- ロックダウン VPN プロファイルは IKEv2 経由の強制トンネル接続を使用します。
- VPN 接続が利用できない場合、送信ネットワーク トラフィックはブロックされます。
- デバイスで許可されるロックダウン VPN プロファイルは 1 つのみです。

デモンストレーション : Windows 10 での VPN 接続の構成

講師は、次のデモンストレーションをおこないます。

- VPN サーバーの役割を構成する
- クライアントをイントラネットからパブリック ネットワークへ移動する
- 新しい VPN 接続を作成してテストする
- VPN サーバーがクライアントの VPN 接続を監視および管理できることを確認する

デモンストレーションの手順

VPN サーバーの役割を構成する

1. LON-RTR のサーバー マネージャーで、リモート アクセス管理コンソールを開き、作業の開始ウィザードで [VPN のみを展開します] をクリックして VPN を有効にします。
2. ルーティングとリモート アクセス コンソールが開いた場合、[LON-RTR] を右クリックし、VPN サーバーを次のオプションで構成します。
    - リモート アクセス (ダイヤルアップまたは VPN)
    - リモート アクセス : VPN
    - このサーバーをインターネットに接続するネットワーク インターフェイス : 131.107.0.2
    - 終了するまですべての既定値を受け入れ、警告ウィンドウで [OK] をクリックします。
3. ネットワーク ポリシー サーバー コンソールを開き、サーバーのネットワークポリシー [Microsoft ルーティングとリモート アクセス サーバーへの接続] を有効にします。
4. 両方のコンソールを閉じて、LON-RTR を再起動します。

クライアントをイントラネットからパブリック ネットワークへ移動する

1. LON-CL1 で、ネットワーク接続を開きます。
2. Ethernet を無効にします。
3. Ethernet 2 を有効にします。
4. Ethernet 2 で [インターネット プロトコル バージョン 4 (TCP/IPv4)] のプロパティを開き、次の設定を確認します。
    - IP アドレス : 131.107.0.20

- サブネット マスク : 255.255.255.0
- 優先 DNS サーバー : 131.107.0.100

5. ネットワーク接続を閉じます。

新しい VPN 接続を作成してテストする

1. LON-CL1 で、設定アプリを開き、[ネットワークとインターネット] で [VPN] に移動します。
2. [VPN 接続を追加する] で次の値を入力し、[保存] をクリックします。
   - VPN プロバイダー : Windows (ビルトイン)
   - 接続名 : Adatum HQ VPN
   - サーバー名またはアドレス : 131.107.0.2
3. Adatum HQ VPN に接続します。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。
4. Adatum HQ VPN の状態が「接続済み」として表示されます。

VPN サーバーがクライアントの VPN 接続を監視および管理できることを確認する

1. LON-RTR に戻り、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. リモート アクセス管理を開き、[リモート クライアントの状態] を開きます。
3. 接続の状態を確認します。Adatum¥Administrator が接続されていることを確認します。また、[アクセスの詳細] と [接続の詳細] の値を確認します。
4. リモート アクセス管理コンソールで、[RRAS 管理を開く] をクリックし、ルーティングとリモート アクセス ウィンドウを開きます。
5. [リモート アクセス クライアント] ノードと [ポート] ノードの値を確認します。[ポート] ノードで、[状態] 列を使用してアクティブなポートを右クリックして詳細を表示します。
6. ルーティングとリモート アクセス コンソールを閉じます。リモート アクセス管理コンソールに戻るので、[リモート クライアントの状態] を開きます。
7. コンソールを使用して現在の接続を切断します。

注 : 通常、これはおこないません。その理由は、リモート接続しているユーザーが作業を保存していない場合があり、突然切断されることになるためです。ここでは自分が接続を開始してテストしているため、切断しても問題ありません。

8. LON-CL1 に切り替え、ネットワーク接続を開きます。
9. [Adatum HQ VPN] という名前の新しい接続オブジェクトがあり、それが切断されていることを確認します。
10. ネットワーク接続ウィンドウを閉じます。
11. LON-RTR と LON-CL1 で開いているウィンドウをすべて閉じ、両方からサインアウトします。

接続マネージャー管理キットの概要

CMAK は、VPN 接続プロファイルを作成するために使用できるウィザード ベースのインターフェイスです。CMAK により、リモート サーバーとネットワークに対して事前定義された接続を作成することで、ユーザーのリモート接続オプションをカスタマイズすることができます。CMAK ウィザードは、実行可能ファイルを作成します。作成した実行可能ファイルは、多くの方法で配布することができます。また、展開作業においてオペレーティング システム イメージの一部として含めることができます。

- リモート サーバーとネットワーク上で事前定義された接続を作成することで、ユーザーのリモート接続エクスペリエンスをカスタマイズできる
- クライアント コンピューターで実行可能な、ネットワーク接続を確立するためのファイルを作成する
- RAS 接続の構成に関するヘルプ デスクへの要求が減少
  - 構成が既知であるため、問題解決に役立つ
  - ユーザーが自身の接続オブジェクトを構成する際の、ユーザー エラーの可能性を削減

CMAK は、既定ではインストールされないオプションのコンポーネントです。ユーザーがリモート ネットワークに接続するためにインストール可能な接続プロファイルを作成するには、CMAK をインストールする必要があります。

接続プロファイルの配布

CMAK ウィザードは、接続プロファイルをコンパイルして、ファイル名拡張子 .exe を持つ単一の実行可能ファイルを生成します。このファイルを任意の方法でユーザーに配布することができます。次のような方法があります。

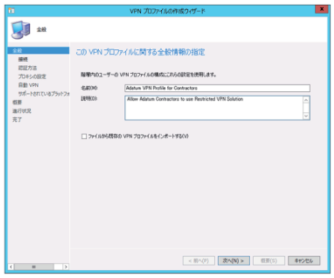
- 組織の新しいコンピューターにインストールするクライアント コンピューター イメージの一部として接続プロファイルを含めます。
- ユーザーが手動でインストールできるように、接続プロファイルをリムーバブル メディアで配布します。ユーザーにアクセスを許可する CD または DVD、USB フラッシュ ドライブ、またはその他のリムーバブル メディアで接続プロファイルのインストール プログラムを提供できます。リムーバブル メディアによっては、自動起動機能がサポートされており、ユーザーがメディアをクライアント コンピューターに挿入すると、自動的にインストールを開始できます。
- 自動化されたソフトウェア配布ツールで接続プロファイルを配布します。

多くの組織では、System Center 2012 R2 Configuration Manager などのデスクトップ管理やソフトウェア展開のためのツールを使用して、クライアント コンピューターが必要とするソフトウェアをパッケージ化して展開できるようにしています。
インストールはユーザーが意識せずにおこなうことができ、インストールが成功したかどうかが管理コンソールに報告されるように構成することができます。

管理ソリューションによる VPN 接続プロファイルの準備

CMAK と同様に、System Center 2012 R2 Configuration Manager を使用して VPN 接続プロファイルを作成することもできます。さらに、Configuration Manager を使用して、これらのプロファイルを Windows 10 デバイスに直接配布して、ユーザーが VPN にすぐに接続できるようにすることもできます。また、Configuration Manager 証明書プロファイルで構成されたサーバー検証やクライアント認証の証明書など、多様なセキュリティ設定を含めて、それらを VPN プロファイル内に展開することもできます。

- System Center 2012 R2 Configuration Manager が必要
- Microsoft Intune と統合される



次のデバイスの種類に対して、VPN プロファイルを構成できます。

- 32 ビットおよび 64 ビット バージョンの Windows 8.1 および Windows 10 を実行するデバイス
- Windows RT 8.1 を実行するデバイス
- Windows Phone 8.1 および Windows Phone 10 を実行するデバイス

注 : Windows Phone 8.1 をサポートするには、オプションの Windows Phone 8.1 拡張機能をインストールする必要があります。

- iOS 5、iOS 6、iOS 7、および iOS 8 を実行するデバイス
- Android 4.0 以降を実行するデバイス (System Center 2012 R2 Configuration Manager Service Pack 1 の場合のみ)

注 : プロファイルを iOS、Android、Windows Phone、登録済みの Windows 8.1 の各デバイスに展開するには、これらのデバイスを Microsoft Intune に登録する必要があります。

Configuration Manager のモバイル デバイス管理を使用するには、Intune サブスクリプションを所有する必要があります。これは、ドメインまたはオンプレミスのインフラストラクチャやサービスに依存しない、クラウドベースのデバイス管理ソリューションを提供します。Intune はスタンドアロンのエンタープライズ管理ソリューションを提供します。Intune を Configuration Manager と統合すると、デバイスを登録して、これらのデバイスに VPN プロファイルを提供できます。いったん展開すれば、接続を使用する以外、複雑なユーザー操作は不要です。

活動の分類

各項目を適切なカテゴリに分類してください。各項目の右側にカテゴリの番号を記入して解答してください。

項目	
1	SSL または TLS を使用する
2	IPsec に依存している
3	ヘッダーを管理するために TCP を使用する
4	PPTP と L2F を組み合わせたもの
5	Microsoft Point-to-Point 暗号化を使用する
6	Windows Vista 以降に組み込まれている
7	Windows 7 以降で使用される
8	使用されている最も古いトンネリング プロトコル
9	HTTPS を使用する

カテゴリ 1		カテゴリ 2		カテゴリ 3
PPTP		L2TP		SSTP

レッスン 4
RemoteApp のサポート

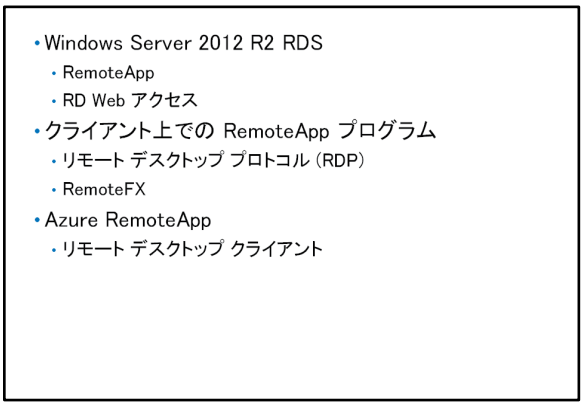
アプリケーションを各クライアントにローカルにインストールする代わりに、RD セッション ホスト サーバーにインストールして、そのアプリケーションを RemoteApp プログラムとして発行することができます。これにより、ユーザーは、クライアント コンピューターにローカルにインストールされていないアプリケーションでも実行することができます。ユーザーは、RD Web アクセス ポータルまたはスタート メニューから RemoteApp プログラムを起動できます。また、ユーザーが RemoteApp とデスクトップ接続機能を使用している場合は、関連付けられたファイル名拡張子を持つファイルをダブルクリックして RemoteApp プログラムを起動することもできます。信頼済み証明書を使用して RDS の展開を構成すると、RemoteApp プログラムの起動時にダイアログが表示されず、ユーザーにシームレスなエクスペリエンスを提供できます。BYOD シナリオでは、モバイル デバイスや、組織の場所から離れたところにある任意のデバイスに RemoteApp 機能を提供するように求められる場合があります。Azure RemoteApp を使用すると、デバイスはインターネットに接続できればどこからでも、高レベルな Azure セキュリティで RemoteApp を展開できます。

目的

このレッスンにより、次のことを習得できます。

- RemoteApp を展開するオプションを説明することができます。
- RDS を使用して RemoteApp をサポートするために必要なインフラストラクチャを説明することができます。
- RemoteApp を発行するためのセッション コレクションを説明することができます。
- RDS RemoteApp のアプリケーションを発行することができます。
- Azure RemoteApp を説明することができます。
- Azure RemoteApp でアプリケーションを発行する方法を説明することができます。
- RemoteApp コレクションを作成するプロセスを説明することができます。

RemoteApp の展開オプション



アプリケーションをリモートで使用できるように RemoteApp プログラムとして発行するには、まず各 RD セッション ホスト サーバーで、アプリケーションを提供するセッション コレクションにそれをインストールする必要があります。アプリケーションを適切に計画してインストールすると、ユーザーはマルチユーザー環境でアプリケーションにアクセスできます。RD セッション ホストの役割をインストールしてから、リモートで展開するすべてのアプリケーションをインストールする必要があります。また、Azure RemoteApp を使用すると、RemoteApp プログラムを RD セッション ホスト サーバーに展開して、それらのホストを維持する負担を軽減することができます。これにより、Azure ポータルから RemoteApp プログラム自体のサポートに集中できます。

Windows Server 2012 R2 の RemoteApp

Windows Server 2008 から Windows Server 2012 R2 までの間に RemoteApp は大幅に変更されました。Windows Server 2008 では、各 RD セッション ホスト サーバーで Microsoft 管理コンソールを使用して RemoteApp を管理していました。Windows Server 2012 では、RemoteApp はサーバー マネージャーで RDS を介して管理されます。また、すべての RD セッション ホスト サーバーを 1 つのサーバー マネージャーから集中管理することもできます。発行済みの RemoteApp プログラムおよびリモート デスクトップへのリンクを作成して、RD Web アクセスから使用できるようにします。RD Web アクセスは RD セッション ホスト RemoteApp プログラムへのポータルとして機能するオンプレミスの Web サイトです。この場合、ユーザーは Web サイトから RemoteApp を検索して実行します。

クライアント上での RemoteApp プログラム

RemoteApp プログラムは、ローカルにインストールしたアプリケーションと同様に、ローカルのクライアント デスクトップと統合できます。RemoteApp プログラムはローカルにインストールされたアプリケーションと並行して実行されるため、ユーザーは RemoteApp プログラムがリモートで実行されているとは気づかない場合もあります。RemoteApp プログラムには次の機能があります。

- **ダイアログを表示せずに RemoteApp プログラムを起動 :** RemoteApp プログラムのリンクまたはアイコンをクリックすると、ダイアログの表示やユーザー操作なしにプログラムを起動できます。バックグラウンドでは、クライアントはリモート デスクトップ プロトコル (RDP) 接続を確立し、サインインし、リモート プログラムを起動し、そのウィンドウを表示します。
- **独自のウィンドウで実行 :** RemoteApp プログラムは、クライアントで独自のウィンドウに表示します。他のアプリケーション ウィンドウと同じように、ウィンドウの移動、サイズ変更、最小化、最大化、または閉じることができます。RemoteApp ウィンドウは、ウィンドウの移動またはサイズ変更の間にもその内容を表示できます。
- **ファイル名関連付けを使用した RemoteApp プログラムの起動 :** RemoteApp プログラムは、[RD Web アクセス] ページから、スタート メニューから、または関連付けられたファイル名拡張子を持つファイルをダブルクリックして起動できます。
- **ライブ サムネイルとアプリケーションの切り替え :** RemoteApp プログラム アイコンは、プログラムが最小化されている場合でもタスク バーに表示されます。RemoteApp プログラムの複数のインスタンスを実行している場合、複数のタブ付きプログラム アイコンがタスク バーに表示されます。タスク バー アイコンにポインターを重ねると、プログラム ウィンドウのライブ サムネイルが表示されます。標準のキーの組み合わせ Alt+Tab を使用すると、RemoteApp プログラムを含めて、実行中のプログラム間を切り替えることができます。
- **ローカルにインストールされたアプリと同様のアイコンを表示 :** RemoteApp プログラムでは、ローカルにインストールされたアプリケーションと同様のアイコンがタスク バーに表示されますが、アイコンにリモート デスクトップのシンボルが付きます。アイコン オーバーレイをサポートしているため、RemoteApp プログラムの状態の変化に気づくことができます。例えば、Outlook では新しいメールの受信を通知する手紙マークのオーバーレイが使用されます。

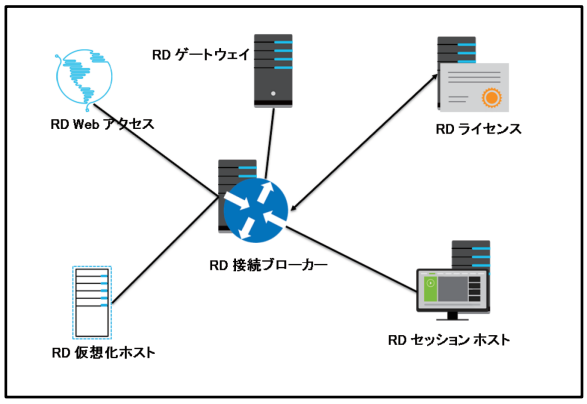
Azure RemoteApp

RemoteApp を RD セッション ホストから実行した場合と Azure から実行した場合とでは、ユーザーからするとほとんど違いはわかりません。Azure と RDS RemoteApp では、RDP を RemoteFX ワイド エリア ネットワーク (WAN) 加速設定で使用してアプリケーション ウィンドウを配信できます。この場合、アプリはモバイル デバイス上ではなく、クラウドにあるリソース上で実行されるため、モバイル デバイスはデスクトップと同じように強力になります。

Azure RemoteApp で使用するためのアプリの準備は、難しくも複雑でもありません。ユーザーは、Azure RemoteApp プログラムが作成されるとすぐに、これにサインインして使用できます。アプリは、通常の更新プログラムによって常に最新に維持され、Microsoft マルウェア対策ソフトウェアを通じて継続的なマルウェア対策が提供されます。管理者は、どのアプリをどのユーザーに提供するかを考慮するだけで済みます。

Azure では、登録ユーザーごとに 50 GB の専用の RemoteApp 記憶域が提供されるため、記憶域の容量が少ないモバイル デバイスでも RemoteApp から Azure にファイルやデータを保存できます。

リモート デスクトップ サービスにより RemoteApp をサポートするために必要なインフラストラクチャ



RemoteApp は実装されている使用可能な RDS インフラストラクチャに依存します。RDS は Windows Server 2012 R2 の役割で、次の役割サービスを含みます。

- **RD セッション ホスト :** この役割サービスにより、サーバーは、RemoteApp を介した Windows ベースのプログラムや Windows デスクトップ全体をホストすることができます。ユーザーは RD セッション ホスト サーバーに接続し、アプリケーションを実行して RD セッション ホストが提供するネットワーク リソースを使用できます。ユーザーは、RDC クライアントまたはその他の RDP クライアントを使用する場合、RD セッション ホスト サーバーにアクセスできます。RD セッション ホストは、RDS 展開でセッションベースのデスクトップを提供する場合に必要な役割サービスです。
- **リモート デスクトップ仮想化ホスト (RD 仮想化ホスト) :** この役割サービスは、Windows Server 2012 R2 の Hyper-V の役割と統合して、仮想デスクトップとして使用できる仮想マシンを提供します。また、RD 仮想化ホストは、確立されたクライアント セッションを監視し、リモート デスクトップ接続ブローカー (RD 接続ブローカー) サーバーに報告します。仮想マシンは、保存された状態であった場合、中断された場所から再開します。仮想マシンは、設定された期間に仮想マシンへの接続がない場合、保存された状態になります。プールされた仮想マシンの場合、ユーザーがサインアウトしたときに初期状態に戻されます。RD 仮想化ホストは、RDS 展開が仮想マシンベースのデスクトップを提供する場合に必要な役割サービスです。
- **RD 接続ブローカー :** この役割サービスは、RemoteApp プログラムや仮想デスクトップへの接続を管理し、クライアントの接続要求を適切なエンドポイントに転送します。また、RD 接続ブローカーは、セッションの再接続とセッションの負荷分散もおこないます。例えば、ユーザーがセッションから切断され、後で接続を確立する場合、RD 接続ブローカーの役割サービスは、ユーザーが既存のセッションに再接続されるようにします。
- **RD Web アクセス :** この役割サービスは、RemoteApp プログラム、リモート デスクトップ、仮想デスクトップなどの RDS リソースに、ユーザーが Web ブラウザー経由でアクセスするためのリンクを提供します。Web ページでは、そのユーザーに公開されているすべての RDS リソースのカスタマイズされたビューが表示されます。この役割サービスはリソースのフォルダー分けをサポートしており、管理者はリモート アプリケーションを論理的にグループ分けすることができます。また、RDWeb フィードで使用可能な RDS リソースを公開し、それをクライアント デバイスのスタート メニューに組み込むことができます。RD Web アクセスは、各 RDS 展開に必須の役割サービスです。
- **リモート デスクトップ ライセンス (RD ライセンス) :** この役割サービスは、RD セッション ホスト サーバーに接続するために各デバイスまたはユーザーに必要なリモート デスクトップ サービス クライアント アクセス ライセンス (RDS CAL) を管理します。RD ライセンスを使用して、RD ライセンス サーバーに RDS CAL をインストール、発行し、その可用性を追跡します。

- **リモート デスクトップ ゲートウェイ (RD ゲートウェイ) :** この役割サービスを使用して、承認されたリモート ユーザーは、インターネット接続されたデバイスから、RDP トラフィックを HTTPS エンベロープにカプセル化することで、組織内のネットワーク上のリソースに接続できます。リモート デスクトップの接続承認ポリシー (RD CAP) とリモート デスクトップのリソース承認ポリシー (RD RAP) を構成して、アクセスを制御します。RD CAP では、接続を承認するユーザーを指定し、RD RAP では承認されたユーザーが接続できるリソースを指定します。

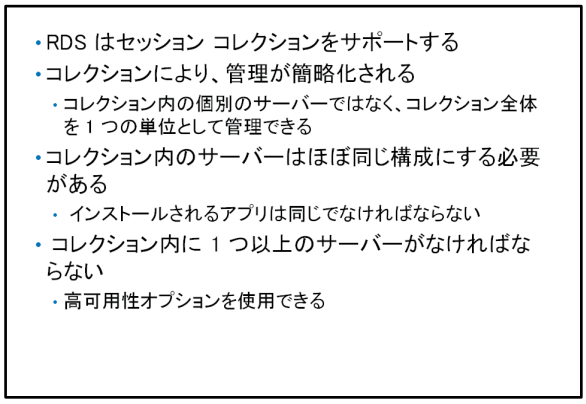
オンプレミス サーバーに対してリモートでのアプリケーション展開を計画する場合は、次の要素を考慮します。

- **マルチユーザー環境に対する適合性 :** これは最も重要な考慮事項です。これまで、大半のエンド ユーザー アプリケーションは、マルチユーザー環境でも問題なく機能しています。ただし、これは必ずしもそうとは限りません。アプリケーションがマルチユーザー構成をサポートしているかどうかをアプリケーション ベンダーに確認する必要があります。ベンダーによっては、マルチユーザー環境にアプリケーションを展開できるようにする修正プログラムを提供しています。提供されない場合は、アプリケーションを従来のデスクトップに展開するか、マルチユーザー環境をサポートしている別のアプリケーションを探す必要があります。
- **アプリケーションの互換性 :** 既存のアプリケーションについて、RD セッション ホスト サーバーで互換性の問題がないかどうかを調査する必要があります。必ずアプリケーションを完全にテストしてから、運用環境に組み込んでください。互換性のないアプリケーションを相互に分離して実行できるようにするために、複数の RD セッション ホスト サーバーが必要になる場合があります。さらに、アプリケーション サイロを作成するために、複数のセッション コレクションが必要になる場合もあります。
- **アプリケーションの依存関係 :** 関連するアプリケーションまたは他のローカルのアプリケーションと依存関係を持つアプリケーションは、同じ RD セッション ホスト サーバーにインストールしてください。特にベンダーによる指定がない限り、例えば、アプリケーション スイート内のすべてのアプリケーションは、同じ RD セッション ホスト サーバーにインストールする必要があります。
- **容量の要件 :** 1 つの RD セッション ホスト サーバーでサポートできるクライアント数については、決まった数はありません。リモートで配信されるアプリケーションのリソース要件は、アプリケーション要件、同時セッション数、RD セッション ホストが実行している各種アプリケーションやその他のサービスの数など、さまざまな要素に依存します。サイジングのガイドとして役立つツールをいくつか利用できます。サーバー管理者は、RD セッション ホスト サーバーのパフォーマンスを念入りに監視し、エンド ユーザーからのフィードバックに耳を傾け、必要に応じてサーバー リソースを追加する必要があります。

RD 接続ブローカー、RD Web アクセス、および RD セッション ホストまたは RD 仮想化ホストのいずれかの役割サービスを、各 RDS 展開にインストールして RDS を管理する必要があります。必要な場合は、追加の RDS 役割サービスをインストールできます。また、同じ RDS 役割サービスを持つ複数のサーバーをインストールして、高可用性を実現することもできます。RDS は Active Directory 環境にのみ展開できますが、AD DS は RDS 役割サービスではありません。

注 : RDS 対応のインストーラー (Windows インストーラーなど) を使用するアプリケーションをインストールする場合、RD セッション ホストは、インストール中はインストール モードに自動的に切り替わり、アプリケーションがインストールされると実行モードに戻ります。

RemoteApp を発行するためのセッション コレクションの概要



Windows Server 2012 R2 では、RDS セッション ファームという用語は使用せず、代わりにセッション コレクションという用語を使用するようになりました。ファームとセッションの違いは、コレクションは、ファームとは異なり、DNS にエントリを持たない点です。このため、クライアントは完全なアドレスを読み取り、このアドレスで RDS 展開とコレクションをホストし、RD ゲートウェイ プロパティを含む RD 接続ブローカーへのアクセスを提供します。ファームと同様に、コレクションは、RDS サーバーを個別に管理するのではなく、RDS サーバーのグループに対して 1 つの管理ポイントを提供します。接続するエンド ユーザー側には、何も違いはありません。

セッション コレクションを作成する場合、限定された構成オプション セットのみ使用できます。このことは、サーバー マネージャーまたは Windows PowerShell のどちらを使用してコレクションを作成しているかに関係なく、当てはまります。セッション コレクションを作成する場合、その初期設定の変更、追加設定の構成、追加タスクの実行が可能です。例えば、RemoteApp プログラムの発行、コレクションへの RD セッション ホストの追加または削除をおこなったり、コレクション内のサーバーからの既存の接続を切断したりできます。

変更できるセッション コレクションのプロパティを次の表に示します。

ページ	説明
全般	[全般] ページで、コレクション名と説明を編集できます。また、RD Web アクセスにコレクションを表示するかどうかを指定できます。既定の設定では、RD Web アクセスにコレクションを表示します。
ユーザー グループ	コレクション内の RD セッション ホストに接続して、コレクション内の任意の RemoteApp プログラムにアクセスできるようにする AD DS セキュリティ グループを指定できます。RemoteApp プログラムを実行するには、ユーザーは RemoteApp プログラムへのアクセス権も必要であることに注意してください。
セッション	[セッション] ページでは、次のセッション設定を構成できます。 • セッションの切断後からセッション終了までの時間 • アクティブ セッションのセッション時間制限 • アイドル セッション時間制限 • セッション制限に達した場合または接続が中断された場合に、セッションを切断するかまたは終了するか • 一時フォルダー設定 (セッションごとに一時フォルダーを使用するかどうか、および終了時にそれを削除するかどうか)
セキュリティ	• クライアントとサーバー間のセキュリティ設定を指定できます。既定では、クライアントがサポートできる最も安全な層を使用するようにセキュリティ設定をネゴシエートします。 • 暗号化レベルを指定できます。既定では、クライアント互換の暗号化レベルが使用されます。 • リモート デスクトップをネットワーク レベル認証で実行しているクライアントからの接続のみを許可するように指定することもできます。

ページ	説明
負荷分散	コレクション内に複数の RD セッション ホスト サーバーがある場合、各 RD セッション ホストで作成できるセッション数を指定し、相対的な重みを使用してコレクション内のサーバー間でセッションの作成を優先度付けすることができます。
クライアント設定	ユーザーがセッションベースのデスクトップ展開に接続する場合、クリップボードやプリンターなど、クライアント デバイス上のデバイスやリソースを指定できます。また、ユーザー セッションごとのリダイレクトされるモニターの最大数を制限することもできます。
ユーザー プロファイル ディスク	クライアントがコレクション内のサーバーに接続する際のユーザー プロファイル ディスクの使用を構成できます。このサーバーにユーザー プロファイル ディスクが保存されますが、そのディスクのサイズを制限することができます。ユーザー プロファイル ディスクから除外するユーザー プロファイルのファイルとフォルダーを指定することもできます。

Windows PowerShell を使用してセッション コレクション設定を構成する場合は、Set-RDSessionCollectionConfiguration コマンドレットを使用できます。

RD セッション ホスト サーバーへのアプリケーションのインストール

RD セッション ホスト サーバーへのアプリケーションのインストールは、従来のデスクトップへのアプリケーションのインストールとは異なります。RD セッション ホスト サーバーは、インストール モードと実行モードの 2 つのモードで動作します。マルチユーザー アプリケーションを適切にインストールするには、サーバーをインストール モードにする必要があります。インストール モードでは、Windows オペレーティング システムは、アプリケーションがマルチユーザー環境で機能するのに適したレジストリ エントリと初期化 (.ini) ファイル設定が構成されるようにします。アプリケーションが正常にインストールされた後、サーバーを実行モードに戻す必要があります。サーバーのモードを変更するには、次を使用できます。

- コマンド プロンプト
- コントロール パネル項目

注 : インストール モードは、RD セッション ホストの役割サービスがインストールされていないコンピューターには適用されません。このようなサーバーは常に実行モードで実行されます。

コマンド プロンプト

コマンド プロンプトを使用してアプリケーションを RD セッション ホスト サーバーにインストールするには、コマンド プロンプトを開いて次の手順を実行します。

- change user /install コマンドを使用してサーバーをインストール モードにします。
- アプリケーションをインストールします。
- change user /execute コマンドを使用してサーバーを実行モードに戻し、ユーザーがアプリケーションにアクセスできるようにします。

参考資料 : 現在のサーバーのモードを確認するには、change user /query コマンドを使用します。change user コマンドについては、次のサイトを参照してください。
ユーザーの変更
https://technet.microsoft.com/ja-jp/library/cc730696.aspx

コントロール パネル項目

コントロール パネルの [プログラム] セクションに、[リモート デスクトップ サーバーへのアプリケーションのインストール] 項目が表示されます。この項目はサーバーを自動的にインストール モードにするウィザードを開始し、アプリケーションの実行可能なインストール ファイルの場所の入力を求めるダイアログを表示します。管理者はアプリケーションをインストールしてウィザードを完了させます。インストールが完了すると、RD セッション ホストは実行モードに戻ります。

参考資料 : Microsoft Application Virtualization (App-V) を RDS で使用して、仮想化アプリケーションを RemoteApp プログラムとして展開することができます。App-V と RDS の統合については、次のサイトを参照してください。
INTEGRATING APP-V WITH MICROSOFT® VDI
http://go.microsoft.com/fwlink/?LinkID=510044&clcid=0x409

デモンストレーション : リモート デスクトップ サービス RemoteApp のアプリケーションの発行

講師は、次のデモンストレーションをおこないます。

- RD Web アクセスで RemoteApp プログラムを発行する
- 発行された RemoteApp をクライアントで検証する
- 仮想マシンを戻す

デモンストレーションの手順

RD Web アクセスで RemoteApp プログラムを発行する

1. LON-SVR2 で、エクスプローラーを開き、C:¥RemoteAppSoftware XmlNotepad.msi ファイルを実行します。XML Notepad 2007 セットアップ ウィザードで、すべての既定値を受け入れます。終了したら閉じます。
2. Internet Explorer とエクスプローラーを閉じます。
3. サーバー マネージャーで、[RDS] を開き、[QuickSessionCollection] をクリックします。
4. 詳細ウィンドウで、RemoteApp プログラム ウィンドウを見つけ、[タスク] をクリックして、[RemoteApp プログラムの発行] を選択します。
5. RemoteApp プログラムの発行ウィンドウで、RemoteApp で展開できるさまざまなプログラムのすべてを確認します。
6. RemoteApp プログラムの選択ウィンドウで、[追加] をクリックします。
7. [ウィンドウを開く] で、C:¥Program Files (X86)¥XML Notepad 2007 に移動し、[XmlNotepad.exe] を選択します。
8. RemoteApp プログラムの選択ウィンドウで、[次へ] をクリックします。
9. [確認] ページで、[発行] をクリックします。
10. [完了] ページで [閉じる] をクリックします。

発行された RemoteApp をクライアントで検証する

1. LON-CL1 で、Internet Explorer (Microsoft Edge ブラウザーではない) を開き、https://lon-svr2.adatum.com/RDWeb に移動します。LON-SVR2 の RD Web アクセス Web ページが表示されます。

注 : Lync Web ブラウザー ヘルパーを展開するように求めるメッセージ バーが開いた場合は、[有効にしない] をクリックし、Internet Explorer セットアップ ウィンドウが開いた場合は、[お勧めのセキュリティと互換性の設定を使う] を選択して、[OK] をクリックします。待機状態のタブを閉じて Microsoft.com へ移動します。

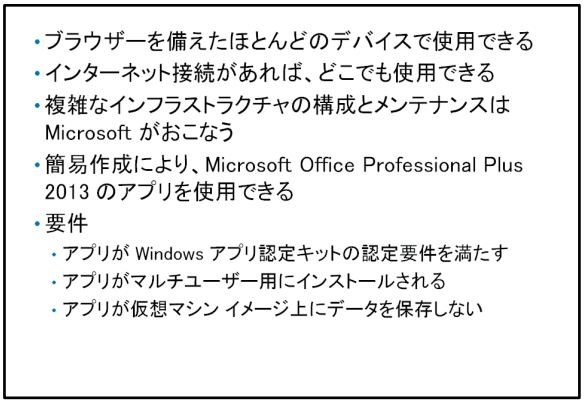
2. Microsoft リモート デスクトップ サービスの Web アクセス アドオンを許可します。
3. ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
4. [時間単価型リソース] ページに、使用可能な RemoteApp プログラムが表示されます。電卓、ペイント、ワードパット、および XmlNotePad が表示されるはずです。[XmlNotePad] をクリックします。
5. RemoteApp セキュリティ ウィンドウで、[接続] をクリックします。表示されるまでしばらくかかる場合があります。
6. XML Notepad ウィンドウが表示されたら、[開く] アイコン (フォルダーのような形) をクリックします。表示されるのが LON-CL1 ではなく LON-SRV2 のフォルダー構造であることに注意してください。管理者としてサインインしているため、ディレクトリ ツリーを遡ってこのことを確認することもできます。
7. 開いているウィンドウをすべて閉じ、サインアウトします。

仮想マシンを戻す

デモンストレーションが完了したら、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-SVR2 と 23697-2B-LON-CL1 に対して、手順 2 ～ 3 を繰り返します。

Azure RemoteApp の概要



Azure RemoteApp は RDS RemoteApp と似ていますが、同じではありません。ユーザーから見るとほぼ同じで、アプリを RDS から使用しても Azure から使用しても、ユーザー インターフェイスは同じです。ただし、認証要件は異なり、ユーザーはそれぞれ別の URL を使用して RemoteApp を起動します。Azure の基本的なインフラストラクチャ要件は、ブラウザー、インターネット接続、およびデバイスです。

Azure には 2 つの異なる管理ポータル、Azure クラシック ポータルと、以前はプレビュー ポータルと呼ばれていた Azure ポータルがあり、これらを使用して Azure サブスクリプションを管理できます。各ポータルの URL は、次のように若干異なります。

- **Azure クラシック ポータル :** https://manage.windowsazure.com
- **Azure ポータル :** https://portal.azure.com

この 2 つのポータルは、ポータル内から相互に切り替えることもできます。

Azure RemoteApp を使用するメリット

Azure RemoteApp は、全体的な Azure サブスクリプションの一部で、Azure で RemoteApp をホストするには別のコストがかかります。Basic、Standard、Premium などのプランがあります。価格はさまざまですので、詳細については Azure ポータルを参照してください。Azure RemoteApp にはコストが伴いますが、独自のインフラストラクチャを使用して RDS RemoteApp を展開する場合でもコストはかかります。RDS RemoteApp をどのサーバーに配置し、物理サーバー上で仮想化するかどうかだけでなく、どの種類とレベルの冗長化やフォールト トレランスが必要で、消費が増大した場合はどのようにしてインフラストラクチャを拡張してすばやく需要に対応できるかなど、さまざまな考慮が必要になります。RDS では、サーバーと接続するユーザーおよびデバイスの両方に対して、ライセンス料が伴います。テープ、ディスク ドライブ、リモート バックアップ サーバーなどを使用して、バックアップを実行し、バックアップ ソリューションを用意する必要があります。

Azure では、Microsoft がこのような計画とサポートのすべてを実行します。そのため、管理者はアプリを展開して、ユーザーに管理と認証方法を提供するだけで済みます。Azure に登録している多くの組織が、AD DS をサブスクリプションの Azure AD と同期して、ユーザーがドメイン メンバーであるデバイスから Azure RemoteApp プログラムに接続したときに、ユーザーに SSO 機能を提供しています。

Azure RemoteApp のもう 1 つの主なメリットは、実質的にどのようなプラットフォームでも実行できることです。Windows 10 と Windows 10 Mobile、Apple iOS と OS X、および Android デバイスはすべて、Azure RemoteApp を使用できます。Azure に登録しているユーザーは、これらのどのデバイスでも、デバイスがインターネットに接続できればどこからでも Azure RemoteApp を使用できます。

Azure RemoteApp の要件

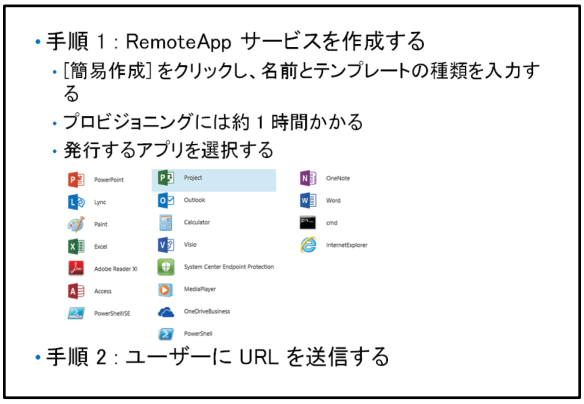
Azure RemoteApp は、Windows Server 2012 R2 イメージ上で 32 ビットまたは 64 ビットの Windows ベースのアプリをストリーミングします。そのため、アプリは Windows Server オペレーティング システム上で実行できる必要があります。さらに、アプリは次の条件を満たす必要があります。

- アプリが Windows アプリ認定キットの認定要件を満たし、RDS プログラミング ガイドラインに準拠している必要があります。
- アプリは、シングル ユーザー用ではなくマルチユーザー用にインストールする必要があります。
- アプリは、イメージ上または RemoteApp インスタンス上に、ローカルにデータを保存しないようにする必要があります。RemoteApp コレクションの作成後、インスタンスは複製してステートレスにし、アプリケーションのみを含める必要があります。データは外部ソースまたはユーザーのプロファイルに保存してください。
- カスタム イメージには、失われる可能性のあるデータを絶対に含めないでください。

参考資料 : Azure RemoteApp の要件については、次のサイトを参照してください。
アプリの要件
https://azure.microsoft.com/ja-jp/documentation/articles/remoteapp-appreqs/

Azure RemoteApp でのアプリケーションの発行

Azure RemoteApp を展開する最も簡単な方法は、管理ポータルの [アプリケーション サービス] の [RemoteApp] セクションに組み込まれている簡易作成機能を使用することです。これは必要な RemoteApp プログラムを含む Windows Server 2012 R2 仮想マシンを展開し、そこから RemoteApp イメージを作成します。RemoteApp プログラムを使用するときには、イメージがユーザーのデバイスに読み込まれ、その中のアプリが、ローカルにインストールされたアプリと同じように使用できるようになります。閉じると、RemoteApp イメージはオフになります。



簡易作成機能を使用して Azure RemoteApp を展開するには、次に示す 2 つの主要手順に従います。

手順 1 : RemoteApp サービスを作成する

1. Azure クラシック ポータルにサインインし、コンソール ツリーで RemoteApp まで下にスクロールします。
2. コンソール ツリーの下の正符号 (+) をクリックします。詳細ウィンドウで [簡易作成] をクリックします。
3. 詳細ウィンドウの右端で、RemoteApp の一意の名前を入力します。RemoteApp プログラムの名前は先頭を文字にする必要があり、文字と数字のみを含めることができ、3 ～ 13 文字の長さにする必要があります。[地域] ドロップダウン リストで地域を選択し、[プラン] ドロップダウン リストで [Basic]、[Standard] などを選択します。最後に、[テンプレート イメージ] ドロップダウン リストで、Office Professional Plus (30-day trial)、Office 365 ProPlus (Subscription required)、または Windows Server 2012 を選択します。
4. 名前を適用して前述のように選択をおこなった後、ウィンドウの右下にある [RemoteApp コレクションの作成] チェック マーク アイコンをクリックします。
5. RemoteApp 簡易作成は、最初に仮想マシンを作成してからそのイメージを作成する必要があるため、この時点で処理が完了するまでに約 1 時間ほどかかります。この処理の間、RemoteApp 詳細ウィンドウには、RemoteApp の状態は [準備中] と表示されます。
6. 準備の完了後、状態は [アクティブ] に変わります。RemoteApp 名をクリックすると、[RemoteApp コレクションが作成されました] ページが開きます。
7. [RemoteApp プログラムの発行] と [ユーザー アクセスの構成] という 2 つのボタンがあります。両方の操作をおこなう必要があります。
8. [RemoteApp プログラムの発行] リンクをクリックします。RemoteApp プログラムの選択ウィンドウが開き、RemoteApp プログラムとして実行するすべてのアプリのチェック ボックスをオンにすることができます。Office Professional Plus で使用できるアプリの選択には、次のものがあります。
    - Windows PowerShell Integrated Scripting Environment (ISE)
    - Lync
    - OneNote
    - OneDrive for Business
    - PowerPoint
    - Windows Media Player

- Microsoft Project
- Access
- Visio
- Excel
- System Center Endpoint Protection
- ペイント
- Adobe Reader XI
- Outlook
- 電卓
- Cmd
- Word
- Windows PowerShell
- Internet Explorer

注 : これらの多くは、標準の Windows オペレーティング システム コンポーネント (例えば cmd とペイント) ですが、Microsoft 以外のデバイスに展開されても、Windows ベースのシステムで実行しているかのように動作します。

9. アプリの選択をおこなった後、ウィンドウの右下にあるチェック ボックスをオンにします。
10. 画面の下部にアプリが発行中であることを示すグレーのバーが表示され、発行が終了すると消えます。これはほんの数分で終了します。

次の手順では、ユーザーに Azure RemoteApp へのアクセス権を付与します。この手順に進む前に、ユーザーを作成する必要があります。また AD DS を Azure AD と同期していない場合は、同期する必要があります。

手順 2 : ユーザーに URL を送信する

1. コンソール ツリーで [Azure AD] アイコンをクリックし、Azure AD のユーザーを作成します。RemoteApp コレクションで戻る矢印をクリックすると、コンソール ツリーを最大化できます。
2. 詳細ウィンドウで、[既定] フォルダーリをクリックし、[ユーザー] 列をクリックして、ページ下部にある [ユーザーの追加] アイコンをクリックします。
3. [このユーザーに関する情報の入力] ページで、ドロップダウン矢印を使用してユーザーの種類 ([組織内の新しいユーザー]、[既存の Microsoft アカウントを持つユーザー]、[別の Azure AD ディレクトリ内のユーザー]) を選択します。ユーザーの種類の選択後、[ユーザー名] ボックスに名前を入力できます。定数「@」の後ろに Azure AD 用の別のドロップダウン矢印があることを確認します。このウィンドウの下部に、進む矢印とその矢印の右に数字「2」と「3」があります。これは、設定するページがあと 2 ページあることを示しています。
4. 2 ページ目には、3 つのボックス、ユーザーの [名]、[姓]、[表示名] があります。この情報の入力後、[ロール] という名前のドロップダウン リストを確認します。これには次の 6 つのロールが含まれます。[ユーザー]、[全体管理者]、[課金管理者]、[サービス管理者]、[ユーザー管理者]、[パスワード管理者]。1 つを選択し、進む矢印をクリックして最後のページに進みます。

5. 最後のページは、[一時パスワードの取得] ページです。パスワードをメモしておきます。ユーザーは、RemoteApp プログラムに最初にサインインしたときに、このパスワードを変更する必要があります。その際、一時パスワードと永続的なパスワードを入力する必要があります。[作成] をクリックします。[新しいパスワード] ページが再度読み込まれます。その横に [コピー] アイコンがあります。ページの右下隅にあるチェック アイコンをクリックします。
6. これで、RemoteApp に戻り、アプリへのユーザー アクセスを設定できます。
7. 名前の付いた RemoteApp ウィンドウで、[ユーザー アクセスの構成] リンクをクリックします。
8. Microsoft アカウントによって一覧される、Azure 管理者は、既にアクセス権を持っていることに注意してください。[ユーザー名を入力] ボックスを確認します。先ほど作成したユーザー名を入力します。ページの下部にある [保存] アイコンをクリックし、ページの左上の戻る矢印をクリックします。

注 : [RemoteApp プログラムの発行] 領域の下にあるリモート デスクトップ クライアントのダウンロード URL を確認します。その横にある [コピー] アイコンを使用して URL をコピーして、それを RemoteApp ユーザーに送信します。

RemoteApp コレクションの作成プロセス

簡易作成オプションを使用して基幹業務 (LOB) アプリを発行することはできません。[簡易作成] ではなく、[VPN 接続の作成] をクリックして開始します。また、RDS サーバーの役割でセットアップされた Azure 仮想マシンを使用してアプリを展開することもできます。Azure には、RDS の役割をインストールして事前設定された Windows Server 2012 R2 の VM テンプレートが用意されています。

[VPN 接続の作成] を使用するには、次の 8 つの主な手順に従います。

1. ディレクトリ同期を構成します。RemoteApp では、[パスワードの同期] オプションを使用して Azure AD 同期を構成するか、このオプションを使用せずに、AD FS とフェデレーションをおこなうドメインを使用して Azure AD 同期を構成するかのどちらかによって、Azure AD と統合する必要があります。
2. コレクションに使用するイメージを選択します。カスタム イメージを作成するか、または前述した事前設定された仮想マシンなど、サブスクリプションに含まれる Microsoft イメージのいずれかを使用することができます。
3. 仮想ネットワークをセットアップします。仮想ネットワークは、ユーザーが RemoteApp リソースを介してローカル ネットワーク上のデータにアクセスするのを許可します。Azure 仮想ネットワークを使用すると、コレクションは、その仮想ネットワークに展開されている他の Azure サービスや仮想マシンに直接ネットワーク アクセスできます。
4. RemoteApp コレクションを作成します。ここで実際に [VPN 接続の作成] オプションをクリックします。コレクションの名前を入力し、使用するプランとして [Standard]、[Basic] などを選択します。[RemoteApp コレクションの作成] をクリックします。作成には数分かかります。完了すると、[RemoteApp コレクションが作成されました] ページが表示されます。

5. コレクションを仮想ネットワークにリンクします。ここで、[仮想ネットワークを関連付ける] をクリックし、ドロップダウン リストで使用する仮想ネットワークを選択し、使用する地域を選択します。ローカル Active Directory ドメインに RemoteApp サービス アカウントを追加する場合は、ここで [ローカル ドメインに参加する] をクリックします。ドメイン名、組織単位、サービス アカウントのユーザー名、およびパスワードが必要です。
6. テンプレート イメージをコレクションに追加します。新しいテンプレート イメージを作成するか、既存のイメージ、つまり、Azure RemoteApp に既にインポートまたはアップロードされたものにリンクすることができます。LOB アプリをインストールしている仮想マシンをアップロードおよびインポートすることができます。また、以前から存在するイメージを使用することもできますが、その場合は、ここで説明した手順よりもクイック スタートを使用する方が簡単です。
7. RemoteApp プログラムを発行します。この手順については、前のトピックで説明しました。
8. ユーザー アクセスを構成します。この手順については、前のトピックで説明しました。

操作手順の並べ替え

RemoteApp コレクションを作成します。次の各手順に番号を付けて正しい順序を示してください。

	手順
	RemoteApp アプリを発行します。
	コレクションを仮想ネットワークにリンクします。
	ディレクトリ同期を構成します。
	仮想ネットワークをセットアップします。
	コレクションに使用するイメージを選択します。
	RemoteApp コレクションを作成します。
	テンプレート イメージをコレクションに追加します。
	ユーザー アクセスを構成します。

演習 B : Microsoft Azure RemoteApp の構成

シナリオ

あなたは、最近入手した Azure の評価版サブスクリプションを検討し、Azure RemoteApp を評価することになりました。オンライン サービスの機能を評価するために、Azure RemoteApp を構成し、サンプル アプリケーションを発行します。

目的

この演習により、次のことを習得できます。

- RemoteApp コレクションを作成することができます。
- Azure RemoteApp を使用してアプリケーションを発行することができます。
- リモート接続を検証することができます。

演習のセットアップ

予定所要時間 : 75 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL4 MSL-TMG1
ユーザー名	Adatum¥Administrator Admin
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$$w0rd
5. Hyper-V マネージャーで [23697-2B-LON-CL4] をクリックし、操作ウィンドウで [起動] をクリックします。
6. 操作ウィンドウで [接続] をクリックします。仮想マシンが起動するまで待ちます。
7. 次の資格情報を使用してサインインします。
    - ユーザー名 : Admin
    - パスワード : Pa$$w0rd
8. MSL-TMG1 が稼働していることを確認する必要があります。稼働していない場合は、次を実行します。
    - Hyper-V マネージャーで [MSL-TMG1] をクリックし、操作ウィンドウで [起動] をクリックします。

- この MSL-TMG1 マシンにサインインする必要はありません。練習 1 を開始する前にサインイン画面で稼働していることを確認します。
- 第 5 章で Azure 評価版サブスクリプションを使用して作成した Azure アカウントとパスワードを使用する必要があります。

練習 1 : RemoteApp コレクションの作成

シナリオ

あなたは、クライアント コンピューターからの Azure RemoteApp をテストする前に、コレクションを作成する必要があります。これは、Azure ポータル内の簡易作成機能を使用することにより実行できます。

主な作業は次のとおりです。

1. RemoteApp コレクションを作成する

▶ 作業 1 : RemoteApp コレクションを作成する

1. LON-CL4 で、Microsoft Edge ブラウザーを開き、https://manage.windowsazure.com に移動します。
2. 第 5 章で作成した Azure 評価版サブスクリプション アカウントとパスワードを使用して、Azure ポータルにサインインします。
3. Azure ポータルのコンソール ツリーで、[RemoteApp] をクリックし、次のプロパティを使用して、RemoteApp コレクションを作成します。
   - 名前 : RA236972B
   - リージョン : あなたの地域を選択します。
   - プラン : Basic
   - テンプレート イメージ : Office Professional Plus 2013 (30-day trial)

注 : サインインしている Azure アカウントが受講者の個人的なアカウントである場合、また、その Azure アカウントにリンクされている Office 365 のアカウントをお持ちの場合は、試用版ではなく Office 365 のアカウントを使用します。

4. RA236972B のプロビジョニングが進行している間、練習 3、作業 1「サンプル ユーザーを作成する」に進んで、その作業を完了することができます。完了したら、この作業に戻ります。この作業が完了するまでに約 1 時間ほどかかります。
5. [状態] 列がプロビジョニング中からアクティブに変わったら、[RA236972B] をクリックします。
6. Microsoft Edge を開いたままにします。

結果 : この練習により、Azure RemoteApp コレクションを作成することができました。

練習 2 : Azure RemoteApp によるアプリケーションの発行

シナリオ

オンプレミスの RDS インフラストラクチャから RemoteApp の動作を確認することができました。あなたは、Azure RemoteApp の同様の機能を十分にテストすることを決定しました。Azure RemoteApp を使用すると、オンプレミスの RDS インフラストラクチャを増加させる必要性を減らすことができます。この練習でも使用予定の、第 4 章で使用した Azure テスト サブスクリプションを持っています。

主な作業は次のとおりです。

1. アプリケーションを発行してユーザー アクセスを構成する

▶ 作業 1 : アプリケーションを発行してユーザー アクセスを構成する

1. Microsoft Edge で、詳細ウィンドウの [RemoteApp プログラムの発行] セクションを確認します。[RemoteApp プログラムの発行] をクリックします。
2. RemoteApp プログラムの選択ウィンドウで、[Adobe Reader XI] と [OneDriveBusiness] を選択して、アプリを発行します。
3. [RemoteApp コレクションが作成されました] メッセージが表示されたら、[ユーザー アクセスの構成] をクリックします。
   1) Admin のドキュメント ライブラリで、[User1Creds.txt] ファイルを開きます。
   2) User1 のユーザー プリンシパル名 (UPN) をコピーし、[ユーザー名を入力] ボックスに貼り付け、ユーザーの選択を保存します。
4. [RA236972B] ページに戻り、[リモート デスクトップ クライアントのダウンロード URL] セクションを確認します。

注 : RemoteApp ユーザーが Azure デスクトップ クライアントをダウンロードし、RemoteApp プログラムを実行できるように、RemoteApp ユーザーに電子メールまたは送信できることを確認します。

結果 : この練習により、Azure RemoteApp を使用して、アプリを発行することができました。

練習 3 : リモート接続の検証

シナリオ

あなたは、ユーザーを作成し、LON-CL4 コンピューター上の Azure RemoteApp プログラムをテストする必要があります。

主な作業は次のとおりです。

1. サンプル ユーザーを作成する
2. リモート デスクトップ クライアントをダウンロードして、リモート接続を確認する

▶ 作業 1 : サンプル ユーザーを作成する

1. Azure ポータルのコンソール ツリーで、[ACTIVE DIRECTORY] をクリックします。
2. Active Directory 詳細ウィンドウで、[ユーザー] 列をクリックします。
3. ユーザーを次のプロパティに追加します。
   - ユーザーの種類 : 組織内の新しいユーザー
   - ユーザー名 : User1
   - 名 : User
   - 姓 : 1
   - 表示名 : User1
   - ロール : ユーザー
4. [一時パスワードの取得] ページで、一時パスワードをコピーします。
5. メモ帳にパスワードと User1 のユーザー プリンシパル名 (UPN) を貼り付け、ファイルを User1Creds.txt として Admin¥Documents ライブラリに保存します。
6. 必要に応じて、練習 1、作業 1 の手順 4「RemoteApp コレクションを作成する」に戻り、プロビジョニングが完了していることを確認します。

▶ 作業 2 : リモート デスクトップ クライアントをダウンロードして、リモート接続を確認する

1. LON-CL4 で、開いているウィンドウをすべて閉じます。
2. Microsoft Edge ブラウザーを開き、https://www.remoteapp.windowsazure.com に移動します。
3. すべての画面の指示に従って、クライアントをダウンロードします。
4. リモート デスクトップ クライアントをインストールし、User1Cred.txt に入力した値を使用します。

注 : エクスプローラーのドキュメント フォルダー内で User1Cred.txt ドキュメントを検出することができます。ダブルクリックしてファイルを開きます。終了したら閉じます。

5. パスワードを「Pa$$w0rd」に更新してサインインします。
6. Adobe ReaderXI RemoteApp を開きます。
7. [ライセンス条項] ページが表示されたら、[同意しない] をクリックし、[終了] をクリックします。
8. スタート メニューで [すべてのアプリ] をクリックします。新しい項目の Azure RemoteApp があることを確認します。
9. 開いているウィンドウをすべて閉じ、サインアウトします。

結果 : この練習により、クライアント コンピューターでの Azure RemoteApp の実行を検証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-CL4 に対して、手順 2 ～ 3 を繰り返します。

質問 : User1 のアカウントを作成した際、一時パスワードのコピーができました。この一時パスワードを転送するための電子メール アドレスを入力するエリアがあります。この操作を実行することで生じる危険性はどのようなものですか。

質問 : リモート デスクトップ クライアントをダウンロードして、Azure RemoteApp サイン イン ウィンドウでサインインした後、RemoteApp プログラムを再起動するためには、どこに戻ればいいですか。

復習とまとめ

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
ルーティングとリモート アクセス コンソールで VPN を構成し、そのすぐ後に、Windows 10 クライアントの設定アプリで VPN 接続を作成した。接続を試みても、VPN 接続は失敗した。すべての操作を確認したが、正しく構成されている。	
すべての Windows 10 のノート PC には、組織全体のリソースとして、DirectAccess が確立されているが、ブランチ オフィスにいる従業員は、失敗することがあると述べている。	
基幹業務 (LOB) アプリを Azure RemoteApp 経由で展開する必要があり、簡易作成オプションを使用して RemoteApp を指定したが、LOB アプリがイメージに表示されない。	

復習問題

質問 : RD Web アクセス ポータルを変更するために使用できるツールはどれですか。

質問 : DirectAccess はクライアントとサーバーの設定を構成するために 2 つの GPO に依存しています。それらの GPO はどのように作成されますか。

質問 : Point-to-Point プロトコル (PPP) は PPP フレーム内で IP パケットをカプセル化し、カプセル化された PPP パケットを Point-to-Point リンクに送信します。PPP は何のために設計されましたか。

ツール

ツール	用途	アクセス方法
リモート アクセス管理	DirectAccess や VPN を構成し、接続とクライアントを監視し、クライアント接続を切断する。	リモート アクセスの役割をインストール後、サーバー マネージャーで、[ツール] を選択
DirectAccess 作業の開始ウィザード	DirectAccess インフラストラクチャを確立する。	リモート アクセス管理で、リモート アクセスの役割をインストール後、サーバー マネージャーで、[ツール] を選択
ルーティングとリモート アクセス サービス	VPN やネットワークのルーティングを構成し、接続とクライアントを監視する。	リモート アクセスの役割をインストール後、サーバー マネージャーで、[ツール] を選択

ツール	用途	アクセス方法
Azure ポータル	Azure AD へのユーザーの追加、Azure RemoteApp プログラムの作成を含む Azure の管理をおこなう。	http://aka.ms/n3ni6x
Azure Remote Desktop クライアントのダウンロード	スタート メニューに RemoteApp フォルダーを追加し、Windows 10 上のアプリをすべて追加する。	http://aka.ms/ivcv8x