第 4 章

グループ ポリシーによるデスクトップとアプリケーション設定の管理

目次

概要

組織全体にわたってコンピューティング環境の一貫性を維持するには、困難が伴います。管理者は、ユーザーとコンピューターの設定および制限を構成し、それらを強制的に適用するメカニズムを必要としています。グループ ポリシーにより、管理者は構成設定を一元的に管理して適用できるので、この一貫性を確保できます。

この章では、グループ ポリシーの概念、およびグループ ポリシーを実装するために使用できる方法について説明します。

目的

この章により、次のことを習得できます。

- グループ ポリシーの処理と管理について説明することができます。
- グループ ポリシーを使用して、ユーザーとデスクトップの一般的な設定を構成することができます。
- グループ ポリシーの基本設定を使用して、設定を管理することができます。

レッスン 1
グループ ポリシー オブジェクトの管理

個々のコンピューターで管理および構成タスクを実行することもできますが、多くの場合、グループ ポリシー オブジェクト (GPO) を使用して、計画された構成設定を実装する方がより効率的です。グループ ポリシーは、Windows オペレーティング システムと、そのオペレーティング システムで実行されるアプリケーションの両方を一元的に構成管理するためのインフラストラクチャを提供します。

このレッスンでは、グループ ポリシー構造の概要について説明し、エンタープライズ環境でドメインベースの GPO を使用する方法を定義します。グループ ポリシーを正しく適用するには、グループ ポリシーが機能するしくみを理解することが重要です。また、このレッスンでは、ユーザーとグループに適用できる設定の種類についても説明します。

さらに、Windows 10 に組み込まれたツールを使用して、グループ ポリシーの基本的なトラブルシューティングをおこなう方法についても説明します。

目的

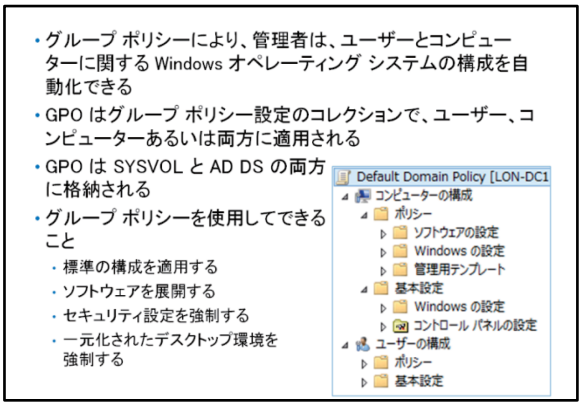
このレッスンにより、次のことを習得できます。

- GPO とそのコンテンツ、およびその格納方法について説明することができます。
- グループ ポリシーの継承を制御することができます。
- Active Directory グループと Windows Management Instrumentation (WMI) を使用して、適用されるグループ ポリシー設定をフィルター処理することができます。
- グループ ポリシーを使用して、適用される設定を決定することができます。
- グループ ポリシーをデスクトップから管理することができます。
- GPO を構成することができます。

エンタープライズ環境でグループ ポリシーを適用する方法

グループ ポリシーにより、管理者は、ユーザーとコンピューターに関する Windows オペレーティング システムの構成を自動化することができます。グループ ポリシーを使用して、次のことをおこなうことができます。

- カスタマイズされた構成または特別な構成を適用する。
- アプリケーションを展開する。
- セキュリティ設定を強制する。
- 標準化されたデスクトップ環境を強制する。



GPO

GPO は、ユーザー、コンピューター、またはその両方に構成設定を適用するポリシー設定を 1 つ以上含むオブジェクトです。GPO テンプレートは SYSVOL に格納され、GPO コンテナー オブジェクトは Active Directory ドメイン システム (AD DS) に格納されます。グループ ポリシーの管理コンソール (GPMC) を使用して GPO を管理することができます。GPMC では、グループ ポリシー管理エディターを使用して GPO を開いて編集できます。

GPO をドメインや組織単位などの Active Directory オブジェクトにリンクし、それらに含まれるオブジェクトに設定を適用します。GPO をグループに直接リンクすることはできませんが、セキュリティ フィルター処理または項目レベルのターゲット設定を使用することで、グループ メンバーシップに基づいて、ポリシーの適用をフィルター処理できます。

GPO では、コンピューターのデスクトップからスクリーン セーバーのタイムアウトに至るまで、さまざまなコンピューター設定を定義できます。グループ ポリシーの変更は、ドメイン コントローラーで構成します。グループ ポリシー クライアントは、その変更をドメイン コントローラーからドメイン内の各クライアント コンピューターにダウンロードします。グループ ポリシーでは、XML ベースのテンプレートを使用してレジストリ設定を記述します。

グループ ポリシー オブジェクト エディター

グループ ポリシー オブジェクト エディターは、GPO のグループ ポリシー設定を作成するために使用する Microsoft 管理コンソール (MMC) スナップインです。GPMC で GPO を編集する際、グループ ポリシー オブジェクト エディターが自動的に開きます。また、gpedit.msc コマンドを使用して、コマンドラインからローカル グループ ポリシー エディターを開くこともできます。

グループ ポリシー設定

グループ ポリシー設定は、グループ ポリシーの最小単位のコンポーネントで、AD DS 内のオブジェクト (コンピューター、ユーザー、またはその両方) に適用する特定の構成設定を定義します。グループ ポリシーには、コンピューティング環境のほとんどすべての領域に影響する数千の構成設定があります。ただし、すべての設定を、Windows Server と Windows オペレーティング システムのすべてのバージョンに適用できるわけではありません。新しい Windows バージョンにはそれぞれ、その特定の Windows バージョンにのみ適用される新しい設定や機能が導入されています。処理できないグループ ポリシー設定がコンピューターに適用された場合、その設定は単純に無視されます。

グループ ポリシー設定の構造

次の表は、グループ ポリシー オブジェクト エディターのユーザーとコンピューターそれぞれの構成領域における、設定のカテゴリについて説明しています。

<table>
<tr><th>セクション</th><th colspan="3">説明</th></tr>
<tr><td rowspan="4">コンピューターの構成
/ユーザーの構成</td><td colspan="3">この領域には、コンピューターまたはユーザーの構成を変更する次のような設定があります。</td></tr>
<tr><td rowspan="3">ポリシー</td><td colspan="2">この領域には、Windows 2000 オペレーティング システム以降で使用可能な設定のカテゴリがあります。</td></tr>
<tr><td>ソフトウェアの設定</td><td>ユーザーに割り当てるソフトウェア設定は、すべてのコンピューターでそのユーザー固有になります。
コンピューターに展開されるソフトウェア設定は、そのコンピューターのすべてのユーザーに適用されます。</td></tr>
<tr><td>Windows の設定</td><td>コンピューターに対するスクリプトの設定、セキュリティの設定、およびサービスの品質が含まれます。
ユーザー設定には、フォルダー リダイレクトも含まれます。</td></tr>
</table>

セクション	説明		
		管理用テンプレート	レジストリを変更する数千の設定を含み、ユーザーおよびコンピューター環境のさまざまな側面を制御します。Microsoft または他のベンダーは、新しい管理用テンプレートを作成している場合があります。例えば、Office テンプレートは、Microsoft Web サイトからダウンロードしてグループ ポリシーに追加できます。 コンピューター設定は、レジストリの HKeyLocalMachine ハイブを変更します。ユーザー設定は、レジストリの HKey Current User ハイブを変更します。
	基本設定	この領域には、Windows Vista オペレーティング システム以降で使用可能な設定のカテゴリがあります。	
		Windows の設定	ネットワーク ドライブのマッピング、ファイルのコピー、レジストリの一部変更など、さまざまな設定が含まれます。
		コントロール パネルの設定	Internet Explorer、プリンター、電源、サービスに関する設定など、コントロール パネルの変更が含まれます。

管理用テンプレート セクションのほとんどの設定には、次の 3 つの状態があります。

- **未構成 :** ユーザーやコンピューターに対する特定の設定の既存構成は、GPO によって変更されません。
- **有効 :** ポリシー設定を適用します。
- **無効 :** ポリシー設定を無効にします。

新しい GPO では、すべての設定が [未構成] に設定されます。[ポリシー] セクションと [基本設定] セクションについては、以降のレッスンでより詳しく説明します。

GPO の記憶域

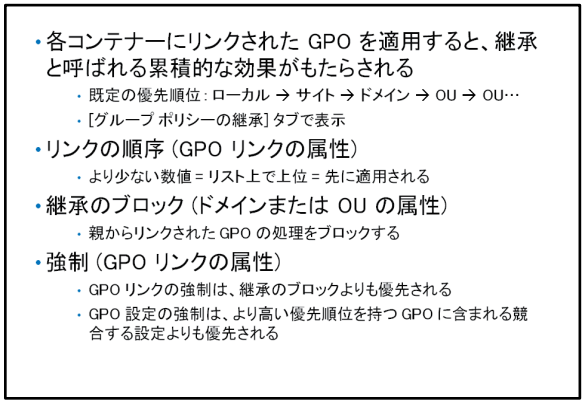
AD DS は、GPO に関する設定と情報を次の 2 つの異なるコンポーネントに格納し、その各コンポーネントは 2 つの異なる場所に格納されます。

- **グループ ポリシー テンプレート :** このテンプレートには、構成する設定が含まれます。グループ ポリシー テンプレートは、接続しているドメイン コントローラーの SYSVOL に格納され、それがドメインの残りのドメイン コントローラーに複製されます。グループ ポリシー テンプレートは、%SystemRoot%¥SYSVOL¥Domain¥Policies¥GPOGUID に配置されます。この場合、GPOGUID は GPO のグローバルー意識別子 (GUID) です。GPO を作成すると、SYSVOL にグループ ポリシー テンプレートが格納され、AD DS にはグループ ポリシー コンテナーが格納されます。

- **グループ ポリシー コンテナー :** このコンテナーは Active Directory オブジェクトであり、ドメイン パーティションの System¥Policies コンテナーにある Active Directory データベースに格納されます。各グループ ポリシー コンテナーには、AD DS 内のオブジェクトを一意に識別する GUID 属性が含まれます。グループ ポリシー コンテナーは、リンクやバージョン番号などの GPO の基本属性を定義しますが、設定は一切含まれません。既定では、グループ ポリシーの更新時に、グループ ポリシーのクライアント側拡張機能は、新しいまたは更新された GPO の GPO 設定のみを適用します。

グループ ポリシーの継承の管理

グループ ポリシー戦略を立てるには、まずグループ ポリシーが適用されるしくみを理解する必要があります。このトピックでは、グループ ポリシーが処理されるしくみ、および継承を使用してグループ ポリシーの適用が制御されるしくみについて説明します。



GPO を作成して、適用する設定を構成したら、それらをサイト、ドメイン、または組織単位 (OU) にリンクする必要があります。GPO は特定の順序で適用され、この順序により、オブジェクトに適用される設定が決定されます。Active Directory ドメインを作成すると、2 つの既定のポリシーが自動的に作成されます。これらのポリシーを使用して、ドメインとドメイン コントローラーの両方にパスワードとセキュリティ設定を提供できます。

GPO のリンク

GPO を作成して、適用するすべての設定を定義したら、次の手順として、ポリシーを Active Directory オブジェクトにリンクします。GPO リンクは、ポリシーとオブジェクトの論理的な接続です。GPMC または Windows PowerShell を使用して、1 つの GPO を複数のオブジェクトにリンクできます。次のオブジェクトの種類にのみリンクできます。

- サイト
- ドメイン
- OU

GPO をユーザー、グループ、またはコンピューターに直接リンクすることはできません。また、Builtin、Computers、Users、Managed Service Accounts など、AD DS 内のシステム コンテナーに GPO をリンクすることもできません。これらの Active Directory システム コンテナーに配置されているユーザーとコンピューターは、ドメイン レベルでリンクされている GPO からのみグループ ポリシー設定を受け取ります。

グループ ポリシー設定が適用されるしくみ

認証をおこなったドメイン コントローラーから GPO を要求されることで、クライアント コンポーネント (グループ ポリシー CSE と呼ばれる) がグループ ポリシーを起動します。次に、CSE がポリシー設定を解釈して適用します。Windows 10 は、コンピューターが起動した際、コンピューター設定を適用し、ユーザーがコンピューターにサインインした際、ユーザー設定を適用します。

コンピューター設定とユーザー設定は両方とも定期的に更新され、その更新間隔は構成可能です。既定の更新間隔は、90 分にランダムな時間 (最大 30 分) を加算した時間です。ただし、グループ ポリシー設定を構成することで、更新間隔を変更できます。コンピューター設定の場合、更新間隔設定は [コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[システム]、[グループ ポリシー] ノードに配置されています。

ユーザー設定の場合は、[ユーザーの構成] の対応する設定に配置されています。セキュリティの設定は、この更新間隔の例外になります。グループ ポリシーの [セキュリティの設定] セクションは、少なくとも 16 時間ごとに更新されます。セキュリティの設定の更新間隔は、グループ ポリシーでは構成できませんが、レジストリで変更できます。

グループ ポリシーの処理順序

コンピューターが起動するか、ユーザーがサインインすると、グループ ポリシー クライアントは AD DS 内のコンピューター オブジェクトまたはユーザー オブジェクトの場所を調べ、コンピューターまたはユーザーが属するスコープで GPO を評価します。次に、CSE は、これら GPO のポリシー設定を適用します。GPO のランクは、最初にサイトにリンクされたポリシー、次にドメインにリンクされたもの、次に OU にリンクされたものの順序になります。OU の順序は、最上位レベルの OU から、ユーザーまたはコンピューターのオブジェクトが存在する OU へと下がっていきます。グループ ポリシーの既定の動作では、階層の中で順序がより低いドメインと OU が (特に OU が)、より高い順序でリンクされた GPO から設定を継承します。この階層化された設定の適用形式は、プロセスの中で後で適用される GPO が、先に適用された設定を上書きすることを意味します。それは、後で適用される方が優先順位が高いためです。グループ ポリシー クライアントは、ドメイン コントローラーからすべての設定をダウンロードし、これらの規則に基づいて適用する必要があるポリシーを算出します。

グループ ポリシーの継承の構成

GPO を順序に従って適用することにより、ポリシーの継承と呼ばれる効果が生じます。ユーザーまたはコンピューターのポリシーの結果セット (RSoP) は、サイト、ドメイン、および OU の各ポリシーの累積的な効果になります。

既定では、継承された GPO は、ドメインまたは OU に直接リンクされた GPO よりも優先順位が低くなります。例えば、ドメインにリンクされた GPO のポリシー設定を構成して、ドメイン内のすべてのユーザーがレジストリ編集ツールを使用できないように設定したとします。ドメイン内のすべてのユーザーは、GPO とそのポリシー設定を継承します。ただし、管理者に対しては通常、レジストリ編集ツールを使用できるようにするので、管理者のアカウントを含む OU に GPO をリンクし、レジストリ編集ツールの使用を許可するようにそのポリシー設定を構成します。管理者の OU にリンクされた GPO は、継承された GPO よりも優先順位が高いので、管理者はレジストリ編集ツールを使用できるようになります。

リンクの順序

GPMC で OU を選択すると、その OU にリンクされた GPO のリンクの順序が、[リンクされたグループ ポリシー オブジェクト] タブに表示されます。複数の GPO を、同じ Active Directory オブジェクトにリンクできます。GPO のリンクの順序により、このようなシナリオでの GPO の優先順位が決定されます。リンクの順序が上位の GPO は、順序が下位の GPO よりも優先順位が高くなります。

GPO のリンクの優先順位を変更するには、次の手順を使用します。

1. GPMC のコンソール ツリーで、Active Directory オブジェクトを選択します。
2. 詳細ウィンドウで、[リンクされたグループ ポリシー オブジェクト] タブをクリックします。
3. GPO を選択します。
4. [上]、[下]、[一番上へ移動]、または [一番下へ移動] の各矢印をクリックして、選択した GPO のリンクの順序を変更します。

参考資料 : ドメイン内でパスワード ポリシーを構成する唯一の方法は、ドメイン内でリンクの順序が最も上位の GPO を使用することです。パスワード ポリシーについては、次のサイトを参照してください。
Active Directory Back to Basics‐Password Policies
http://aka.ms/wtsi9c

継承のブロック

ポリシー設定を継承しないように、ドメインまたは OU を構成できます。継承をブロックするには、GPMC のコンソール ツリーでドメインまたは OU を右クリックして、[継承のブロック] をクリックします。

[継承のブロック] はドメインまたは OU のプロパティなので、グループ ポリシー階層の親にリンクされた GPO のすべてのグループ ポリシー設定がブロックされます。例えば、OU で継承をブロックすると、GPO の適用は、その OU に直接リンクされた GPO から開始されます。したがって、より上位レベルの OU、ドメイン、またはサイトにリンクされた GPO は適用されません。

継承のブロックにより、グループ ポリシーの優先順位と継承の評価がより難しくなるので、[継承のブロック] は慎重に使用する必要があります。セキュリティのグループ フィルター処理を使用すると、適切なユーザーとコンピューターにのみ適用されるように GPO のスコープを細かく設定できるので、[継承のブロック] が不要になります (このトピックについては、この章で後ほど説明します)。

GPO リンクの強制

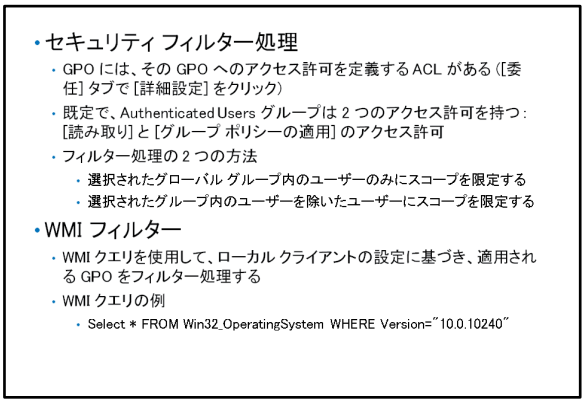
既定の継承を変更する最終的な方法は、GPO リンクの強制を設定することです。GPO リンクを強制するには、コンソール ツリーで GPO リンクを右クリックし、ショートカット メニューから [強制] をクリックします。

GPO リンクの [強制] を設定すると、GPO に最高レベルの優先順位が適用されます。その GPO のポリシー設定は、通常であればより高い優先順位を持つ他の GPO に含まれる、競合するすべてのポリシー設定よりも優先されます。[強制] により、ポリシーは、そのスコープ内のすべてのオブジェクトに適用されます。また、[強制] により、ポリシーは競合するすべてのポリシーに上書きされ、[継承のブロック] が設定されている場合でも適用されます。

強制機能は、企業の IT セキュリティ ポリシーと使用ポリシーで強制される構成が存在し、その構成を定義する GPO を設定する際に役立ちます。つまり、GPO リンクを強制することで、他の GPO がこれらの設定を上書きしないようにすることができます。

グループ ポリシー設定のフィルター処理

2 つの異なる方法 (セキュリティ フィルター処理と WMI フィルター処理) を使用して、GPO が適用されるユーザーとコンピューターをフィルター処理できます。



セキュリティ フィルター処理によるグループ スコープの変更

[強制] と [継承のブロック] を使用して、サイト、ドメイン、および OU への GPO の適用を制御できますが、GPO のスコープに属するすべてのユーザーまたはコンピューターではなく、特定のユーザーまたはコンピューターのグループにのみ GPO を適用することが必要な場合があります。GPO を直接セキュリティ グループにリンクすることはできませんが、GPO を特定のセキュリティ グループに適用する方法はあります。

各 GPO には、その GPO へのアクセス許可を定義するアクセス制御リスト (ACL) があります。GPO をユーザーまたはコンピューターに適用するには、2 つのアクセス許可 ([読み取り] の許可と [グループ ポリシーの適用] の許可) が必要になります。

例えば、コンピューターが属する OU へのリンクにより、GPO のスコープをコンピューターに対して指定しても、そのコンピューターに [読み取り] および [グループ ポリシーの適用] のアクセス許可がない場合、その GPO のダウンロードと適用はおこなわれません。したがって、セキュリティ グループに適切なアクセス許可を設定することで、指定したコンピューターとユーザーにのみ設定が適用されるように、GPO をフィルター処理できます。

既定では、Authenticated Users グループは、新しい各 GPO に対する [読み取り] および [グループ ポリシーの適用] の各アクセス許可が許可されています。つまり既定では、ユーザーとコンピューターが他のグループのメンバーかどうかには関係なく、その GPO はドメイン、サイト、または OU に設定されたすべてのユーザーとコンピューターに影響します。したがって、GPO のスコープをフィルター処理するには、次の 2 つの方法があります。

- GPMC にある GPO の [スコープ] タブの [セキュリティ フィルター処理] セクションで、GPO を適用するグループを追加できます。ただし、グローバル グループのみ使用可能で、Authenticated Users グループは削除する必要があります。
- GPMC にある GPO の [委任] タブで、[詳細設定] をクリックして、セキュリティ フィルター処理を変更します。GPO を適用しないグループを決定し、それらのグループの [グループ ポリシーの適用] アクセス許可を [拒否] に設定します。GPO に対する [グループ ポリシーの適用] アクセス許可を拒否にすると、ユーザーとコンピューターが [グループ ポリシーの適用] を許可された別のグループのメンバーの場合でも、そのユーザーとコンピューターには GPO の設定が適用されません。

セキュリティ グループのフィルター処理を使用して、テストにおける GPO のスコープを管理できます。テスト OU を作成して、GPO のテスト用スコープを管理する代わりに、GPO を運用環境で使用する場所にリンクすることも検討できます。この場合、Authenticated Users グループまたは本番のセキュリティ グループに GPO の適用を許可する代わりに、GPO のスコープを適切なユーザーとコンピューターに限定するように特別に設計されたセキュリティ グループの構成を検討します。これを実施するメリットは、GPO を独立したテスト OU にリンクすることによって、スコープや優先順位を人為的に制限することがないので、GPO を運用環境で実行する際の非常に実際に近い状況が得られることです。つまり、GPO が、既に運用環境に存在する他の GPO とどのように相互作用するのかをより深く理解すると同時に、テスト用スコープに属する特定のユーザーとコンピューターに対するフル コントロールもそのまま維持されます。

WMI フィルターの使用

WMI は、管理者がネットワークの管理対象オブジェクトを監視および制御できるようにするための、管理インフラストラクチャ テクノロジです。WMI クエリは、ランダム アクセス メモリ (RAM)、ディスク容量、オペレーティング システムのバージョン、Service Pack レベルなどの特性に基づいて、システムをフィルター処理できます。WMI を使用すると、コンピューターに含まれる全オブジェクトのほとんどすべてのプロパティを表示できるので、WMI クエリで使用できる属性のリストには、事実上制限はありません。WMI クエリは、WMI Query Language (WQL) を使用して作成します。

WMI クエリを使用して WMI フィルターを作成し、それを使用して GPO をフィルター処理できます。グループ ポリシーを使用して、アプリケーションと Service Pack を展開する場合、GPO を作成してアプリケーションを展開した後、WMI フィルターを使用して、Windows 10 などの特定のオペレーティング システムと Service Pack を搭載したコンピューターにのみポリシーを適用するように指定できます。次の WMI クエリは、このようなシステムを特定しています。

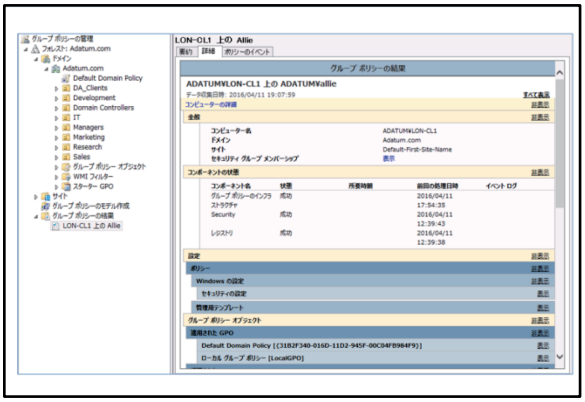
```
Select * FROM Win32_OperatingSystem WHERE Version="10.0.10240"
```

グループ ポリシー クライアントがダウンロードした GPO を評価する際は、ローカル システムに対してクエリを実行します。システムがクエリの条件を満たす場合、クエリの結果は論理的に「True」になり、CSE は GPO を処理します。

WMI には名前空間が含まれ、その中にクエリ可能なクラスが存在します。root¥CIMv2 名前空間には、Win32_Operating System などの有用なクラスが多数存在します。

注 : Scriptomatic 2.0 ツールを使用すると、存在する WMI の名前空間とクラスを検査できます。また、このツールを使用して、ネットワーク上の各コンピューターに対してスクリプトを実行し、さまざまな属性と値を検索することもできます。Scriptomatic ツールをダウンロードするには、Microsoft ダウンロード センター (https://technet.microsoft.com/ja-jp/scriptcenter/ff189401.aspx) にアクセスしてください。

グループ ポリシーの結果の確認



組織内のユーザーまたはコンピューターに関する GPO およびポリシー設定の累積的な効果を分析するために、GPMC にはグループ ポリシーの結果ウィザードが用意されています。グループ ポリシーの結果ウィザードを使用すると、どのポリシー設定がユーザーまたはコンピューターに適用されるか、およびその理由を正確に知ることができます。

グループ ポリシーの結果ウィザードは、Windows Vista 以降のバージョンの Windows オペレーティング システムを実行するローカルまたはリモート コンピューターで、WMI プロバイダーをクエリできます。WMI プロバイダーは、グループ ポリシーがシステムに適用される方法に関するすべての詳細を報告します。WMI プロバイダーは、次の情報を保有しています。

- 処理が発生した日時
- 適用された GPO
- 適用されなかった GPO とその理由
- 発生したエラー
- 優先されたポリシー設定自体とそのソース GPO

次のリストは、グループ ポリシーの結果ウィザードを実行するための要件を示しています。

- 対象のコンピューターはオンラインである必要がある。
- 対象のコンピューターに対する管理資格情報を保有している必要がある。
- 対象のコンピューターは、Windows XP 以降のオペレーティング システムを実行している必要がある。
- 対象のコンピューターで、WMI にアクセスできる必要がある。つまり、このコンピューターはオンラインでネットワークに接続され、ポート 135 と 445 を通じてアクセスできる必要がある。
- 対象のコンピューターで、WMI サービスが稼働している。
- ユーザーの RSoP を分析する場合、そのユーザーはコンピューターに少なくとも 1 回はサインインしている必要がある。

RSoP レポートを実行するには、GPMC のコンソール ツリーで [グループ ポリシーの結果] を右クリックし、[グループ ポリシーの結果ウィザード] をクリックします。ウィザードで、コンピューターを選択するように求められます。次に、そのコンピューターで WMI プロバイダーに接続して、コンピューターにサインインしたユーザーのリストを指定します。いずれかのユーザーを選択します。または、ユーザー構成ポリシーの RSoP 分析をスキップすることもできます。

ウィザードは、ダイナミック HTML 形式で詳細な RSoP レポートを作成します。[IE セキュリティ強化の構成] が設定されている場合、GPMC により、動的なコンテンツをコンソールに表示することを許可するように求められます。[表示または非表示] リンクをクリックするか、セクションの見出しをダブルクリックすることで、レポートの各セクションを展開または折りたたむことができます。

RSoP レポートは、次の 3 つのタブに表示されます。

- **概要 :** 最終更新時におけるグループ ポリシー処理の状態が表示されます。
- **詳細 :** コンピューターまたはユーザーに適用される RSoP 設定が表示されます。このタブには、グループ ポリシーの実施の影響を通じてユーザーに起こった内容が正確に表示されます。[設定] タブからは多くの情報が得られますが、IPsec、ワイヤレス、ディスク クォータのポリシー設定など、一部のデータは報告されません。次の項目を確認できます。
  - システムに関して収集された情報
  - 適用された GPO と適用されなかった GPO
  - GPO に影響を与えたセキュリティ グループのメンバーシップ (このセキュリティ グループのメンバーシップにより GPO がフィルター処理されている)
  - 分析された WMI フィルター
  - CSE の状態
- **ポリシーのイベント :** 対象のコンピューターのイベント ログから取得したグループ ポリシー イベントを表示します。

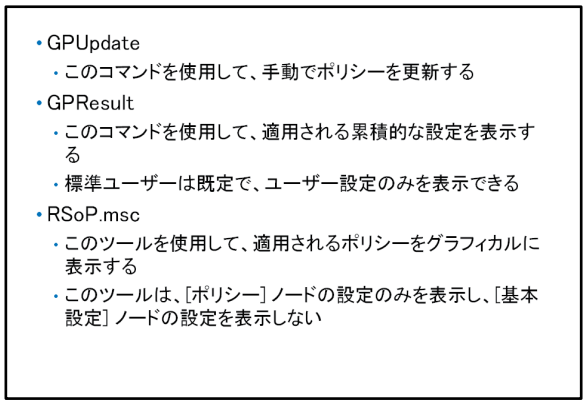
グループ ポリシーの結果ウィザードを使用して RSoP レポートを生成した後、そのレポートを右クリックして、クエリの再実行、レポートの印刷、または XML ファイルや HTML ファイルとしてのレポートの保存をおこなうことができます。HTML ファイルでは、引き続き各セクションの動的な展開と折りたたみが可能です。両方のファイルの種類が Internet Explorer で開けるので、RSoP レポートは GPMC の外部に持ち出すことができます。

コンソール ツリー内の [グループ ポリシーの結果] フォルダーにあるレポート自体のノードを右クリックすると、[詳細表示] に切り替えることができます。[詳細表示] では、RSoP は RSoP スナップインを使用して表示され、IPsec、ワイヤレス、ディスク クォータのポリシー設定を含む、適用されたすべての設定が報告されます。

グループ ポリシーのデスクトップによる管理

グループ ポリシーの管理のほとんどは GPMC で実行されますが、クライアントにサインインした際、ユーザーまたはコンピューターに適用されるグループ ポリシー設定の更新が必要なことに気付く場合があります。また、グループ ポリシーが期待どおりに適用されていない状況に遭遇する場合もあります。次のような問題を診断し、解決することが必要になることがあります。

- 特定の GPO が適用されていない。
- GPO がまったく適用されていない。
- コンピューターまたはユーザーの RSoP が、期待した内容と異なっている。



GPUpdate

グループ ポリシー処理をトラブルシューティングする際は、次回のバックグラウンド更新を待たずに手動でグループ ポリシーの更新を起動することが必要になる場合があります。グループ ポリシーの更新を起動するには、GPUpdate コマンドを使用します。このコマンドを単独で使用すると、バックグラウンドのグループ ポリシー更新と同じ処理がおこなわれます。更新をコンピューターまたはユーザーのいずれかの設定に制限するには、コンピューターとユーザーの両方のポリシーを更新するコマンドで、/<target:computer> または /<target:user> のいずれかのパラメーターを使用します。既定では、バックグラウンドの更新時には、新規および更新された GPO の設定のみが適用されます。
/force スイッチを使用すると、システムは、ユーザーまたはコンピューターに対してスコープが指定されたすべての GPO のすべての設定を再適用します。一部のポリシー設定では、設定を有効にするためにサインアウトまたは再起動が必要になります。GPUpdate で /logoff スイッチおよび /boot スイッチを使用することで、サインアウトまたは再起動が実行されます。サインアウトまたは再起動が必要な設定を適用する際、これらのスイッチを使用できます。

例えば、次のコマンドでは適用の完全な更新が実行され、更新されたポリシー設定を適用するために、必要に応じて再起動とサインアウトが実行されます。

```
gpupdate /force /logoff /boot
```

GPResult

GPResult.exe とグループ ポリシーの結果ウィザードにより、グループ ポリシーの処理と適用に関する問題を、より深く理解できます。これらのツールは、WMI RSoP プロバイダーを検査して、システムで発生した内容を正確に報告することに留意してください。RSoP レポートを調べることで、多くの場合、GPO のスコープが正しくないことや、GPO の適用の妨げとなるポリシー処理のエラーに気付くことができます。

GPResult コマンドは、グループ ポリシーの結果ウィザードのコマンドライン バージョンです。GPResult は、ウィザードと同じ WMI プロバイダーを使用します。同じ情報が生成されるので、同じグラフィカル レポートを作成できます。GPResult は、Windows XP 以降の Windows オペレーティング システムで実行されます。

通常、GPResult コマンドを実行する際は次のオプションを使用します。

```
/s <コンピューター名>
```

/s オプションは、リモート システムの名前または IP アドレスを指定します。コンピューター名としてドット (.) を使用した場合、または /s オプションを使用しない場合、RSoP の分析はローカル コンピューターに対して実行されます。

次のオプションを使用すると、ユーザーまたはコンピューターのいずれかの設定に対して、RSoP の分析が表示されます。/scope オプションを省略すると、RSoP の分析にはユーザーとコンピューターの両方の設定が含まれます。

```
/scope [user | computer]
```

次のオプションは、RSoP データを表示するユーザーの名前を指定します。

```
/USER <ユーザー名>
```

次のオプションを使用すると、RSoP データの要約が表示されます。

```
/r
```

次のオプションを使用すると、RSoP データのより詳細な情報が表示されます。

```
/v
```

次のオプションを使用すると、システムに適用されるすべてのポリシー設定を含む、非常に詳細なデータが表示されます。多くの場合、一般的なグループ ポリシーのトラブルシューティングで必要とするよりも多くの情報が提供されます。

```
/z
```

次のスイッチを使用して、リモート システムの Administrators グループの資格情報を指定します。これらの資格情報がない場合、GPResult はサインインで使用された資格情報を使用して実行されます。

```
/u<ドメイン¥ユーザー> /p<パスワード>
```

次のオプションを使用すると、レポートが XML または HTML 形式で保存されます。これらのオプションは、Windows Vista Service Pack 1 (SP1) 以降のバージョン、および Windows Server 2008 以降のバージョンで使用できます。

```
[/x | /h] <ファイル名>
```

Windows PowerShell の同等のコマンドレット、Invoke-GPUpdate は、Active Directory モジュールに含まれています。このコマンドレットを使用するには、リモート サーバー管理ツール (RSAT) を Windows 10 マシンにインストールする必要があります。

RSoP.msc

コマンド プロンプトで RSoP.msc を実行し、グループ ポリシーを通じて適用される設定をグラフィカルに表示することができます。このツールにより、現在のユーザーとコンピューターに適用されている設定を使用する MMC スナップインが、自動的に作成されます。このツールは、[基本設定] ノードの設定を表示する最新バージョンにはなっていないので、[ポリシー] ノードの設定のみを表示します。

デモンストレーション : GPO 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。

- GPO を作成する
- GPO を OU にリンクする
- 継承のブロックを構成する
- セキュリティ設定のフィルター処理を構成する
- RSoP レポートを作成する

デモンストレーションの手順

GPO を作成する

1. グループ ポリシーの管理を起動します。
2. 新しい GPO を作成し「Desktop Settings GPO」という名前を付けます。

GPO を OU にリンクする

1. Desktop Settings GPO を Research OU にリンクします。

注 : Desktop Settings GPO と Default Domain Policy の両方が Research OU に適用されることに注意してください。

継承のブロックを構成する

1. [継承のブロック] を Research OU に設定します。

注 : 感嘆符が表示されていることに注意してください。これは Research OU で継承がブロックされていることを示しています。また、[グループ ポリシーの継承] タブに [Desktop Settings GPO] のみが表示されていることにも注意してください。

セキュリティ設定のフィルター処理を構成する

1. Desktop Settings GPO で、[委任] タブに移動して [詳細設定] をクリックします。
2. Adatum¥IT グループの [グループ ポリシーの適用] アクセス許可に [拒否] を割り当てます。

RSoP レポートを作成する

1. グループ ポリシーの結果ウィザードを実行して、すべての既定値を受け入れます。
2. [要約]、[詳細]、[ポリシーのイベント] の各タブを確認します。
3. 既定の名前と場所を使用して、レポートを保存します。
4. HTML ドキュメントをダブルクリックし、Internet Explorer でレポートを開きます。

注 : ファイルの内容が、GPMC で表示されるレポートと同じであることに注意してください。

知識の確認

質問	
GPO にリンクできる Active Directory オブジェクトの種類はどれですか。適合するものをすべて選択します。	
正しい解答を選択してください。	
	ユーザー
	ドメイン
	セキュリティ グループ
	サイト
	OU

質問	
次のツールのうち、グループ ポリシーのトラブルシューティングに使用できるものはどれですか。適合するものをすべて選択します。	
正しい解答を選択してください。	
	GPRefresh
	GPUpdate
	GPReport
	GPResult
	RSoP.msc

レッスン 2
グループ ポリシーによるエンタープライズ デスクトップの構成

管理用テンプレート、セキュリティの設定、アプリケーション プログラムのインストールと更新をおこなうソフトウェア展開 (該当する場合) などのグループ ポリシー設定を使用して、組織全体に標準化されたデスクトップ環境を実装できます。組織のポリシーに従ってユーザーのコンピューター設定を構成できるように、これらの設定の構成方法を理解することが重要です。

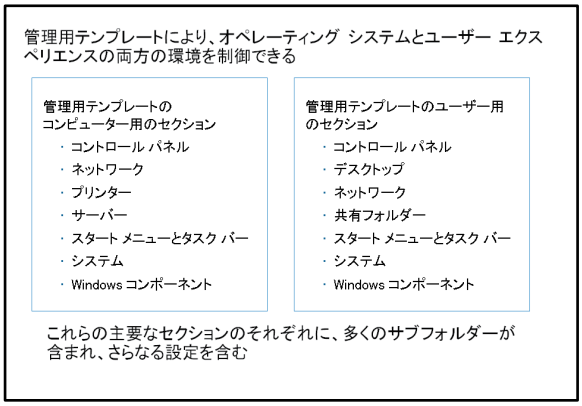
目的

このレッスンにより、次のことを習得できます。

- 管理用テンプレートについて説明することができます。
- 管理用テンプレートのセントラル ストアの実装方法について説明することができます。
- Windows 10 の新しい管理用テンプレート設定について説明することができます。
- 一般的なデスクトップ設定のいくつかを説明することができます。
- 一般的なセキュリティ設定のいくつかを説明することができます。
- グループ ポリシーを使用してソフトウェアを展開し管理する方法について説明することができます。
- グループ ポリシーを使用して設定を構成することができます。

管理用テンプレートの概要

管理用テンプレートを使用して、オペレーティング システムの環境とユーザー エクスペリエンスを制御することができます。管理用テンプレートには、ユーザー用とコンピューター用の 2 セットがあります。ただし、一部の管理用テンプレートは、ユーザーとコンピューターの両方に使用できます。

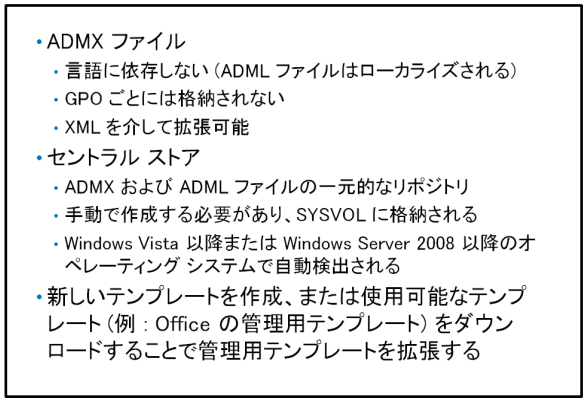


GPMC にある [管理用テンプレート] セクションを使用すると、レジストリに対する数千の変更を展開できます。管理用テンプレートには、次のような特性があります。

- ネットワーク、システム、Windows オペレーティング システムのコンポーネントなど、特定の領域に焦点を当てたサブフォルダーに編成されています。
- コンピューター セクションの設定では、レジストリの HKEY_LOCAL_MACHINE ハイブを編集し、ユーザー セクションの設定では、レジストリの HKEY_CURRENT_USER ハイブを編集します。組み込みのすべての管理用テンプレートでは、設定が通常配置される場所の下にある特別な Policies サブキーに、テンプレートの設定が保存されます。例えば、スタート メニューの設定で [実行の削除] を有効にした場合、キー NoRun は、HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Explorer ではなく、HKEY_CURRENT_USER¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer に作成されます。つまり、グループ ポリシーを使用して設定を構成した場合、レジストリ内の同じ設定は上書きされません。グループ ポリシーを使用して設定を構成しないように変更した場合、Windows オペレーティング システムは再度レジストリ内の元の設定を使用するようになります。

- 一部の管理用テンプレートは、ユーザーとコンピューターの両方に使用できます。例えば、設定を使用して、ユーザーとコンピューターの両方のテンプレートで Skype を実行できないようにすることができます。設定が競合する場合は、コンピューターの設定が優先されます。
- 一部の管理用テンプレート設定は、Windows オペレーティング システムの特定のバージョンでのみ使用できます。例えば、新しい設定の多くは、Windows 10 オペレーティング システムにのみ適用できます。設定をクリックすると、その設定をサポートする Windows オペレーティング システムのバージョンを表示できます。それは、詳細ウィンドウの [要件] セクションに表示されます。
- GPO では、GPO がユーザーまたはコンピューターに適用されなくなった後、組み込みのすべての管理用テンプレートに関する設定が、レジストリから削除されます。ただし、GPO がコンピューターに適用されなくたった後でも、管理用テンプレートのセットを拡張した場合、一部の設定がコンピューターにそのまま残っていることがあります (これはタトゥーイングと呼ばれる場合があります)。このような場合、管理用テンプレートの設定を手動で調整するか、設定をそのまま残すかを選択できます。

エンタープライズでの管理用テンプレートの管理



Windows Vista オペレーティング システムと Windows Server 2008 オペレーティング システムでは、レジストリベースのポリシー設定を表示する新しい形式が採用されました。ADM ファイルは、ADMX ファイルと呼ばれるこれら標準ベースの XML ファイルに置き換えられます。

Windows Vista 以降と Windows Server 2008 以降の Windows クライアントおよび Windows Server オペレーティング システムでは、これらのファイルを独自にコピーして保有します。すべての ADMX ファイルを格納するセントラル ストアを作成することで、ADMX ファイルの管理を簡略化できます。多くのベンダーは、管理用テンプレートを使用してアプリケーションを管理するために、固有の ADMX ファイルを作成しています。

ADMX ファイル

Windows Vista 以降と Windows Server 2008 以降の Windows クライアントおよび Windows Server オペレーティング システムのグループ ポリシー ツールは、既存の環境で保有するカスタムの ADM ファイルを引き続き認識しますが、ADMX ファイルに置き換えられた ADM ファイルは無視されます。ADM ファイルとは異なり、ADMX ファイルは個々の GPO ごとには格納されません。グループ ポリシー管理エディターは、ローカルの ADMX ファイル ストアから自動的に設定を読み取り表示します。既定では、ADMX ファイルは Windows¥PolicyDefinitions フォルダーに格納されますが、一元的な場所に格納することもできます。

ADMX ファイルは、ADM ファイルとは異なり、言語に依存しません。設定に関する普通の言語での説明は、ADMX ファイルには含まれません。それらの説明は、言語固有の ADML ファイルに格納されます。つまり、異なる言語を話すそれぞれの管理者は、言語固有の ADML ファイルを使用して同じ GPO を参照し、自分の言語でポリシーの説明を確認します。ADML ファイルは、言語固有のサブフォルダーである PolicyDefinitions フォルダーに格納されます。既定では、Windows 10 に含まれる ADML 言語ファイルは、インストールされたオペレーティング システムの言語のみです。追加の言語は、手動でインストールする必要があります。

注 : ADMX ファイルには、常に ADML ファイルが付随しています。説明を簡略化するために、ここでは ADMX ファイルにのみ言及しています。ADMX ファイルには管理用テンプレートの設定が含まれ、ADML ファイルにはその設定のテキストが含まれます。

セントラル ストア

ドメインベースのエンタープライズ環境では、ADMX ファイルの格納場所としてセントラル ストアを作成し、GPO の作成または編集のアクセス許可を持つユーザーはだれでもアクセスできるようにすることができます。Windows Vista 以降の Windows オペレーティング システムと Windows Server 2008 以降の Windows Server オペレーティング システムのグループ ポリシー管理エディターは、セントラル ストアに格納された ADMX ファイルから管理用テンプレートのポリシー設定を自動的に読み取り、表示します。この場合、ローカルに格納された設定は無視されます。ドメイン コントローラーが利用できない場合、グループ ポリシー管理エディターはローカル ストアを使用します。

まず、セントラル ストアを作成する必要があり、それをドメイン コントローラーで手動で更新します。ADMX ファイルの使用は、GPO を作成または編集するコンピューターのオペレーティング システムに依存します。セントラル ストアにより、管理者が複数の Windows ワークステーションおよびサーバーから GPO を編集している企業でも、一貫性が確保されます。

ADMX ファイルと ADML ファイルのセントラル ストアを作成するには、¥¥Domain FQDN¥SYSVOL¥Domain FQDN¥Policies に PolicyDefinitions という名前のフォルダーを作成します。例えば、corp.contoso.com ドメイン用のセントラル ストアを作成するには、¥¥corp.contoso.com¥SYSVOL¥corp.contoso.com¥Policies に PolicyDefinitions フォルダーを作成します。管理者は、PolicyDefinitions フォルダーのすべてのファイルとサブフォルダーを、SYSVOL のフォルダーにコピーする必要があります。

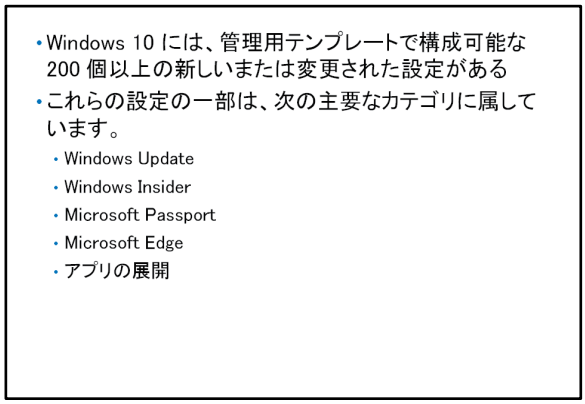
管理用テンプレートの拡張

管理用テンプレートは、コンピューターまたはユーザーのオブジェクトに展開できる数千の構成可能な設定を提供します。管理用テンプレートの特徴は、他の方法では使用できない設定を、管理用テンプレートに追加で含めるように拡張できることです。管理用テンプレートを拡張するには、次の 4 つの主な手順を実行します。

1. 管理用テンプレートをダウンロードするか、新しいカスタム テンプレートを作成する : Microsoft を含む多くのベンダーが、無料でダウンロードできる管理用テンプレートを提供しています。管理用テンプレートを拡張する一例が、Office のテンプレートです。Office の管理用テンプレートでは、Office スイートに含まれる各アプリケーション用の特別な設定など、Office 専用の設定をカスタマイズできます。
2. 管理用テンプレートをセントラル ストアにコピーする : 新しい管理用テンプレートをセントラル ストアに追加すると、新しい設定が含まれる新しいフォルダーまたはフォルダーのセットが、カスタマイズ用に使用できるようになります。
3. GPO の管理用テンプレート設定をカスタマイズする : 通常の GPO 設定をカスタマイズするのと同じ方法で、管理用テンプレート設定をカスタマイズできます。使い慣れたグループ ポリシー管理エディターを使用して、管理者は簡単にアプリケーションをカスタマイズできます。
4. 管理用テンプレート設定を含めて GPO を展開する : GPO を展開した後、管理用テンプレート設定を通じてアプリケーションを構成します。

Windows 10 の新しい管理用テンプレート設定

Windows の新しい各バージョンでは、新しい設定が管理用テンプレート セットに追加されます。Windows の新しいバージョンは、これらの設定を既存の ADMX ファイルと新しいファイルの両方に追加します。オリジナルのファイルを変更した場合は、SYSVOL のセントラル ストアを更新する前にバックアップを作成する必要があります。



参考資料 : Microsoft が Windows の新しいバージョンをリリースする際、管理用テンプレートで構成可能なすべての設定が記載された Excel スプレッドシートもリリースされます。Windows 10 のスプレッドシートは、現在リリース済みです。このスプレッドシートと以前のバージョンのスプレッドシートをダウンロードするには、http://aka.ms/vk84hh にアクセスしてください。

Windows 10 には、管理用テンプレートで構成可能な 200 以上の新しいまたは変更された設定があります。これらの設定の一部は、次の主要なカテゴリに属しています。

- Windows Update
- Windows Insider
- Microsoft Passport
- Microsoft Edge
- アプリの展開

Windows Update

Windows as a Service により、新しい機能を使用可能になった時点で受け取ることができます。Windows 10 Pro または Enterprise Edition を使用している場合は、アップグレードを延期できます。この設定は、グループ ポリシーの [コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Windows Update]、[アップグレードを延期する] を使用して変更します。

Windows Insider

企業は、IT 部門が確実に許可された変更のみを実施する、安定した運用環境を望んでいます。これらのシナリオでは、Windows 10 の新しいビルドのダウンロードをユーザーに許可することは選択肢にありません。ユーザーが Windows Update の [詳細オプション] で Insider のコントロールにアクセスできるかどうかを、制御することができます。この設定は、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[データの収集とプレビュー ビルド] に配置されています。

Microsoft Passport

Windows 10 の新しいセキュリティ機能である Microsoft Passport は、パスワードを使用する代わりに Windows Hello または PIN を使用して Windows 10 にサインインするユーザーを、セキュリティで保護できます。次の構成が可能です。

- ユーザーがサインインする際、コンピューターは Microsoft Passport を使用する必要がある。
- 生体認証デバイスを使用するかどうか。
- PIN の複雑さ。

ユーザー向けの設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Microsoft Passport for Work] に配置されています。コンピューター向けの設定は、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Microsoft Passport for Work] に配置されています。

Microsoft Edge

新しい組み込みの Windows 10 ブラウザーには、コンピューター向けまたはユーザー向けに構成可能な 10 個の設定があります。ユーザー向けの設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Microsoft Edge] に配置されています。コンピューター向けの設定は、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Microsoft Edge] に配置されています。

次の構成が可能です。

- スクリプトの実行
- パスワード マネージャーの構成
- ポップアップの実行
- クッキーの構成
- エンタープライズ サイト一覧の構成
- すべてのイントラネット トラフィックを Internet Explorer に送るかどうか

アプリの展開

1 つのボリュームのみを保有するタブレットで、外部ドライブやセキュア デジタル (SD) カードなどのシステム ボリューム以外のボリュームに、アプリを格納できるかどうかを構成できます。また、アプリのデータを、システム ボリューム以外に格納できるかも制御できます。アプリの展開の設定は、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[アプリ パッケージの展開] に配置されています。

管理対象の一般的なデスクトップ設定

管理用テンプレートには、数千の設定があります。ユーザーのデスクトップ向けに構成する最も一般的な設定には、次のものがあります。

- デスクトップの壁紙
- スクリーン セーバー設定
- エクスプローラー設定
- ユーザーのログオン時に実行するプログラムの指定
- 詳細な状態メッセージの表示
- Windows Update の設定
- ブラウザーの設定

・デスクトップの壁紙
・スクリーン セーバー設定
・エクスプローラー設定
・ユーザーのログオン時に実行するプログラムの指定
・詳細な状態メッセージの表示
・Windows Update の設定
・ブラウザーの設定

デスクトップの壁紙

[デスクトップの壁紙] 設定を構成することで、すべてのユーザーのコンピューターに、企業のデスクトップを表示させることができます。この設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[デスクトップ]、[デスクトップ] に配置されています。壁紙への汎用名前付け規則 (UNC) パス (またはローカル パス)、および壁紙の配置スタイルを構成します。

スクリーン セーバー設定

構成すべき一般的な設定に、スクリーン セーバーがあります。スクリーン セーバーには、いくつかの設定があります。それらの設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[コントロール パネル]、[個人設定] に配置されています。スクリーン セーバーが機能するには、次の 3 つの設定を構成する必要があります。

- **スクリーン セーバーを有効にする :** この設定を有効にします。
- **特定のスクリーン セーバーを強制する :** スクリーン セーバーとして指定する実行可能ファイルを指定します。
- **スクリーン セーバーのタイムアウト :** スクリーン セーバーが起動するまでのタイムアウトを、秒単位で構成します。

[スクリーン セーバーをパスワードで保護する] を設定すると、ユーザーがスクリーン セーバーを停止する場合、コンピューターのロックを解除する必要があります。

エクスプローラー設定

エクスプローラーを使用する際、ユーザーが同じエクスペリエンスを維持できるように、エクスプローラーに関する多くの設定を構成できます。テンプレートには、次のものがあります。

- 以前のバージョンの設定
- サムネイルとサムネイルのキャッシュをオフにする
- 起動時にリボンを最小化する
- メニュー バーを表示する
- ごみ箱を構成する

エクスプローラーの設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[エクスプローラー] に配置されています。

ユーザーのログオン時に実行するプログラムの指定

ユーザーがサインインした際、自動的に起動するプログラムを構成するには、いくつかの方法があります。スケジュールされたタスクとスクリプトを構成し、さらに、ユーザーがサインインした際、特定のプログラムを実行するように、この設定を構成できます。この設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[システム]、[ログオン] に配置されています。この設定を構成する際は、実行するプログラムのリストを作成します。実行可能ファイルが %systemroot% に配置されている場合を除いて、完全なローカル パスまたは UNC パスを指定する必要があります。

詳細な状態メッセージの表示

グループ ポリシーを使用して構成する設定が多いほど、ユーザーがサインインする際にかかる時間が長くなります。既定では、デスクトップが読み込まれるまで、しばらくの間、ユーザーにはウェルカム メッセージのみが表示されます。サインイン時に詳細なステータス メッセージを表示する場合は、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[システム] に配置されているこの設定を有効にします。この設定を有効にすると、ウェルカム メッセージの代わりに、設定を適用している各 CSE のメッセージが表示されます。

Windows Update の設定

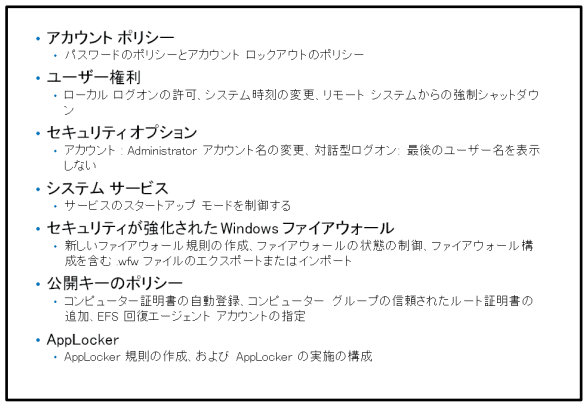
Microsoft Update を既定にする代わりに、Windows Server Update Services (WSUS) サーバーを使用するように、コンピューターを構成できます。また、Windows Update に関連するその他の設定を構成することもできます。Windows Update を構成するための設定は、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Windows Update] に配置されています。

ブラウザーの設定

Internet Explorer と Microsoft Edge の両方を構成する設定がいくつかあります。これらの設定のほとんどは、Internet Explorer を構成します。Internet Explorer の設定のほとんどは、グループ ポリシーを通じて構成できます。この設定は、[ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Internet Explorer] に配置されています。

管理対象の一般的なセキュリティ設定

グループ ポリシーを使用して、組織内の複数のユーザーとコンピューターにセキュリティ設定を適用できます。例えば、グループ ポリシーを使用してパスワード ポリシー設定を構成し、それらを複数のユーザーに展開できます。



アカウント ポリシー

次の構成が可能です。

- ドメイン ユーザーのパスワード ポリシー
- アカウント ロックアウト ポリシー
- Kerberos バージョン 5 (v5) プロトコル

ユーザー権利

一般的に使用されるユーザー権利、およびそれらによって構成されるポリシーの例を次に示します。

- **ワークステーションをドメインに追加する :** ドメインにワークステーションを追加できるユーザーまたはグループを決定します。
- **ローカル ログオンを許可する :** コンピューターにサインインできるユーザーを決定します。
- **システム時刻の変更 :** コンピューターの内部クロックの日付と時刻を変更できるユーザーまたはグループを決定します。
- **リモート システムからの強制シャットダウン :** ネットワーク上のリモートの場所からコンピューターをシャットダウンできるユーザーを決定します。
- **システムのシャットダウン :** コンピューターにローカルにサインインして、コンピューターをシャットダウンできるユーザーを決定します。

セキュリティ オプション

グループ ポリシーを使用して、セキュリティ オプションにアクセスし、構成することもできます。構成が可能な一般的な設定には、次のものがあります。

- **パスワードが無効になる前にユーザーに変更を促す :** ユーザーのパスワードの期限が切れる何日前に、オペレーティング システムが警告を表示するかを決定します。
- **対話型ログオン : 最後のユーザー名を表示しない :** Windows サインイン ウィンドウに、コンピューターに最後にサインインしたユーザーの名前を表示するかどうかを決定します。
- **対話型ログオン : ログオン時のユーザーへのメッセージのテキスト :** ユーザーがサインインする際に表示するメッセージを指定します。一般的なメッセージは、システムはプライベートな利用または承認された利用のみ許可されるので、このシステムを使用するすべての試みは監視されるという警告です。
- **アカウント : Administrator アカウント名の変更 :** Administrator アカウントのセキュリティ ID (SID) に異なるアカウント名を関連付けるかどうかを決定します。

- **ユーザー アカウント制御 (UAC) :** ユーザーおよび管理者の昇格時におけるプロンプトの動作など、UAC プロンプトの動作を変更します。

システム サービス

自動的に起動するサービスと、そのサービスを実行するサービス アカウントを構成できます。ただし、サービスを構成するには、GPO を編集するコンピューターに、そのサービスがインストールされている必要があります。したがって、通常はサービスがインストールされているコンピューターに、RSAT をインストールします。

セキュリティが強化された Windows ファイアウォール

クライアントのファイアウォールは、グループ ポリシーを使用して構成できます。そのためには、クライアントを構成した後、ファイアウォール構成を .wfw ファイルにエクスポートします。このファイルを、GPO にインポートできます。

公開キーのポリシー

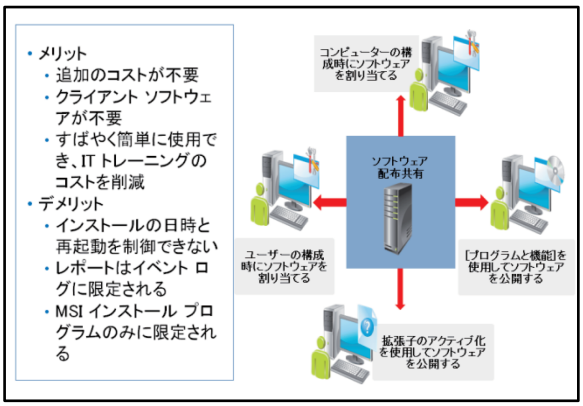
証明書の使用が増えると、管理者はこの設定を構成する機会が多くなります。公開キー ポリシーを使用して、次の構成を実行できます。

- コンピューター証明書の自動登録を使用する。
- コンピューター グループの信頼されたルート証明書を追加する。
- 暗号化ファイル システム (EFS) 回復エージェント アカウントを指定する。
- EFS の使用を無効にする。

アプリケーション制御ポリシー

Windows 7 で AppLocker 機能が導入されました。この機能により、アプリケーション、インストーラー、スクリプト、およびユニバーサル アプリの許可と拒否を構成できます。Windows 10 Enterprise および Education Edition のみ、AppLocker 機能を使用できます。

アプリケーションの展開と管理



Windows 10 には、グループ ポリシーにソフトウェアのインストール機能が搭載されています。AD DS、グループ ポリシー、および Windows インストーラー サービスはこの機能を使用して、組織のコンピューターに対して、ソフトウェアの展開、メンテナンス、および削除をおこないます。

グループ ポリシーによるソフトウェアの管理

ソフトウェアのライフ サイクルは、準備、展開、メンテナンス、および削除の 4 つのフェーズで構成されます。グループ ポリシーを使用して、準備フェーズを除くすべてのフェーズを管理できます。グループ ポリシー設定をサイト、ドメイン、または OU 内のユーザーやコンピューターに適用し、ソフトウェアを自動的にインストール、アップグレード、または削除できます。

グループ ポリシー設定をソフトウェアに適用することで、ソフトウェアを各コンピューターに個別に展開することなく、ソフトウェアの展開フェーズを管理できます。

グループ ポリシーを使用したソフトウェア ライフ サイクルの管理には、考慮する必要があるいくつかのメリットとデメリットがあります。グループ ポリシーを使用してソフトウェア ライフ サイクルを管理するメリットには、次のものがあります。

- グループ ポリシーによるソフトウェア配布は、グループ ポリシーと AD DS の一部として使用できます。したがって、グループ ポリシーは既にインストールされ、使用の準備が整っているので、組織はグループ ポリシーを使用することで追加のコストを負担することはなく、いつでも実装のために使用できます。
- グループ ポリシーによるソフトウェア配布では、クライアント ソフトウェア、エージェント ソフトウェア、または追加の管理ソフトウェアは必要ありません。IT 管理者は、使い慣れたツールを使用してソフトウェアのライフ サイクルを管理できます。
- グループ ポリシーによるソフトウェア配布は、すばやく簡単に使用できます。そのため、ソフトウェアの迅速な配布と、IT トレーニング コストの削減の両方が可能になります。

グループ ポリシーを使用してソフトウェア ライフ サイクルを管理するデメリットには、次のものがあります。

- グループ ポリシーによるソフトウェア配布には、最小限の機能セットしかありません。そのため、インストールの日時、再起動の抑制や Windows の再起動を含む再起動プロセスなど、配布の制御面の機能が制限されています。
- グループ ポリシーによるソフトウェア配布には、レポート機能がありません。したがって、ソフトウェアが配布されたコンピューターの数、インストールが失敗したコンピューター、ソフトウェアが配布されなかったコンピューターなどの情報を、簡単に収集することができません。
- グループ ポリシーによるソフトウェア配布は、Windows インストーラー パッケージの展開に限定されています。IT 管理者は、グループ ポリシーを使用してソフトウェアを展開する前に、MSI インストール以外のプログラムを MSI パッケージに変換する必要があります。

注 : 大規模な組織 (特に 500 台以上のコンピューターを所有する組織) の場合、および個別のソフトウェア配布要件がある組織の場合、System Center 2012 R2 Configuration Manager がエンタープライズレベルの機能と制御を提供します。これらの機能と制御により、グループ ポリシーによるソフトウェア配布のデメリットが排除されます。

ソフトウェアをクライアントに配布する場合、2 つの展開オプションを使用できます。

- 管理者は、ソフトウェアを割り当てることにより、ユーザーまたはコンピューターに対してソフトウェアを事前にインストールすることができます。
- 管理者は、ソフトウェアを AD DS で公開することにより、ユーザーは必要なときにソフトウェアをインストールできるようになります。

GPO のユーザーとコンピューターの両方の構成セクションには、[ソフトウェアの設定] セクションがあります。このセクションには、[ソフトウェアのインストール] ノードがあります。新しいパッケージを [ソフトウェアのインストール] ノードに追加して、割り当てるかまたは公開するかを指定することで、GPO にソフトウェアを追加できます。

また、パッケージの高度な展開を選択することもできます。このオプションを使用して、カスタム展開のために、カスタマイズ ファイルをパッケージに適用します。

ソフトウェアの割り当て

ソフトウェアの割り当てには、次の特性があります。

- ソフトウェアをユーザーに割り当てると、そのユーザーがサインインした際、ユーザーのスタート メニューでそのソフトウェアがアドバタイズされます。ユーザーがアプリケーションのアイコン、またはそのアプリケーションに関連付けられているファイルをダブルクリックすると、そのソフトウェアのインストールが開始されます。また、サインイン時にソフトウェアがインストールされるように構成することもできます。
- ユーザーは、展開されたアプリケーションを共有することはできません。ソフトウェアをユーザーに割り当てた場合、グループ ポリシーを通じてあるユーザーに対してインストールされたアプリケーションを、他のユーザーが使用することはできません。ソフトウェアがユーザーの一部により使用されている場合は、通常、ソフトウェアをユーザーに割り当てることが推奨されます。
- アプリケーションをコンピューターに割り当てると、コンピューターが次回起動した際、アプリケーションがインストールされます。アプリケーションをコンピューターに割り当てて、ユーザーには割り当てないことにより、アプリケーションはそのコンピューターのすべてのユーザーが使用できるようになります。コンピューターを使用するユーザーに関係なく、ソフトウェアをコンピューターの特定のセット、または環境内のすべてのコンピューターにインストールする必要がある場合、ソフトウェアをコンピューターに割り当てることが推奨されます。一般的にこの方法は、監視エージェント、セキュリティ関連のエージェント、管理エージェントなどのエージェント ソフトウェアを使用する際に採用されます。ソフトウェアにライセンス コストが伴い、不要なライセンスを購入したくない場合は、ソフトウェアをコンピューターに割り当てることをお勧めします。

ソフトウェアの公開

ソフトウェアの公開には、次の特性があります。

- ユーザーがコントロール パネルで、[プログラム]、[プログラムと機能] の順にクリックすると、[ネットワークからプログラムをインストール] リンクに公開されたアプリケーションが表示されます。この場合、ユーザーは次のいずれかの方法を使用して、アプリケーションをインストールできます。
  - **コントロール パネル :** コントロール パネルでアプリケーションをダブルクリックします。
  - **拡張子のアクティブ化 :** ユーザーがプログラムに関連付けられたファイルの種類をクリックすると、拡張子のアクティブ化によりプログラムのインストールが開始されます。
- コントロール パネルは、アプリケーションをインストールするアクセス許可がないユーザーに対しては、アプリケーションを表示しません。
- コンピューターに対して、アプリケーションを公開することはできません。

デモンストレーション : グループ ポリシー設定の構成

講師は、次のデモンストレーションをおこないます。

- ユーザーおよびコンピューターの管理用テンプレート設定を構成する
- セキュリティ設定を構成する

デモンストレーションの手順

1. LON-DC1 のグループ ポリシーの管理で、Desktop Settings GPO を編集します。
2. [ユーザーの構成]、[ポリシー]、[管理用テンプレート]、[システム]、[ログオン] の順に展開し、[ユーザーのログオン時に実行するプログラムを指定する] 設定のリストを「notepad.exe」に変更します。

3. 新しい GPO を作成し「Computer Settings GPO」という名前を付けます。
4. Computer Settings GPO を編集します。
5. [コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[システム] で、[詳細な状態メッセージを表示する] を [有効] に設定します。
6. [コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[ローカル ポリシー]、[セキュリティ オプション] の順に展開します。
7. [対話型ログオン : ログオン時のユーザーへのメッセージのタイトル] 設定を「Welcome to the Adatum corporate domain」に構成します。
8. [対話型ログオン : ログオン時のユーザーへのメッセージのテキスト] 設定を「You are not allowed to use this computer for inappropriate behavior」に構成します。
9. Computer Settings GPO を Adatum.com ドメインにリンクします。
10. 23697-2B-LON-CL1 に切り替えて、起動します。
11. [OK] をクリックしてメッセージを承諾します。
12. ユーザー名「Adatum¥Allie」、パスワード「Pa$$w0rd」を使用してサインインします。
13. サインインの前に承諾する必要がある使用条件に注意してください。
14. 通常のウェルカム メッセージの代わりに、グループ ポリシー クライアントが実行したアクションに関するさまざまなテキストが表示されることに注意してください。
15. メモ帳が開くことに注意してください。
16. LON-CL1 からサインアウトします。

知識の確認

質問	
Windows 10 の管理用テンプレートで構成できる新しい設定は、次のうちどれですか (適合するものをすべて選択します)。	
正しい解答を選択してください。	
	Microsoft Edge
	Microsoft Passport
	Windows Insider
	ストレージ センサー
	コマンド プロンプト

質問	
グループ ポリシーを通じてソフトウェアを展開するために使用できる方法はどれですか (適合するものをすべて選択します)。	
正しい解答を選択してください。	
	コンピューターに割り当てる
	ユーザーに割り当てる
	[プログラムと機能] でユーザーに公開する
	[プログラムと機能] でコンピューターに公開する
	拡張子のアクティブ化でユーザーに公開する

演習 A : グループ ポリシー オブジェクトと設定の構成

シナリオ

A. Datum 社で、あなたは、Windows 10 を実行するコンピューターを管理するための最新の要件を受け取りました。社内のさまざまな部門で、100 台の内部コンピューターが使用されています。次のような他と異なる要件を持つ、一部の部門があります。

- マシン フロアのコンピューターでは、Windows Update を無効にする必要があります。機器で実行されるアプリケーションと更新プログラムに互換性があることを製造元が確認するまで、これらのコンピューターが更新されてはいけません。また、これらのコンピューターのすべての Windows Insider ビルドへのアクセスを無効にする必要もあります。
- マシン フロアのコンピューターでは、リモート管理を許可しない必要があります。これにより、機器に影響を与える可能性があるリモート変更がおこなわれないようにします。
- マシン フロアのすべてのコンピューターは、Microsoft Edge をより高いセキュリティで実行する必要があります。ローカルにパスワードを保存することは許されず、ポップアップとクッキーは許可され、オート コンプリートは無効にする必要があります。
- マシン フロア以外のコンピューターは、すべて、リモート管理される必要があります。
- マシン フロア以外のすべてのコンピューターで、リモート デスクトップが許可される必要があります。
- マシン フロア以外のすべてのコンピューターで、Windows PowerShell リモート処理を有効にする必要があります。
- マシン フロア以外のコンピューターは、Windows Update の新しい配信の最適化機能を使用する必要があります。これにより、クライアントは更新プログラムを共有することができるので、サーバーの帯域幅が節約されます。
- デスクトップ コンピューターに適用する構成を、サーバーおよびドメイン コントローラーに適用してはいけません。
- MachineFloor と CorpComputers という 2 つの新しい OU を作成します。

目的

この演習により、次のことを習得できます。

- グループ ポリシーを使用して、Windows 10 を管理することができます。

演習のセットアップ

予定所要時間 : 50 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 23697-2B-LON-CL2
ユーザー名	Adatum¥Administrator
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 : Administrator
   - パスワード : Pa$$w0rd
   - ドメイン : Adatum

練習 1 : グループ ポリシーによる Windows 10 の管理

シナリオ

あなたは、グループ ポリシーを使用して、A. Datum 社の要件のとおりに、標準化された設定を実装するように、依頼されました。

主な作業は次のとおりです。

1. 組織単位 (OU) の構造を作成する
2. 管理用テンプレートのセントラル ストアを作成する
3. MachineFloor のコンピューターのグループ ポリシーを構成する
4. CorpComputers のグループ ポリシー設定を構成する
5. グループ ポリシー設定を検証する

▶ 作業 1 : 組織単位 (OU) の構造を作成する

1. LON-DC1 の Active Directory 管理センターで、「MachineFloor」と「CorpComputers」という 2 つの OU を作成します。
2. LON-CL1 のコンピューター アカウントを [MachineFloor] OU に移動します。
3. LON-CL2 のコンピューター アカウントを [CorpComputers] OU に移動します。
4. Active Directory 管理センターを閉じます。
5. 23697-2B-LON-CL1 と 23697-2B-LON-CL2 を起動します。

▶ 作業 2 : 管理用テンプレートのセントラル ストアを作成する

1. LON-DC1 で、E:¥Labfiles¥PolicyDefinitions フォルダーを ¥¥LON-DC1¥SYSVOL¥Adatum.com¥Policies フォルダーにコピーします。

▶ 作業 3 : MachineFloor のコンピューターのグループ ポリシーを構成する

1. LON-DC1 のグループ ポリシーの管理で「MachineFloor GPO」という新しい GPO を作成します。
2. [コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[システム]、[インターネット通信の管理]、[インターネット通信の設定] の順に展開し、[Windows Update のすべての機能へのアクセスをオフにする] 設定を有効にすることで、MachineFloor GPO を編集します。
3. MachineFloor GPO で、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[データの収集とプレビュー ビルド] の順に展開し、[Insider ビルドに関するユーザー コントロールの切り替え] 設定を無効にします。
4. MachineFloor GPO で、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Windows リモート管理 (WinRM)]、[WinRM サービス] の順に展開し、[WinRM によるリモート サーバー管理を許可する] 設定を無効にします。

5. MachineFloor GPO で、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[システム サービス]、[Windows Remote Management (WS-Management)] の順に展開し、[このポリシーの設定を定義する] チェック ボックスをオンにし、サービスを無効にします。
6. MachineFloor GPO で、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[セキュリティが強化された Windows ファイアウォール]、[セキュリティが強化された Windows ファイアウォール - LDAP://CN=<GUID>] の順に展開し、新しい受信の規則を作成して、事前に定義された [Windows リモート管理] をブロックします。
7. MachineFloor GPO で、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Microsoft Edge] の順にクリックし、[Web サイトでオートフィルを使用できるようにする] 設定を無効にします。
8. MachineFloor GPO で、次の設定を無効にします。
   - パスワード マネージャーの構成を許可する
   - ポップアップの実行を許可する
   - Configure how Microsoft Edge treats cookies

▶ 作業 4 : CorpComputers のグループ ポリシー設定を構成する

1. LON-DC1 のグループ ポリシーの管理で「CorpComputers GPO」という新しい GPO を作成します。
2. CorpComputers GPO で、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Windows リモート管理 (WinRM)]、[WinRM サービス] の順に展開します。
3. [WinRM によるリモート サーバー管理を許可する] 設定を有効にし、[IPv4 フィルター] を「アスタリスク (*)」に設定します。
4. CorpComputers GPO で、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[システム サービス]、[Windows Remote Management (WS-Management)] の順に展開し、サービスが自動的に開始するように設定します。
5. CorpComputers GPO で、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[リモート デスクトップ サービス]、[リモート デスクトップ セッション ホスト]、[接続] の順に展開します。
6. [ユーザーがリモート デスクトップ サービスを使ってリモート接続することを許可する] 設定を有効にします。
7. CorpComputers GPO で、[コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント]、[Delivery Optimization] の順に展開します。
8. [Download Mode] 設定を有効にし、[Download Mode] を [LAN] に設定します。
9. グループ ポリシー管理エディターを閉じます。

▶ 作業 5 : グループ ポリシー設定を検証する

グループ ポリシー オブジェクト (GPO) を適用する前に設定を確認する

1. LON-DC1 で、Windows PowerShell を起動し、次のコマンドレットを入力して、Enter キーを押します。

```
Invoke-Command -Computername LON-CL2 -ScriptBlock {hostname}
```

注 : LON-CL2 上でコマンドレットを実行できないことを確認します。

2. LON-CL2 へのリモート デスクトップ接続を確立します。

注 : リモート デスクトップ接続クライアントが接続を作成しようとすると、一定期間経過後にエラー メッセージが表示されることを確認します。

3. LON-CL1 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。
4. 更新プログラムをダウンロードできるか確認します。

注 : エラー メッセージが表示されるまでにしばらく時間がかかることに注意してください。また、「オンラインにして更新プログラムをダウンロードすることができませんでした。」というメッセージが表示される場合もあります。.

5. Insider ビルドを開始できるか確認します。

注 : [開始する] をクリックすることができることを確認します。

6. サインアウトし、ユーザー名「Adatum¥Allie」、パスワード「Pa$$w0rd」を使用して再度サインインします。
7. Microsoft Edge を起動し、[詳細設定を表示] に移動します。

注 : [パスワードを保存する] が [オン] に設定され、クッキーがブロックされていないことを確認します。

8. LON-CL1 からサインアウトします。

GPO をリンクする

1. LON-DC1 で、[CorpComputers GPO] と [CorpComputers Firewall policy] を [CorpComputers] OU にリンクします。
2. [MachineFloor GPO] を [MachineFloor] OU にリンクします。

GPO を適用し設定を確認する

1. LON-CL1 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. LON-CL1 と LON-CL2 の両方を再起動するために、コマンド プロンプトで次のコマンドを実行します。

```
gpupdate
```

3. コンピューターが再起動するまで待ち、次に進みます。
4. LON-DC1 に切り替えます。
5. LON-DC1 を再起動します。
6. 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。
7. Windows PowerShell ウィンドウを開きます。
8. Windows PowerShell ウィンドウで次のコマンドレットを入力し、Enter キーを押します。

```
Invoke-Command -Computername LON-CL2 -ScriptBlock {hostname}
```

注 : LON-CL2 でコマンドレットが実行できるようになったことを確認します。

9. LON-CL2 へのリモート デスクトップ接続の設定を試みます。

注 : サインイン プロンプトが表示されることに注意してください。

10. LON-CL1 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。
11. 更新プログラムをダウンロードできるか確認します。

注 : エラー メッセージが即座に表示されることを確認します。

12. Insider ビルドを開始できるか確認します。

注 : [開始する] をクリックできないことを確認します。

13. LON-CL1 からサインアウトし、ユーザー名「Adatum¥Allie」、パスワード「Pa$$w0rd」を使用して再度サインインします。
14. Microsoft Edge を起動し、[詳細設定を表示] に移動します。

注 : いくつかの設定は、グループ ポリシー経由で構成されているため、グレーアウトされていることを確認します。

15. ユーザー名「Adatum¥Allie」を使用して LON-CL1 からサインアウトします。

結果 : この練習により、GPO とセントラル ストアを作成し、いくつかのグループ ポリシー設定を構成して、それらが適用されていることを確認することができました。

▶ 次の演習の準備をする

次の演習のために、仮想マシンを起動したままにします。

レッスン 3
グループ ポリシーの基本設定の概要

Windows Server 2008 オペレーティング システムがリリースされる前は、管理者はグループ ポリシーを使用して、ユーザーおよびコンピューターの環境に影響する一般的な設定を制御することができませんでした。一般的にこれらの設定 (マップ済みドライブなど) は、ログオン スクリプトまたはイメージング ソリューションにより提供されていました。

一方、Windows Server 2012 オペレーティング システムでは、グループ ポリシーの基本設定が GPMC に組み込まれ、これによりマップ済みドライブなどの設定をレジストリの変更として構成できるようになりました。さらに、Windows 10 を実行しているコンピューターに RSAT をインストールすることで、基本設定を構成することもできます。これにより、グループ ポリシーを使用して、多くの一般的な設定を提供できるようになります。

目的

このレッスンにより、次のことを習得できます。

- グループ ポリシー設定とグループ ポリシーの基本設定の違いを説明することができます。
- 一般的に構成するグループ ポリシーの基本設定について説明することができます。
- グループ ポリシーの基本設定で、項目レベルのターゲット設定が機能するしくみについて説明することができます。
- グループ ポリシーの基本設定を構成することができます。

グループ ポリシー設定とグループ ポリシーの基本設定の違い

グループ ポリシーの基本設定は、構成をユーザーまたはコンピューターに適用するという点で、ポリシー設定と似ていますが、それらを構成および適用する方法に関していくつかの違いがあります。これら 2 つの大きな違いの 1 つは、基本設定は強制されないことです。

次に、グループ ポリシー設定とグループ ポリシーの基本設定の違いについて、一覧で示します。

グループ ポリシー設定	グループ ポリシーの基本設定
標準ユーザーが編集できないレジストリの領域に設定を書き込むことで、ポリシー設定を厳しく強制する	アプリケーションやオペレーティング システム機能が設定の格納に使用するレジストリの標準の場所に書き込まれる
グループ ポリシーが管理する設定のユーザー インターフェイスを無効にする	ユーザー インターフェイスを無効にしない
設定は、定期的な間隔で適用される	一度のみ適用されるように構成できる
GPO が削除されると、設定が削除される	既定で、GPO が削除されても、設定は削除されない

グループ ポリシー設定	グループ ポリシーの基本設定
管理用テンプレートのグループ ポリシー設定は、ユーザーが編集できないレジストリの領域に書き込まれ、GPO が適用されなくなると簡単に削除されます。	レジストリに対する変更は、以前に構成された値に設定が上書きされる、レジストリの標準の場所に書き込まれ、GPO が適用されなくなっても削除できません。
グループ ポリシー設定は、ポリシーが管理する設定のユーザー インターフェイスを無効にします。	グループ ポリシーの基本設定は、これを無効にしません。
グループ ポリシー設定は、定期的な間隔で適用されます。	グループ ポリシーの基本設定は、一度のみ、または定期的な間隔で適用できます。

グループ ポリシー設定	グループ ポリシーの基本設定
通常、Windows オペレーティング システムは構成された設定のユーザー インターフェイスを無効にするので、ユーザーがグループ ポリシー設定を変更することはできません。	ユーザーは、グループ ポリシーを通じて適用されるグループ ポリシーの基本設定を変更できます。
グループ ポリシー設定は、グループ メンバーシップ、時刻、ファイルの存在、IP アドレスなど、特定の条件に一致するユーザーまたはコンピューターのみを設定のターゲットにすることはできません。	グループ ポリシーの基本設定は、グループ メンバーシップ、時刻、ファイルの存在、IP アドレスなど、特定の条件に一致するユーザーまたはコンピューターのみを基本設定のターゲットにできる、項目レベルのターゲット設定機能を備えています。

場合によっては、グループ ポリシー設定とグループ ポリシーの基本設定の両方を使用して、同一のグループ ポリシー設定を構成することができます。グループ ポリシー設定とグループ ポリシーの基本設定で競合する構成をおこない、それらを同じオブジェクトに適用した場合、グループ ポリシー設定の値が常に適用されます。

一般的なグループ ポリシーの基本設定の展開

グループ ポリシーの基本設定を作成した後、そのプロパティを構成する必要があります。異なる基本設定には、異なる入力情報が必要になります。例えば、ショートカットの基本設定にはターゲット パスが必要になり、環境変数には変数の型と値が必要になります。また、グループ ポリシーの基本設定は、展開を支援するために、一般的な設定プロパティのさまざまな機能を提供します。多くの企業はグループ ポリシーの基本設定を使用して、ログオン スクリプトにあらかじめ構成されるさまざまな設定を変換しています。

- グループ ポリシーの基本設定で構成可能な項目
  - ドライブ マップ
  - レジストリ
  - ショートカット
  - インターネット設定
  - 電源オプション
  - プリンター
  - ファイル
- グループ ポリシーの基本設定のプロパティの構成
  - 全般タブ : アクションを指定するための設定が含まれる
  - 共通プロパティ タブ : 基本設定の動作を制御するための設定が含まれる
  - その他のプロパティは、基本設定項目によって異なる

全般タブ

基本設定項目のほとんどには [全般] タブがあり、このタブで基本的な構成を指定します。ここでの最初のステップは、基本設定のアクション (作成、削除、置換、または更新) を指定することです。選択するアクションに応じて、さまざまな設定が使用可能になります。例えば、ドライブのマッピングを作成する際は、UNC パスと割り当てるドライブ文字のオプションを指定する必要があります。

共通プロパティ タブ

共通プロパティは、すべての基本設定で一貫しています。[共通] タブを使用して、次の設定により、基本設定の動作を制御できます。

- **エラーが発生した場合、この拡張機能内で項目の処理を中止する :** 基本設定の処理中にエラーが発生した場合、この GPO 内の他の基本設定は処理されません。
- **ログオンしているユーザーのセキュリティ コンテキストで実行する :** 基本設定をシステム アカウントまたはサインイン ユーザーとして実行できます。この設定は、サインイン ユーザーのコンテキストを強制します。
- **この項目が適用されなくなったら削除する :** ポリシー設定とは異なり、変更を実施した GPO が削除されても、Windows オペレーティング システムは基本設定により実施された構成の変更を削除しません。この設定は、その動作を変更します。

- **1 回だけ適用し、再適用しない :** 一般的に、基本設定は、グループ ポリシー設定と同じ間隔で更新されます。この設定は、その動作を、1 回だけ設定が適用されるように変更します。
- **項目レベルで対象化する :** グループ ポリシーの基本設定の最も強力な機能の 1 つは、項目レベルのターゲット設定です。基本設定の対象となるユーザーまたはコンピューターを正確に決定できるように、この機能を使用して簡単に条件を指定できます。条件には次のものがあります (ただし、これに限定されません)。
  - コンピューター名
  - IP アドレスの範囲
  - オペレーティング システム
  - セキュリティ グループ
  - ユーザー
  - WMI クエリ

次の表には、グループ ポリシーの基本設定で構成できるさまざまな項目がすべて含まれています (Windows の設定とコントロール パネルの設定の基本設定を含む)。このリストは、コンピューター用とユーザー用の両方で同じですが、コンピューターとユーザーのどちらに対して構成するかは、各項目で異なる可能性があります。

Windows の設定の基本設定	コントロール パネルの設定の基本設定
• アプリケーション • ドライブ マップ • 環境 • ファイル • フォルダー • ini ファイル • レジストリ • ショートカット	• データ ソース • デバイス • フォルダー オプション • インターネット設定 • ローカル ユーザーとグループ • ネットワーク オプション • 電源オプション • プリンター • 地域のオプション • タスク • スタート メニュー

ドライブのマッピング

ネットワーク ドライブのマッピングは、おそらく最も使用される基本設定項目です。一部のネットワーク ドライブは企業で汎用的に使用されますが、ほとんどの部署では独自のネットワーク ドライブを保有しています。ドライブのマッピングでは、特定のドライブ文字を特定のネットワーク共有に対応付けることにより、この状況を解決します。項目レベルのターゲット設定を使用すれば、ユーザーが特定グループのメンバーの場合、この制限が可能になります。つまり、特定のサブネットの IP アドレスを保有するコンピューターにサインインした際、特定のドライブ マップのみを参照するようにユーザーを制限できます。

レジストリ

多くのログオン スクリプトは、レジストリを変更するために .reg ファイルを使用します。これらの変更をおこなうには、レジストリの基本設定項目を使用します。レジストリに対する変更には、単一のレジストリ項目と項目のコレクションが含まれます。ウィザードを実行して、ローカル コンピューターまたはリモート コンピューターのレジストリの一部をインポートすることができます。

ショートカット

新しいユーザーが仕事を開始する際、デスクトップに作成されたショートカットのメリットを活用し、重要な情報を容易に見つけることができます。ショートカットには、次の 3 種類があります。

- ファイル システム オブジェクト (ファイル、フォルダー、またはドライブ)
- URL (Web サイト、Web ページ、または FTP サイト)
- シェル オブジェクト (プリンターまたはコントロール パネル項目)

インターネット設定

Internet Explorer のインターフェイスを使用して、Internet Explorer の設定を構成できます。どの Web サイトがどのセキュリティ ゾーンに属するかの構成など、インターネットの一部の設定は基本設定を使用して構成することはできません。この目的のためには、管理用テンプレートを使用できます。

電源オプション

電源オプションの基本設定項目を使用して、電源プランを構成できます。これらの基本設定は、ローカル コンピューターで作成する場合と同じインターフェイスを使用して作成できます。電源プランの構成では、電力を節約することと、コンピューターの電源をあまりに早くオフにしないようにすることを、適切にバランスさせます。

プリンター

基本設定を使用して、次の 3 種類のプリンターを作成できます。

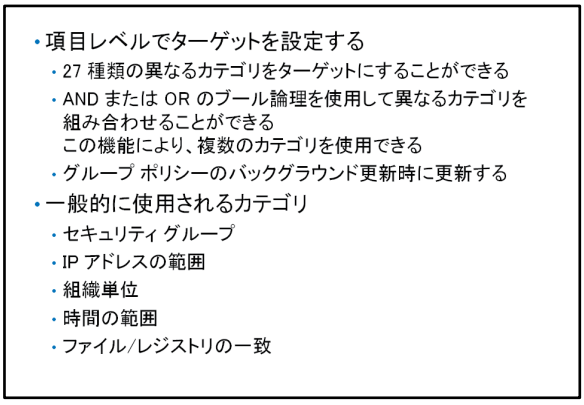
- **共有プリンター :** プリント サーバーの共有プリンターへの接続を作成します。これは、ユーザー専用の設定です。
- **TCP/IP プリンター :** IP アドレスを使用してネットワーク プリンターに接続します。
- **ローカル プリンター :** USB または他の種類のケーブルで接続されたローカル プリンターを作成します。

ファイル

多くの組織は、会社がデザインした Office テンプレートをネットワーク共有に配置しています。このことは、会社のネットワークに接続していないローミング ユーザーにとって、問題となる可能性があります。ファイルの基本設定項目を使用すると、ネットワーク共有からユーザーのコンピューターにファイルをコピーすることができます。また、この基本設定項目を使用して、ローカルに配置されたファイルを、中央のファイル サーバーにコピーすることもできます。この場合、Windows 10 コンピューターに配置されているログ ファイルや他の重要なファイルも対象にできます。

グループ ポリシーの基本設定のターゲット設定とフィルター処理

項目レベルのターゲット設定はグループ ポリシーの基本設定の機能であり、コンピューター オブジェクトまたはユーザー オブジェクトが定義された条件に一致する場合のみ、グループ ポリシー設定をそのオブジェクトに適用することができます。これにより、正確にターゲットを特定して、必要な場所と時間に設定を適用することができます。項目レベルのターゲット設定には、次の機能があります。



- **27 種類の異なるカテゴリをターゲットにする :** 項目レベルのターゲット設定では、コンピューター オブジェクトとユーザー オブジェクトをターゲットにする際、27 種類の異なるカテゴリを使用できます。これにより、正確なターゲット設定が可能になります。
- **AND または OR のブール論理を使用して異なるカテゴリを組み合わせる :** ターゲット設定のために単一のカテゴリを使用する代わりに、複数のカテゴリを使用できます。例えば、ノート PC のみに、そのノート PC のユーザーが営業グループのメンバーである場合に限り、プリンターを展開するには、項目レベルのターゲット設定を使用してこれを実現できます。この手順としては、ポータブル型で営業グループのメンバーに使用され、特定の IP サブネットに属するコンピューターに、あるプリンター グループを展開し、次に IP サブネットを変えて別のプリンター セットを展開します。
- **グループ ポリシーのバックグラウンド更新時に、項目レベルのターゲット設定を更新する :** つまり、項目レベルのターゲット設定を使用してコンピューター オブジェクトとユーザー オブジェクトを構成することで、これらのオブジェクトを柔軟に管理できます。

ターゲット設定を構成するために、27 種類のカテゴリを使用できます。ターゲットにするカテゴリのいくつかは、他のカテゴリよりも、より一般的に使用されます。

それらのカテゴリには、次のものがあります。

- バッテリーの存在
- コンピューター名
- CPU 速度
- 日付の一致
- ディスク領域
- ドメイン
- 環境変数
- ファイルの一致
- IP アドレスの範囲
- 言語
- LDAP クエリ
- MAC アドレスの範囲
- MSI クエリ
- ネットワーク接続
- オペレーティング システム
- 組織単位 (OU)
- PCMCIA の存在
- ポータブル コンピューター
- 処理モード
- RAM
- レジストリー致
- セキュリティ グループ
- サイト
- ターミナル セッション

- 時間の範囲
- ユーザー
- WMI クエリ

一般的に使用されるカテゴリ

- **セキュリティ グループ :** 任意の Active Directory セキュリティ グループを、ターゲットとして使用できます。ターゲットにするオブジェクトがそのグループに配置されている場合、基本設定項目が適用されます。
- **IP アドレスの範囲 :** コンピューターに割り当てられた IP アドレスに応じて、異なる基本設定を適用する場合、この設定を使用します。ターゲットの IP アドレスが指定された範囲に属する場合、基本設定項目が適用されます。
- **組織単位 :** 特定の OU に配置されているオブジェクトにのみ、基本設定項目を適用することができます。同じセキュリティ グループを共有していないユーザーとコンピューターが存在する場合、この機能を使用します。
- **時間の範囲 :** 開始時間と終了時間を指定し、その時間帯にのみ基本設定項目が適用されるようにすることができます。例えば、営業時間と営業時間外で、異なる電源オプションを指定することができます。
- **ファイル/レジストリの一致 :** このカテゴリにより、ファイル/レジストリのエントリを選択し、指定したファイル/レジストリのエントリが存在する場合のみ、基本設定項目を適用することができます。例えば、コンピューターに特定のソフトウェアがインストールされている場合のみ、ドライブをそのソフトウェアのドライブとして対応付けることができます。

デモンストレーション : グループ ポリシーの基本設定の構成

講師は、次のデモンストレーションをおこないます。

- グループ ポリシーの基本設定で電源プランを構成する
- 設定が適用されたことを確認する

デモンストレーションの手順

グループ ポリシーの基本設定で電源プランを構成する

1. LON-DC1 のグループ ポリシーの管理で「Adatum Power Plans GPO」という名前で新しい GPO を作成します。
2. Adatum Power Plans GPO を編集し、[コンピューターの構成] で新しい電源プラン (Windows 7 以降) の基本設定項目を作成します。
3. 新しい電源プラン (Windows 7 以降) のプロパティ ウィンドウの [詳細設定] タブで、次の値を使用します。
    - [バランス] を [省電力] に変更
    - 現在使用されている電源プランとして設定 : オン
    - [スリープ]、[次の時間が経過後スリープする]、[バッテリ駆動] (分) : 30
    - [スリープ]、[次の時間が経過後スリープする]、[電源に接続] (分) : 120
    - [ディスプレイ]、[次の時間が経過後ディスプレイの電源を切る]、[バッテリ駆動] (分) : 15
    - [ディスプレイ]、[次の時間が経過後ディスプレイの電源を切る]、[電源に接続] (分) : 60
4. [共通] タブで、[項目レベルでターゲットを設定する] が選択されていることを確認します。

5. 項目レベルでターゲットを設定するために、[IP アドレスの範囲] を構成します。
6. [開始] と [終了] の両方のボックスに「172.16.0.40」と入力し、[OK] をクリックします。

設定が適用されたことを確認する

1. Adatum Power Plans GPO を Adatum.com ドメインにリンクします。
2. LON-CL1 コンピューターに切り替え、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。
3. グループ ポリシー設定を更新します。
4. gpresult コマンドを実行して、Adatum Power Plans GPO が適用された GPO として一覧に表示されることを確認します。
5. [電源オプション] を起動して、[省電力] が [現在使用されている電源プラン] であることを確認します。

知識の確認

質問	
次のうちで構成可能な基本設定はどれですか。適合するものをすべて選択します。	
正しい解答を選択してください。	
	ドライブ マップ
	プリンター
	ディスプレイ
	Microsoft Office
	レジストリ

記述が正しい場合は、右側の列にチェック マークを入れます。

記述	解答
グループ ポリシーの基本設定は、構成された設定のユーザー インターフェイスを無効にします。	

演習 B : グループ ポリシーの基本設定によるデスクトップ設定の管理

シナリオ

A. Datum 社では、現在、ログオン スクリプトを使用して、ユーザーの部門に基づいて、ドライブとプリンターのマッピングを構成しています。あなたは、グループ ポリシーの基本設定を検証し、そのメリットを説明して、ログオン スクリプト方式をやめさせたいと考えています。

目的

この演習により、次のことを習得できます。

- グループ ポリシーの基本設定を構成して、ドライブとプリンターのマッピングに適用することができます。

演習のセットアップ

予定所要時間 : 40 分

仮想マシン	23697-2B-LON-DC1 23697-2B-LON-CL1 23697-2B-LON-CL2
ユーザー名	Adatum¥Administrator
パスワード	Pa$$w0rd

この演習では、用意された仮想マシン環境を使用します。すべての仮想マシンは、前の演習から引き続き起動しているものとします。次の仮想マシンが起動している必要があります。

- 23697-2B-LON-DC1
- 23697-2B-LON-CL1
- 23697-2B-LON-CL2

練習 1 : ドライブおよびプリンターのマッピングを適用するためのグループ ポリシーの基本設定の構成

シナリオ

ログオン スクリプトの使用をやめる前に、ログオン スクリプトに代わって、グループ ポリシーの基本設定によりドライブのマッピングとネットワーク プリンターの展開ができることを確認する必要があります。

主な作業は次のとおりです。

1. グループ ポリシーの基本設定を構成してドライブ マッピングを構成する
2. グループ ポリシーの基本設定を構成してプリンターを構成する
3. 基本設定が適用されていることを検証する

▶ 作業 1 : グループ ポリシーの基本設定を構成してドライブ マッピングを構成する

ファイル共有を作成する

1. LON-DC1 で、次の 2 つのフォルダーを作成し、共有します。

- E:¥Research
- E:¥Sales

2. 各セキュリティ グループに [読み取り/書き込み] 共有アクセス許可を付与します。

GPO を作成する

1. グループ ポリシーの管理で「Adatum Mapped Drives GPO」という名前の新しい GPO を作成します。
2. 新しい GPO を編集して、[ユーザーの構成] で、次の属性により、新しく割り当てられたドライブの基本設定項目を作成します。
   - [全般] タブをクリックします。
     - 場所 : ¥¥LON-DC1¥Research
     - 再接続 : オン
     - ラベル : Research Data
     - 次の文字を使用 : R
   - [共通] タブをクリックします。
     - ログオンしているユーザーのセキュリティ コンテキストで実行する (ユーザー ポリシー オプション) : オン
     - 項目レベルで対象化する : オン
3. 項目レベルでのターゲット設定を [Research] セキュリティ グループに設定します。
4. 手順 2 ～ 3 を繰り返して、Sales に割り当てられたドライブを作成します。Research へのすべての参照を Sales に置き換えます。

▶ 作業 2 : グループ ポリシーの基本設定を構成してプリンターを構成する

プリンターを作成する

1. LON-DC1 で「ResearchPRT」という名前の新しいローカル プリンターを作成し、共有します。

GPO を作成する

1. 新しい GPO を作成し「Adatum Network Printers GPO」という名前を付けます。
2. 新しい GPO を編集して、[ユーザーの構成] で、次の属性により、新しい共有プリンターの基本設定項目を作成します。
   - [全般] タブをクリックします。
     - 共有パス : ¥¥LON-DC1¥ResearchPRT
     - このプリンターを通常使うプリンターとして設定する : オン
   - [共通] タブをクリックします。
     - ログオンしているユーザーのセキュリティ コンテキストで実行する (ユーザー ポリシー オプション) : オン
     - 項目レベルで対象化する : オン
3. 項目レベルでのターゲット設定を [Research] セキュリティ グループに設定します。

▶ 作業 3 : 基本設定が適用されていることを検証する

GPO を適用する前に設定を確認する

1. LON-CL1 で、ユーザー名「Adatum¥Allie」、パスワード「Pa$$w0rd」を使用してサインインします。
2. ネットワーク ドライブがないことを確認します。
3. ResearchPRT プリンターがないことを確認します。
4. LON-CL2 に切り替え、ユーザー名「Adatum¥Dan」、パスワード「Pa$$w0rd」を使用してサインインします。
5. ネットワーク ドライブがないことを確認します。

GPO をリンクする

1. LON-DC1 に切り替え、[Adatum Mapped Drives GPO] と [Adatum Network Printers GPO] を [Adatum.com] ドメインにリンクします。

GPO を適用し設定を確認する

1. LON-CL1 に切り替え、グループ ポリシー設定を更新します。
2. ネットワーク ドライブが表示されることを確認します。
3. [ResearchPRT (LON-DC1 上)] プリンターが表示されることを確認します。
4. LON-CL2 に切り替え、グループ ポリシー設定を更新します。
5. ネットワーク ドライブが表示されることを確認します。

結果 : この練習により、ドライブ マップとネットワーク プリンターの基本設定を作成し、GPO を使用してそれらを割り当てることができました。

▶ 作業 : 次の章の準備をする

演習が完了したら、仮想マシンを初期状態に戻します。

1. ホスト コンピューターで、Hyper-V マネージャーを起動します。
2. [仮想マシン] リストで、[23697-2B-LON-DC1] を右クリックし、[戻す] をクリックします。
3. [仮想マシンを戻す] ダイアログ ボックスで、[戻す] をクリックします。
4. 23697-2B-LON-CL1 と 23697-2B-LON-CL2 に対して、手順 2 ～ 3 を繰り返します。

復習とまとめ

ベスト プラクティス

- GPO 設定に関するコメントを含め、設定を文書化し、構成された設定を後で簡単に探すことができるようにします。
- 管理用テンプレートのセントラル ストアを使用します。
- グループ ポリシーの基本設定を使用して、ログオン スクリプトで構成された設定を排除します。

一般的な問題とトラブルシューティングのヒント

一般的な問題	トラブルシューティングのヒント
グループ ポリシー設定が、1 つの GPO が適用されている OU 内のすべてのユーザーとコンピューターに適用されていない。	
グループ ポリシーの基本設定が適用されていない。	

復習問題

質問 : セントラル ストアを持つメリットは何ですか。

質問 : あなたの組織では、管理テンプレート セットを拡張しましたか。拡張した場合、インターネットからダウンロードしましたか。または、組織で開発しましたか。