Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

23742A

Windows Server 2016 の ID

製品番号 : 23742A

リリース日 : 2/2017

以下のマイクロソフト ソフトウェアに含まれる仮想環境に関するマイクロソフト ライセンス条項

MICROSOFT WINDOWS IDENTITY FOUNDATION SOFTWARE DEVELOPMENT KIT (SDK)

Microsoft Office 2013

マイクロソフト ソフトウェア ライセンス条項 (以下、「本ライセンス条項」といいます) は、お客様と Microsoft Corporation (またはお客様の所在地に応じた関連会社。以下、「マイクロソフト」といいます) との契約を構成します。以下のライセンス条項をお読みください。本ライセンス条項は、お客様による上記の個々のマイクロソフト ソフトウェア タイトルを始め、仮想環境の一部として提供されるすべてのドキュメント、コンテンツ、クラスルーム セットアップ ガイド、関連ファイルおよび構成ファイル、オンライン サービス、サンプル アプリケーション、ならびにこれらが記録されたメディア (以下、総称して「**仮想環境**」といいます) に適用されます。仮想環境コンポーネントに関連する更新プログラム、追加ソフトウェア、インターネット ベースのサービス、およびサポート サービスにも、本ライセンス条項が適用されます。

仮想環境用のマイクロソフト ソフトウェアの仮想ハード ディスク イメージは、1 つ以上の仮想ハード ディスク上でお客様に提供される場合があります。上記の個々のソフトウェア タイトルは通常、別々にライセンスされますが、お客様には便宜のために本統合ライセンス条項に基づいて提供されます。

以下の記載のとおり、仮想環境を使用することにより、ライセンス認証または検証の間、およびインターネット ベースのサービスのために、特定のコンピューター情報を送信することにもお客様が同意されたものとします。

仮想環境の任意の部分にアクセスすることにより、お客様は本ライセンス条項に同意されたものとします。本ライセンス条項に同意されない場合は、仮想環境コンポーネントにアクセスしたり、当該コンポーネントを使用したりしないでください。

仮想環境を使用する、または仮想環境にアクセスできるようにするお客様の権利は、特定の期間内に限定されます。詳細については、第 8 条をご覧ください。

お客様が本ライセンス条項を遵守し、仮想環境の有効なライセンスを取得していることを条件として、お客様には以下が許諾されます。

1. **定義**。

1.1. 「**認定ラーニング センター**」とは、ラーニング パートナー、マイクロソフト IT Academy プログラム メンバー、またはマイクロソフトが書面をもって指名できるその他同様の法人を意味します。

1.2. 「**認定トレーニング セッション**」とは、認定ラーニング センターのためにそのトレーニング施設で MCT が実施する、マイクロソフト認定インストラクターがマイクロソフト コースを指導するトレーニング クラスを意味します。

1.3. 「**クラスルーム デバイス**」とは、認定ラーニング センターが所有または管理する、認定トレーニング セッションが行われる認定ラーニング センターのトレーニング施設にある専用のパーソナル コンピューターで、特定のマイクロソフト コース タイトルに指定されているハードウェア レベルを満たすか、または超えているものを意味します。

1.4. 「**エンド ユーザー**」とは、認定トレーニング セッションに正規に登録し出席している個人を意味します。

1.5. 「**ラーニング パートナー**」とは、現在ラーニング コンピテンシーを保有および保持している、Microsoft Partner Network プログラムの有効なアクティブ メンバーを意味します。

1.6. 「**MCT**」または「**マイクロソフト認定トレーナー**」とは、(i) 認定トレーニング セッションを指導するために認定ラーニング センターに雇用されており、(ii) マイクロソフト認定資格プログラムに基づいてマイクロソフト認定トレーナーとして現在有効に認定されている、(iii) 認定トレーニング セッションの主題であるテクノロジにおいてマイクロソフト認定資格を現在保持している個人を意味します。

1.7. 「**マイクロソフト コース**」とは、個人を対象としてマイクロソフト テクノロジについて指導する、マイクロソフトからライセンスされているマイクロソフト ブランドのインストラクター指導トレーニング コースの受講生キット バージョンを意味します。マイクロソフト コースのタイトルは、マイクロソフト オフィシャル コース、Microsoft Dynamics、またはマイクロソフト ビジネス グループ コースウェアとしてブランド化されている場合があります。

1.8. 「**マイクロソフト IT Academy プログラム メンバー**」とは、マイクロソフト IT Academy プログラムのアクティブ メンバーである教育機関を意味します。

1.9. 「**お客様**」とは、本ライセンスに基づいて権利を行使するラーニング パートナーまたは MCT を意味します。

2. インストールおよび使用に関する権利。

2.1. その他のマイクロソフト ライセンス条項に優先して適用。本ライセンス条項の条件は、仮想環境ソフトウェアのインストールまたは使用に際し、他のライセンス条項への「同意」が必要な場合であっても、当該ソフトウェアにかかわるすべてのマイクロソフト ライセンス条項の条件に優先して適用されます。

2.2. 限定された使用権。仮想環境は使用許諾されるものであり、販売されるものではありません。仮想環境は、その仮想環境に関連するマイクロソフト コース タイトルと共にのみ使用することができます。したがって、お客様は、仮想環境にアクセスするエンド ユーザーごとに、その仮想環境に関連するマイクロソフト コース タイトルのライセンスを購入し、マイクロソフト コース タイトルの有効なライセンス取得済みの複製を各エンド ユーザーに提供しなければなりません。以下は 2 組の独立した使用権であり、お客様には 1 組のみが適用されます。

a. **お客様自身が提供している各認定トレーニング セッションのラーニング パートナー**の場合、お客様には以下が許諾されます。

   i. お客様の認定トレーニング セッションの主題であるマイクロソフト コース タイトルのクラスルーム セットアップ ガイドに記載されている仮想環境コンポーネントのみをダウンロードし、Microsoft Hyper-V の有効なライセンス取得済みの複製を実行している 1 台のホスト クラスルーム デバイスにインストールして、マイクロソフト コースに関連する仮想環境を構築できます。

   ii. 次のいずれかが許諾されます。

      1. 認定トレーニング セッションが行われているお客様の認定ラーニング センターのトレーニング施設にある 1 台の内部サーバーに仮想環境をインストールできます。**または**

      2. 仮想環境をインストールしているクラスルーム デバイスの数が特定の認定トレーニング セッションに登録されているエンド ユーザーの数を超過しなければ、仮想環境を複製し、Microsoft Hyper-V の有効なライセンス取得済みの複製を実行しているお客様の 1 台のクラスルーム デバイスに仮想環境のインスタンスを 1 つインストールできます。

   iii. 以下の者に限り、クラスルーム デバイスを介してのみ仮想環境にアクセスして使用することを許可できます。

      1. マイクロソフト コースのハンズオン体験を行うためにのみ、お客様の認定トレーニング セッションに参加している期間中だけ、仮想環境に関連するマイクロソフト コース タイトルの有効なライセンスを購入している 1 名のエンド ユーザー。

      2. お客様の認定トレーニング セッションの準備と指導を行う MCT。

b. **お客様自身が指導している各認定トレーニング セッションの MCT** の場合、お客様には以下が許諾されます。

i. 認定トレーニング セッションの主題であるマイクロソフト コース タイトルのクラスルーム セットアップ ガイドに記載されている仮想環境コンポーネントのみをダウンロードし、Microsoft Hyper-V の有効なライセンス取得済みの複製を実行している 1 台のホスト クラスルーム デバイスにインストールして、マイクロソフト コースに関連する仮想環境を構築できます。

ii. 次のいずれかが許諾されます。

1. 認定トレーニング セッションが行われている認定ラーニング センターのトレーニング施設にある 1 台の内部サーバーに仮想環境コンポーネントをインストールできます。**または**
2. 仮想環境をインストールしているクラスルーム デバイスの数が特定の認定トレーニング セッションに登録されているエンド ユーザーの数を超過しなければ、仮想環境コンポーネントのインスタンス 1 つを複製し、Microsoft Hyper-V の有効なライセンス取得済みの複製を実行しているクラスルーム デバイスにインストールできます。

iii. 仮想環境のインスタンス 1 つを複製し、Microsoft Hyper-V の有効なライセンス取得済みの複製を実行しているお客様が所有する 1 台のパーソナル コンピューターにインストールできます。これはお客様が認定トレーニング セッションの指導準備を行う目的でのみ許諾されます。

2.3. その他の権利はないこと。スタンドアロン ベースで仮想環境にアクセスしたり仮想環境を使用したりすることはできません。仮想環境は、その仮想環境に関連するマイクロソフト コースを指導する認定トレーニング セッションと共にのみアクセスまたは使用することができます。本ライセンス条項に基づいてお客様にライセンスされる仮想環境は、実際の運用環境または本番環境で使用できません。仮想環境またはそのコンポーネントを頒布、公に展示、または実行する権利は与えられません。

2.4. 構成部分の分離。マイクロソフト コース タイトルの仮想環境には、複数のメディアまたは複数のダウンロードでお客様に提供されることがある、さまざまなソフトウェア タイトル、コンテンツ、およびその他のコンポーネントが含まれている場合があります。仮想環境は、第 2.2 条の規定のとおり、単一の使用対象製品としてお客様に提供およびライセンスされています。お客様は仮想環境コンポーネントを分離し、複数のデバイスまたはサーバーにインストールすることはできません。

2.5. ネットワーク アクセスがないこと。お客様は、マイクロソフトがマイクロソフト コースの関連するクラスルーム セットアップ ガイドに明記して明示的に許可していない限り、他のネットワークにアクセスできるクラスルーム デバイスまたはサーバーに仮想環境をインストールすることはできません。

2.6. 仮想環境におけるマイクロソフト ソフトウェアの仮想ハード ディスク イメージの複製/再頒布。お客様は以下を認め、同意するものとします。

a. 仮想環境には、マイクロソフト ソフトウェアの仮想ハード ディスク イメージが含まれます。

b. 本ライセンス条項に基づいてお客様に提供されるマイクロソフト ソフトウェアはマイクロソフトの貴重な資産であり、かかるソフトウェアを許可なく複製し、頒布すると、マイクロソフトがかかるマイクロソフト ソフトウェアのライセンス供与から通常回収する収益をマイクロソフトから奪うことになります。

c. マイクロソフトは、本ライセンス条項に記載のとおり、マイクロソフト テクノロジを利用してエンド ユーザーの技能習得を支援する目的でのみ、お客様にマイクロソフト ソフトウェアを無料で提供します。

d. お客様は、本ソフトウェアのいかなる部分も販売、レンタル、リース、貸与、移管、譲渡、またはサブライセンスできません。

e. お客様は、本ライセンスまたは本ライセンス条項をいかなる第三者にもサブライセンス、移管、または譲渡できません。

2.7. 第三者のソフトウェア。仮想環境には、第三者ではなく、本ライセンス条項に基づきマイクロソフトにより使用を許諾された第三者のコードが含まれていることがあります。第三者のコードの注意事項がある場合は、お客様への参考情報としてのみ含まれます。

2.8. オンライン サービス。マイクロソフトがマイクロソフト コースの一部としてオンライン サービス (以下「**オンライン サービス**」といいます) をお客様に提供する場合、お客様によるオンライン サービスの使用には、本条、およびお客様に別途提示されるオンライン サービス契約の本ライセンス条項と矛盾しな

い条項が適用されます。マイクロソフト コース中にオンライン サービスを使用する場合、お客様は (a) 仮想環境に関連するマイクロソフト コース タイトルのハンズオン体験を行うためにのみオンライン サービスを使用できること、(b) お客様 (またはお客様のエンド ユーザー) がオンライン サービスにアクセスするために使用する認証資格情報をどの「有効な」アカウントにも関連付けないこと、(c) お客様がオンライン サービスを使用してアップロード、処理、または保存するすべてのテキスト、音声、画像、またはファイル (以下「データ」といいます) を使用および処理するために必要なすべての権利をマイクロソフト、その関連会社、および必要なすべてのサブライセンシーに許諾すること、(d) お客様がオンライン サービスで個人情報を含むデータを入力、アップロード、処理、または保存したり、エンド ユーザーに当該行為を許可したりしないこと、(e) エンド ユーザーの個人用デバイスでオンライン サービスを使用したり、オンライン サービスに登録したりしないこと、(f) マイクロソフトがお客様への責任を負うことなく、通知なしにいつでもデータを削除できること、ならびに (g) マイクロソフトがオンライン サービスのサポート サービスを一切提供しないことに同意するものとします。

3. 追加のライセンス条件および追加の使用権。

3.1 お客様は、本ライセンス条項の契約条件と次のセキュリティ要件に準拠する場合にのみ、仮想環境を使用することができます。

a. お客様は、予定されている認定トレーニング セッションの主題であるマイクロソフト コース タイトルのクラスルーム セットアップ ガイドに仮想環境コンポーネントとして記載されているコンポーネントに限り、アクセス、インストール、および使用することができます。また、仮想環境に関連するマイクロソフト コース タイトルを指導する認定トレーニング セッションを提供または指導する目的に限り、仮想環境を使用することができます。

b. お客様は、仮想環境を構築するために、本ライセンス条項に付属するソフトウェアの仮想ハードディスク イメージのみを使用することができます。

c. お客様は、お客様が予定している認定トレーニング セッションの主題であるマイクロソフト コース タイトルのクラスルーム セットアップ ガイドに従って、仮想環境を構築およびセットアップしなければなりません。お客様は、マイクロソフトがマイクロソフト コース タイトルの関連するクラスルーム セットアップ ガイドに記載して明示的に許可していない限り、お客様または第三者のコンテンツまたはソフトウェアを仮想環境に含めたり、使用したりすることはできません。

d. お客様は、マイクロソフトがマイクロソフト コース タイトルの関連するクラスルーム セットアップ ガイドに記載して明示的に許可していない限り、他のネットワークにアクセスできるクラスルーム デバイスまたはサーバーに仮想環境をインストールすることはできません。

e. 認定トレーニング セッションの開始前に、お客様はすべてのエンド ユーザーに次の声明の印刷された複製を提供しなければなりません。

何らかの方法で仮想環境にアクセスして仮想環境を使用することで、お客様は (a) このトレーニング セッションのハンズオン体験を行う目的に限り、このクラスルーム デバイスからのみ仮想環境にアクセスして仮想環境を使用できること、(b) 仮想環境の技術的な制限を回避して使用できないこと、(c) マイクロソフトの書面による事前の許可なく、いかなる形態または手段によっても、ソフトウェアまたは仮想環境コンポーネントをダウンロード、複製、送信、または転送できないこと、(d) 仮想環境で個人情報を入力、アップロード、処理、または保存できないこと、(e) この仮想環境の使用またはアクセスを第三者に許可できないこと、および (f) 本ライセンス条項が、仮想環境コンポーネントのインストールまたは使用に際し、他のライセンス条項への「同意」が必要な場合であっても、当該コンポーネントにかかわるすべてのマイクロソフト ライセンス条項の条件に優先して適用されることを認め、同意するものとします。**仮想環境を使用することにより、お客様は以下の条項を遵守することに同意するものとします。この条項に同意されない場合、仮想環境を使用することはできません。**

この仮想環境は、現状有姿でお客様に提供されます。マイクロソフトは、明示的または暗黙的を問わず、一切の保証を負いません。

f. お客様は、上記の第 3.1 条 e 項の声明を遵守することに同意したエンド ユーザーにのみ、仮想環境へのアクセスと使用を許可することができます。

g. 各認定トレーニング セッションの開始前に、お客様は、かかる認定トレーニング セッションの主題であるマイクロソフト コース タイトルの有効なライセンス取得済みの複製を各エンド ユーザーに提供する必要があります。

h. お客様は、仮想環境へのアクセス、仮想環境の転送、複製、またはダウンロードを他者に許可することはできません。

i. お客様は、仮想環境のインストール、ライセンス認証、使用、ライセンス認証解除、およびセキュリティに関するマイクロソフトのすべての指示を厳密に遵守する必要があります。

j. お客様は、マイクロソフトがマイクロソフト コース タイトルの関連するクラスルーム セットアップ ガイドに記載して明示的に許可していない限り、仮想環境またはそのコンポーネントを改変することはできません。

k. お客様がラーニング パートナーの場合、認定トレーニング セッションの終了時にお客様の内部サーバーおよびクラスルーム デバイスすべてから仮想環境のあらゆる複製を削除しなければなりません。

l. お客様が MCT の場合、認定トレーニング セッションの終了時に (1) お客様個人のコンピューターならびに (2) お客様が仮想環境をインストールしたラーニング パートナーの内部サーバーおよびクラスルーム デバイスすべてから仮想環境のあらゆる複製を削除しなければなりません。

3.2 仮想環境にライセンス認証されていないオペレーティング システム ソフトウェアが含まれる場合、ソフトウェアを仮想環境用に構成する前に、マイクロソフトからプロダクト キーを取得し、そのソフトウェアのライセンス認証を行う必要があります。マイクロソフト プロダクト キーを入手する方法および当該プロダクト キーを使用してソフトウェアのライセンス認証を行う方法に関する具体的な手順は、マイクロソフト コース タイトルのクラスルーム セットアップ ガイドに記載されています。割り当てられたプロダクト キーの使用に関する責任は、お客様が負うものとします。お客様は、お客様のプロダクト キーを第三者と共有したり、第三者に割り当てられたプロダクト キーを使用したりすることはできません。

ライセンス認証により、ソフトウェアの使用が特定のデバイスに関連付けられます。ライセンス認証中、本ソフトウェアにより本ソフトウェアおよび当該デバイスに関する情報がマイクロソフトに送信されます。この情報には、本ソフトウェアのバージョン、言語、プロダクト キーのほか、デバイスのインターネット プロトコル (IP) アドレス、および、デバイスのハードウェア構成に関する情報が含まれます。**本ソフトウェアを使用することにより、お客様はこうした情報の送信に同意されたものとします**。正式にライセンスを取得している場合、お客様は、ライセンス認証が認められている期間中は、インストール プロセスにおいてインストールされた本ソフトウェアのバージョンを使用する権利を有します。**本ソフトウェアがライセンス認証されていない場合、お客様は、ライセンス認証が認められた期間の終了後に本ソフトウェアを使用する権利を有しません。**これは、不正使用を防止するための措置です。**ライセンス認証を無視または回避することは、禁止されています**。デバイスがインターネットに接続されている場合、本ソフトウェアはライセンス認証を行うためにマイクロソフトへ自動的に接続されます。本ソフトウェアのライセンス認証は、インターネットまたは電話により、手動で行うこともできます。その場合、インターネットおよび電話の通信料金が発生することがあります。お客様がコンピューターのハードウェア構成を変更した場合や、本ソフトウェアの設定を変更した場合には、本ソフトウェアのライセンス認証を再度行う必要が生じることがあります。**本ソフトウェアは、ライセンス認証が実行されるまで、ライセンス認証が必要なことをお知らせします。**

3.3 仮想環境にプロダクト キーなしで使用できるオペレーティング システム ソフトウェアが含まれる場合、お客様は、仮想環境に当該ソフトウェアをインストールした後にそのオペレーティング システムの状態を確認する必要があります。オペレーティング システムが「通知」モードである場合、お客様は、認定トレーニング セッションの前に当該ソフトウェアに対して rearm コマンドを実行し、オペレーティング システムの状態を変更しなければなりません。

4. **インターネット ベースのサービス**。マイクロソフトは、仮想環境のソフトウェアについてインターネット ベースのサービスを提供することがあります。マイクロソフトは、いつでもこのサービスを変更または中止できるものとします。仮想環境にソフトウェアのプレリリース版が含まれる場合、そのインターネット ベースのサービスの一部が既定で有効になっていることがあります。本ソフトウェアのこれらのバージョンにおける既定の設定は、製品版における機能の構成方法には必ずしも反映されません。ただし、インターネットを介した送信を行うように本ソフトウェアを構成する場合、次の条項が適用されます。

   a. インターネット ベースのサービスに関する同意。本ソフトウェアのなかには、インターネットを介してマイクロソフトまたはサービス プロバイダーのコンピューター システムに接続する機能が含まれていることがあります。接続が行われた際、通知が行われない場合があります。お客様は、場合によって、これらの機能を解除するか、または使用しないことができます。**これらの機能を使用することで、お客様はかかる情報の送信に同意し、かかる情報をマイクロソフトに送信するすべてのエンド ユーザーから必要なすべての同意を得ることに対して責任を負うものとします。**マイクロソフトがこれらの情報を利用してお客様を特定したり、お客様に連絡したりすることはありません。

   b. コンピューター情報。インターネット ベースのサービスとして知られる機能ではインターネット プロトコルを使用しており、お客様のインターネット プロトコル (IP) アドレス、オペレーティング システムの種類、ブラウザーの種類、使用している本ソフトウェアの名称およびバージョン、本ソフトウェアを実行するデバイスの言語コードなどのコンピューター情報を適切なシステムに送信します。マイクロソフトは、お客様にインターネット ベースのサービスを提供するためにこの情報を使用します。

   c. 情報の使用。マイクロソフトは、ソフトウェア製品やサービスの改善のために、情報および報告を利用する場合があります。また、ハードウェア ベンダーやソフトウェア ベンダーなど、他の企業と情報を共有する場合があります。これらの第三者は、マイクロソフト製ソフトウェアと連携して動作する自社製品の改良のため、この情報を使用することがあります。

   d. インターネット ベース サービスの不正使用。お客様は、これらのサービスに損害を及ぼす可能性のある方法、または第三者によるこれらのサービスの使用を妨げる可能性のある方法で、これらのサービスを使用することはできません。また、サービス、データ、アカウント、またはネットワークへの不正アクセスを試みるためにこれらのサービスを使用することは一切禁じられています。

5. **ライセンスの適用範囲**。仮想環境は使用許諾されるものであり、販売されるものではありません。本ライセンス条項は、お客様に仮想環境を使用する限定的な権利を付与します。マイクロソフトはその他の権利をすべて留保します。適用される法令によりこの制限を超える権利が与えられる場合を除き、お客様は本ライセンス条項で明示的に許可される方法でのみ仮想環境を使用できます。そのため、お客様は、使用方法を制限するために仮想環境コンポーネントに組み込まれている技術的制限に従わなければなりません。お客様は、以下を行うことも、以下を行うことを他者に許可することもできません。

   a. 認定トレーニング セッションに参加しているエンド ユーザーの数を超える仮想環境の複製を作成したり、クラスルーム デバイスにインストールしたりすること。

   b. 認定トレーニング セッションに参加しているエンド ユーザーの数を超えるクラスルーム デバイスにサーバー上の仮想環境へのアクセスを許可すること。

   c. 仮想環境にアクセスしたり、仮想環境を使用したりすることを他者に許可すること。ただし、仮想環境に関連するマイクロソフト コース タイトルを指導する認定トレーニング セッションに参加している期間中だけ、認定トレーニング セッションの主題であるマイクロソフト コース タイトルの有効なライセンスを購入しているエンド ユーザーに許可する場合を除きます。

   d. 仮想環境を送信、公開、リンク設定、投稿、公に展示、または転送すること。また、その他の許可されていない方法または違法な方法で仮想環境を使用すること。

   e. 仮想環境の複製、使用、ダウンロード、アクセス権提供、または頒布を行うこと。ただし、本ライセンス条項で明示的に許諾されている場合を除きます。

   f. 仮想環境をレンタル、販売、リース、または貸与すること。また、仮想環境をサーバー、またはさらなる複製もしくはアクセスのための場所に複製すること。ただし、本ライセンス条項で明示的に許諾されている場合を除きます。

g. (i) 商用ソフトウェア ホスティング サービス、(ii) 一般的なビジネス目的、または (iii) 本ライセンス条項に基づいてマイクロソフトがお客様に明示的に許可していない目的のために、仮想環境にアクセスしたり使用したりすること。

h. 仮想環境に基づく派生作品にコンテンツまたはソフトウェアを追加すること。また、かかる派生作品を変更、改変、改造、編集、またはその他の方法で作成すること。

i. 別のオペレーティング システム、または別のオペレーティング システムで実行されているアプリケーション内で仮想環境を使用すること。

j. 仮想環境の技術的な制限を回避する方法で使用すること。

k. 何らかの方法で仮想環境をリバース エンジニアリング、逆コンパイル、カスタマイズ、または逆アセンブルすること。

任意のデバイス上の仮想環境にアクセスする権利は、仮想環境、およびその仮想環境にアクセスするデバイスにおいてマイクロソフトの特許またはその他の知的財産権を行使する権利を、お客様に付与するものではありません。

6. **権利および所有権の留保**。マイクロソフトおよびそのサプライヤーは、仮想環境およびそのコンポーネントに関する権原、著作権、およびその他の知的財産権をすべて留保します。

7. **ソフトウェアの使用期限**。仮想環境の一部のソフトウェアは、最初の起動後、マイクロソフト コースのクラスルーム セットアップ ガイドで当該ソフトウェアについて記載されている日付に動作を停止する場合があります。その場合、それ以外の通知は表示されません。お客様は、仮想環境で rearm コマンドを使用し、動作期間を追加するようにソフトウェアをリセットできる場合があります。起動ごとに本ソフトウェアが動作する日数と rearm コマンドを実行できる回数はさまざまです。詳しくはマイクロソフト コースのクラスルーム セットアップ ガイドに記載されています。

お客様は、仮想環境のいずれかのソフトウェアが動作を停止し、rearm コマンドを利用可能な回数を使い切った場合、仮想環境へのあらゆるアクセスと使用を中止しなければなりません。ソフトウェアが実行を停止した後に仮想環境にアクセスし、使用したり、仮想環境からデータを取得したりすることはできません。

8. **期間および契約解除**。本契約は (a) クラスルーム セットアップ ガイドに記載されているソフトウェアの最も早い満了日、および rearm コマンドの利用可能な回数を使い切った日、(b) マイクロソフトが本契約を解除した日、(c) (i) お客様がラーニング パートナーの場合、Microsoft Partner Network プログラムでのお客様のラーニング コンピテンシー ステータスの満了日もしくは解除日、(ii) お客様が MCT の場合、MCT としてのステータスの解除日もしくは満了日、または (d) 仮想環境に含まれるプレリリース ソフトウェアの最も早いベータ期間の終了日のうちの最も早い日をもって自動的かつ直ちに終了します。

マイクロソフトは、お客様が本ライセンス条項のいずれかの契約条件を遵守しなかったと確信できる理由がある場合、本契約を直ちに解除できます。

何らかの理由による本契約の解除をもって、本契約に基づいてお客様に与えられるすべての権利が直ちに終了します。お客様は仮想環境へのすべてのアクセスおよび使用を直ちに中止し、お客様が所有または管理する仮想環境およびそのコンポーネントのすべての複製を永久的に削除および破棄しなければなりません。

9. **フィードバック**。お客様は、マイクロソフトに対して仮想環境に関するフィードバックを提供する場合、その方法や目的を問わず、お客様のフィードバックを使用、共有、および商品化する権利を無償でマイクロソフトに譲渡するものとします。また、お客様はフィードバックを含むマイクロソフトのソフトウェアもしくはサービスの特定部分を使用またはその特定部分と連携する第三者の製品、技術、およびサービスに必要なすべての特許権を無償でそれらの第三者に譲渡するものとします。お客様は、マイクロソフトがお客様のフィードバックをソフトウェア、製品、テクノロジ、サービス、またはドキュメントに取り込んだために、マイクロソフトが第三者からソフトウェア、製品、テクノロジ、サービス、またはドキュメントのライセンスを取得しなければならないようなフィードバックを提供しないものとします。これらの権利は本ライセンス条項の終了後も効力を維持するものとします。

10. 輸出規制。仮想環境のソフトウェアは米国および日本国の輸出に関する規制の対象となります。お客様は、本ソフトウェアに適用されるすべての国内法および国際法 (輸出対象国、エンド ユーザーおよびエンド ユーザーによる使用に関する制限を含みます) を遵守しなければなりません。詳細については www.microsoft.com/japan/exporting をご覧ください。

11. サポート サービス。仮想環境は現状有姿で提供されるため、マイクロソフトはサポート サービスを提供しない場合があります。

12. 完全合意。本ライセンス条項およびお客様が使用する追加ソフトウェア、更新プログラム、インターネット ベースのサービス、オンライン サービス (該当する場合) ならびにサポート サービスに関する条件は、仮想環境およびサポート サービスについてのお客様とマイクロソフトとの間の完全なる合意です。

13. 準拠法。

a. 米国。お客様が仮想環境コンポーネントを米国内で入手された場合、抵触法にかかわらず、本ライセンス条項の解釈および契約違反への主張は、米国ワシントン州法に準拠するものとします。消費者保護法、公正取引法、および不法行為を含みますがこれに限定されない他の主張については、お客様が所在する地域の法律に準拠します。

b. 日本および米国以外。お客様が仮想環境コンポーネントを日本国および米国以外の国で入手された場合、本ライセンス条項は適用される地域法に準拠するものとします。

14. 法的効力。本ライセンス条項は、一定の法的な権利を規定します。お客様は、地域や国によっては、本ライセンス条項の定めにかかわらず、本ライセンス条項と異なる権利を有する場合があります。本ライセンス条項は、お客様の地域または国の法律により権利の拡大が認められない限り、それらの権利を変更しないものとします。

15. あらゆる保証の免責。仮想環境、その各コンポーネント、およびオンライン サービスは、現状有姿で提供されます。仮想環境、その各コンポーネント、およびオンライン サービスの使用に伴う危険は、お客様の負担とします。マイクロソフトは、明示的な瑕疵担保責任または保証責任を一切負いません。本ライセンス条項では変更できないお客様の地域の法律による追加の消費者の権利が存在する場合があります。お客様の地域の国内法等によって認められる限り、マイクロソフトは、商品性、特定目的に対する適合性、および侵害の不存在に関する瑕疵担保責任または黙示の保証責任を負いません。

オーストラリア限定。お客様は、オーストラリア消費者法に基づく法定保証を有し、これらの条項は、それらの権利に影響を与えることを意図するものではありません。

16. 救済手段および責任の制限および除外。マイクロソフトおよびそのサプライヤーの責任は、お客様が仮想環境に実際に支払った金額と 5.00 米ドルのいずれか高い額を上限とする直接損害に限定されます。その他の損害 (結果的損害、逸失利益、特別損害、間接損害、および付随的損害を含みますがこれらに限定されません) に関しては、一切責任を負いません。

この制限は、以下に適用されるものとします。

a. 仮想環境、そのコンポーネント、オンライン サービスおよび第三者のインターネット サイト上のコンテンツ (コードを含みます)、または第三者のプログラムに関連した事項

b. 契約違反、保証違反、厳格責任、過失、または不法行為等の請求 (適用される法令により認められている範囲において)

この制限は、マイクロソフトが損害の可能性を認識していたか、または認識し得た場合にも適用されます。また、一部の国では付随的損害および結果的損害の免責、または責任の制限が認められないため、上記の制限事項が適用されない場合があります。

第 1 章

ドメイン コントローラーのインストールと構成

目次

レッスン 1
AD DS の概要

目次

質問と解答

質問 : OU の 2 つの主な目的は何ですか。

解答 : OU の 2 つの主な目的は、管理の委任にフレームワークを提供することと、適切な GPO の適用範囲を制御するための構造を提供することです。

質問 : AD DS フォレストに追加のツリーを展開する必要がある理由は何ですか。

解答 : 2 つ以上の ドメイン ネーム システム (DNS) の名前空間が必要な場合は、AD DS フォレストに追加のツリーを展開することができます。

参考資料

AD DS の概要

参考資料 : ドメインおよびフォレストについては、次のサイトを参照してください。
Active Directory ドメイン サービスの概要
https://technet.microsoft.com/ja-jp/library/hh831484.aspx

Windows Server 2016 の AD DS の新機能

参考資料 : PAM については、次のサイトを参照してください。
Active Directory Domain Services の Privileged Access Managemen
thttp://aka.ms/Ibsyai

参考資料 : Azure AD 参加については、次のサイトを参照してください。
エンタープライズ向け Windows 10: デバイスを仕事に使用する方法
https://docs.microsoft.com/ja-jp/azure/active-directory/active-directory-azureadjoin-windows10-devices-overview

参考資料 : Windows Server 2016 の AD DS で Microsoft Passport を使用する方法については、次のサイトを参照してください。
Microsoft Passport 経由でのパスワードを使用しない ID の認証
https://docs.microsoft.com/ja-jp/azure/active-directory/active-directory-azureadjoin-passport

参考資料 : Windows Server 2016 の新しい AD DS 機能については、次のサイトを参照してください。
Active Directory ドメイン サービスの新機能 - Technical Preview
http://aka.ms/Nzrl6u

デモンストレーション : Active Directory 管理センターによる AD DS の管理

デモンストレーションの手順

Active Directory 管理センター内で移動する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。

2. [Adatum (ローカル)] をクリックします。
3. [ダイナミック アクセス制御] をクリックします。
4. [グローバル検索] をクリックします。
5. ナビゲーション ウィンドウで、ツリー ビューに切り替え、[Adatum (ローカル)] ノードを展開して、Adatum.com ドメインの詳細を表示します。

Active Directory 管理センターで管理タスクを実行する

1. Active Directory 管理センターで、[概要] をクリックします。
2. [パスワードのリセット] セクションで、[ユーザー名] ボックスに「Adatum¥Adam」と入力します。
3. [パスワード] ボックスと [パスワードの確認入力] ボックスに「Pa55w.rd」と入力します。
4. [ユーザーは次回ログオン時にパスワード変更が必要] チェック ボックスをオフにし、[適用] をクリックします。
5. [グローバル検索] セクションで、[検索] ボックスに「lon」と入力し、Enter キーを押します。

オブジェクトを作成する

1. Active Directory 管理センターのナビゲーション ウィンドウのツリー ビューで、[Adatum (ローカル)] を展開し、[Computers] コンテナーをクリックします。
2. タスク ウィンドウの [Computers] セクションで、[新規] をクリックし、[コンピューター] を選択します。
3. [コンピューターの作成] ダイアログ ボックスに、次に示す情報を入力し、[OK] をクリックします。
   - コンピューター名 : LON-CL4
   - コンピューター (NetBIOS) 名 : LON-CL4
4. [OK] をクリックします。

オブジェクトのすべての属性を表示する

1. Active Directory 管理センターで、[Adatum (ローカル)] をクリックし、管理の一覧で [Computers] をダブルクリックします。
2. [LON-CL4] を選択し、タスク ウィンドウの [LON-CL4] セクションで、[プロパティ] をクリックします。
3. LON-CL4 のプロパティ ウィンドウで、[拡張] セクションまで下方にスクロールし、[属性エディター] タブをクリックして、コンピューター オブジェクトのすべての属性が使用できることを確認します。
4. [キャンセル] をクリックし、LON-CL4 のプロパティ ウィンドウを閉じます。

Active Directory 管理センターで Windows PowerShell 履歴ビューアーを使用する

1. Active Directory 管理センターで、画面下の [Windows PowerShell 履歴] ツール バーをクリックします。
2. 最近のタスクの実行に使用された New-ADComputer コマンドレットの詳細が表示されます。
3. LON-DC1 で、開いているウィンドウをすべて閉じます。

レッスン 2
AD DS ドメイン コントローラーの概要

目次

質問と解答

質問 : ドメイン コントローラーをグローバル カタログにする必要がありますか。

解答 : グローバル カタログの配置は、ユーザーがサインインするのにかかる時間に影響するため、慎重に計画する必要があります。単一ドメイン環境では、すべてのドメイン コントローラーは、ドメインの完全なコピーを保持しているため、グローバル カタログをホストする必要があります。複数ドメインのシナリオでは、グローバル カタログの配置を計画する際、ユーザーのサインイン時間、プログラムの依存関係、グローバル カタログの高可用性の必要性、およびレプリケーション トラフィックを考慮する必要があります。

質問 : 複数のドメインがあるフォレストでは、グローバル カタログのコピーをすべてのドメイン コントローラーに格納する必要がある。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

単一ドメイン環境では、グローバル カタログのコピーを保持するようにすべてのドメイン コントローラーを構成する必要がありますが、複数ドメイン環境では、ドメイン内のすべてのドメイン コントローラーがグローバル カタログ サーバーでもある場合を除いて、インフラストラクチャ マスターをグローバル カタログ サーバーとして構成しないようにします。

参考資料

役割の転送と強制移動

参考資料 :

- Windows PowerShell を使用して FSMO の役割を転送または強制移動する方法については、次のサイトを参照してください。
  Move (Transfering or Seizing) FSMO Roles with AD-Powershell Command to Another Domain Controller
  http://aka.ms/Rn7kfi
- ntdsutil.exe を使用して FSMO の役割を転送または強制移動する方法の詳細については、次のサイトを参照してください。
  Ntdsutil.exe を使用してドメイン コントローラーに FSMO の役割を強制または転送する
  https://support.microsoft.com/ja-jp/kb/255504

デモンストレーション : DNS 内の SRV レコードの表示

デモンストレーションの手順

DNS マネージャーを使用して SRV レコードを表示する

1. LON-DC1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. サーバー マネージャーで、[ツール] メニューをクリックします。
3. [ツール] リストで、[DNS] をクリックします。
4. DNS マネージャー ウィンドウの [ツリー] メニューで、[LON-DC1]、[前方参照ゾーン] の順に展開し、[Adatum.com] をクリックします。次の 4 つの DNS サブゾーンが表示されます。
   - _msdcs
   - _sites
   - _tcp
   - _udp
5. [Adatum.com]、[_sites]、[Default-First-Site-Name]、[_tcp] の順に展開し、次のレコードを選択します。
   - _ldap Service Location (SRV) [0][100][389] lon-dc1.adatum.com
6. 受講者に十分な専門知識と興味がある場合は、c:¥windows¥system32¥config を開き、メモ帳で netlogon.dns ファイルを開きます。このドメイン コントローラーによって DNS に登録されたすべてのサービス レコード (SRV レコード) を表示します。

レッスン 3
ドメイン コントローラーの展開

目次

質問と解答

質問 : 仮想化環境でドメイン コントローラーを最も短時間でレプリケートできるのは、どのような方法ですか。

解答 : ドメイン コントローラーを複製する方法が、最も短時間でレプリケートできます。

フィードバック : 特にコンピューターが Hyper-V などの仮想化環境で稼働する場合、同一に構成された複数のコンピューターを最も迅速に展開する方法は、これらのコンピューターを複製することです。複製すると、コンピューターの仮想ハード ディスクはコピーされ、コンピューター名や IP アドレスなどの一部の構成は一意に変更されます。この後、コンピューターはすぐに動作できます。

質問 : ドメイン コントローラーを Azure に展開する際の 2 つの主な考慮事項は何ですか。

解答 : ロールバックと仮想マシンの制限です。

フィードバック :

- **ロールバック :** AD DS システムがロールバックされると、重複した更新シーケンス番号 (USN) が作成される可能性があります。また、ドメイン コントローラーのレプリケーションは、USN に依存するため、重複した番号は問題を引き起こす可能性があります。これを防ぐために、Windows Server 2016 の Active Directory では、VM-Generation ID という識別子が導入されています。VM-Generation ID はロールバックを検出し、仮想 AD DS がドメイン内の他のドメイン コントローラーと収束するまで、仮想ドメイン コントローラーの変更を外部に複製することを防ぎます。
- **仮想マシンの制限 :** Azure 仮想マシンは、14 GB のランダム アクセス メモリ (RAM) と 1 つのネットワーク アダプターに制限されており、チェックポイントもサポートされていません。

参考資料

Windows Server 2016 の Server Core インストールへのドメイン コントローラーのインストール

参考資料 :

- Windows PowerShell の Install-ADDSDomainController コマンドレットを使用する方法については、次のサイトを参照してください。
  Active Directory ドメイン サービスをインストールする (レベル 100)
  http://aka.ms/A9jlvk
- 詳細については、次のサイトを参照してください。
  AD DS Deployment Cmdlets in Windows PowerShell
  http://aka.ms/Lnxifx

メディアからのインストールによるドメイン コントローラーのインストール

参考資料 : AD DS のインストールに必要な手順については、次のサイトを参照してください。
Active Directory ドメイン サービスをインストールする (レベル 100)
http://aka.ms/Rvcwlz

ドメイン コントローラーを仮想化するためのベスト プラクティス

参考資料 : ドメイン コントローラーの仮想化については、次のサイトを参照してください。
Running Domain Controllers in Hyper-V
http://aka.ms/Tjjl9g

デモンストレーション : ドメイン コントローラーの複製

デモンストレーションの手順

複製されるドメイン コントローラーを準備する

1. LON-DC2 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. Active Directory 管理センターで、[Adatum (ローカル)] をダブルクリックし、管理の一覧で、[Domain Controllers] OU をダブルクリックします。
3. 管理の一覧で、まだ選択していない場合は [LON-DC2] を選択し、タスク ウィンドウの [LON-DC2] セクションで、[グループに追加] をクリックします。
4. [グループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください] ボックスに「Cloneable」と入力し、[名前の確認] をクリックします。
5. グループ名が [Cloneable Domain Controllers] に展開されていることを確認し、[OK] をクリックします。
6. スタート メニューで、[Windows PowerShell] をクリックします。
7. 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。

```
Get-ADDCCloningExcludedApplicationList
```

8. 重要なアプリの一覧を確認します (運用環境では、アプリごとに確認するか、既定でインストールされているアプリ数の少ないドメイン コントローラーを使用する必要があります)。次のコマンドレットを入力し、Enter キーを押します。

```
Get-ADDCCloningExcludedApplicationList -GenerateXML
```

9. DCCloneConfig.xml ファイルを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
New-ADDCCloneConfigFile
```

10. LON-DC2 をシャットダウンするために、次のコマンドレットを入力し、Enter キーを押します。

```
Stop-Computer
```

11. 仮想マシンがシャットダウンされるのを待っている間、シャットダウンの確認を求められます。

ソース仮想マシンをエクスポートする

1. ホスト コンピューターの Hyper-V マネージャーの詳細ウィンドウで、[23742A-LON-DC2] 仮想マシンを選択します。
2. 操作ウィンドウの [23742A-LON-DC2] セクションで、[エクスポート] をクリックします。

3. [仮想マシンのエクスポート] ダイアログ ボックスで、場所に「C:¥Program Files¥Microsoft Learning ¥23742」と入力し、[エクスポート] をクリックします。エクスポートが完了するまで待ちます。
4. 操作ウィンドウの [23742A-LON-DC2] セクションで、[スタート] をクリックします。

複製ドメイン コントローラーを作成して、起動する

1. ホスト コンピューターの Hyper-V マネージャーの操作ウィンドウで、ホスト コンピューターの名前が付いたセクションにある [仮想マシンのインポート] をクリックします。
2. 仮想マシンのインポート ウィザードの [開始する前に] ページで、[次へ] をクリックします。
3. [フォルダーの検索] ページで [参照] をクリックし、C:¥Program Files¥Microsoft Learning¥23742 ¥23742A-LON-DC2 フォルダーを参照して、[フォルダーの選択]、[次へ] の順にクリックします。
4. [仮想マシンの選択] ページで、まだ選択していない場合は [23742A-LON-DC2] を選択し、[次へ] をクリックします。
5. [インポートの種類の選択] ページで、[仮想マシンをコピーする (新しい一意な ID を作成する)] を選択し、[次へ] をクリックします。
6. [仮想マシン ファイルのフォルダーを選択します] ページで、[仮想マシンを別の場所に格納する] チェック ボックスをオンにします。各フォルダーの場所で、C:¥Program Files¥Microsoft Learning ¥23742¥ をパスとして指定し、[次へ] をクリックします。
7. [仮想ハード ディスクを保存するフォルダーを選択します] ページで、C:¥Program Files¥Microsoft Learning¥23742¥ をパスとして指定し、[次へ] をクリックします。
8. [インポート ウィザードの完了] ページで、[完了] をクリックします。
9. 管理の一覧で、23742A-LON-DC2 という名前の仮想マシンが新しくインポートされたことを確認して選択します。この仮想マシンの [状態] は [オフ] になっています。操作ウィンドウの下のセクションで、[名前の変更] をクリックします。
10. 「23742A-LON-DC3」という名前を入力し、Enter キーを押します。
11. 操作ウィンドウの [23742A-LON-DC3] セクションで、[起動]、[接続] の順にクリックし、仮想マシンが起動することを確認します。
12. サーバーの起動中に、[ドメイン コントローラーの複製が x% 完了しました] というメッセージが表示される場合があります。

復習とまとめ

復習問題

質問 : WAN 接続が限られているリモートの場所に追加のドメイン コントローラーをインストールする必要がある場合、どの展開方法を使用しますか。

解答 : [メディアからのインストール] を使用します。この方法により、WAN リンク上に AD DS データベース全体をコピーする必要がなくなります。

質問 : Windows Server 2016 の Server Core インストールをドメイン コントローラーに昇格する必要がある場合、使用するツールは何ですか。

解答 : Windows Server 2016 の Server Core インストールをドメイン コントローラーに昇格するには、次のツールを使用できます。

- AD DS をリモートでインストールできるサーバー マネージャー
- Windows PowerShell
- Server Core 上で dcpromo /unattend コマンド を使用

質問 : クラウドでドメイン コントローラーを実行する場合、どちらのサービスの使用を検討する必要がありますか。Azure AD ですか。IaaS (サービスとしてのインフラストラクチャ) Azure 仮想マシンですか。

解答 : 解答はさまざまです。受講者のニーズに依存します。Azure AD は、Web ベースのアプリケーションの ID 管理とアクセス管理を提供するよう設計されています。IaaS Azure 仮想マシンを使用することで、完全な機能を備えた AD DS ドメイン コントローラーを展開することができます。

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
構文エラー	構文エラーは、Windows PowerShell コマンドレット入力時に、タイプミスをした場合やパラメーターを忘れてしまった場合に起きます。コマンドが失敗した理由を特定するためにコンソール出力を調べます。
前提条件の問題	多くの致命的なエラーは、前提条件チェッカーが検出したエラーに直接関連するため、結果を慎重に検討し、提供されたガイダンスに従います。
ネットワークとフォレストの構成の問題	ネットワーク構成の問題やその他 AD DS フォレスト構成の問題により、新しいドメイン コントローラーの昇格が妨げられる場合があります。dcpromoui.log ファイルと dcpromo.log ファイルを使用して、特定のプロモーション エラーまたは構成の問題を示すエラーのイベント ログを表示します。また、dcdiag.exe と repadmin.exe を使用すると、全体のフォレストの状態を確認することもできます。

第 2 章

AD DS でのオブジェクトの管理

目次

レッスン 1
ユーザー アカウントの管理

目次

質問と解答

質問 : 移動プロファイルの目的はなんですか。

解答 : ユーザー プロファイルをネットワーク共有に格納し、同期します。これにより、ユーザーはコンピューター間を移動した場合も、新しいコンピューターにサインインする際に同じプロファイルを受け取ることができます。

質問 : アカウントを無効にすることと、アカウントがロック アウトされていることの違いは何ですか。

解答 : アカウントの無効化は、アカウントが使用されるのを防ぐために、管理者が意図的におこなう操作です。アカウントのロックアウトは、何度もサインインを失敗した結果としてのみ発生する可能性があります (パスワード ポリシーによる強制が構成されていることを前提とします)。

デモンストレーション : ユーザー アカウントの管理

デモンストレーションの手順

新しいユーザー アカウントを作成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. Active Directory 管理センターで、[Adatum (ローカル)] をクリックし、[Managers] OU をダブルクリックします。
3. タスク ウィンドウで、[新規] をクリックし、[ユーザー] をクリックします。
4. [ユーザーの作成] ダイアログ ボックスで、[姓] フィールドに「Sales」と入力します。
5. [名] フィールドに「Manager」と入力します。
6. [ユーザー UPN ログオン] ボックスに「SalesManager」と入力します。
7. [パスワード] の [パスワードの確認入力] フィールドに「Pa55w.rd」と入力し、[OK] をクリックします。

ユーザー アカウントを削除する

1. [Art Odum] アカウントをクリックします。
2. タスク ウィンドウで [削除] をクリックします。
3. [削除の確認] ボックスで、[はい] をクリックします。

ユーザー アカウントを移動する

1. [Burton Bartels] アカウントを右クリックします。
2. メニューから [移動] をクリックします。
3. [Development] OU をクリックし、[OK] をクリックします。
4. 左側のウィンドウで、[Adatum (ローカル)] をクリックします。
5. 右側のウィンドウで、[Development] OU をダブルクリックし、Burton Bartels のアカウントが存在することを確認します。

ユーザー属性を構成する

1. [Burton Bartels] アカウントをダブルクリックします。
2. 左側のウィンドウで、[組織] をクリックし、[部署] フィールドを [Managers] から「Development」に変更します。
3. 左側のウィンドウで、[所属するグループ] をクリックします。

4. [所属するグループ] セクションで、[Managers]、[削除] の順にクリックします。
5. [追加] をクリックします。[グループの選択] ダイアログ ボックスで、選択するオブジェクト名を入力してください (例) ウィンドウに「Development」と入力し、[OK] をクリックします。
6. [OK] をクリックし、Burton Bartels のプロパティを閉じます。
7. Active Directory 管理センターを閉じます。次のデモンストレーションのために、サーバー マネージャーを開いたままにします。

デモンストレーション : テンプレートによるアカウントの管理

デモンストレーションの手順

ユーザー テンプレートを作成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory ユーザーとコンピューター] の順にクリックします。
2. [Adatum.com] を展開し、[Sales] OU をクリックします。
3. ツール バーの新しいユーザー アイコンをクリックします。
4. [新しいオブジェクト - ユーザー] ダイアログ ボックスに、次の情報を入力し、[次へ] をクリックします。
   - 姓 : _template
   - 名 : sales
   - ユーザー ログオン名 : salestemplate
5. [パスワード] フィールドと [パスワードの確認入力] フィールドに「Pa55w.rd」と入力します。
6. [ユーザーは次回のログオン時にパスワード変更が必要] チェック ボックスをオフにし、[パスワードを無期限にする]、[アカウントは無効] をオンにして、[次へ] をクリックします。
7. [完了] をクリックします。

テンプレートのプロパティを構成する

1. [_template sales] アカウントをダブルクリックします。
2. [_template sales のプロパティ] 画面で、[所属するグループ] タブをクリックし、[追加] をクリックします。
3. [グループの選択] ダイアログ ボックスに「Sales」と入力し、[OK] をクリックします。
4. [組織] タブをクリックします。[部署] フィールドに「Sales」と入力します。
5. [上司] セクションで、[変更] をクリックします。[ユーザーまたは連絡先の選択] ダイアログ ボックスで「Erin」と入力し、[名前の確認] をクリックします。[OK] をクリックします。
6. [プロファイル] タブをクリックします。[ユーザー プロファイル] の [ログオン スクリプト] フィールドに「¥¥lon-dc1¥netlogon¥logon.bat」と入力し、[OK] をクリックします。

テンプレートをコピーして新しいユーザーを作成する

1. [_template sales] アカウントを右クリックし、[コピー] をクリックします。
2. [オブジェクトのコピー - ユーザー] ダイアログ ボックスの [名] フィールドに「User」と入力します。[姓] フィールドに「Sales」と入力します。
3. [ユーザー ログオン名] フィールドに「SalesUser」と入力し、[次へ] をクリックします。

4. [パスワード] フィールドと [パスワードの確認入力] フィールドに「Pa55w.rd」と入力します。
5. [パスワードを無期限にする] と [アカウントは無効] チェック ボックスをオフにし、[ユーザーは次回のログオン時にパスワード変更が必要] チェック ボックスをオンにして、[次へ] をクリックします。
6. [完了] をクリックします。
7. [Sales User] アカウントをダブルクリックし、[所属するグループ] タブをクリックします。そのユーザーが Sales グループのメンバーであることを確認します。
8. [組織] タブをクリックします。[部署] が Sales で、[上司] が Erin Bull であることを確認します。
9. [プロファイル] タブをクリックします。ログオン スクリプトのパスが ¥¥lon-dc1¥netlogon¥logon.bat であることを確認します。[OK] をクリックし、ダイアログ ボックスを閉じます。
10. Active Directory ユーザーとコンピューターを閉じます。

レッスン 2
AD DS でのグループの管理

目次

デモンストレーション : Windows Server でのグループの管理

デモンストレーションの手順

新しいグループを作成し、メンバーを追加する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. [Adatum (ローカル)] を展開し、[IT] をダブルクリックします。
3. タスク リストで、[IT] の [新規] をポイントし、[グループ] をクリックします。
4. [グループの作成] ダイアログ ボックスで、[グループ名] ボックスに「IT Managers」と入力します。既定でグローバル セキュリティ グループとなることを確認します。
5. 左側のウィンドウで、[メンバー] をクリックし、[追加] をクリックします。
6. [ユーザー、連絡先、コンピューター、サービス アカウントまたはグループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] ボックスに「Beth; Logan」と入力し、[名前の確認] をクリックして、[OK] をクリックします。
7. [OK] をクリックし、[グループの作成 : IT Managers] ダイアログ ボックスを閉じます。

ユーザーをグループに追加する

1. [Maj Hojski] というユーザーを右クリックし、[グループに追加] をクリックします。
2. [グループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] に「IT Managers」と入力します。
3. [名前の確認] をクリックし、[OK] をクリックします。

グループの種類とスコープを変更する

1. [IT Managers] グループをダブルクリックします。
2. IT Managers ウィンドウで、[グループの種類] の [配布] をクリックします。強調表示されたメッセージを読みます。[グループのスコープ] の [ユニバーサル] をクリックし、[OK] をクリックします。

グループの管理者を構成する

1. [IT Managers] グループをダブルクリックします。
2. [管理者] セクションで、[編集] をクリックします。
3. [ユーザー、連絡先、またはグループを選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] に「Parsa」と入力し、[名前の確認] をクリックして、[OK] をクリックします。
4. [管理者がメンバーシップ一覧を変更できる] チェック ボックスをオンにします。
5. [OK] をクリックし、IT Managers のプロパティ ウィンドウを閉じます。
6. Active Directory 管理センターを閉じます。

レッスン 3
AD DS でのコンピューター オブジェクトの管理

目次

質問と解答

質問 : コンピューターがドメインとの間で信頼関係を失うのはどのような理由からですか。

解答 : 通常、ローカル コンピューターで入力されたパスワードと Active Directory で格納しているパスワードの不一致の結果です。

レッスン 4
AD DS 管理のための Windows PowerShell の使用

目次

質問と解答

質問 : Windows PowerShell Integrated Scripting Environment とは何ですか。

解答 : Windows PowerShell Integrated Scripting Environment により、Windows PowerShell スクリプトを作成し、実行し、テストするための環境が提供されます。標準の Windows PowerShell ウィンドウでは使用できない構文の色付け、タブ補完、視覚的なデバッグ機能、および状況依存のヘルプが使用できます。

参考資料

Windows PowerShell によるオブジェクトのクエリ

参考資料 : 詳細については、次のサイトを参照してください。
about_ActiveDirectory_Filte
http://aka.ms/Kv5dy3

参考資料 : 詳細については、次のサイトを参照してください。
UserAccountControl フラグを使用して、ユーザー アカウントのプロパティを操作する方法
https://support.microsoft.com/ja-jp/kb/305144

Windows PowerShell によるオブジェクトの変更

参考資料 : 詳細については、次のサイトを参照してください。
Set-ADUser
http://aka.ms/K34c8d

デモンストレーション : グラフィカル ツールによる一括操作の実行

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory ユーザーとコンピューター] の順にクリックします。
2. [Adatum.com] を展開し、[Research] OU をクリックします。
3. 詳細ウィンドウで、[種類] をクリックし、オブジェクトを種類で並べ替えます。
4. リストの先頭のユーザー オブジェクトの [Arturs Priede] をクリックします。
5. Shift キーを押したまま、リストを下までスクロールし、最後のユーザー オブジェクト [Vera Pace] をクリックします。
6. 選択されたオブジェクトのブロックを右クリックして、[プロパティ] をクリックします。
7. [複数の項目のプロパティ] ダイアログ ボックスで、[事業所] の横のチェック ボックスをオンにし、フィールドに「Winnipeg」と入力して、[OK] をクリックします。
8. 任意のユーザー オブジェクトをダブルクリックし、[事業所] フィールドが [Winnipeg] に設定されていることを確認します。
9. [キャンセル] をクリックし、Active Directory ユーザーとコンピューターを閉じます。

デモンストレーション : Windows PowerShell による一括操作の実行

デモンストレーションの手順

IT 部門に新しいグローバル グループを作成する

1. LON-DC1 で、[スタート] をクリックし、[Windows PowerShell] をクリックします。
2. 管理者 : 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。

```
New-ADGroup -Name Helpdesk -Path "ou=IT,dc=Adatum,dc=com" -GroupScope Global
```

IT 部門のすべてのユーザーを Helpdesk グループに追加する

1. 管理者 : 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。

```
Get-ADUser -Filter "Department -eq 'IT'" | Foreach {Add-ADGroupMember "Helpdesk" -members $_}
```

Research 部門のすべてのユーザーの住所を設定する

1. 管理者 : 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。

```
Get-ADuser -Filter {Department -eq "Research"} | Set-ADuser -StreetAddress "1530 Taylor Ave." -City "Winnipeg" -State
"Manitoba" -Country "CA"
```

注 : このコマンドレットでは、フィルター処理で引用符の代わりに角かっこが使用されており、foreach ループの代わりに Set-ADUser コマンドレットが使用されていることに注意してください。

新しい OU を作成する

1. 管理者 : 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。

```
New-ADOrganizationalUnit London -Path "dc=Adatum,dc=com"
```

スクリプトを実行して、.csv ファイルから新しいユーザーを作成する

1. エクスプローラーを開き、アドレス バーに「E:¥Labfiles¥Mod02」と入力して、Enter キーを押します。
2. [DemoUsers.csv] を右クリックし、[プログラムから開く] をクリックして、[メモ帳] をクリックします。ファイルの構造を説明します。
3. メモ帳を閉じます。
4. Windows PowerShell ウィンドウに切り替え、「cd E:¥Labfiles¥Mod02」と入力します。
5. 「.¥DemoUsers.ps1」と入力し、Enter キーを押して、スクリプトを実行します。

ユーザー アカウントが作成され、変更されていることを確認する

1. サーバー マネージャーで、[ツール]、[Active Directory ユーザーとコンピューター] の順にクリックします。
2. London OU が存在することを確認します。
3. [London] OU をクリックします。.csv ファイルで定義されたとおり、3 人のユーザーが存在することを確認します。ユーザーのアカウントが無効なことを確認します。これは、パスワードが設定されていないためです。
4. [IT] OU をクリックします。Helpdesk グループが存在することを確認します。

5. [Helpdesk] グループをダブルクリックし、[Helpdesk のプロパティ] で [メンバー] タブをクリックします。メンバーに IT 部門のユーザーが設定されていることを確認し、[キャンセル] をクリックします。
6. [Research] OU をクリックし、そのユーザー アカウントの 1 つをダブルクリックします。
7. そのユーザーのプロパティのページで、[住所] タブをクリックします。住所のフィールドが想定したとおりに設定されていることを確認し、[キャンセル] をクリックします。

レッスン 5
OU の実装と管理

目次

質問と解答

質問 : オブジェクト制御の委任ウィザードを使用するメリットは何ですか。

解答 : オブジェクト制御の委任ウィザードにより、選択したタスクに基づいてアクセス許可を割り当てることで、管理の委任を簡略化することができます。

デモンストレーション : OU に関する管理アクセス許可の委任

デモンストレーションの手順

新しい OU を作成する

1. LON-DC1 の Active Directory ユーザーとコンピューターで、[Adatum.com] をクリックします。
2. ツール バーの新しい組織単位 (OU) アイコンをクリックします。
3. [新しいオブジェクト - 組織単位 (OU)] ダイアログ ボックスで、[名前] フィールドに「Human Resources」と入力し、[OK] をクリックします。

オブジェクト制御の委任ウィザードを使用してタスクを割り当てる

1. [Adatum.com] ドメイン オブジェクトを右クリックし、[制御の委任] をクリックします。
2. オブジェクト制御の委任ウィザードで、[次へ] をクリックします。
3. [ユーザーまたはグループ] ページで、[追加] をクリックします。
4. [ユーザー、コンピューターまたはグループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] に「Helpdesk」と入力し、[名前の確認]、[OK]、[次へ] の順にクリックします。
5. [委任するタスク] ページで、[ユーザーのパスワードをリセットして次回ログオン時にパスワードの変更を要求する] と [コンピューターのドメインへの参加] チェック ボックスをオンにし、[次へ] をクリックします。
6. [完了] をクリックします。

Research OU のユーザーの住所と役職を変更する権限を Research グループに割り当てる

1. Active Directory ユーザーとコンピューターで、[表示]、[拡張機能] の順にクリックします。
2. [Research] OU を右クリックし、[プロパティ] をクリックします。
3. [セキュリティ] タブをクリックし、[詳細設定]、[追加] の順にクリックします。
4. Research のアクセス許可エントリ ウィンドウで、[プリンシパルの選択] をクリックします。
5. [ユーザー、コンピューター、サービス アカウントまたはグループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] に「Research」と入力します。[名前の確認] をクリックし、[OK] をクリックします。
6. [適用先] ドロップダウン リストで、[子ユーザー オブジェクト] を選択します (リストの下の方にあります)。
7. [プロパティ] セクションで、下にスクロールして、[自宅住所の書き込み] チェック ボックスをオンにします。
8. さらに下にスクロールし、[役職の書き込み] チェック ボックスをオンにして、[OK] をクリックします。
9. [OK] をクリックし、[Research のプロパティ] ダイアログ ボックスを閉じます。

演習の復習の質問と解答

演習 A : AD DS オブジェクトの管理

質問と解答

質問 : どのオブジェクトの種類をグローバル グループのメンバーにすることができますか。

解答 : 同じドメインのユーザーと他のグローバル グループ を、メンバーにすることができます。

質問 : 任意のコンピューターをドメインに参加させるためには、どのような資格情報が必要ですか。

解答 : コンピューターをドメインに参加させるアクセス許可を持つユーザーの資格情報を入力する必要があります。通常、ドメイン管理者の資格情報です。

演習 B : AD DS の管理

質問と解答

質問 : なぜ、このスクリプトで作成されたユーザーが有効になっているでしょうか。

解答 : スクリプトでユーザーを作成する際に、ユーザーのパスワードを割り当てているためです。

質問 : New-ADUser コマンドレットによって作成されたアカウントはどのような状態ですか。

解答 : これらのアカウントの作成時にパスワードが割り当てられていない場合、既定でアカウントは無効になります。

復習とまとめ

ベスト プラクティス

AD DS 管理のベスト プラクティスを次に示します。

- グループ メンバーシップによって付与されるアクセス許可をすべて理解していない場合は、組み込みグループを使用して管理アクセスを委任することは避けてください。
- 特別な管理グループを作成し、それらのグループに、割り当てられたタスクを完了するために必要な権限とアクセス許可のみを割り当てます。
- Windows PowerShell スクリプトを開発し、タスクを繰り返し実行します。
- 日常的なアクティビティに管理者アカウントを使ってサインインしないでください。管理者アカウントは、管理タスクを実行する必要がある場合にのみ使用します。

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
ユーザーは、ネットワーク リソースに全くアクセスできない。	グループ メンバーシップを確認します。競合の原因となっている入れ子のグループを探します。
AD DS の管理権限をユーザーに割り当てたが、タスクを実行するツールがないと言われた。	Windows 10 用のリモート サーバー管理ツールをダウンロードして、ユーザーのコンピューターにインストールし、ユーザーが必要とする管理ツールを提供する必要があります。

実際の問題とシナリオ

多くの組織では、ユーザー アカウントを、役割を果たすユーザーに基づいて作成するのではなく、ユーザーの担当業務に基づいて作成します。例えば、組織に受付担当者が常駐している場合、継続性を実現するために、その役割を果たすユーザーは、「受付」という汎用アカウントを使用します。そうすれば、新しいユーザーがその役職に就く際、「受付」のユーザーのパスワードを変更するだけでよく、アプリケーション、設定、ドキュメント、電子メールなどの整合性を維持することがきます。

ツール

次の表に、この章で参照しているツールを一覧表示します。

ツール	用途	アクセス方法
Windows PowerShell	すべての管理タスクのコマンド ラインとスクリプト	スタート メニューで「PowerShell」と入力して検索する
Active Directory 管理センター	AD DS で日常の管理タスクを実行する	サーバー マネージャーの [ツール] メニュー、または [コントロール パネル] の [管理ツール]
Active Directory ユーザーとコンピューター	AD DS で日常の管理タスクを実行する	サーバー マネージャーの [ツール] メニュー、または [コントロール パネル] の [管理ツール]
オブジェクト制御の委任ウィザード	管理タスクを実行するためのアクセス許可を割り当てる	Active Directory ユーザーとコンピューターで OU を右クリックする

第 3 章

高度な AD DS インフラストラクチャの管理

目次

レッスン 1
高度な AD DS 展開の概要

目次

質問と解答

質問 : 複数フォレストの AD DS 展開を実装するのに必要なのは、次のどの要件ですか。

( ) セキュリティ分離の要件

( ) スキーマ要件

( ) DNS 名前空間の要件

( ) 企業の合併

( ) 分散管理の要件

解答 :

(√) セキュリティ分離の要件

(√) スキーマ要件

( ) DNS 名前空間の要件

( ) 企業の合併

( ) 分散管理の要件

フィードバック :

セキュリティ分離の要件とスキーマ要件は、複数のフォレストを実装する必要があるオプションでのみ提示された要件です。DNS 名前空間の要件と分散管理の要件には複数のドメインが必要ですが、単一のフォレストが複数の名前空間を持つことができ、さらに管理の自律性に複数のフォレストは必ずしも必要ではありません。企業の合併のシナリオにおいて、組織間のコラボレーションの必要性がほとんどない場合は、フォレストを個別に管理し続ける場合もありますが、個別のフォレストは必須ではありません。

質問 : Azure 上の仮想マシンにレプリカ ドメイン コントローラーを展開する前に、次のタスクのどれを実行する必要がありますか。

( ) オンプレミス ネットワークから Azure 仮想ネットワークへのレプリケーションを制御する AD DS サイトを作成する。

( ) 読み取りと書き込みのキャッシュが無効になっている仮想マシンに追加のハード ディスクを追加する。

( ) Azure 仮想ネットワークを作成し、構成する。

( ) 必要な SRV レコードをドメインの Azure DNS ゾーンに手動で作成する。

( ) Set-AzureStaticVNetIP コマンドレットを使用して、仮想マシンの初期動的 IP アドレスを静的として構成する。

解答 :

( ) オンプレミス ネットワークから Azure 仮想ネットワークへのレプリケーションを制御する AD DS サイトを作成する。

(√) 読み取りと書き込みのキャッシュが無効になっている仮想マシンに追加のハード ディスクを追加する。

(√) Azure 仮想ネットワークを作成し、構成する。

( ) 必要な SRV レコードをドメインの Azure DNS ゾーンに手動で作成する。

(√) Set-AzureStaticVNetIP コマンドレットを使用して、仮想マシンの初期動的 IP アドレスを静的として構成する。

フィードバック：

レプリケーションを精密に制御するために、AD DS サイトを作成することが推奨されますが、そうする必要はありません。ただし、キャッシュが無効化されている Azure 仮想マシンに追加のハード ディスクを作成する必要があり、このハード ディスクには、NTDS.DIT ファイルと SYSVOL フォルダーを含む必要があります。また、Azure 仮想ネットワークをプロビジョニングして正しく構成し、仮想マシンを接続しておく必要もあります。Azure DNS に SRV レコードを手動で作成することは不可能であるため、不正解です。AD DS を展開する前に、仮想マシンの静的 IP アドレスを構成する必要があります。これは、シャットダウンまたはサービスの復旧操作により仮想マシンの割り当てが解除されても、IP が変更されないようにするためです。

レッスン 2
分散 AD DS 環境の展開

目次

質問と解答

質問 : Windows Server 2016 でドメイン コントローラーを展開する際、最小のドメインの機能レベルはどれですか。

( ) Windows Server 2003

( ) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

解答 :

( ) Windows Server 2003

(√) Windows Server 2008

( ) Windows Server 2008 R2

( ) Windows Server 2012 R2

( ) Windows Server 2016

フィードバック :

Windows Server 2016 のドメイン コントローラーを展開する際に必要な、最小のドメインの機能レベルは Windows Server 2008 です。Windows Server 2003 はサポートされません。Windows Server 2003 のドメインやフォレストの機能レベルではサポートは継続されていますが、Windows Server 2003 以前で使用されていた非推奨の FRS ではなく DFS レプリケーションを使用して SYSVOL フォルダーを複製するようにするために、Windows Server 2008 の機能レベルである必要があります。Windows Server 2016 ドメイン コントローラーを導入する前に、Windows Server 2003 で動作しているすべてのドメイン コントローラーをドメインから削除する必要があります。

質問 : DNS 名前空間全体の名前解決を最適化するために使用できるのは、次のどれですか。

( ) 条件付フォワーダー

( ) AD DS サイト

( ) DNS サフィックス検索順

( ) DNS スタブ ゾーン

( ) グローバル カタログ サーバー

解答 :

(√) 条件付フォワーダー

( ) AD DS サイト

(√) DNS サフィックス検索順

(√) DNS スタブ ゾーン

( ) グローバル カタログ サーバー

フィードバック :

条件付フォワーダー、DNS スタブ ゾーン、DNS サフィックス検索順が正解です。ドメイン ツリーを上下にスキャンしたり、またはフォレスト全体をスキャンして名前解決したりしなくても済むように、条件付フォワーダーと DNS スタブ ゾーンでショートカットを作成することができます。DNS サフィックス検索順を構成すると、クライアントが単一ラベル名を解決するために DNS デボルブに依存する必要がなくなります。

AD DS サイトとグローバル カタログ サーバーは不正解です。AD DS サイトは、AD DS 統合 DNS ゾーンのレプリケーションを最適化するのには役立ちますが、名前解決を本質的に効率化するものではありません。グローバル カタログ サーバーは、DNS 名前解決に関与していません。

参考資料

AD DS ドメインの機能レベル

参考資料 : Windows Server 2016 の AD DS の新機能については、次のサイトを参照してください。
http://aka.ms/Bxg2z0

参考資料 : AD DS ドメインの機能レベルについては、次のサイトを参照してください。
Understanding Active Directory Domain Services (AD DS) Functional Levels
http://aka.ms/Ynmvma

以前のバージョンから Windows Server 2016 AD DS への移行

参考資料 : ADMT の使用方法については、次のサイトを参照してください。
ADMT Guide: Migrating and Restructuring Active Directory Domains
http://aka.ms/Jiauyg

デモンストレーション : 既存のフォレスト内の新しいドメインへのドメイン コントローラーのインストール

デモンストレーションの手順

AD DS のバイナリを TOR-DC1 にインストールする

1. TOR-DC1 で、[スタート] をクリックし、[サーバー マネージャー] をクリックします。サーバー マネージャーで、[役割と機能の追加] をクリックします。
2. 役割と機能の追加ウィザードで、[次へ] をクリックします。
3. [インストールの種類の選択] ページで、[役割ベースまたは機能ベースのインストール] が選択されていることを確認し、[次へ] をクリックします。
4. [対象サーバーの選択] ページで、[サーバー プールからのサーバーの選択] が選択されていることを確認します。[サーバー プール] ページで、[TOR-DC1.Adatum.com] が強調表示されていることを確認し、[次へ] をクリックします。
5. [サーバーの役割の選択] ページで、[Active Directory ドメイン サービス] チェック ボックスをオンにし、[機能の追加] をクリックして、[次へ] をクリックします。

6. [機能の選択] ページで、[次へ] をクリックします。
7. [Active Directory ドメイン サービス] ページで、メッセージを確認し、[次へ] をクリックします。
8. [インストール オプションの確認] ページで、メッセージを確認し、[インストール] をクリックします。インストールが完了するまでに数分かかります。
9. [結果] ページで、[このサーバーをドメイン コントローラーに昇格する] をクリックします。ウィザードは継続します。

Active Directory ドメイン サービス構成ウィザードを使用して、TOR-DC1 を AD DS ドメイン コントローラーとして構成する

1. 配置構成ウィンドウで、[新しいドメインを既存のフォレストに追加する] を選択し、[ドメインの種類を選択] の [子ドメイン] が選択されていることを確認します。
2. [親ドメイン名] フィールドで、[Adatum.com] が表示されていることを確認します。
3. [新しいドメイン名] ボックスに「NA」と入力し、[次へ] をクリックします。
4. [ドメイン コントローラー オプション] ページで、[ドメインの機能レベル] として [Windows Server Technical Preview] が選択されていることを確認し、[ドメイン ネーム システム (DNS) サーバー] と [グローバル カタログ (GC)] が選択されていることを確認します。
5. [ディレクトリ サービス復元モード (DSRM) のパスワードを入力してください] セクションで、両方のボックスに「Pa55w.rd」と入力し、[次へ] をクリックします。
6. [DNS オプション] ページで、[次へ] をクリックします。
7. [追加オプション] ページで、[次へ] をクリックします。[パス] ページで、[次へ] をクリックします。[オプションの確認] ページで、[次へ] をクリックします。前提条件のチェック ウィンドウで、[インストール] をクリックします。
8. 情報を確認し、AD DS フォレストで作成した新しい AD DS ドメイン内の AD DS ドメイン コントローラーとして TOR-DC1 再起動することができます。
9. TOR-DC1 で、ユーザー名「NA¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。新しいドメインのインストールを確認するために、一部の AD DS ツールを確認します。

レッスン 3
AD DS の信頼の構成

目次

質問と解答

質問 : フォレストの信頼を作成する前に有効になっている必要があるものは次のどれですか。

( ) 各フォレストのルート ドメイン間の名前解決

( ) Windows Server 2003 以上のフォレストの機能レベル

( ) Windows Server 2008 以上のフォレストの機能レベル

( ) Windows Server 2012 以上のフォレストの機能レベル

( ) ドメイン コントローラーにおける認証の選択

解答 :

(√) 各フォレストのルート ドメイン間の名前解決

(√) Windows Server 2003 以上のフォレストの機能レベル

( ) Windows Server 2008 以上のフォレストの機能レベル

( ) Windows Server 2012 以上のフォレストの機能レベル

( ) ドメイン コントローラーにおける認証の選択

フィードバック :

フォレストの信頼を作成するために、各フォレストのルート ドメイン間で名前解決を構成する必要があります。また、Windows Server 2003 以上のフォレストの機能レベルである必要もあります。

質問 : 信頼されたセキュリティ プリンシパルの認証範囲を制御可能にするのは、次のどの AD DS 信頼設定ですか。

( ) 名前サフィックス ルーティング

( ) Kerberos の制約付き委任 (KCD)

( ) 認証の選択

( ) SID フィルタリング

( ) SID 履歴

解答 :

( ) 名前サフィックス ルーティング

( ) Kerberos の制約付き委任 (KCD)

(√) 認証の選択

( ) SID フィルタリング

( ) SID 履歴

フィードバック :

認証の選択により、指定したコンピューターでのみサービスの認証を許可することで、信頼されたセキュリティ プリンシパルの認証範囲を管理できます。

参考資料

AD DS の信頼の高度な設定の構成

参考資料 :

- 外部の信頼を検疫する SID フィルターについては、次のサイトを参照してください。
  Configuring SID Filter Quarantining on External Trusts
  http://aka.ms/Sveqfn
- フォレストの信頼での認証の選択を有効にする方法については、次のサイトを参照してください。
  Enable Selective Authentication over a Forest Trust
  http://aka.ms/Blp826
- 名前サフィックス ルーティングについては、次のサイトを参照してください。
  Name Suffix Routing
  http://aka.ms/Egc6g7

デモンストレーション : フォレストの信頼の構成

デモンストレーションの手順

条件付フォワーダーを使用して DNS 名前解決を構成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[DNS] の順にクリックします。DNS マネージャーが開きます。
2. DNS マネージャーで、[LON-DC1] を展開し、[条件付フォワーダー] を右クリックして、[新規条件付きフォワーダー] をクリックします。
3. 新規条件付フォワーダー ウィンドウで、[DNS ドメイン] ボックスに「treyresearch.net」と入力します。
4. [マスター サーバーの IP アドレス] ボックスに「172.16.10.10」と入力します。開かれたスペースをクリックし、[OK] をクリックします (エラーが表示されても無視してください)。
5. DNS マネージャーを閉じます。
6. [TREY-DC1] に切り替え、手順 1 ～ 5 を繰り返します。ドメイン名「adatum.com」と IP アドレス「172.16.0.10」を使用します。

双方向の選択的なフォレストの信頼を構成する

1. LON-DC1 で、[ツール]、[Active Directory ドメインと信頼関係] の順にクリックします。
2. Active Directory ドメインと信頼関係ウィンドウで、[Adatum.com] を右クリックし、[プロパティ] をクリックします。
3. [Adatum.com のプロパティ] ダイアログ ボックスの [信頼] タブで、[新しい信頼] をクリックします。
4. 新しい信頼ウィザードで、[次へ] をクリックします。
5. [信頼の名前] ページで、[名前] ボックスに「treyresearch.net」と入力し、[次へ] をクリックします。
6. 新しい信頼ウィザードで、[フォレストの信頼] をクリックし、[次へ] をクリックします。
7. [信頼の方向] ページで、[双方向] をクリックし、[次へ] をクリックします。
8. [信頼の方向] ページで、[このドメインと指定されたドメインの両方] をクリックし、[次へ] をクリックします。

9. [ユーザー名] ボックスに「Administrator」と入力します。[パスワード] ボックスに「Pa55w.rd」と入力し、[次へ] をクリックします。
10. [出力方向の信頼認証レベル - ローカル フォレスト] ページで、[認証の選択] をクリックし、[次へ] をクリックします。
11. [出力方向の信頼認証レベル - 指定されたフォレスト] ページで、[認証の選択] をクリックし、[次へ] をクリックします。
12. [信頼の選択の完了] ページで、[次へ] をクリックします。
13. [信頼の作成完了] ページで、[次へ] をクリックします。
14. [出力方向の信頼の確認] ページで、[確認する]、[次へ] の順にクリックします。
15. [入力方向の信頼の確認] ページで、[確認する]、[次へ] の順にクリックします。
16. [新しい信頼ウィザードの完了] ページで、[完了] をクリックします。
17. [Adatum.com のプロパティ] ダイアログ ボックスで、[OK] をクリックします。

演習の復習の質問と解答

演習 : AD DS のドメインと信頼関係の管理

質問と解答

質問 : Adatum.com と TreyResearch.net の間にフォレストの信頼を作成する際、2 つのフォレスト間の名前解決を可能にするために、DNS スタブ ゾーンが作成されました。DNS スタブ ゾーンの作成の代わりに、どのような代替策を使用することができますか。

解答 : 各フォレストに DNS スタブ ゾーンを作成する代わりに、条件付フォワーダーを使用することもできます。セカンダリ ゾーンも必要な名前解決をおこなうことができますが、不要なレプリケーションを起こす可能性があります。

質問 : フォレストの信頼を作成する際、完全な信頼の代わりに、選択的な信頼を作成した理由は何ですか。

解答 : 信頼を構成する際、認証の選択を使用すると、信頼されたドメインやフォレストのユーザーが認証できるリソースをより詳細に制御できます。認証の選択を使用しなければ、信頼されたドメインやフォレストのユーザーは、すべてのリソースを認証できます。

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
次のようなエラー メッセージが表示された。 • DNS 参照エラー • RPC サーバーを使用できません • ドメインが存在しません • ドメイン コントローラーが見つかりませんでした	通常、これらのエラーは、DNS の参照エラーやファイアウォールの不正な構成が原因で発生します。ネットワーク上で使用可能な稼働中の DNS サーバーが 2 つ以上あることを確認します。また、すべてのコンピューターで、ネットワーク構成に 2 つ以上の DNS サーバーが構成されていることも確認します。 さらに、DNS サーバーが、DNS ドメイン以外の DNS レコード (インターネットアドレスなど) のクエリを正常に解決できることを確認します。 nslookup、dnslint, DCdiag、netdiag、repadmin、replmon、およびイベント ビューアーなど、さまざまなトラブルシューティング ツールを使用します。
ユーザーが認証されず、別の AD DS ドメインや Kerberos 領域のリソースにアクセスできない。	Active Directory ドメインと信頼関係コンソール、(Domain.msc)、または Netdom コマンドライン ツールを使用して、信頼関係を検証します。必要に応じて、信頼パスワードをリセットします。信頼関係が正しい方向で構成されているかチェックします。 すべての AD DS ドメイン コントローラーが、DNS データベース内の適切な SRV レコードをすべて登録しているか確認します (AD DS ドメイン コントローラーの Netlogon サービスを再起動し、DNS データベース内の SRV レコードを強制的に再登録することができます)。

復習問題

質問 : あなたは、A. Datum 社の AD DS 管理者です。現在、AD DS 環境は、Adatum.com の名前空間を使用する単一フォレストかつ単一ドメインのモデル内に構成されています。最近、A.Datum 社は、Trey Research という会社の買収により、ヨーロッパから北米へ拡張すると発表しました。現在、Trey Research 社は、北米とアジアで操業しています。Trey Research 社の AD DS 環境は、treyresearch.net という単一のフォレストで構成され、フォレストのルート ドメインは空で、子ドメインは操業するそれぞれの大陸に合わせてあります (na.treyresearch.net および asia.treyresearch.net)。A. Datum 社の長期的な目標は、A. Datum 社の日常業務に、Trey Research 社を完全に統合することです。A. Datum 社の首脳部も、Trey Research 社が使用する地域の業務モデルを取り込みたいと考えています。A. Datum 社の AD DS 管理者として、あなたは、adatum.com フォレストと treyresearch.net フォレストをどのようにして統合しますか。AD DS 統合の短期的および長期的な目標と、さまざまな要件により、その方法がどのように変わるかについて話し合います。

解答 : 短期的な目標

- adatum.com の AD DS フォレストと treyresearch.net の AD DS フォレスト間で、フォレストの信頼を作成します。これにより、フォレスト間の認証と承認が可能になり、A. Datum 社と Trey Research 社の両方の従業員がどちらのフォレストのリソースにもアクセスできるようになります。

長期的な目標

- 次の新しい子ドメインを adatum.com に作成します。
  - europe.adatum.com
  - na.adatum.com
  - asia.adatum.com
- adatum.com フォレストのためにフォレストの再構築作業を計画する必要があります。
  - 既存の adatum.com ドメイン オブジェクトを europe.adatum.com に移行します。adatum.com フォレスト ルート ドメイン内に、必要なフォレスト レベルのオブジェクトを残します。
  - na.treyresearch.net ドメイン オブジェクトを na.adatum.com に移動します。
  - asia.treyresearch.net ドメイン オブジェクトを asia.adatum.com に移動します。

フィードバック：

このシナリオでの短期的な目標は、AD DS 環境をできるだけ早く統合し、両社の従業員がすぐに共同作業を開始できるようにすることです。これを最も速く、最も簡単に実現する方法は、2 つのフォレスト間にフォレストの信頼を作成することです。この方法は、A. Datum 社の短期的および長期的なニーズの両方で機能する可能性がありますが、首脳部は、Trey Research 社が長期的な戦略の一部であることを表明し、Trey Research 社で採用済みのモデルに類似した地域の業務モデルを採用したいと考えていると示しています。これら 2 つの重要な情報を考慮すると、AD DS の長期的な計画では、A. Datum 社が運用することになる地域ごとに adatum.com フォレストを再構築し、子ドメインを作成する必要があります。

Trey Research 社の買収が単なる短期的な目的であり、将来的に再編成する可能性が高い場合は、その時に Trey Research 社から簡単に分離できるよう、フォレストの信頼のみを実装すると決定してもかまいません。

また、地域の業務モデルが要件でない場合は、単一フォレストと単一ドメインのモデルを保持し、すべての treyresearch.net オブジェクトを adatum.com フォレスト ルート ドメインに移行すると決定してもかまいません。

第 4 章

AD DS のサイトおよびレプリケーションの実装と管理

目次

レッスン 1
AD DS レプリケーションの概要

目次

質問と解答

質問 : サイト内のドメイン コントローラー間で接続オブジェクトを手動で作成した場合に生じる状況について説明してください。

解答 : 知識整合性チェッカーはフェールオーバー時に、手動で作成された接続オブジェクトを検証することも使用することもないので、通常は手動で接続オブジェクトを作成する必要はなく、推奨されません。また、知識整合性チェッカーは手動で作成された接続オブジェクトを削除しません。手動で作成した接続オブジェクトが不要になった場合、手動で削除することを忘れないようにする必要があります。

質問 : グローバル カタログのレプリケーションが重要である理由は何ですか。

解答 : グローバル カタログ サーバーは、構成パーティションの情報を基に他のグローバル カタログ サーバーを認識し、グローバル カタログ サーバー間でレプリケーションをおこないます。そのため、グローバル カタログのデータをレプリケーションするには、構成パーティションのレプリケーションが重要になります。

レッスン 2
AD DS サイトの構成

目次

質問と解答

質問 : 次のうち、AD DS サイトを実装する際の目的として不適切なものはどれですか。

( ) ネットワークの場所間の帯域幅の使用量を削減する

( ) 組織内の単一の場所にグループポリシー設定を適用する

( ) クライアント コンピューターによって認証に使用されるドメイン コントローラーを制御する

( ) 障害復旧用のバックアップ サイトを作成する

( ) 特定のネットワーク セグメントのアプリやサービスへのアクセスを制御する

解答 :

( ) ネットワークの場所間の帯域幅の使用量を削減する

( ) 組織内の単一の場所にグループポリシー設定を適用する

( ) クライアント コンピューターによって認証に使用されるドメイン コントローラーを制御する

(√) 障害復旧用のバックアップ サイトを作成する

( ) 特定のネットワーク セグメントのアプリやサービスへのアクセスを制御する

参考資料

クライアント コンピューターがサイト内でドメイン コントローラーを見つける方法

参考資料 : 詳細については、次のサイトを参照してください。
Finding a Domain Controller in the Closest Site
http://aka.ms/Cjpzdd

デモンストレーション : AD DS サイトの構成

デモンストレーションの手順

1. LON-DC1 で、[スタート]、[サーバー マネージャー] の順にクリックします。
2. サーバー マネージャーで、[ツール]、[Active Directory サイトとサービス] の順にクリックします。
3. Active Directory サイトとサービス コンソールで、[Sites] を展開し、[Default-First-Site-Name] をクリックします。
4. [Default-First-Site-Name] を右クリックし、[名前の変更] をクリックし「LondonHQ」と入力して、Enter キーを押します。
5. ナビゲーション ウィンドウで、[Sites] を右クリックし、[新しいサイト] をクリックします。
6. [新しいオブジェクト - サイト] ダイアログ ボックスで、[名前] ボックスに「Toronto」と入力します。
7. [DEFAULTIPSITELINK] を選択し、[OK] をクリックします。
8. [Active Directory ドメイン サービス] ダイアログ ボックスで、[OK] をクリックします。
9. ナビゲーション ウィンドウで、[Subnets] を右クリックし、[新しいサブネット] をクリックします。
10. [新しいオブジェクト - サブネット] ダイアログ ボックスで、[プレフィックス] ボックスに「172.16.0.0/24」と入力します。

11. [このプレフィックスのサイト オブジェクトを選んでください] で、[LondonHQ] をクリックし、[OK] をクリックします。
12. ナビゲーション ウィンドウで、[Subnets] を右クリックし、[新しいサブネット] をクリックします。
13. [新しいオブジェクト - サブネット] ダイアログ ボックスで、[プレフィックス] ボックスに「172.16.1.0/24」と入力します。
14. [このプレフィックスのサイト オブジェクトを選んでください] で、[Toronto] をクリックし、[OK] をクリックします。
15. ナビゲーション ウィンドウで、[LondonHQ] を展開し、[Servers] を展開します。

    ※以降の操作 (手順 16 ～ 19) をデモンストレーションで紹介する場合は、TOR-DC1 を adatum.com ドメインの追加のドメイン コントローラーとして構成してからおこなってください。
16. [TOR-DC1] を右クリックし、[移動] をクリックします。
17. [サーバーの移動] ダイアログ ボックスで、[Toronto] をクリックし、[OK] をクリックします。
18. ナビゲーション ウィンドウで、[Toronto] を展開し、[Servers] を展開します。
19. TOR-DC1 が Toronto サイトにあることを確認します。

レッスン 3
AD DS レプリケーションの構成と監視

目次

質問と解答

質問 : サイト レプリケーションのスケジュール設定で構成できる最も短いレプリケーション期間は 15 分です。

( ) 正

( ) 誤

解答 :

(√) 正

( ) 誤

参考資料

レプリケーションの監視および管理ツール

参考資料 : 詳細については、次のサイトを参照してください。
AD DS Administration Cmdlets in Windows PowerShell
http://aka.ms/Itjgof

デモンストレーション : AD DS サイト間レプリケーションの構成

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory サイトとサービス] の順にクリックします。
2. Active Directory サイトとサービス コンソールで、[Sites]、[Inter-Site Transports] の順に展開します。
3. [IP] をクリックし、[DEFAULTIPSITELINK] を右クリックし、[名前の変更] をクリックし、「LON-TOR」と入力して、Enter キーを押します。
4. [LON-TOR] を右クリックし、[プロパティ] をクリックします。[コスト]、[レプリケートの間隔]、および [スケジュールの変更] について説明します。
5. [LON-TOR のプロパティ] ダイアログ ボックスの [レプリケートの間隔] スピン ボックスで、値を 60 分に設定します。
6. [スケジュールの変更] をクリックします。
7. 月曜日の午後 12 時から金曜日の午後 4 時までの範囲を、次のようにして強調表示します。
   - [月曜日午後 12 時] タイルをクリックし、マウス ボタンを押しながら、[金曜日午後 4 時] タイルにカーソルをドラッグします。
8. [レプリケーションが利用不可] をクリックし、[OK] をクリックします。
9. [OK] をクリックし、[LON-TOR のプロパティ] ダイアログ ボックスを閉じます。
10. ナビゲーション ウィンドウで、[IP] を右クリックし、[プロパティ] をクリックします。
11. [IP のプロパティ] ダイアログ ボックスで、[サイト リンクをすべてブリッジ] を説明します。
12. [OK] をクリックし、[IP のプロパティ] ダイアログ ボックスを閉じます。

演習の復習の質問と解答

演習 : AD DS のサイトとレプリケーションの実装

質問と解答

質問 : LON-DC2 という新しいドメイン コントローラーを LondonHQ サイトに追加することを決定しました。どのようにして、Toronto サイトへのすべてのレプリケーション トラフィックが LON-DC2 を通過するようにできますか。

解答 : LON-DC2 を、LondonHQ サイトの優先ブリッジヘッド サーバーとして構成する必要があります。

質問 : LON-DC2 という新しいドメイン コントローラーを LondonHQ サイトに追加しました。結果として変更される AD DS パーティションはどれですか。

解答 : スキーマ パーティションを除き、すべてのパーティションが変更される可能性があります。AD DS レプリケーションの正しい構成のために、新しいドメイン コントローラーを、ドメイン パーティションと構成パーティションの両方に追加します。DNS サーバーで Active Directory 統合ゾーンを使用している場合、ドメイン コントローラーのレコードもアプリケーション パーティション内で更新されます。

質問 : この演習では、Toronto サイトと TestSite サイトに別のサイト リンクを作成しました。LondonHQ が、接続オブジェクトを自動的に TestSite サイトに直接作成しないようにするには、何をする必要がありますか。

解答 : 自動サイト リンク ブリッジをオフにして、LondonHQ、Toronto、および TestSite 間のサイトの推移性を無効にする必要があります。

復習とまとめ

ベスト プラクティス

環境内で、Active Directory サイトとレプリケーションを管理する場合、次のようなベスト プラクティスを実装します。

- 各サイトに 1 つ以上のグローバル カタログ サーバーを必ず配置します。
- すべてのサイトに適切なサブネットが関連付けられていることを確認します。
- サイト間レプリケーション用のレプリケーション スケジュールを構成する場合、長期間のレプリケーションがおこなわれない間隔を設定してはいけません。
- レプリケーション用のプロトコルとして簡易メール転送プロトコル (SMTP) は必要のない限り使用しません。

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
あるクライアントが、自身のサイトでドメイン コントローラーを見つけることができない。	• ドメイン コントローラーのすべての SRV レコードが DNS に存在するかどうかを確認します。 • ドメイン コントローラーが、そのサイトに関連付けられたサブネットの IP アドレスを持っているかどうかを確認します。 • クライアントがドメイン メンバーであること、クライアントの時刻が正しく設定されていることを確認します。
サイト間のレプリケーションが機能しない。	• サイト リンクが正しく構成されていることを確認します。 • レプリケーション スケジュールを確認します。 • サイト間のファイアウォールが AD DS レプリケーションのトラフィックを許可するかどうかを確認します。 • repadmin /bind を使用します。
同じサイトにある 2 つのドメイン コントローラー間のレプリケーションが機能しない。	• 両方のドメイン コントローラーが同じサイト内に表示されるかどうかを確認します。 • ドメイン コントローラーで、AD DS が正しく機能しているかどうかを確認します。 • ネットワーク通信と、それぞれのサーバーでの時刻設定が有効であることを確認します。

復習問題

質問 : マルチサイトの企業では、すべてのサブネットが特定され、サイトに関連付けられることが重要です。その理由は何ですか。

解答 : クライアントの IP アドレスとサブネットの定義に基づいて、クライアントを正しいサイトに帰属させることで、ドメイン コントローラーやその他のサービスを見つけるプロセスを効率化することができます。クライアントがサイトに所属しない IP アドレスを持っている場合、そのクライアントはドメイン内のすべてのドメイン コントローラーに対してクエリをおこないます。これは、効率的な戦略ではありません。実際、単一のクライアントがさまざまなサイトのドメイン コントローラーに対してクエリを実行することはできますが、変更がまだレプリケートされていない場合、想定外の結果がもたらされる可能性があります。そのため、各クライアントが自身の所属するサイトを認識していることが重要です。ドメイン コントローラーがクライアントのサイトの場所を特定できるようにすることで、これを実現することができます。

質問 : サイト間レプリケーションの間隔を減らすことの長所と短所は何ですか。

解答 : サイト間レプリケーションの間隔を短縮することで、整合性を高めることができます。あるサイトでおこなわれた変更が、他のサイトにより迅速にレプリケートされます。しかし、実際にはわずかながら短所があります。レプリケーションの間隔が 15 分でも、3 時間でも、同じ変更をレプリケートする必要があると考えるならば、問題はレプリケーションの量ではなく、主にレプリケーションのタイミングです。ただし、一部の極端な状況では、低い頻度で多数の変更が発生するよりも、高い頻度で少数の変更が発生することが望ましくない場合があります。

質問 : ブリッジヘッド サーバーの目的は何ですか。

解答 : ブリッジヘッド サーバーは、サイト外との双方向のすべてのレプリケーションを担当します。あるサイトのすべてのドメイン コントローラーをもう 1 つのサイトのすべてのドメイン コントローラーでレプリケートする代わりに、ブリッジヘッド サーバーを使用してサイト間レプリケーションを管理することができます。ただし、パフォーマンスやその他の要因から、専用のブリッジヘッド サーバーが特に必要でない場合、ベスト プラクティスは、サイト ドメイン コントローラーの使用可能なプールからブリッジヘッド サーバーを ISTG に選択させることです。

ツール

次の表に、この章で参照しているツールを一覧表示します。

ツール	使用目的	アクセス方法
Active Directory サイトとサービス コンソール	サイト、サブネット、サイト リンク、サイト リンク ブリッジを作成し、レプリケーションを強制し、知識整合性チェッカーを再起動する。	サーバー マネージャー
Repadmin.exe	各ドメイン コントローラーのレプリケーションの状態をレポートし、レプリケーション トポロジを作成してレプリケーションを強制し、レプリケーション メタデータの詳細レベルを表示する。	コマンド ライン

ツール	使用目的	アクセス方法
Dcdiag.exe	AD DS のレプリケーションとセキュリティの全体的な正常性に関して、さまざまなテストを実行し、レポートを作成する。	コマンド ライン
Get-ADReplicationConnection	指定したフィルターに基づく特定の AD DS レプリケーション接続または一連の AD DS レプリケーション接続を表示する。	Windows PowerShell
Get-ADReplicationFailure	AD DS レプリケーション障害の説明を表示する。	Windows PowerShell
Get-ADReplicationPartnerMetadata	1 つ以上のレプリケーション パートナーのレプリケーション メタデータを表示する。	Windows PowerShell
Get-ADReplicationSite	指定したフィルターに基づく特定の AD DS レプリケーション サイトまたは一連のレプリケーション サイトを表示する。	Windows PowerShell
Get-ADReplicationSiteLink	指定したフィルターに基づく特定の Active Directory サイト リンクまたは一連のサイト リンクを表示する。	Windows PowerShell
Get-ADReplicationSiteLinkBridge	指定したフィルターに基づく特定の Active Directory サイト リンク ブリッジまたは一連のサイト リンク ブリッジを表示する。	Windows PowerShell
Get-ADReplicationSubnet	指定したフィルターに基づく特定の Active Directory サブネットまたは一連の Active Directory サブネットを表示する。	Windows PowerShell

第 5 章

グループ ポリシーの実装

目次

レッスン 1
グループ ポリシーの概要

目次

質問と解答

活動の分類

次の項目を分類してください。

項目	
1	ドメイン
2	ユーザー
3	組織単位
4	コンピューター
5	サイト
6	グループ
7	Users コンテナー
8	Computers コンテナー

カテゴリ 1		カテゴリ 2
GPO をリンクできるもの		GPO をリンクできないもの

解答 :

カテゴリ 1		カテゴリ 2
GPO をリンクできるもの		GPO をリンクできないもの
ドメイン 組織単位 サイト		ユーザー コンピューター グループ Users コンテナー Computers コンテナー

デモンストレーション : グループ ポリシーのツールとコンソールの確認

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. 必要に応じて、グループ ポリシーの管理コンソールに切り替えます。
3. グループ ポリシーの管理コンソールのナビゲーション ウィンドウで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] をクリックします。
4. [グループ ポリシー オブジェクト] を右クリックし、[新規] をクリックします。
5. [新しい GPO] ダイアログ ボックスに「Disable Control Panel」と入力し、[OK] をクリックします。
6. 詳細ウィンドウで、[Disable Control Panel] を右クリックし、[編集] をクリックします。
7. グループ ポリシー管理エディターのナビゲーション ウィンドウの [ユーザーの構成] で、[ポリシー]、[管理用テンプレート] の順に展開し、[コントロール パネル] をクリックします。
8. 詳細ウィンドウで、[コントロール パネルと PC 設定へのアクセスを禁止する] をダブルクリックします。
9. [コントロール パネルと PC 設定へのアクセスを禁止する] ダイアログ ボックスで、[管理用テンプレート] の設定に使用可能な 3 つの値、[未構成]、[有効]、[無効]、および [ヘルプ] テキストを確認します。
10. [有効] をクリックします。[コメント] ボックスに、「Enabled <date> by <your name>」と入力し、ここでは、<date> を今日の日付に、<your name> をあなたの名前にそれぞれ置き替え、[OK] をクリックします。
11. ナビゲーション ウィンドウの [ユーザーの構成] の [基本設定] を展開し、[ポリシー] ノードと [基本設定] ノードに異なるカテゴリを表示させます。
12. グループ ポリシー管理エディターを閉じます。
13. グループ ポリシーの管理コンソールのナビゲーション ウィンドウで、[グループ ポリシー オブジェクト] を展開し、[Disable Control Panel] をクリックします。
14. 詳細ウィンドウで、[スコープ] タブ、[詳細] タブ、[設定] タブを表示します。
15. ナビゲーション ウィンドウで、[Adatum.com] を右クリックし、[既存の GPO のリンク] をクリックします。
16. [GPO の選択] ダイアログ ボックスで、[Disable Control Panel]、[OK] の順にクリックします。
17. ナビゲーション ウィンドウで、[Adatum.com] をクリックします。
18. 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] タブと [グループ ポリシーの継承] タブを表示します。
19. [スタート] をクリックし、[Windows PowerShell] をクリックします。
20. 管理者 : Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate
```

21. コンピューターとユーザーの両方の設定が、正常に更新されたことを確認します。
22. 次のコマンドを入力し、Enter キーを押します。

```
gpresult /r
```

23. コマンド出力の [ユーザー設定] セクションの [適用された GPO] リストに、[Disable Control Panel] GPO が表示されていることを確認します。
24. Windows PowerShell ウィンドウを閉じます。

レッスン 2
GPO の実装と管理

目次

質問と解答

質問 : 既定で GPO を作成できるのは、どのグループのメンバーですか (3 つ選択してください)。

( ) Domain Admins

( ) Account Operators

( ) Enterprise Admins

( ) GPO Admins

( ) Group Policy Creator Owners

解答 :

(√) Domain Admins

( ) Account Operators

(√) Enterprise Admins

( ) GPO Admins

(√) Group Policy Creator Owners

フィードバック :

GPO Admins グループは存在しません。Domain Admins グループと Enterprise Admins グループは、ドメインで、GPO の作成を含むすべての管理タスクを実行することができます。Group Policy Creator Owners は、ドメインまたはフォレストに対する管理者権限を取得せずに GPO を作成できるようにしたいと考えている場合に、ユーザーを追加することができる唯一のグループです。Account Operators はユーザー、コンピューター、およびグループの管理をおこなう権限を持ちますが、Group Policy に関する権限はありません。

デモンストレーション : グループ ポリシー管理の委任

デモンストレーションの手順

Beth を LON-SVR1 のローカル管理者にする

1. LON-DC1 に切り替えます。
2. タスク バーで、[エクスプローラー] アイコンをクリックします。
3. エクスプローラーのナビゲーション ウィンドウで、[Allfiles (E:)]、[Labfiles] の順に展開し、[Mod05] をクリックします。
4. 詳細ウィンドウで、[Set-LocalAdmin.ps1] を右クリックし、[PowerShell で実行] をクリックします。「Y」と入力し、ダイアログが表示されたら、Enter キーを押します。

委任する前にユーザーのアクセス許可を確認する

1. LON-SVR1 に切り替えます。
2. ユーザー名「Adatum¥Beth」、パスワード「Pa55w.rd」を使用してサインインします。
3. サーバー マネージャーで、[役割と機能の追加] をクリックします。
4. 役割と機能の追加ウィザードの [開始する前に] ページで、[次へ] をクリックします。
5. [インストールの種類の選択] ページで、[次へ] をクリックします。
6. [対象サーバーの選択] ページで、[次へ] をクリックします。
7. [サーバーの役割の選択] ページで、[次へ] をクリックします。

8. [機能の選択] ページで、[グループ ポリシーの管理] チェック ボックスをオンにし、[次へ] をクリックします。
9. [インストール オプションの確認] ページで、[インストール] をクリックします。
10. インストールが完了したら、[閉じる] をクリックします。
11. サーバー マネージャーで、[ツール]、[グループ ポリシー管理] の順にクリックします。
12. 必要に応じて、グループ ポリシーの管理コンソールに切り替えます。
13. グループ ポリシーの管理で、[フォレスト：Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] をクリックします。
14. [グループ ポリシー オブジェクト] コンテナーを右クリックし、Beth には GPO を作成するためのアクセス許可がないので、[新規] 項目が選択不可になっていることに注意してください。
15. ナビゲーション ウィンドウで、[Adatum.com] ドメインを右クリックし、Beth に GPO をドメインにリンクするためのアクセス許可がないので、メニュー項目 [既存の GPO のリンク] が選択不可になっていることに注意してください。
16. ナビゲーション ウィンドウで、[IT] OU を右クリックし、Beth に GPO を [IT] OU にリンクするためのアクセス許可がないので、メニュー項目 [既存の GPO のリンク] が選択不可になっていることに注意してください。
17. [スタート] をクリックし、[Windows PowerShell] をクリックします。
18. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
GPResult /r
```

19. コンピューター設定のグループ ポリシー結果の表示が Beth に許可されていないので、このコマンドの出力では、ユーザー設定のみが表示されることに注意してください。

アクセス許可を委任する

1. LON-DC1 で、グループ ポリシーの管理コンソールに切り替えます。
2. グループ ポリシーの管理のナビゲーション ウィンドウで、[グループ ポリシー オブジェクト] コンテナーをクリックし、詳細ウィンドウで、[委任] タブをクリックします。
3. [追加] をクリックします。[ユーザー、コンピューター、またはグループの選択] ダイアログ ボックスで「Beth」と入力し、[名前の確認] をクリックして、[OK] をクリックします。
4. ナビゲーション ウィンドウで、[IT] OU をクリックし、詳細ウィンドウで、[委任] タブをクリックします。
5. [アクセス許可] ドロップダウン リストから [GPO のリンク] を選択し、[追加] をクリックします。
6. [ユーザー、コンピューター、またはグループの選択] ダイアログ ボックスで「Beth」と入力し、[名前の確認] をクリックして、[OK] をクリックします。
7. [グループとユーザーの追加] ダイアログ ボックスで、[OK] をクリックします。
8. ナビゲーション ウィンドウで、[Adatum.com] ドメインをクリックし、詳細ウィンドウで、[委任] タブをクリックします。
9. [アクセス許可] ドロップダウン リストから [グループ ポリシー結果データの表示] を選択し、[追加] をクリックします。
10. [ユーザー、コンピューター、またはグループの選択] ダイアログ ボックスに「Authenticated Users」と入力し、[名前の確認]、[OK] の順にクリックします。
11. [グループとユーザーの追加] ダイアログ ボックスで、[OK] をクリックします。

委任後にアクセス許可を確認する

1. LON-SVR1 に切り替えます。
2. グループ ポリシーの管理に切り替えます。
3. グループ ポリシーの管理コンソールで、[Adatum.com] ドメインを右クリックし、[最新の情報に更新] をクリックします。
4. ナビゲーション ウィンドウで、[グループ ポリシー オブジェクト] を右クリックし、[新規] をクリックします。
5. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「Beth’s GPO」と入力し、[OK] をクリックします。
6. ナビゲーション ウィンドウで、[Adatum.com] ドメインを右クリックし、[既存の GPO のリンク] が選択不可になっていることに注意してください。
7. ナビゲーション ウィンドウで、[IT] を右クリックし、[既存の GPO のリンク] をクリックします。
8. [GPO の選択] ダイアログ ボックスで、[Beth’s GPO]、[OK] の順にクリックします。
9. Windows PowerShell ウィンドウに切り替えます。
10. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
GPResult /r
```

11. コマンドの出力で、コンピューターとユーザーの両方の設定が表示されることに注意してください。

レッスン 3
グループ ポリシーのスコープとグループ ポリシーの処理

目次

質問と解答

質問 : 次のオプションのうち、既定のグループ ポリシーの処理順序を変更するために GPMC で構成できるものはどれですか (該当するものをすべて選択してください)。

( ) WMI フィルター

( ) セキュリティ フィルター

( ) 継承のブロック

( ) 強制

( ) ループバック処理

解答 :

(√) WMI フィルター

(√) セキュリティ フィルター

(√) 継承のブロック

(√) 強制

(√) ループバック処理

フィードバック :

どのオプションも、グループポリシーの通常の適用方法を変更することができますが、トラブルシューティングが難しくなるため、それらのオプションを慎重に使用する必要があります。

質問 : 複数の WMI フィルターを GPO にリンクできます。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

複数の WMI フィルターを GPO にリンクすることはできませんが、複数の WMI クエリを含む高度な WMI フィルターを作成することはできます。

デモンストレーション : GPO のリンク

デモンストレーションの手順

2 つの GPO を作成して編集する

1. LON-DC1 で、必要に応じて、サーバー マネージャーを開きます。
2. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
3. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] コンテナーを右クリックして、[新規] をクリックします。

4. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「Remove Run Command」と入力し、[OK] をクリックします。
5. グループ ポリシーの管理コンソールで、[グループ ポリシー オブジェクト] コンテナーを右クリックし、[新規] をクリックします。
6. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「Do Not Remove Run Command」と入力し、[OK] をクリックします。
7. [グループ ポリシー オブジェクト] を展開し、[Remove Run Command] GPO を右クリックして、[編集] をクリックします。
8. グループ ポリシー管理エディターの [ユーザーの構成] で、[ポリシー]、[管理用テンプレート]、[タスク バーと [スタート] メニュー] の順に展開し、[[スタート] メニューから [ファイル名を指定して実行] を削除する] をダブルクリックします。
9. [スタート] メニューから [ファイル名を指定して実行] を削除するウィンドウで、[有効]、[OK] の順にクリックします。
10. グループ ポリシー管理エディターを閉じます。
11. グループ ポリシーの管理で、[Do Not Remove Run Command] GPO を右クリックし、[編集] をクリックします。
12. グループ ポリシー管理エディターの [ユーザーの構成] で、[ポリシー]、[管理用テンプレート]、[タスク バーと [スタート] メニュー] の順に展開し、[[スタート] メニューから [ファイル名を指定して実行] を削除する] をダブルクリックします。
13. [スタート] メニューから [ファイル名を指定して実行] を削除するウィンドウで、[無効]、[OK] の順にクリックします。グループ ポリシー管理エディターを閉じます。

GPO を異なる場所にリンクする

1. グループ ポリシーの管理コンソールで、ナビゲーション ウィンドウの [Adatum.com] ドメイン ノードを右クリックし、[既存の GPO のリンク] をクリックします。
2. GPO の選択ウィンドウで、[Remove Run Command]、[OK] の順にクリックします。[Remove Run Command] GPO が Adatum.com ドメインにリンクされます。
3. グループ ポリシーの管理コンソールで、ナビゲーション ウィンドウの [IT] OU を右クリックし、[既存の GPO のリンク] をクリックします。
4. GPO の選択ウィンドウで、[Do Not Remove Run Command]、[OK] の順にクリックします。[Remove Run Command] GPO が [IT] OU にリンクされます
5. ナビゲーション ウィンドウで、[IT] OU をクリックし、詳細ウィンドウで、[グループ ポリシーの継承] タブをクリックします。[グループ ポリシーの継承] タブに GPO の優先順位が表示されます。

GPO のリンクを無効化する

1. 左側のウィンドウで、[Adatum.com] の下に一覧表示されている [Remove Run Command] リンクを右クリックし、[リンクの有効化] をクリックして、チェック マークをオフにします。[IT] OU のグループ ポリシーの継承ウィンドウを最新の状態に更新し、右側のウィンドウの結果を確認します。[Remove Run Command] GPO が表示されないことを確認します。

GPO のリンクを削除する

1. 左側のウィンドウで、[IT] OU を展開し、[Do Not Remove Run Command] リンクを右クリックして、[削除] をクリックします。ウィンドウが表示されたら、[OK] をクリックします。
2. 左側のウィンドウで、[IT] OU をクリックし、詳細ウィンドウで、[グループ ポリシーの継承] タブをクリックします。[Do Not Remove Run Command] GPO が削除されたことと、[Remove Run Command] GPO が存在しないことを確認します。

3. 左側のウィンドウで、[Adatum.com] の下に一覧表示されている [Remove Run Command] GPO を右クリックし、[リンクの有効化] をクリックして、リンクを再度有効化します。[IT] OU のグループ ポリシーの継承ウィンドウを最新の状態に更新し、右側のウィンドウの結果を確認します。
4. グループ ポリシーの管理を閉じます。

デモンストレーション : グループ ポリシーの適用の管理

デモンストレーションの手順

新しい GPO を作成して IT OU にリンクする

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[IT] OU を展開します。
3. [IT] を右クリックし、[このドメインに GPO を作成し、このコンテナーにリンクする] をクリックします。
4. 新しい GPO ウィンドウで、[名前] ボックスに「Remove Help menu」と入力し、[OK] をクリックします。
5. グループ ポリシーの管理コンソールで、[グループ ポリシー オブジェクト] を展開し、[Remove Help menu] GPO を右クリックして、[編集] をクリックします。
6. グループ ポリシー管理エディターの [ユーザーの構成] で、[ポリシー]、[管理用テンプレート]、[タスク バーと [スタート] メニュー] の順に展開し、[[スタート] メニューから [ヘルプ] を削除する] をダブルクリックします。
7. [スタート] メニューから [ヘルプ] を削除するウィンドウで、[有効]、[OK] の順にクリックします。
8. グループ ポリシー管理エディターを閉じます。

セキュリティ グループのフィルター処理を使用してグループ ポリシーの適用をフィルターする

1. [IT] を展開し、[Remove Help menu] GPO のリンクをクリックします。
2. [GPMC] メッセージ ボックスで、[OK] をクリックします。
3. 詳細ウィンドウで、[セキュリティ フィルター処理] の [Authenticated Users] をクリックし、[削除] をクリックします。
4. 確認ダイアログ ボックスで、[OK] をクリックします。
5. 詳細 ウィンドウの [セキュリティ フィルター処理] で、[追加] をクリックします。
6. [ユーザー、コンピューター、またはグループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] ボックスに「Beth Burke」と入力し、[OK] をクリックします。

WMI フィルター処理を使用してグループ ポリシーの適用をフィルターする

1. グループ ポリシーの管理コンソールで、[WMI フィルター] を右クリックし、[新規] をクリックします。
2. [新しい WMI フィルター] ダイアログ ボックスで、[名前] ボックスに「OS Version Filter」と入力します。
3. クエリウィンドウで、[追加] をクリックします。
4. [WMI クエリ] ダイアログ ボックスで、[クエリ] ボックスに次のクエリを入力し、[OK] をクリックします。

```
select * from Win32_OperatingSystem where Version like "6.%"
```

5. [警告] ダイアログ ボックスが表示されたら、[OK] をクリックします。
6. [新しい WMI フィルター] ダイアログ ボックスで、[保存] をクリックします。
7. [グループ ポリシー オブジェクト] フォルダーを右クリックし、[新規] をクリックします。
8. 新しい GPO ウィンドウで、[名前] ボックスに「Software Updates」と入力し、[OK] をクリックします。
9. [グループ ポリシー オブジェクト] を展開し、[Software Updates] GPO をクリックします。
10. 詳細 ウィンドウの [WMI フィルター処理] で、[この GPO は次の WMI フィルターにリンクされています] リストから [OS Version Filter] を選択します。
11. 確認ダイアログ ボックスで、[はい] をクリックします。
12. グループ ポリシーの管理を閉じます。

レッスン 4
GPO の適用のトラブルシューティング

目次

参考資料

グループ ポリシー イベント ログの検査

参考資料 : グループ ポリシー ログ表示ツールをダウンロードするには、次のサイトにアクセスしてください。
http://aka.ms/E8oi7g

デモンストレーション : グループ ポリシーのモデル作成ウィザードによる what-if 分析の実行

デモンストレーションの手順

GPResult.exe を使用してレポートを作成する

1. LON-DC1 で、[スタート] をクリックし「cmd」と入力して、Enter キーを押します。
2. 管理者 : コマンド プロンプト ウィンドウで「cd ¥」と入力し、Enter キーを押します。
3. 次のコマンドを入力し、Enter キーを押します。

```
GPResult /r
```

4. コマンド プロンプトで、出力を確認します。
5. 次のコマンドを入力し、Enter キーを押します。

```
GPResult /h results.html
```

6. コマンド プロンプトを閉じます。
7. [スタート]、[Windows アクセサリ]、[Internet Explorer] の順にクリックします。
8. Internet Explorer で、Alt キーを押して、[ファイル]、[開く] の順にクリックします。
9. [ファイルを開く] ダイアログ ボックスで、[開く] ボックスに「C:¥results.html」と入力し、[OK] をクリックします。
10. 警告メッセージが表示されたら、[ブロックされているコンテンツを許可] をクリックします。
11. レポートの結果を確認します。
12. Internet Explorer を閉じます。

グループ ポリシーの結果ウィザードを使用してレポートを作成する

1. LON-DC1 でサーバー マネージャーを開き、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. グループ ポリシーの管理のナビゲーション ウィンドウで、[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。
3. グループ ポリシーの結果ウィザードで、[次へ] をクリックします。
4. [コンピューターの選択] ページで、[次へ] をクリックします。
5. [ユーザー選択] ページで、[次へ] をクリックします。
6. [選択の要約] ページで、[次へ] をクリックします。
7. [グループ ポリシーの結果ウィザードの完了] ページで、[完了] をクリックします。

8. グループ ポリシーの結果を確認します。
9. [グループ ポリシーの結果] を展開し、[LON-DC1 上の Administrator] を右クリックし、[レポートの保存] をクリックします。
10. [GPO レポートの保存] ダイアログ ボックスで、[デスクトップ] をクリックし、[保存] をクリックします。

グループ ポリシーのモデル作成ウィザードを使用してレポートを作成する

1. [グループ ポリシーのモデル作成] を右クリックし、[グループ ポリシーのモデル作成ウィザード] をクリックします。
2. グループ ポリシーのモデル作成ウィザードで、[次へ] をクリックします。
3. [ドメイン コントローラーの選択] ページで、[次へ] をクリックします。
4. [ユーザーとコンピューターの選択] ページの [ユーザー情報] で、[ユーザー]、[参照] の順にクリックします。
5. [ユーザーの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください (例)] ボックスに「Beth」と入力し、[OK] をクリックします。
6. [コンピューター情報] で、[コンテナー] オプションが選択されていることを確認し、[参照] をクリックします。
7. [コンピューター コンテナーの選択] ダイアログ ボックスで、[Adatum] を展開し、[IT]、[OK] の順にクリックします。
8. [ユーザーとコンピューターの選択] ページで、[次へ] をクリックします。
9. [シミュレーションの詳細オプション] ページで、[次へ] をクリックします。
10. [代替 Active Directory パス] ページで、[次へ] をクリックします。
11. [ユーザー セキュリティ グループ] ページで、[次へ] をクリックします。
12. [コンピューター セキュリティ グループ] ページで、[次へ] をクリックします。
13. [ユーザーの WMI フィルター] ページで、[次へ] をクリックします。
14. [コンピューターの WMI フィルター] ページで、[次へ] をクリックします。
15. [選択の要約] ページで、[次へ] をクリックします。
16. [グループ ポリシーのモデル作成ウィザードの完了] ページで、[完了] をクリックします。
17. レポートを確認します。
18. 開いているウィンドウをすべて閉じます。

演習の復習の質問と解答

演習 A : グループ ポリシー インフラストラクチャの実装

質問と解答

質問 : 多くの組織では、GPO を特定の OU にリンクするのではなく、セキュリティ グループのフィルター処理に依存して、GPO のスコーピングをおこなっています。このような組織では、通常、GPO は、ドメイン自体または第 1 レベル OU のような Active Directory 論理構造の高位にリンクされます。GPO のスコープの管理に、GPO のリンクではなく、セキュリティ グループのフィルター処理を使用することで、どのようなメリットがありますか。

解答 : GPO の適用範囲を OU に依存することの根本的な問題は、OU が AD DS 内で固定された柔軟性のない構造であることです。単一のユーザーまたはコンピューターは、1 つの OU 内にのみ存在することができます。組織が大きく複雑になると、構成要件をコンテナー構造と 1 対 1 の関係で一致させることが難しくなります。セキュリティ グループを使用すると、ユーザーまたはコンピューターは、必要な数だけ多くのグループにメンバーとして所属できるようになり、追加や削除も簡単におこなえるようになります。その際、ユーザーやコンピューター アカウントのセキュリティや管理に影響を与えることもありません。

質問 : 作成した各 GPO に、適用除外グループ、すなわち [グループ ポリシーの適用] アクセス許可を拒否するグループを作成すると便利な理由は何ですか。

解答 : GPO のすべての設定がスコープ内のすべてのユーザーとコンピューターに常に適用される必要があるように保証できるシナリオはごくわずかです。適用を除外するグループを設定することにより、ユーザーまたはコンピューターを除外しなければならない状況にいつでも対応することができます。これは、互換性と機能の問題のトラブルシューティングにも役立ちます。特定の GPO の設定がアプリケーションの機能を妨げる場合もあります。アプリケーションが Windows オペレーティング システムのクリーン インストールで動作するかどうかをテストするには、ユーザーまたはコンピューターを GPO のスコープから一時的に除外する必要があります。

質問 : あなたの組織では、ループバック ポリシー処理を使用していますか。どのようなシナリオで、どのようなポリシー設定に対して、ループバック ポリシー設定は付加価値がありますか。

解答 : 解答はさまざまです。シナリオには、会議室、売店、仮想デスクトップ インフラストラクチャ コンピューター、その他の標準的な環境が含まれます

演習 B : グループ ポリシー インフラストラクチャのトラブルシューティング

質問と解答

質問 : どのような状況で、あなたは、RSoP レポートを使用して、組織でグループ ポリシーの適用のトラブルシューティングをしましたか。

解答 : 解答はさまざまです。受講者の経験や状況に依存します。解答には、次が含まれます。

- セキュリティ フィルターにより、1 つの GPO が適用されなかった、グループ ポリシーの問題を解決する。
- ドメイン ネーム システム (DNS) の問題が原因で、1 つのクライアント側の拡張に 20 秒かかった、グループ ポリシーの問題を解決する。
- 間違った GPO で構成された GPO の設定を特定する。
- ループバック処理により、不適切なユーザー設定が適用された、グループ ポリシーの問題を特定する。

質問 : どのような状況で、グループ ポリシーのモデル作成を使用しましたか。まだ使用していない場合、どのような状況でグループ ポリシーのモデル作成を使用すると予想しますか。

解答 : 解答はさまざまです。受講者の経験や状況に依存します。解答には、次が含まれます。

- グループ ポリシーのモデル作成のシミュレーションに基づいてグループポリシーを正しく構成するように管理する。
- ユーザーをセキュリティ グループに追加した結果をテストする。
- ユーザーを別の OU に移動した結果をテストする。
- コンピューターのループバック処理の構成結果をテストする。

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
グループ ポリシー設定が、GPO が適用されている OU の中のすべてのユーザーやコンピューターに適用されない。	• GPO のセキュリティ フィルター処理を確認します。 • GPO の WMI フィルターを確認します。
グループ ポリシー設定を適用するために、2 回の再起動が必要な場合がある。	[コンピューターの起動およびログオンで常にネットワークを待つ] ポリシー設定を有効にします。

復習問題

質問 : あなたは、グループ ポリシーを介して、OU にログオン スクリプトを割り当てました。スクリプトは、[Scripts] とい名前の共有ネットワーク フォルダーにあります。OU 内の一部のユーザーはスクリプトを受信していますが、その他のユーザーは受信していません。どのような原因が考えられますか。

解答 : セキュリティのアクセス許可に問題があると考えられます。スクリプト フォルダーに読み取りアクセス許可がないユーザーは、スクリプトを実行することができません。また、GPO のセキュリティ フィルター処理が原因でこのような問題が発生する可能性もあります。

質問 : 低速リンクを経由する場合に、どのような GPO の設定が既定で適用されますか。

解答 : レジストリ ポリシーの処理とセキュリティ ポリシーは、低速リンクが検出された場合でも適用されます。この設定を変更することはできません。

質問 : あなたは、ドメイン レベルのポリシーを強制しますが、Managers グループをそのポリシーから除外する必要があります。どのようにして、実現しますか。

解答 : ドメイン レベルでリンクを強制するように設定し、セキュリティ グループのフィルター処理を使用し、Managers グループに対してグループ ポリシーの適用アクセス許可を拒否します。

第 6 章

グループ ポリシーによるユーザー設定の管理

目次

レッスン 1
管理用テンプレートの実装

目次

質問と解答

討論 : 管理用テンプレートの使用

質問 : デスクトップのセキュリティを現在どのように提供していますか。

解答 : 解答はさまざまです。

質問 : ユーザーがシステムに対してどの程度管理アクセスできますか。

解答 : 解答はさまざまです。

質問 : 組織ではどのグループ ポリシー設定が役立ちますか。

解答 : 解答はさまざまです。

質問と解答

質問 : [ユーザーの構成] ノードの [管理用テンプレート] ノードで使用可能なセクションはどれですか (該当するものをすべて選択してください)。

( ) デスクトップ

( ) Windows コンポーネント

( ) サーバー

( ) システム

( ) コントロール パネル

解答 :

(√) デスクトップ

(√) Windows コンポーネント

( ) サーバー

(√) システム

(√) コントロール パネル

フィードバック :

一部のセクションは、GPO のコンピューターとユーザー セクションの両方の [管理用テンプレート] に表示されます。デスクトップ セクションはユーザー セクションのみに、サーバー セクションはコンピューター セクションのみに表示されます。Windows コンポーネント、システム、コントロール パネルは、GPO のコンピューターとユーザー セクションの両方に表示されますが、両方のセクションで構成できる設定は異なります。

質問 : セントラル ストアは、GPMC を使用して作成できます。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

セントラル ストアを作成するためには、手動で SYSVOL に PolicyDefinitions フォルダーを作成し、.admx ファイルと .adml ファイルの両方をコピーする必要があります。

参考資料

セキュリティ テンプレートのインポート

 **参考資料 :** 詳細については、次のサイトを参照してください。
Security Compliance Manager (SCM)
http://aka.ms/Ypdcmd

管理用テンプレートの管理

 **参考資料 :** 詳細については、次のサイトを参照してください。
ADMX Migrator
http://aka.ms/Ny5p5c

 **参考資料 :** 詳細については、次のサイトを参照してください。
Office 2016 Administrative Template files (ADMX/ADML) and Office Customization Tool
http://aka.ms/Nknzlx

デモンストレーション : 管理用テンプレートによる設定の構成

デモンストレーションの手順

管理用テンプレートのポリシー設定を構成する

1. LON-DC1 に切り替えます。
2. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
3. ナビゲーション ウィンドウで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] コンテナーをクリックします。
4. [グループ ポリシー オブジェクト] コンテナーを右クリックし、[新規] をクリックします。
5. [新しい GPO] ダイアログ ボックスで、[名前] フィールドに「GPO1」と入力し、[OK] をクリックします。
6. 詳細ウィンドウで [GPO1] を右クリックし、[編集] をクリックします。
7. グループ ポリシー管理エディターのナビゲーション ウィンドウで、[ユーザーの構成]、[ポリシー]、[管理用テンプレート] の順に展開し、[システム] をクリックします。
8. 詳細ウィンドウで、[コマンド プロンプトにアクセスできないようにする] をダブルクリックします。
9. [コマンド プロンプトにアクセスできないようにする] ダイアログ ボックスで、[未構成]、[有効]、[無効] の 3 つの項目を確認し、[キャンセル] をクリックします。

管理用テンプレートのポリシー設定をフィルター処理する

1. [管理用テンプレート] を右クリックし、[フィルター オプション] をクリックします。
2. [キーワード フィルターを有効にする] チェック ボックスをオンにします。
3. [単語のフィルター] ボックスに「スクリーン セーバー」と入力します。
4. ボックスの横のドロップダウン リストで、[すべて] を選択し、[OK] をクリックします。
5. 管理用テンプレートのポリシー設定のフィルター処理に注目し、[スクリーン セーバー] という単語を含むもののみであることを示します。表示された設定をしばらく検証します。ヘルプ テキストにも [スクリーン セーバー] が含まれる場合があるため、タイトルに [スクリーン セーバー] を含まない設定が表示されることを説明します。
6. コンソール ツリーの [ユーザーの構成] で、[管理用テンプレート] を右クリックし、[フィルター オプション] をクリックします。
7. [キーワード フィルターを有効にする] チェック ボックスをオフにします。
8. [構成] ドロップダウン リストで、[はい] を選択し、[OK] をクリックします。管理用テンプレートのポリシー設定のフィルター処理に注目し、有効または無効として構成済みのもののみであることを示します。構成済みの設定はありません。
9. コンソール ツリーの [ユーザーの構成] で、[管理用テンプレート] を右クリックし、[フィルター有効] をオフにします。

ポリシー設定にコメントを追加する

1. コンソール ツリーの [ユーザーの構成] で、[ポリシー]、[管理用テンプレート]、[コントロール パネル] の順に展開し、[個人用設定] をクリックします。
2. 詳細ウィンドウで、[スクリーン セーバーを有効にする] ポリシー設定をダブルクリックします。
3. [コメント] セクションに「Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver」と入力します。[有効] をクリックし、ポリシーを有効にして、[OK] をクリックします。
4. [スクリーン セーバーをパスワードで保護する] ポリシー設定をダブルクリックし、[有効] をクリックします。
5. [コメント] セクションに「Corporate IT Security Policy implemented with this policy in combination with Enable screen saver」と入力し、[OK] をクリックします。

GPO にコメントを追加する

1. グループ ポリシー管理エディターのナビゲーション ウィンドウで、ルート ノードの [GPO1 [LON-DC1.ADATUM.COM]] を右クリックし、[プロパティ] をクリックします。
2. [コメント] タブをクリックします。
3. 「Adatum corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO: <自身の名前>」と入力し、[OK] をクリックします。。
4. グループ ポリシーの管理コンソールで、GPO1 の [詳細] タブにコメントが表示されることを確認します。
5. グループ ポリシー管理エディターを閉じます。

既存の GPO をコピーして新しい GPO を作成する

1. GPMC のナビゲーション ウィンドウで、[グループ ポリシー オブジェクト] コンテナーをクリックし、[GPO1] を右クリックして、[コピー] をクリックします。
2. [グループ ポリシー オブジェクト] コンテナーを右クリックし、[貼り付け] をクリックして、[OK] を 2 回クリックします。

新しい GPO を作成して別の GPO からエクスポートした設定をインポートする

1. GPMC のナビゲーション ウィンドウで、[グループ ポリシー オブジェクト] コンテナーをクリックし、[GPO1] を右クリックして、[バックアップ] をクリックします。
2. [場所] ボックスに「c:¥」と入力し、[バックアップ] をクリックします。
3. バックアップが完了したら、[OK] をクリックします。
4. GPMC のナビゲーション ウィンドウで、[グループ ポリシー オブジェクト] コンテナーを右クリックし、[新規] をクリックします。
5. [名前] ボックスに「ADATUM Import」と入力し、[OK] をクリックします。
6. GPMC のナビゲーション ウィンドウで、[ADATUM Import] GPO を右クリックし、[設定のインポート] をクリックします。
7. 設定のインポート ウィザードで、[次へ] を 3 回クリックします。
8. [GPO1] を選択し、[次へ] を 2 回クリックします。
9. [完了]、[OK] の順にクリックします。
10. GPMC を閉じます。

レッスン 2

フォルダー リダイレクト、ソフトウェア インストール、およびスクリプトの構成

目次

質問と解答

フォルダー リダイレクトを構成するための設定

質問 : 多くの場合、同一部門のユーザーは異なるコンピューターにサインインします。これらのユーザーは自身のドキュメント フォルダーにアクセスする必要があり、データをプライベートにする必要もあります。この場合、フォルダー リダイレクトのどの設定を選択しますか。

解答 : ルート パスの下に各ユーザーのフォルダーを作成します。これにより、そのユーザーのみがアクセスできる [ドキュメント] フォルダーを作成します。

質問 : 次のフォルダーのうち、フォルダー リダイレクトを使用してリダイレクトできるのはどれですか (該当するものをすべて選択してください)。

( ) ドキュメント

( ) お気に入り

( ) AppData (Roaming)

( ) AppData (Local)

( ) Program Files

解答 :

(√) ドキュメント

(√) お気に入り

(√) AppData (Roaming)

( ) AppData (Local)

( ) Program Files

フィードバック :

[ドキュメント]、[お気に入り]、および [AppData (Roaming)] をリダイレクトできます。ユーザーの AppData フォルダーには、[Local]、[LocalLow]、および [Roaming] という 3 つのフォルダーが存在します。フォルダー リダイレクトを使用して、[Roaming] のみをリダイレクトできます。[Program Files] をリダイレクトすることはできません。このフォルダーは、ローカル ハード ドライブに存在する必要があります。

活動の分類

次の項目を分類してください。

項目	
1	ログオン スクリプト
2	スタートアップ スクリプト
3	ソフトウェアの割り当て
4	ログオフ スクリプト
5	シャットダウン スクリプト

項目	
6	フォルダー リダイレクト
7	ソフトウェアの公開

カテゴリ 1		カテゴリ 2		カテゴリ 3
ユーザーの構成		コンピューターの構成		ユーザーの構成とコンピューターの構成

解答 :

カテゴリ 1		カテゴリ 2		カテゴリ 3
ユーザーの構成		コンピューターの構成		ユーザーの構成とコンピューターの構成
ログオン スクリプト ログオフ スクリプト フォルダー リダイレクト ソフトウェアの公開		スタートアップ スクリプト シャットダウン スクリプト		ソフトウェアの割り当て

デモンストレーション : フォルダー リダイレクトの構成

デモンストレーションの手順

共有フォルダーを作成する

1. LON-DC1 のタスク バーで、[エクスプローラー] アイコンをクリックします。
2. ナビゲーション ウィンドウで、[PC] をクリックします。
3. 詳細ウィンドウで、[ローカル ディスク (C:)] をダブルクリックし、[ホーム] タブの [新しいフォルダー] をクリックします。
4. [名前] ボックスに「Redir」と入力し、Enter キーを押します。
5. [Redir] フォルダーを右クリックし、[共有] をクリックして、[特定のユーザー] をクリックします。
6. [ファイルの共有] ダイアログ ボックスで、ドロップダウン リストをクリックし、[Everyone] を選択して、[追加] をクリックします。

7. Everyone グループで、[アクセス許可のレベル] ドロップダウン リストをクリックし、[読み取り/書き込み] をクリックします。
8. [共有] をクリックし、[終了] をクリックします。
9. ローカル ディスク (C:) ウィンドウを閉じます。

ドキュメント フォルダーをリダイレクトするための GPO を作成する

1. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. ナビゲーション ウィンドウで、[Adatum.com] ドメインを右クリックし、[このドメインに GPO を作成し、このコンテナーにリンクする] をクリックします。
3. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「Folder Redirection」と入力し、[OK] をクリックします。
4. ナビゲーション ウィンドウで、[Folder Redirection] を右クリックし、[編集] をクリックします。
5. グループ ポリシー管理エディターで、[ユーザーの構成]、[ポリシー]、[Windows の設定]、[フォルダー リダイレクト] の順に展開します。
6. [ドキュメント] を右クリックし、[プロパティ] をクリックします。
7. [ドキュメントのプロパティ] ダイアログ ボックスの [ターゲット] タブで、[設定] ドロップダウン リストから [基本 - 全員のフォルダーを同じ場所にリダイレクトする] を選択します。
8. [対象のフォルダーの場所] ボックスが、[ルート パスの下に各ユーザーのフォルダーを作成する] に設定されていることを確認します。
9. [ルート パス] ボックスに「¥¥LON-DC1¥Redir」と入力し、[OK] をクリックします。
10. [警告] ダイアログ ボックスで、[はい] をクリックします。
11. グループ ポリシー管理エディターを閉じます。

フォルダー リダイレクトをテストする

1. LON-CL1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. [スタート] を右クリックし、[コマンド プロンプト] をクリックします。
3. コマンド プロンプトで、次のコマンドを入力し、Enter キーを押します。

```
Gpupdate /force
```

4. サインアウトして、再度ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
5. タスクバーで、[エクスプローラー] アイコンをクリックします。
6. ナビゲーション ウィンドウの [クイック アクセス] セクションで、[ドキュメント] を右クリックし、[プロパティ] をクリックします。
7. [全般] タブで、[場所] フィールドに ¥¥lon-dc1¥redir¥Administrator という値が設定されていることを確認します。
8. これが表示されない場合、手順 2 ～ 7 を繰り返し、リダイレクトを再確認します。
9. LON-CL1 からサインアウトします。

デモンストレーション : GPO によるスクリプトの構成

デモンストレーションの手順

メッセージを表示するログオン スクリプトを作成する

1. LON-DC1 で、[スタート] をクリックし「notepad」と入力して、[メモ帳] をクリックします。
2. メモ帳で、次のコマンドを入力し、Enter キーを押します。

```
Msgbox "This is the script"
```

3. [ファイル] メニューをクリックし、[名前を付けて保存] をクリックします。
4. [名前を付けて保存] ダイアログ ボックスで、[ファイル名] ボックスに「Logon.vbs」と入力します。
5. [ファイルの種類] リストで、[すべてのファイル (*.*)] を選択します。
6. ナビゲーション ウィンドウで、[デスクトップ] をクリックし、[保存] をクリックします。
7. メモ帳を閉じます。
8. デスクトップで、[Logon.vbs] ファイルを右クリックし、[コピー] をクリックします。

スクリプトを使用するための GPO を作成しリンクする

1. サーバー マネージャーを開き、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. [フォレスト : Adatum.com] を展開し、[ドメイン] を展開します。
3. [Adatum.com] を右クリックし、[このドメインに GPO を作成し、このコンテナーにリンクする] をクリックします。
4. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「User Logon Script」と入力し、[OK] をクリックします。
5. [Adatum.com] を展開し、[User Logon Script] GPO を右クリックし、[編集] をクリックします。
6. グループ ポリシー管理エディターの [ユーザーの構成] で、[ポリシー]、[Windows の設定] の順に展開し、[スクリプト (ログオン/ログオフ)] をクリックします。
7. 詳細ウィンドウで、[ログオン] をダブルクリックします。
8. [ログオンのプロパティ] ダイアログ ボックスで、[ファイルの表示] をクリックします。
9. 詳細ウィンドウで、空白部分を右クリックし、[貼り付け] をクリックします。
10. Logon ウィンドウを閉じます。
11. [ログオンのプロパティ] ダイアログ ボックスで、[追加] をクリックします。
12. [スクリプトの追加] ダイアログ ボックスで、[参照] をクリックします。
13. [Logon.vbs] スクリプトをクリックし、[開く] をクリックします。
14. [OK] を 2 回クリックし、すべてのダイアログ ボックスを閉じます。
15. グループ ポリシー管理エディターとグループ ポリシーの管理コンソールを閉じます。

クライアント コンピューターにサインインして結果をテストする

1. LON-CL1 で、サインアウトしてから、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. [スタート] を右クリックし、[コマンド プロンプト] をクリックします。
3. コマンド プロンプトで、次のコマンドを入力し、Enter キーを押します。

```
Gpupdate /force
```

4. LON-CL1 で、ユーザー名「Adatum¥Connie」、パスワード「Pa55w.rd」を使用してサインインします。
5. スクリプトが実行され、前に GPO に構成したメッセージが表示されることを確認します。

注：表示されるまで最大 10 分かかる場合があります。メッセージが表示されない場合は、LON-CL1 を再起動し、手順 1 ～ 4 を繰り返します。

6. LON-CL1 からサインアウトします。

レッスン 3
グループ ポリシーの基本設定の構成

目次

質問と解答

質問 : ユーザーの Internet Explorer エクスペリエンスを構成するために使用できるグループ ポリシーの基本設定はどれですか (該当するものをすべて選択してください)。

( ) Internet Explorer

( ) ショートカット

( ) レジストリ

( ) 電源オプション

( ) フォルダー オプション

解答 :

(√) Internet Explorer

(√) ショートカット

(√) レジストリ

( ) 電源オプション

( ) フォルダー オプション

フィードバック :

グループ ポリシーの基本設定の Internet Explorer の設定を使用して、Internet Explorer を構成することができます。ショートカットにより、ユーザーが Internet Explorer で開くことができるお気に入りを作成できます。レジストリを使用して、Internet Explorer のレジストリ ベースの設定を構成できます。電源オプションまたはフォルダー オプションを使用して、Internet Explorer を構成することはできません。

質問 : 項目レベルでのターゲット設定を使用することで、ユーザーが所属する AD DS フォレストに応じてグループ ポリシーの基本設定を制限することができます。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

フォレストを超えて、グループ ポリシーを適用することはできません。項目レベルでのターゲット設定では、ドメイン、サイト、セキュリティ グループ、および組織単位を使用することができます。

質問 : どのようなシナリオで、グループ ポリシーの基本設定および項目レベルでのターゲット設定を使用したことがありますか。

解答 : 解答はさまざまです。受講者の解答に加えて、講師自身の経験を説明します。

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

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を使用してプリンターを作成する

1. LON-DC1 で、[スタート] を右クリックし、[コントロール パネル] をクリックします。
2. コントロール パネルで、[デバイスとプリンターの表示] をクリックします。
3. [プリンターの追加] をクリックします。
4. [デバイスを追加します] ダイアログ ボックスで、[プリンターが一覧にない場合] をクリックします。
5. [プリンターの追加] ダイアログ ボックスで、[ローカル プリンターまたはネットワーク プリンターを手動設定で追加する] をクリックし、[次へ] をクリックします。
6. [プリンター ポートの選択] ページで、[次へ] をクリックします。
7. [プリンター ドライバーのインストール] ページで、[次へ] をクリックします。
8. [プリンター名を入力してください] ページで、[プリンター名] ボックスに「Brother」と入力し、[次へ] をクリックします。
9. [プリンター共有] ページで、[次へ] をクリックします。
10. [Brother が正しく追加されました] ページで、[完了] をクリックします。
11. コントロール パネルを閉じます。
12. 必要に応じて、サーバー マネージャーに切り替えます。
13. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
14. ナビゲーション ウィンドウで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[Adatum.com] ドメインをクリックします。
15. [Adatum.com] ドメインを右クリックし、[このドメインに GPO を作成し、このコンテナーにリンクする] をクリックします。
16. [新しい GPO] ダイアログ ボックスに「GP Prefs」と入力し、[OK] をクリックします。
17. ナビゲーション ウィンドウで、[GP Prefs] を右クリックし、[編集] をクリックします。
18. グループ ポリシー管理エディターで、[ユーザーの構成]、[基本設定]、[コントロール パネルの設定] の順に展開し、[プリンター] を右クリックし、[新規作成] をポイントして、[共有プリンター] をクリックします。
19. [新しい共有プリンターのプロパティ] ダイアログ ボックスで、[共有パス] ボックスに「¥¥LON-DC1¥Brother」と入力します。
20. [このプリンターを通常使うプリンターとして設定する] チェック ボックスをオンにします。

基本設定のターゲットを設定する

1. [共通] タブで、[項目レベルで対象化する] チェック ボックスをオンにし、[対象化] をクリックします。
2. [ターゲット エディター] ダイアログ ボックスで、[新しい項目] をクリックし、[IP アドレスの範囲] をクリックします。
3. [開始点] ボックスに「172.16.0.50」、[終了点] ボックスに「172.16.0.99」と入力し、[OK] を 2 回クリックします。

グループ ポリシーの基本設定を使用して電源プランを構成する

1. グループ ポリシー管理エディターで、[コンピューターの構成]、[基本設定]、[コントロール パネルの設定] の順に展開し、[電源オプション] をクリックします。
2. [電源オプション] を右クリックし、[新規作成] をポイントして、[電源プラン (Windows 7 以降)] をクリックします。
3. [新しい電源プラン (Windows 7 以降) のプロパティ] ダイアログ ボックスで、[バランス] ドロップダウン リストをクリックし「Adatum Power Plan」と入力します。
4. [現在使用されている電源プランとして設定] チェック ボックスをオンにします。

基本設定のターゲットを設定する

1. [共通] タブで、[項目レベルでターゲットを設定する] チェック ボックスをオンにし、[ターゲット設定] をクリックします。
2. [ターゲット エディター] ダイアログ ボックスで、[新しい項目] をクリックし、[オペレーティング システム] をクリックします。
3. [製品] リストから [Windows 10] を選択し、[OK] を 2 回クリックします。
4. グループ ポリシー管理エディターを閉じます。

基本設定をテストする

1. LON-CL1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. [スタート] を右クリックし、[コマンド プロンプト] をクリックします。
3. コマンド プロンプトで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate /force
```

4. [スタート] を右クリックし、[コントロール パネル] をクリックします。
5. [ハードウェアとサウンド]、[デバイスとプリンター] の順にクリックします。
6. [Brother (LON-DC1 上)] プリンターの存在を確認します。
7. 戻る矢印をクリックし、[電源オプション] をクリックします。
8. [Adatum Power Plan] が存在し、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。

演習の復習の質問と解答

演習 : グループ ポリシーによるユーザー設定の管理

質問と解答

質問 : ユーザーのリダイレクトされたフォルダーを異なるサーバーに分けるには、どのオプションを使用することができますか。

解答 : フォルダー リダイレクトの [詳細設定] を使用して、セキュリティ グループごとに、異なるサーバー上の異なる共有フォルダーを選択することができます。

質問 : OU 内の選択されたオブジェクトに GPO を割り当てる方法を 2 つ挙げてください。

解答 : Windows Management Instrumentation (WMI) フィルターを使用して、コンピューターがノート PC かどうか、どのバージョンのオペレーティング システムがインストールされているかなど、グループ ポリシーを適用するための条件を定義することができます。また、GPO 自体に対するアクセス許可を使用して、ユーザーまたはコンピューターに対して GPO 設定の適用を許可または拒否することができます。

質問 : 新しい電源オプションを構成するために、グループ ポリシーの基本設定を作成しました。どのようにして、ノート PC にのみ適用することができますか。

解答 : 項目レベルでのターゲティングを使用して、基本設定をポータブル コンピューターに適用することができます。コンピューターのハードウェア プロファイルによりポータブル コンピューターとして識別された場合、基本設定が適用されます。

復習とまとめ

ベスト プラクティス

グループ ポリシーの管理に関連するベスト プラクティス

- GPO で設定を構成する場合は、GPO 設定に関するコメントを含めます。
- 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 ポリシー設定が使えない設定の構成については、グループ ポリシーの基本設定を使用します。

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
OU にフォルダー リダイレクトを構成したが、ユーザー フォルダーのいずれもネットワークの場所にリダイレクトされていない。ルート フォルダーを確認すると、ユーザーごとに名前が付いたサブフォルダーが作成済みでが、それらは空である。	問題は、アクセス許可に関連する可能性が高いと考えられます。グループ ポリシーにより、ユーザーの名前が付いたフォルダーが作成されたが、ユーザーはその中にリダイレクトされたフォルダーを作成できるアクセス許可を持っていません。
Windows 7 と Windows 10 コンピューターが混在している。GPO の管理用テンプレートに複数の設定を構成した後、Windows 7 オペレーティング システムを使用しているユーザーから、適用されている設定とされていない設定があるとレポートされた。	Windows 7 のような古いオペレーティング システムには適用されない設定もあるので、適用できるオペレーティング システムを確認します。どのオペレーティング システムに適用されているか、設定自体を確認します。
グループ ポリシーの基本設定が適用されていない。	項目レベルでのターゲット設定用の基本設定、または構成の誤りがないかを確認します。

復習問題

質問 : いくつかのグループ ポリシー設定で、有効になる前に 2 回サインインする必要があるのはなぜですか。

解答 : ユーザーは、通常、キャッシュされた資格情報でサインインします。そのため、グループ ポリシーが現在のセッションに適用されない場合があります。設定は、次のサインインで有効になります。

質問 : セントラル ストアの利点は何ですか。

解答 : セントラル ストアは、SYSVOL 内の単一のフォルダーで、必要なすべての .admx ファイルと .adml ファイルを収容します。セントラル ストアをセットアップすると、グループ ポリシー管理エディターは、セントラル ストアを認識し、すべての管理用テンプレートを、ローカル コンピューターからではなくセントラル ストアから読み込みます。

質問 : 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主な違いは何ですか。

解答 : グループ ポリシー設定は、クライアント側に一部の設定を適用し、変更のためのクライアント 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、設定をおこないますが、クライアントによる設定の変更を許可します。

第 7 章

Active Directory ドメイン サービスのセキュリティ保護

目次

レッスン 1
ドメイン コントローラーのセキュリティ保護

目次

質問と解答

質問 : ドメイン コントローラー内のハード ドライブのセキュリティを強化するためには、どうしますか。

解答 : セキュリティを強化するには、BitLocker ドライブ暗号化を使用して、ドメイン コントローラーのハード ドライブを暗号化することを検討します。

デモンストレーション : パスワード レプリケーション ポリシーの構成

デモンストレーションの手順

RODC の委任されたインストールのステージングをおこなう

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory サイトとサービス] の順にクリックします。
2. Active Directory サイトとサービスのナビゲーション ウィンドウで、[Sites] をクリックします。[操作] メニューの [新しいサイト] をクリックします。
3. [新しいオブジェクト - サイト] ダイアログ ボックスで、[名前] フィールドに「Munich」と入力し、[DEFAULTIPSITELINK] サイト リンク オブジェクトを選択して、[OK] をクリックします。
4. [Active Directory ドメイン サービス] メッセージ ボックスで、[OK] をクリックします。
5. サーバー マネージャーに切り替え、[ツール]、[Active Directory 管理センター] の順にクリックします。
6. Active Directory 管理センターのナビゲーション ウィンドウで、[Adatum (ローカル)] をクリックし、詳細ウィンドウの [Domain Controllers] OU をダブルクリックします。
7. タスク ウィンドウの [Domain Controllers] セクションで、[読み取り専用ドメイン コントローラー アカウントの事前作成] をクリックします。
8. Active Directory ドメイン サービス インストール ウィザードの [Active Directory ドメイン サービス インストール ウィザードの開始] ページで、[次へ] をクリックします。
9. [ネットワーク資格情報] ページで、[次へ] をクリックします。
10. [コンピューター名の指定] ページで、コンピューター名「MUC-RODC1」を入力し、[次へ] をクリックします。
11. [サイトの選択] ページで、[Munich] をクリックし、[次へ] をクリックします。
12. [追加のドメイン コントローラー オプション] ページで、既定の設定を受け入れ、[DNS サーバー] と [グローバル カタログ] チェック ボックスをオンにして、[次へ] をクリックします。
13. [RODC のインストールと管理の委任] ページで、[設定] をクリックします。
14. [ユーザーまたはグループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください] フィールドに「Bill」と入力し、[名前の確認] をクリックします。
15. Bill Norman が解決されていることを確認し、[OK] をクリックします。
16. [RODC のインストールと管理の委任] ページで、[次へ] をクリックします。
17. [要約] ページで、選択内容を確認し、[次へ] をクリックします。
18. [Active Directory ドメイン サービス インストール ウィザードの完了] ページで、[完了] をクリックします。

RODC のパスワード レプリケーション ポリシーを表示する

1. Active Directory 管理センターの [Domain Controllers] OU で、[MUC-RODC1] を選択します。
2. タスク ウィンドウの [MUC-RODC1] セクションで、[プロパティ] をクリックします。
3. [MUC-DC1 (無効)] のプロパティ ダイアログ ボックスで、[拡張] まで下にスクロールし、[パスワード レプリケーション ポリシー] タブをクリックします。
4. パスワード レプリケーション ポリシーの既定のグループ、ユーザー、およびコンピューターを確認します。
5. ダイアログ ボックスを開いたままにします。

RODC 特有のパスワード レプリケーション ポリシーを構成する

1. サーバー マネージャーに切り替え、[ツール]、[Active Directory ユーザーとコンピューター] の順にクリックします。
2. ナビゲーション ウィンドウで、[Adatum.com] を展開し、[Users] をクリックします。
3. [操作] メニューで、[新規作成] をクリックし、[グループ] をクリックします。
4. [新しいオブジェクト - グループ] ダイアログ ボックスで、グループ名として「Munich Allowed RODC Password Replication Group」と入力し、[OK] をクリックします。
5. [Munich Allowed RODC Password Replication Group] をダブルクリックし、[メンバー] タブをクリックして、[追加] をクリックします。
6. [ユーザー、連絡先、コンピューター、サービス アカウントまたはグループの選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください] ボックスに「Ana」と入力し、[名前の確認] をクリックします。
7. [複数の名前が見つかりました] ダイアログ ボックスで、[Ana Cantrell] を選択し、[OK] をクリックします。
8. [ユーザー、連絡先、コンピューター、サービス アカウントまたはグループの選択] ダイアログ ボックスで、[OK] をクリックし、[Munich Allowed RODC Password Replication Group のプロパティ] ダイアログ ボックスで、[OK] をクリックします。
9. Active Directory ユーザーとコンピューターを閉じます。
10. Active Directory 管理センターに切り替え、MUC-RODC1 のプロパティを開きます。[拡張] セクションの [パスワード レプリケーション ポリシー] タブで、[追加] をクリックします。
11. [グループ、ユーザー、およびコンピューターの追加] ダイアログ ボックスで、[この RODC に対するアカウントのパスワードのレプリケートを許可する] を選択し、[OK] をクリックします。
12. [ユーザー、コンピューター、サービス アカウント、またはグループを選択] ダイアログ ボックスで、[選択するオブジェクト名を入力してください] ボックスに「Munich」と入力し、[名前の確認] をクリックして、[OK] をクリックします。
13. [MUC-RODC1 (無効)] ダイアログ ボックスで、[OK] をクリックします。

パスワードのポリシーの結果を確認する

1. Active Directory 管理センターのタスク ウィンドウで、[MUC-RODC1] セクションの [プロパティ] をクリックします。
2. [MUC-RODC1 (無効) のプロパティ] ダイアログ ボックスの [拡張] セクションの [パスワード レプリケーション ポリシー] タブで、[詳細設定] をクリックします。

注 : [MUC-RODC1 の詳細なパスワード レプリケーション ポリシー] ダイアログ ボックスに、この RODC に格納されているパスワードを持つすべてのアカウントが表示されます。

3. [次の条件を満たすユーザーとコンピューターを表示する] ドロップダウン リストで、[この読み取り専用ドメイン コントローラーに対して認証されたアカウント] をクリックし、このページには、必要なアクセス許可を持ち、この RODC によって認証済みのアカウントのみが表示されることを説明します。
4. [ポリシーの結果] タブで、[追加] をクリックし、[ユーザーまたはコンピューターの選択] ダイアログ ボックスの [選択するオブジェクト名を入力してください] フィールドに「Ana」と入力し、[名前の確認] をクリックして、[OK] をクリックします。
5. Ana は、[設定の結果] に [許可] と表示されることに注意してください。
6. すべてのダイアログ ボックスを閉じるかキャンセルします。

レッスン 2
アカウント セキュリティの実装

目次

質問と解答

質問 : Windows デバイスにサインインするために生体認証機能を使用することができる技術はどれですか。

解答 : Windows Hello は、Windows 10 と Windows 10 Mobile で実装された新しいテクノロジです。これにより、指紋、虹彩スキャン、その他の生体認証データを使用して、認証することができます。

参考資料

Windows Server 2016 のアカウント セキュリティ オプション

参考資料 : 資格情報の保護と管理については、次のサイトを参照してください。
資格情報の保護と管理
http://aka.ms/R5bfid

デモンストレーション : ドメイン アカウント ポリシーの構成

デモンストレーションの手順

ドメイン ベースのパスワードのポリシーを構成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com]、[グループ ポリシー オブジェクト] の順に展開し、[Default Domain Policy] を右クリックして、[編集] をクリックします。
3. グループ ポリシー管理エディターのナビゲーション ウィンドウで、[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]、[アカウント ポリシー] の順に展開し、[パスワードのポリシー] をダブルクリックして、[パスワードの履歴を記録する] をダブルクリックします。
4. [パスワードの履歴を記録するのプロパティ] ダイアログ ボックスの [パスワードの履歴を記録する回数] フィールドに「20」と入力し、[OK] をクリックします。
5. [パスワードの有効期間] をダブルクリックします。
6. [パスワードの有効期間のプロパティ] ダイアログ ボックスの [パスワードの有効期間] フィールドに「45」と入力し、[OK] をクリックします。
7. [パスワードの変更禁止期間] をダブルクリックします。
8. [パスワードの変更禁止期間のプロパティ] ダイアログ ボックスの [パスワードの変更禁止期間] フィールドが [1] であることを確認し、[OK] をクリックします。
9. [パスワードの長さ] をダブルクリックします。
10. [パスワードの長さのプロパティ] ダイアログ ボックスの [パスワードの長さ] フィールドに「10」と入力し、[OK] をクリックします。
11. [複雑さの要件を満たす必要があるパスワード] をダブルクリックします。
12. [複雑さの要件を満たす必要があるパスワードのプロパティ] ダイアログ ボックスで、[有効] をクリックし、[OK] をクリックします。

13. グループ ポリシー管理エディターを閉じないでください。

アカウント ロックアウトのポリシーを構成する

1. グループ ポリシー管理エディターのナビゲーション ウィンドウで、[アカウント ロックアウトの ポリシー] をクリックし、[ロックアウト期間] をダブルクリックします。
2. [ロックアウト期間のプロパティ] ダイアログ ボックスで、[このポリシーの設定を定義する] をクリックし、[分] フィールドに「30」と入力して、[OK] をクリックします。
3. [提案された値の変更] ダイアログ ボックスで、[アカウントのロックアウトのしきい値] の自動構成を含め、提案された値を確認して、[OK] をクリックします。
4. [ロックアウト カウンターのリセット] をダブルクリックします。
5. [ロックアウト カウンターのリセットのプロパティ] ダイアログ ボックスで、[ロックアウト カウンターのリセット] フィールドに「15」と入力し、[OK] をクリックします。
6. グループ ポリシー管理エディターとグループ ポリシーの管理コンソールを閉じます。

デモンストレーション : 細かい設定が可能なパスワード ポリシーの構成

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. Active Directory 管理センターのナビゲーション ウィンドウで、[Adatum (ローカル)] をクリックします。
3. 詳細ウィンドウで、[Managers] OU をダブルクリックします。
4. 詳細ウィンドウで、[Managers] グループを探して右クリックし、[プロパティ] をクリックします。

注 : [Managers] OU ではなく、[Managers グループのプロパティ] ダイアログ ボックスを開いていることを確認します。

5. [Managers] ダイアログ ボックスで、[グループのスコープ] の [グローバル] をクリックし、[OK] をクリックします。
6. Active Directory 管理センターのナビゲーション ウィンドウで、[Adatum (ローカル)] をクリックします。
7. 詳細ウィンドウで、[System] コンテナーをダブルクリックします。
8. 詳細ウィンドウで、[Password Settings Container] を右クリックし、[新規]、[パスワードの設定] の順にクリックします。
9. パスワードの設定の作成ウィンドウで、次の手順を完了します。
    1) [名前] フィールドに「ManagersPSO」と入力します。
    2) [優先順位] フィールドに「10」と入力します。
    3) [パスワードの最小の長さを適用する] チェック ボックスをオンにし、[パスワードの最小の長さ (文字数)] フィールドに「15」と入力します。
    4) [パスワードの履歴を記録する] チェック ボックスをオンにし、[記録するパスワードの数] フィールドに「20」と入力します。
    5) [パスワードは要求する複雑さを満たす] チェック ボックスをオンにします。

6) [最小パスワード有効期間を適用する] チェック ボックスをオンにし、[ユーザーがパスワードを変更できない期間 (日数)] フィールドに「1」と入力します。

7) [最大パスワード有効期間を適用する] チェック ボックスをオンにし、[ユーザーによるパスワードの変更が必要な残りの日数] フィールドに「30」と入力します。

8) [適用するアカウント ロックアウト ポリシー] チェック ボックスをオンにします。

9) [許可される失敗したログオン試行回数] フィールドに「3」と入力します。

10) [失敗したログオン試行回数のカウントがリセットされるまでの時間 (分)] ボックスに「30」と入力し、[管理者が手動でアカウントのロックを解除するまで] をクリックします。

10. [直接の適用先] セクションで、[追加] をクリックします。

11. [選択するオブジェクト名を入力してください] ボックスに「Adatum\Managers」と入力し、[名前の確認] をクリックして、[OK] をクリックします。

12. パスワードの設定の作成 : ManagersPSO ウィンドウで、[OK] をクリックします。

13. Active Directory 管理センターを閉じます。

レッスン 3
認証の監査の実装

目次

質問と解答

質問 : ユーザーがドメイン コントローラーにサインインするとき、ログオン イベントが生成されます。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

ユーザーがドメイン コントローラーにサインインすると、ログオン イベントではなく、アカウント ログオン イベントが生成されます。

デモンストレーション : 認証に関連する監査ポリシーの構成

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. グループ ポリシーの管理コンソールのナビゲーション ウィンドウで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com]、[グループ ポリシー オブジェクト] の順に展開し、[Default Domain Controllers Policy] を選択します。
3. [Default Domain Controllers Policy] を右クリックし、[編集] をクリックします。
4. グループ ポリシー管理エディターのナビゲーション ウィンドウで、[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]、[ローカル ポリシー] の順に展開し、[監査ポリシー] をダブルクリックします。
5. 詳細ウィンドウで、[アカウント ログオン イベントの監査] をダブルクリックし、次の構成オプションを説明します。
   - [このポリシーの設定を定義する] チェック ボックスをオンにすると、ポリシーが適用されます。
   - [成功] をオンにすると、成功監査イベントのみがログに記録されます。
   - [失敗] をオンにすると、失敗監査イベントのみがログに記録されます。

   複数のポリシーにこの設定が含まれ、それぞれの設定の定義が異なる場合、設定を定義する最後に適用されたポリシーに基づいて、成功または失敗の選択が適用されます。あるポリシーで成功監査イベントを定義し、別のポリシーで失敗監査イベントを定義している場合、それらが混合されることはありません。
6. [説明] タブで、説明を確認し、話し合います。[キャンセル] をクリックし、[アカウント ログオン イベントの監査のプロパティ] ダイアログ ボックスを閉じます。
7. ログオン イベントの監査ポリシーについて、手順 5 と 6 を繰り返します。
8. グループ ポリシー管理エディターのナビゲーション ウィンドウで、[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]、[監査ポリシーの詳細な構成]、[監査ポリシー] の順に展開します。
9. [監査ポリシー] で、10 の主要なカテゴリを示し、[アカウント ログオン] をクリックします。
10. 4 つのサブカテゴリを示し、[Kerberos 認証サービスの監査] をダブルクリックします。

11. サブカテゴリの設定が [監査ポリシー] の [アカウント ログオン イベントの監査] の設定と同じであることを示し、サブカテゴリの設定がより詳細なレベルを備え、より選択的な監査が可能なことを説明します。
12. [次の監査イベントを構成する] を選択し、[成功] と [失敗] を選択して、[適用] をクリックします。
13. [説明] タブで、説明、既定の設定、予測される監査ボリュームを確認し、話し合います。
14. [OK] をクリックし、[Kerberos 認証サービスの監査のプロパティ] ダイアログ ボックスを閉じます。

デモンストレーション : ログオン イベントの表示

デモンストレーションの手順

1. LON-DC1 の [スタート] を右クリックし、[コマンド プロンプト] をクリックします。
2. 「gpupdate /force」と入力し、Enter キーを押します。
3. ポリシーが更新されるまで待ちます。
4. サインアウトします。
5. LON-DC1 で、ユーザー名「Adatum¥Aidan」、パスワード「123456」を使用してサインインを試行します。
6. [ユーザー名またはパスワードが正しくありません] というメッセージが表示されます。[OK] をクリックします。
7. ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
8. サインインが完了し、サーバー マネージャーが起動するまで、待ちます。
9. サーバー マネージャーで、[ツール]、[イベント ビューアー] の順にクリックします。
10. イベント ビューアーのナビゲーション ウィンドウで、[Windows ログ] を展開し、[セキュリティ] をクリックします。
11. 詳細ウィンドウで、イベント ID が [4771] のイベントを見つけ、このイベントが失敗の監査イベントであることを示します。失敗の監査イベントをダブルクリックします。このイベントが、Adatum¥Aidan が誤ったパスワードでサインインしようとした際にログに記録されたことを示します。[閉じる] をクリックします。
12. イベント ID が [4768] のイベントを見つけます。成功の監査イベントであることを示します。成功の監査イベントをダブルクリックします。このイベントが、Adatum¥Administrator がサインインに成功した際にログに記録されたことを示します。[閉じる] をクリックします。
13. イベント ビューアーを閉じます。

レッスン 4
管理されたサービス アカウントの構成

目次

質問と解答

質問 : グループの MSA と 標準の MSA にはどのような違いがありますか。

解答 : グループの MSA により、標準の MSA の機能を、ドメイン内の複数のサーバーに拡張できます。

デモンストレーション : グループの MSA の構成

デモンストレーションの手順

ドメインの KDS ルート キーを作成する

1. LON-DC1 のサーバー マネージャーで、[ツール] をクリックし、Windows PowerShell 用の Active Directory モジュールを開きます。
2. コマンド プロンプトで、次のコマンドレットを入力し、Enter キーを押します。

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

MSA を作成して関連付ける

1. コマンド プロンプトで、次のコマンドレットを入力し、Enter キーを押します。

```
New-ADServiceAccount -Name SampleApp_SVR1 -DNSHostname LON-DC1.Adatum.com -
PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
```

2. 次のコマンドレットを入力し、Enter キーを押します。

```
Add-ADComputerServiceAccount -identity LON-SVR1 -ServiceAccount SampleApp_SVR1
```

3. 次のコマンドレットを入力し、Enter キーを押します。

```
Get-ADServiceAccount -Filter *
```

4. SampleApp_SVR1 サービス アカウントが一覧に表示されることを確認します。

MSA をインストールする

1. LON-SVR1 で、[スタート] をクリックし、[サーバー マネージャー] をクリックして、[役割と機能の追加] をクリックします。
2. [次へ] をクリックし、[機能の選択] ページまで移動します。
3. [機能] の一覧で、[リモートサーバー管理ツール]、[役割管理ツール]、[AD DS および AD LDS ツール] の順に展開し、[AD DS ツール] を選択します。
4. [機能の追加] をクリックし、[次へ] をクリックします。
5. [インストール] をクリックし、インストールが完了したら [閉じる] をクリックします。
6. [サーバー マネージャー] の [ツール] メニューから Windows PowerShell 用の Active Directory モジュールを開きます。
7. コマンド プロンプトで、次のコマンドレットを入力し、Enter キーを押します。

```
Install-ADServiceAccount -Identity SampleApp_SVR1
```

8. サーバー マネージャーの [メニュー] ツール バーで、[サービス] をクリックします。
9. サービス コンソールで、[Data Sharing Service] を右クリックし、[プロパティ] をクリックします。

注 : このデモンストレーションでは、Data Sharing Service を例として使用します。運用環境では、MSA を割り当てる必要がある実際のサービスを使用します。

10. [(ローカル コンピューター) Data Sharing Service のプロパティ] ダイアログ ボックスで、[ログオン] タブをクリックします。
11. [ログオン] タブで、[アカウント] をクリックし「Adatum¥SampleApp_SVR1$」と入力します。
12. [パスワード] および [パスワードの確認入力] ボックスの両方を空欄にし、[OK] をクリックします。
13. すべてのメッセージ ダイアログで [OK] をクリックします。

演習の復習の質問と解答

演習 : AD DS のセキュリティ保護

質問と解答

質問 : この演習では、Default Domain Policy 内のすべてのユーザー用のパスワードの設定を構成してから、PSO 内の管理者用のパスワードの設定を構成しました。この解決策を実行できるその他のオプションには、何がありますか。

解答 : すべてのユーザーに対する特定の設定を含む PSO を作成し、この PSO に対して高い優先順位を構成し、Domain Users セキュリティ グループにリンクすることができます。この利点は、ドメインのパスワード ポリシーを管理するためのインターフェイスが 1 つのみとなり、ドメイン全体でドメイン メンバーのローカル アカウントに対する既定の設定を構成できることです。

質問 : この演習では、管理者用の PSO の優先順位の値として 10 を使用しました。その理由は何ですか。

解答 : 管理者用の PSO は、厳しく制限される必要があります。そのため、優先順位の値を低くする必要があります。ただし、管理者の一部のみが人事のデータにアクセスする場合や、頻繁に変更されない管理権限を備えたサービス アカウントに対して文字数の多いパスワードを強制する場合など、将来、より制限された設定で管理者のグループを構成する可能性があります。そのため、10 という値を使用することで、より重要な PSO を実装するための余地を確保します。

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
監査ポリシーの詳細設定を構成したが、適用されない。	[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 [監査 : 監査ポリシー サブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシー カテゴリの設定を上書きする] が設定されていることを確認します。
アカウント ログオンとディレクトリ サービスの変更の監査を構成した。これをテストしているが、サーバーのイベント ログにイベントが表示されない。	複数のドメイン コントローラーを使用している場合、各ドメイン コントローラーのセキュリティ ログを表示する必要があります。また、それぞれのドメイン コントローラーに対して、監査ポリシーが構成されていることを確認します。

復習問題

質問 : 特に AD DS ドメイン コントローラーにとって、物理的なセキュリティが重要な理由は何ですか。

解答 : AD DS ドメイン コントローラーは、すべてのユーザー、コンピューター、ドメイン内のその他のあらゆるオブジェクトについての全情報を格納します。そのサーバーまたはハード ドライブに物理的にアクセスできる侵入者は、セキュリティ ガードを容易にすり抜け、この情報をすべて取得することができます。侵入者は、この情報を使用してネットワークを攻撃したり、悪意を持ってドメイン コントローラーを変更し、ネットワークに戻したりすることができます。

質問 : ドメインの認証に対する監査ポリシーとディレクトリ サービスの変更に対する監査ポリシーを実装する必要があります。これらの監査設定を実装するための最良の方法は何ですか。

解答 : 監査を有効にする場合、イベントが起きる可能性のあるすべての該当するサーバーに対して、同じ監査設定を構成することが重要です。ドメインの認証と AD DS での変更に対する監査を構成する場合、これらの設定を Default Domain Controllers Policy と、Domain Controllers OU にリンクされる GPO に構成する必要があります。

質問 : 組織は、あなたに、信頼性が高く、保護された AD DS インフラストラクチャの保守を求めています。また、ユーザーが Outlook Web Access を使用して会社の電子メールにインターネット経由でアクセスできることも求めています。あなたは、アカウントのロックアウト設定の実装を検討しています。何を検討する必要がありますか。

解答 : アカウントのロックアウト設定は、セキュリティ機能のみではありません。攻撃者に、簡単にアクセスできる DoS インターフェイスを提供します。Outlook Web Access にインターネットからアクセスできる場合、追加のプロトコルまたはサービスを構成して、正規のドメイン ユーザーのみが自身のサインインの資格情報を入力できるようにする必要があります。その他のユーザーが Web サイトを使用して、誤ったパスワードを入力して、有効なユーザー アカウントをロックアウトできてはいけません。

ツール

次の表に、この章で参照しているツールを一覧表示します。

ツール	用途	アクセス方法
Active Directory ユーザーとコンピューター	ユーザー、グループ、コンピューターなどの AD DS 内のオブジェクトを管理する	サーバー マネージャー
Active Directory 管理センター	ユーザー、グループ、コンピューターなどの AD DS 内のオブジェクトを管理する	サーバー マネージャー
グループ ポリシーの管理	GPO の管理、レポート、バックアップ、および復元をおこなう	サーバー マネージャー
Gpupdate.exe	ローカル コンピューターの GPO を手動更新する	コマンド ライン

第 8 章

AD CS の展開と管理

目次

レッスン 1
CA の展開

目次

質問と解答

質問 : スタンドアロン CA ではなく、エンタープライズ CA を展開するメリットを説明している選択肢は、次のどれですか。

( ) ユーザーとデバイスが証明書を受け取る複数の手段を提供します。

( ) AD DS が不要です。

( ) ポリシーに基づき、証明書要求を自動的に発行または拒否することができます。

( ) 侵害を防ぐためにオフラインにすることができます。

( ) テンプレートを使用して、AD DS のデータに基づいて証明書を発行できます。

解答 :

(√) ユーザーとデバイスが証明書を受け取る複数の手段を提供します。

( ) AD DS が不要です。

(√) ポリシーに基づき、証明書要求を自動的に発行または拒否することができます。

( ) 侵害を防ぐためにオフラインにすることができます。

(√) テンプレートを使用して、AD DS のデータに基づいて証明書を発行できます。

フィードバック :

エンタープライズ CA の利点は、証明書テンプレートによる自動登録を含め、証明書を登録するための複数の方法を活用できることです。また、エンタープライズ CA では、発行ポリシーに基づいて要求の自動承認または拒否も可能です。ただし、エンタープライズ CA は、AD DS を必要とし、証明書の登録をサポートするためにオンラインの状態で使用する必要があります。

質問 : 次の中で、複数の下位 CA を展開する理由はどれですか。

( ) 固有の使用ポリシーに基づいて、証明書の発行を分割したい場合。

( ) AD DS 環境内に複数のドメインがあり、それぞれのドメインに下位 CA が必要な場合。

( ) 組織の部門や地理的地域に基づいて、証明書の発行を分割したい場合。

( ) 高可用性と要求の負荷分散のために、複数の下位 CA が必要な場合。

( ) 複数の証明書テンプレートを発行する必要があり、各テンプレートがそれぞれの下位 CA を必要とする場合。

解答 :

(√) 固有の使用ポリシーに基づいて、証明書の発行を分割したい場合。

( ) AD DS 環境内に複数のドメインがあり、それぞれのドメインに下位 CA が必要な場合。

(√) 組織の部門や地理的地域に基づいて、証明書の発行を分割したい場合。

(√) 高可用性と要求の負荷分散のために、複数の下位 CA が必要な場合。

( ) 複数の証明書テンプレートを発行する必要があり、各テンプレートがそれぞれの下位 CA を必要とする場合。

フィードバック：

固有の使用ポリシー、組織の部門、または地理的地域のために複数の CA を展開することができます。さらに、高可用性を確保し、要求を負荷分散するために、複数の CA を展開することができます。

マルチドメイン AD DS 環境に複数の下位 CA は必須ではありませんが、AD DS ドメインがすでに組織の部門や地理的地域に一致している場合は、この方法を使用することができます。1 つの CA を、複数のテンプレートを使用して証明書を発行するように構成できるため、異なる証明書テンプレートを発行する必要がある場合に、複数の下位 CA は必要ありません。

デモンストレーション : エンタープライズ ルート CA の展開

デモンストレーションの手順

1. LON-SVR1 で、[スタート] をクリックし、[サーバー マネージャー] をクリックします。
2. サーバー マネージャーで、[役割と機能の追加] をクリックします。
3. [開始する前に] ページで、[次へ] をクリックします。
4. [インストールの種類の選択] ページで、[次へ] をクリックします。
5. [対象サーバーの選択] ページで、[次へ] をクリックします。
6. [サーバーの役割の選択] ページで、[Active Directory 証明書サービス] を選択します。
7. 役割と機能の追加ウィザードで、[機能の追加] をクリックし、[次へ] をクリックします。
8. [機能の選択] ページで、[次へ] をクリックします。
9. [Active Directory 証明書サービス] ページで、[次へ] をクリックします。
10. [役割サービスの選択] ページで、[証明機関] が選択されていることを確認し、[次へ] をクリックします。
11. [インストール オプションの確認] ページで、[インストール] をクリックします。
12. インストールが正常に終了したら、[インストールの進行状況] ページで、[対象サーバーに Active Directory 証明書サービスを構成する] をクリックします。
13. AD CS の構成ウィザードの [資格情報] ページで、[次へ] をクリックします。
14. [役割サービス] ページで、[証明機関] を選択し、[次へ] をクリックします。
15. [セットアップの種類] ページで、[エンタープライズ CA] を選択し、[次へ] をクリックします。
16. [CA の種類] ページで、[ルート CA] をクリックし、[次へ] をクリックします。
17. [秘密キー] ページで、[新しい秘密キーを作成する] が選択されていることを確認し、[次へ] をクリックします。
18. [CA の暗号化] ページで、暗号化サービス プロバイダー (CSP) とハッシュ アルゴリズムを既定の選択のままにし、[キー長] を [4096] に設定して、[次へ] をクリックします。
19. [CA の名前] ページで、[この CA の共通名] ボックスに「AdatumRootCA」と入力し、[次へ] をクリックします。
20. [有効期間] ページで、[次へ] をクリックします。
21. [CA データベース] ページで、[次へ] をクリックします。
22. [確認] ページで、[構成] をクリックします。
23. [結果] ページで、[閉じる] をクリックします。

24. [インストールの進行状況] ページで、[閉じる] をクリックします。

レッスン 2
CA の管理

目次

質問と解答

質問 : AD CS 展開の役割ベースの管理に関する正しい記述は、次のどれですか。

( ) AD CS は、CA 管理者、証明書マネージャー、および登録者のための 3 つの組み込みの役割とグループを自動的に作成します。

( ) AD CS 役割グループに、1 つ以上の CA アクセス許可 (CA の管理、証明書の発行と管理、読み取り、証明書の要求) を付与することができます。

( ) 証明書の発行と管理の CA アクセス許可を、特定のテンプレートまたはテンプレートのセットに限定することができます。

( ) 組織の特定のニーズに基づいて、カスタムの AD CS 役割グループを作成することができます。

( ) Authenticated Users セキュリティ プリンシパルは、CA で発行されたあらゆる証明書を登録することができます。

解答 :

( ) AD CS は、CA 管理者、証明書マネージャー、および登録者のための 3 つの組み込みの役割とグループを自動的に作成します。

(√) AD CS 役割グループに、1 つ以上の CA アクセス許可 (CA の管理、証明書の発行と管理、読み取り、証明書の要求) を付与することができます。

(√) 証明書の発行と管理の CA アクセス許可を、特定のテンプレートまたはテンプレートのセットに限定することができます。

(√) 組織の特定のニーズに基づいて、カスタムの AD CS 役割グループを作成することができます。

( ) Authenticated Users セキュリティ プリンシパルは、CA で発行されたあらゆる証明書を登録することができます。

フィードバック :

AD CS の役割ベースの管理は概念で、自動的にインストールされる機能ではありません。そのため、すべての役割グループを手動で作成する必要があります。役割グループを作成してから、CA アクセス許可 (CA の管理、証明書の発行と管理、読み取り、証明書の要求) を 1 つ以上割り当てることができます。特定のテンプレートまたはテンプレートのセットを使用して証明書を発行または管理するアクセス許可に対する制限を含め、組織のニーズに従って役割をカスタマイズできます。Authenticated Users セキュリティ プリンシパルは、あらゆる証明書を要求できますが、登録する機能は、CA ではなく、証明書テンプレートにより制御されます。

質問 : CA の AIA と CDP 拡張機能に関する正しい記述は、次のどれですか。

( ) 証明書の検証が適切に機能するためには、各拡張機能には、少なくとも 2 つの有効でアクセス可能な URL が必要です。

( ) オフラインおよびスタンドアロン CA の証明書と CRL を手動で AD DS 環境に発行することができます。

( ) 証明書チェーン エンジンは、接続の速さに基づいて場所を指定するため、AIA および CDP URL を指定する順序は重要ではありません。

( ) 外部クライアントのために証明書の検証をサポートするには、HTTP を使用して、Windows Server 2016 の Web アプリケーション プロキシ経由で、外部 AIA と CDP URL を公開する必要があります。

( ) エンタープライズ CA を使用している場合、内部証明書の検証は、追加の構成なしでおこなうことができます。

解答 :

( ) 証明書の検証が適切に機能するためには、各拡張機能には、少なくとも 2 つの有効でアクセス可能な URL が必要です。

(√) オフラインおよびスタンドアロン CA の証明書と CRL を手動で AD DS 環境に発行することができます。

( ) 証明書チェーン エンジンは、接続の速さに基づいて場所を指定するため、AIA および CDP URL を指定する順序は重要ではありません。

(√) 外部クライアントのために証明書の検証をサポートするには、HTTP を使用して、Windows Server 2016 の Web アプリケーション プロキシ経由で、外部 AIA と CDP URL を公開する必要があります。

(√) エンタープライズ CA を使用している場合、内部証明書の検証は、追加の構成なしでおこなうことができます。

フィードバック :

証明書の検証が機能するためには、AIA と CDP の拡張機能に、1 つ以上の有効でアクセス可能な URL が含まれている必要があります。オフラインおよびスタンドアロン CA では、AD DS 環境に手動で CA 証明書と CRL を発行できます。証明書チェーン エンジンは順番に URL を検索するため、AIA と CDP の URL の順序は重要です。最も使用できる可能性が高い URL を先頭に配置する必要があります。外部クライアントのために証明書の検証をサポートするには、HTTP を使用して、Windows Server 2016 の Web アプリケーション プロキシやその他のサード パーティ製のリバース プロキシ ソリューション経由で、AIA と CDP URL を公開することができます。エンタープライズ CA を使用している場合、証明書の検証は内部クライアントに対して自動的に機能しますが、その他のシナリオでは追加の構成が必要な場合があります。

参考資料

CA の管理

参考資料 : 詳細については、次のサイトを参照してください。

- AD CS Deployment Cmdlets in Windows PowerShell
  http://aka.ms/Giih2g
- AD CS Administration Cmdlets in Windows PowerShell
  http://aka.ms/Dekm5i

デモンストレーション : CA のプロパティの構成

デモンストレーションの手順

1. LON-SVR1 でサーバー マネージャーを開き、[ツール]、[証明機関] の順にクリックします。
2. CA の管理コンソールで、[AdatumRootCA] を右クリックし、[プロパティ] をクリックします。
3. [全般] タブで、[証明書の表示] をクリックします。証明書ウィンドウが開いたら、[全般]、[詳細]、[証明のパス] タブ上のデータを確認し、[OK] をクリックします。
4. [ポリシー モジュール] タブで、[プロパティ] をクリックします。既定のポリシー モジュールで使用可能な設定を確認し、[OK] をクリックします。

5. [終了モジュール] タブで、[プロパティ] をクリックします。既定の終了モジュールで使用可能な公開の設定を確認し、[OK] をクリックします。
6. [拡張機能] タブの [拡張機能を選択してください] ドロップダウン リストで、CDP と AIA の拡張機能で使用可能なオプションを確認します。
7. [セキュリティ] タブで、アクセス制御リスト (ACL) で使用可能なオプションと、既定のアクセス許可を確認します。
8. [証明書マネージャー] タブで、オプションを確認し、セキュリティ プリンシパルを特定の証明書テンプレートに制限する方法を説明し、[キャンセル] をクリックします。
9. CA の管理コンソールを閉じます。

レッスン 3
CA のトラブルシューティングと保守

目次

質問と解答

質問 : AD CS で自動登録が適切に機能することを妨げる可能性がある問題は、次のどれですか。

(　) 証明書の自動登録の対象のコンピューターが、ポリシーの継承がブロックされている AD DS OU 内にある。

(　) 証明書の自動登録の対象のユーザーが、必要なグループ ポリシー設定がリンクされていない、または継承されていない AD DS OU 内にいる。

(　) CA がスタンドアロン CA である。

(　) 証明書テンプレートが CA で発行されていない。

(　) AIA URL が CA の拡張機能タブで誤って構成されている。

解答 :

(√) 証明書の自動登録の対象のコンピューターが、ポリシーの継承がブロックされている AD DS OU 内にある。

(√) 証明書の自動登録の対象のユーザーが、必要なグループ ポリシー設定がリンクされていない、または継承されていない AD DS OU 内にいる。

(√) CA がスタンドアロン CA である。

(√) 証明書テンプレートが CA で発行されていない。

(　) AIA URL が CA の拡張機能タブで誤って構成されている。

フィードバック :

グループ ポリシー オブジェクトの継承は、自動登録を妨げる可能性がある一般的な問題です。ユーザーとコンピューターは、必要な GPO 設定にリンクされ、ポリシーの継承がブロックされていない AD DS 組織内に存在する必要があります。さらに、自動登録が正しく機能するためには、クライアントが AD DS を使用して、使用可能な CA とテンプレートを判断するため、CA はエンタープライズ CA である必要があります。エンタープライズ CA でテンプレートが発行され、ユーザーまたはコンピューターはテンプレートに構成された自動登録のアクセス許可を持っている必要があります。CA で無効な AIA URL または CDP URL が構成されていた場合、自動登録はできますが、クライアント アプリケーションまたはサービスが証明書を使用する際に、証明書の検証が正しくおこなわれない可能性があります。

質問 : PKIView ツールに関する正しい記述は、次のどれですか。

(　) PKIView は、すべてのエンタープライズ CA とその現在の正常性を表示する。

(　) PKIView を使用して、手動でスタンドアロン CA を追加できる。

(　) PKIView を使用して、ユーザーとコンピューターの自動登録を構成できる。

(　) PKIView は、それぞれの CA で定義された場所の CDP または AIA の状態を評価する。

(　) PKIView により、AD CS オンライン レスポンダーの役割サービスの状態を評価できる。

解答 :

(√) PKIView は、すべてのエンタープライズ CA とその現在の正常性を表示する。

(　) PKIView を使用して、手動でスタンドアロン CA を追加できる。

(　) PKIView を使用して、ユーザーとコンピューターの自動登録を構成できる。

(√) PKIView は、それぞれの CA で定義された場所の CDP または AIA の状態を評価する。

(√) PKIView により、AD CS オンライン レスポンダーの役割サービスの状態を評価できる。

フィードバック：

PKIView を使用して、すべてのエンタープライズ CA と現在の正常性を確認できますが、スタンドアロン CA の状態を表示することはできません。ユーザーとコンピューター向けの自動登録は、PKIView ツールではなく、グループ ポリシーを介して構成します。PKIView により、各 CA で定義されたそれぞれの場所の CDP と AIA の状態を評価することができます。同様に、AD CS オンライン レスポンダーの役割サービスを展開済みの場合、その状態も評価できます。

演習の復習の質問と解答

演習 : 2 層の CA 階層の展開と構成

質問と解答

質問 : エンタープライズ ルート CA のみをインストールすることが推奨されない理由は何ですか。

解答 : セキュリティ上の理由から、ルート CA をオフラインにして、ネットワーク アクセスができないようにする必要があります。エンタープライズ ルート CA はオフラインにできないため、キーと ID に対して最大限の保護をおこなうことができません。

質問 : 組織がエンタープライズのルート CA を使用する理由は何ですか。

解答 : 組織が 1 つの CA のみを使用し、証明書テンプレートと自動登録の使用を望む場合、エンタープライズ ルート CA が唯一の選択肢です。

復習とまとめ

ベスト プラクティス

- CA インフラストラクチャを展開する際は、スタンドアロン (ドメインに参加していない) ルート CA とエンタープライズの下位 CA (発行元の CA) を展開する。エンタープライズの下位 CA がルート CA から証明書を受け取った後、ルート CA をオフラインにする。
- ルート CA の証明書失効リスト (CRL) の有効期間を確認する。
- AIA と CRL の場所を複数用意する。

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
AIA の拡張で指定されている CA 証明書の場所が、証明書の名前サフィックスを含むようには構成されていない。クライアントが、証明書チェーンの構築に必要な発行元の CA の証明書の正しいバージョンの場所を見つけられないため、証明書の検証が失敗する可能性がある。	証明機関スナップインを使用して、それぞれの場所が証明書の名前サフィックスを含むように、AIA 拡張機能を構成します。
CA が、発行された証明書の拡張機能に CDP の場所を含むように構成されていない。クライアントが、証明書の失効状態を確認するための CRL を見つけられないため、証明書の検証が失敗する可能性がある。	証明機関スナップインを使用して、CDP 拡張機能を構成し、CRL のネットワークの場所を指定します。

復習問題

質問 : 組織が PKI を利用する理由は何ですか。

解答 : PKI を使用する理由としては、セキュリティの向上、ID 管理の強化、およびコードへのデジタル署名などがあります。

質問 : カスタム ポリシーと終了モジュールを展開する理由は何ですか。

解答 : MIM certificate management などの証明書管理用の追加のアプリケーションがある場合、そのアプリケーションを CA と統合できるように、カスタム ポリシーと終了モジュールをインストールする必要があります。

ツール

- CA の管理コンソール
- Certutil コマンド ライン ユーティリティ
- Windows PowerShell
- PKIView.msc
- サーバー マネージャー

第 9 章

証明書の展開と管理

目次

レッスン 1
証明書テンプレートの展開と管理

目次

質問と解答

質問 : AD CS のバージョン 2 の証明書テンプレートに関する文章のうち、正しいものを次から選んでください (該当するものをすべて選択してください)。

( ) バージョン 2 のテンプレートは自動登録をサポートする。

( ) バージョン 2 のテンプレートで変更できるのは、[セキュリティ] タブのみである。

( ) バージョン 1 のテンプレートを複製してバージョン 2 のテンプレートにアップグレードできる。

( ) バージョン 2 のテンプレートは、Windows Server 2008、Windows Vista、およびそれら以降のオペレーティング システムでのみ利用できる。

( ) バージョン 2 のテンプレートは、Windows Server 2012、Windows 8、およびそれら以降のオペレーティング システムでのみ利用できる。

解答 :

(√) バージョン 2 のテンプレートは自動登録をサポートする。

( ) バージョン 2 のテンプレートで変更できるのは、[セキュリティ] タブのみである。

(√) バージョン 1 のテンプレートを複製してバージョン 2 のテンプレートにアップグレードできる。

( ) バージョン 2 のテンプレートは、Windows Server 2008、Windows Vista、およびそれら以降のオペレーティング システムでのみ利用できる。

( ) バージョン 2 のテンプレートは、Windows Server 2012、Windows 8、およびそれら以降のオペレーティング システムでのみ利用できる。

フィードバック :

バージョン 2 のテンプレートの重要な要素の 1 つに、AD DS ユーザーとコンピューターによる自動登録のサポートがあります。バージョン 1 のテンプレートとは異なり、バージョン 2 のテンプレートはすべての要素を変更することができます。バージョン 1 のテンプレートは、複製してバージョン 2 のテンプレートにアップグレードすることができます。Windows Server 2003 Enterprise Edition、Windows Server 2008 Enterprise、Windows Server 2008 R2 以降は、バージョン 2 のテンプレートをサポートしています。CA が Windows Server 2008 以降を実行している場合に限り、バージョン 2 のテンプレートは完全にサポートされます。

質問 : あなたは、A. Datum Corporation の AD CS 管理者です。AD DS 環境の一部のユーザーは、ユーザー証明書の自動登録が有効になっています。ユーザー証明書の有効期間を短くする必要があります。また、既存の証明書の有効期間が経過したら、ユーザーは新しい証明書をすぐに取得できるようにして不都合が発生しないようにする必要があります。次の文章のうち、実行する必要があるのはどれですか (該当するものをすべて選択してください)。

( ) 既存のテンプレートを複製し、新しいテンプレート名を指定して、新しいテンプレートの有効期間を変更する。

( ) 既存のテンプレートの有効期間を変更する。

( ) 既存のテンプレートの自動登録設定を変更する。

( ) 既存のテンプレートから発行されたすべてのユーザー証明書を失効する。

( ) 新しいテンプレートを変更し、既存のテンプレートを置き換えて、新しいテンプレートを発行する。

解答 :

(√) 既存のテンプレートを複製し、新しいテンプレート名を指定して、新しいテンプレートの有効期間を変更する。

( ) 既存のテンプレートの有効期間を変更する。

( ) 既存のテンプレートの自動登録設定を変更する。

(√) 既存のテンプレートから発行されたすべてのユーザー証明書を失効する。

(√) 新しいテンプレートを変更し、既存のテンプレートを置き換えて、新しいテンプレートを発行する。

フィードバック :

このような状況では、既存のテンプレートを複製し、新しいテンプレート名と有効期間を指定する必要があります。また、新しいテンプレートを更新して、前のテンプレートよりも優先させる必要があります。新しいテンプレートをエンタープライズ CA に発行した後、前のテンプレートに対して自動登録されたユーザーが、もう一度新しいテンプレートに自動登録されます。有効期間が適切な新しい証明書が、以前に発行された証明書と置き換えられた場合は、既存のテンプレートから発行されたすべてのユーザー証明書を失効させ、使用できないようにする必要があります。

既存のテンプレートの有効期間を変更すると、新しいテンプレートを登録するときは正しい設定が適用されますが、以前に発行された証明書には正しい有効期間が設定されないままになります。既存のテンプレートの自動登録設定を変更しても、目的の効果を得ることはできないため、変更の必要はありません。

デモンストレーション : 証明書テンプレートの変更と有効化

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[証明機関] の順にクリックします。
2. [証明機関] コンソールで、[AdatumCA] を展開し、[証明書テンプレート] を右クリックして、[管理] をクリックします。
3. 既定のテンプレートのリストを確認し、テンプレートとそのプロパティを確認します。
4. 詳細ウィンドウで、[IPsec] をダブルクリックします。
5. [IPsec のプロパティ] ダイアログ ボックスで、それぞれのタブで変更できる内容を確認します。
6. [セキュリティ] タブで、登録の権限を定義できることを確認し、[キャンセル] をクリックして、テンプレートを閉じます。
7. 証明書テンプレート コンソールの詳細ウィンドウで、[Exchange ユーザー] 証明書テンプレートを右クリックし、[テンプレートの複製] をクリックします。
8. [新しいテンプレートのプロパティ] ダイアログ ボックスで、[互換性] タブ上のオプションを確認します。
9. [全般] タブをクリックし、[テンプレート表示名] ボックスに「Exchange User Test1」と入力します。
10. [セキュリティ] タブをクリックし、[Authenticated Users] をクリックします。
11. Authenticated Users のアクセス許可で、[登録]、および [自動登録] の [許可] チェック ボックスをオンにし、[OK] をクリックします。
12. 証明書テンプレート コンソールを閉じます。
13. 証明機関コンソールで、[証明書テンプレート] を右クリックし、[新規作成] をポイントして、[発行する証明書テンプレート] をクリックします。

14. [証明書テンプレートの選択] ダイアログ ボックスで、[Exchange User Test1] 証明書をクリックし、[OK] をクリックします。

レッスン 2
証明書の展開、失効、および回復の管理

目次

質問と解答

質問 : 証明書を失効すると、証明書の拇印はどこに公開されますか。

( ) CRL 配布ポイント (CDP)

( ) 機関情報アクセス (AIA)

( ) 証明書失効リスト (CRL)

( ) AD DS

( ) オンライン レスポンダー サービス

解答 :

( ) CRL 配布ポイント (CDP)

( ) 機関情報アクセス (AIA)

(√) 証明書失効リスト (CRL)

( ) AD DS

( ) オンライン レスポンダー サービス

フィードバック :

証明書を失効すると、証明書の拇印は、証明書失効リスト (CRL) に公開されます。CRL 配布ポイント (CDP) は CRL が格納されている URL の場所に、機関情報アクセス (AIA) は CA 証明書が格納されている URL の場所にあります。AD DS は CDP の有効な場所ですが、失効した証明書は AD DS に直接公開されません。オンライン レスポンダー サービスは、CRL のローカル コピーを使用して特定の証明書の状態を検証しますが、失効した証明書はオンライン レスポンダー サービスに直接公開されません。

質問 : AD CS の CA でキー アーカイブを構成するには、次のアクションのうちのどれを実行する必要がありますか (該当するものをすべて選択してください)。

( ) キー回復エージェント テンプレートを構成する。

( ) 指定したユーザーに KRA 証明書を登録する。

( ) グループ ポリシーを使用して KRA 公開キーを公開する。

( ) 回復エージェントを CA で構成する。

( ) キー アーカイブで必要な証明書テンプレートを構成する。

解答 :

(√) キー回復エージェント テンプレートを構成する。

(√) 指定したユーザーに KRA 証明書を登録する。

( ) グループ ポリシーを使用して KRA 公開キーを公開する。

(√) 回復エージェントを CA で構成する。

(√) キー アーカイブで必要な証明書テンプレートを構成する。

フィードバック：

キー アーカイブを構成するには、次の操作を実行する必要があります。

1. 信頼されたユーザーのみが証明書への登録を許可されるようにキー回復エージェント テンプレートを構成する。
2. 指定したユーザーに KRA 証明書を登録する。
3. KRA 証明書を使用して、回復エージェントを CA で構成する。
4. キー アーカイブで必要な証明書テンプレートを構成する。

グループ ポリシーを使用して KRA 公開キーを公開する必要はありません。

デモンストレーション : キー アーカイブ用の CA の構成

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[証明機関] の順にクリックします。
2. CA の管理コンソールで、[AdatumCA] ノードを展開し、[証明書テンプレート] フォルダーを右クリックして、[管理] をクリックします。
3. 詳細ウィンドウで、[キー回復エージェント] を右クリックし、[プロパティ] をクリックします。
4. [キー回復エージェントのプロパティ] ダイアログ ボックスで、[発行の要件] タブをクリックし、[CA 証明書マネージャーの許可] チェック ボックスをオフにします。
5. [セキュリティ] タブをクリックし、Domain Admins グループと Enterprise Admins グループのみが [登録] のアクセス許可を持つグループであることを確認し、[OK] をクリックします。
6. 証明書テンプレート コンソールを閉じます。
7. 証明機関コンソールで、[証明書テンプレート] を右クリックし、[新規作成] をポイントして、[発行する証明書テンプレート] をクリックします。
8. [証明書テンプレートの選択] ダイアログ ボックスで、[キー回復エージェント] テンプレートをクリックし、[OK] をクリックします。
9. [スタート]、[Windows PowerShell] の順にクリックします。
10. Windows PowerShell ウィンドウで「mmc.exe」と入力し、Enter キーを押します。
11. コンソール 1 - [コンソール ルート] コンソールで、[ファイル]、[スナップインの追加と削除] の順にクリックします。
12. [スナップインの追加と削除] ダイアログ ボックスで、[証明書]、[追加] の順にクリックします。
13. [証明書スナップイン] ダイアログ ボックスで、[ユーザー アカウント] を選択し、[完了]、[OK] の順にクリックします。
14. [証明書 - 現在のユーザー] ノードを展開し、[個人] を右クリックし、[すべてのタスク] をポイントして、[新しい証明書の要求] をクリックします。
15. 証明書の登録ウィザードの [開始する前に] ページで、[次へ] をクリックします。
16. [証明書の登録ポリシーの選択] ページで、[次へ] をクリックします。
17. [証明書の要求] ページで、[キー回復エージェント] チェック ボックスをオンにし、[登録]、[完了] の順にクリックします。
18. コンソールを更新すると、個人ストアに KRA が表示されます。証明書のプロパティを右にスクロールし、証明書テンプレートの欄にキー回復エージェントが存在することを確認します。

19. 変更を保存せずにコンソール 1 を閉じます。
20. 証明機関コンソールに戻り、[AdatumCA] を右クリックして、[プロパティ] をクリックします。
21. [AdatumCA のプロパティ] ダイアログ ボックスで、[回復エージェント] タブをクリックし、[キーをアーカイブする] を選択します。
22. [キー回復エージェントの証明書] で、[追加] をクリックします。
23. [キー回復エージェントの選択] ダイアログ ボックスで [その他] をクリックし、キー回復エージェントの証明書 (発行先が Administrator になっている証明書) をクリックし、[OK] を 2 回クリックします。
24. CA の再起動を求めるメッセージが表示されたら、[はい] をクリックします。

レッスン 3
ビジネス環境での証明書の使用

目次

質問と解答

質問 : ビジネス環境における証明書の使用に関する次の文章のうち、正しいものを選んでください (該当するものをすべて選択してください)。

(　) 証明書は、Web サーバーとブラウザーとの間の HTTP トラフィックを暗号化するために使用できる。

(　) 証明書は、ドキュメントにデジタル署名するために使用できる。

(　) デジタル署名されたドキュメントは、内容が変更されると無効になる。

(　) 内部 PKI に属さない外部受信者に暗号化された電子メールを送信するには、公的 CA によって発行された暗号化証明書を使用する必要がある。

(　) 暗号化ファイル システム (EFS) を使用して暗号化されたファイルを読むことができるのは、ファイルを元々暗号化したユーザーのみである。

解答 :

(√) 証明書は、Web サーバーとブラウザーとの間の HTTP トラフィックを暗号化するために使用できる。

(√) 証明書は、ドキュメントにデジタル署名するために使用できる。

(√) デジタル署名されたドキュメントは、内容が変更されると無効になる。

(　) 内部 PKI に属さない外部受信者に暗号化された電子メールを送信するには、公的 CA によって発行された暗号化証明書を使用する必要がある。

(　) 暗号化ファイル システム (EFS) を使用して暗号化されたファイルを読むことができるのは、ファイルを元々暗号化したユーザーのみである。

フィードバック :

証明書は、HTTP トラフィックの暗号化、ドキュメントと電子メールのデジタル署名および/または暗号化、また、クライアント/サーバーの認証に使用されます。デジタル署名されたドキュメントは、内容が変更されると無効になります。外部受信者に暗号化された電子メールを送信するには、受信者の公開キーへのアクセスがある場合に限り、内部または公的に発行された証明書のいずれかを使用することができます。ファイルを暗号化したユーザーだけではなく、EFS 共有のために明示的に指定されたユーザーも、EFS を使用して暗号化されたファイルを読むことができます。暗号化された個人の秘密キーが失われたり削除されたりした場合でも、データ回復エージェントがファイルにアクセスすることができます。また、EFS 証明書テンプレートと発行元の CA でキー アーカイブが以前に構成された場合は、キー回復エージェントを使用して秘密キーを取得することができます。

質問 : A. Datum の AD CS 管理者は、AD DS ユーザーが内部 PKI からの証明書を使用してデジタル署名と暗号化を実行できるようにする必要があります。次の手順のうち、必要なものはどれですか。

(　) キー回復エージェントを有効にする。

(　) データ回復エージェントを有効にする。

(　) ユーザー証明書テンプレートを発行し、自動登録を有効にする必要のあるユーザー グループを構成する。

(　) グループ ポリシーを使用して、ドメインに参加しているコンピューターの EFS を有効にする。

(　) ドメインに参加しているすべてのコンピューターを Windows Server 2016 または Windows 10 にアップグレードする。

解答：

( ) キー回復エージェントを有効にする。

( ) データ回復エージェントを有効にする。

(√) ユーザー証明書テンプレートを発行し、自動登録を有効にする必要のあるユーザー グループを構成する。

( ) グループ ポリシーを使用して、ドメインに参加しているコンピューターの EFS を有効にする。

( ) ドメインに参加しているすべてのコンピューターを Windows Server 2016 または Windows 10 にアップグレードする。

フィードバック：

ユーザー証明書テンプレートを発行し、それを自動登録用に構成するだけで、デジタル署名と暗号化を実行できます。キー回復エージェントとデータ回復エージェントを使用することはベスト プラクティスですが、デジタル署名と暗号化には必要ありません。ドメインに参加しているコンピューターで EFS を有効にする必要はなく、また、ドメインに参加しているすべてのコンピューターを Windows Server 2016 または Windows 10 にアップグレードする必要もありません。

デモンストレーション：ドキュメントへのデジタル署名

デモンストレーションの手順

1. LON-CL1 で、Windows PowerShell ウィンドウを開きます。
2. Windows PowerShell ウィンドウで「mmc.exe」と入力し、Enter キーを押します。
3. コンソール 1 - [コンソール ルート] ウィンドウで、[ファイル]、[スナップインの追加と削除] の順にクリックします。
4. [証明書] を選択して [追加] をクリックし、[ユーザー アカウント] を選択し、[完了]、[OK] の順にクリックします。
5. [証明書 - 現在のユーザー] を展開し、[個人] を右クリックし [すべてのタスク] を選択して、[新しい証明書の要求] をクリックします。
6. 証明書の登録ウィザードで、[次へ] を 2 回クリックします。
7. [証明書の登録] ページで、利用可能なテンプレートのリストから [ユーザー] を選択し、[登録]、[完了] の順にクリックします。
8. 変更を保存せずに、コンソール 1 - [コンソール ルート] ウィンドウを閉じます。
9. Word 2016 を開きます。

注： Microsoft Office ライセンス認証ウィザードが表示されたら、[閉じる] をクリックします。[後で確認する] を選択し、[同意する] をクリックします。

10. [白紙の文書] をクリックし、文字を入力して、デスクトップにファイルを保存します。
11. リボンの [挿入] をクリックし、テキスト 欄にある [署名欄の追加] ドロップダウン リストから [Microsoft Office 署名欄] をクリックします。
12. 署名の設定ウィンドウで、[署名候補者] ボックスに自分の名前、[署名候補者の役職] ボックスに「Administrator」、[署名候補者の電子メール アドレス] に「Administrator@adatum.com」と入力し、[OK] をクリックします。

13. 文書内の署名欄を右クリックし、[署名] をクリックします。
14. 署名ウィンドウで、[変更] をクリックします。
15. [証明書] の一覧で、今日の日付の入った証明書を選択し、[OK] をクリックします。
16. X の右側のボックスに自分の名前を入力し、[署名]、[OK] の順にクリックします。

注 : 受講者には、自分の名前を入力するだけでなく、画像を選択することもできると説明してください。手書きの署名をスキャンした画像も使用できます。

17. 文書を編集できないことを確認します。
18. Word 2016 を閉じ、ダイアログが表示されたら変更を保存します。
19. 次のデモンストレーションで使用するため、サインインしたままにします。

デモンストレーション : EFS によるファイルの暗号化

デモンストレーションの手順

1. LON-CL1 で、前回のデモンストレーションで保存した Word 文書を右クリックし、[プロパティ] をクリックします。
2. [プロパティ] ダイアログ ボックスの [全般] タブで、[詳細設定]、[内容を暗号化してデータをセキュリティで保護する]、[OK] の順にクリックします。
3. [OK] をクリックし、メッセージ ウィンドウで、[ファイルだけを暗号化] を選択し、[OK] をクリックします。
4. 暗号化されたドキュメントを、C:¥ユーザー¥パブリック¥パブリックのドキュメント フォルダーに移動します。
5. LON-CL1 からサインアウトします。
6. ユーザー名「Adatum¥Aidan」、パスワード「Pa55w.rd」を使用してサインインします。
7. エクスプローラーを開き、C:¥ユーザー¥パブリック¥パブリックのドキュメントに移動します。
8. 暗号化された文書を開くことができるか試します。
9. 文書を開くことができないことを確認します。
10. LON-CL1 からサインアウトします。

レッスン 4
スマート カードの実装および管理

目次

質問と解答

質問 : スマート カードに関する文章のうち、正しいものを次から選んでください。

( ) スマート カードは、多要素認証のオプションを提供する。

( ) スマート カードは、対話型サインインに使用できない。

( ) スマート カードには、PIN を使用してのみアクセスできる証明書と秘密キーが含まれている。

( ) スマート カードは、パスワードを凌駕する強化されたセキュリティを提供する。

( ) スマート カードは、デジタル署名と暗号化にのみ使用できる。

解答 :

(√) スマート カードは、多要素認証のオプションを提供する。

( ) スマート カードは、対話型サインインに使用できない。

(√) スマート カードには、PIN を使用してのみアクセスできる証明書と秘密キーが含まれている。

(√) スマート カードは、パスワードを凌駕する強化されたセキュリティを提供する。

( ) スマート カードは、デジタル署名と暗号化にのみ使用できる。

フィードバック :

スマート カードは、多要素認証のオプションを提供します。ユーザーは、スマート カードを物理的に所有し、その PIN についても知っておく必要があります。PIN を入力することで、スマート カードに保存された証明書と秘密キーを、認証、デジタル署名、および暗号化に使用できるようになります。対話型サインインにスマート カードを使用すると、パスワードを凌駕する強化されたセキュリティが提供されます。

質問 : スマート カード インフラストラクチャを実装する場合、証明書管理フレームワークに含める必要があるのは、次のプロセスのうちのどれですか。

( ) 発行

( ) 失効

( ) 更新

( ) ブロックとブロック解除

( ) 一時停止

解答 :

(√) 発行

(√) 失効

(√) 更新

(√) ブロックとブロック解除

(√) 一時停止

フィードバック :

すべてのプロセスを証明書管理計画に含める必要があります。これらのプロセスの一部は、組み込みユーティリティを使用して実行できますが、複雑なため、スマート カード専用のソリューションや、MIM などの証明書管理ソリューションが推奨されます。

演習の復習の質問と解答

演習 : 証明書の展開と使用

質問と解答

質問 : 秘密キーを回復するには、何をする必要がありますか。

解答 : 秘密キーを回復するには、特定のテンプレートに対して秘密キーをアーカイブするように CA を構成し、KRA 証明書を発行する必要があります。

質問 : 制限付き登録エージェントを使用する利点は何ですか。

解答 : 制限付き登録エージェントを使用すると、登録エージェントとして指定されているユーザーのアクセス許可を制限して、他のユーザーに代わってスマート カード証明書を登録することができます。

復習とまとめ

ベスト プラクティス

- 古い証明書テンプレートを置換する際、テンプレートの置き換えを使用します。
- 暗号化に使用される証明書を必ずアーカイブします。
- 証明書の一括展開に自動登録を使用します。
- スマート カードを使用する場合、ユーザーに自身の PIN を定期的に変更させます。
- スマート カードを使用する場合、スマート カード管理ソリューションを実装します。

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
登録中に証明書テンプレートが表示されない。	テンプレートに対して読み取りと登録のアクセス許可が正しく構成されていることを確認します。
自動登録が機能しない。	グループ ポリシーで自動登録オプションが構成され、ユーザーまたはコンピューターのグループに、読み取り、登録、および自動登録のアクセス許可が正しく割り当てられていることを確認します。
ファイルを暗号化したユーザーが暗号化を解除できない。	ユーザーがキーペアの秘密キーを所有していること、および証明書の有効期限が切れていないことを確認します。秘密キーが失われたり、証明書の有効期限が切れたりした場合は、KRA または DRA を使用します。

実際の問題とシナリオ

Contoso 社では、複数のサービスのサポートと保護のため、PKI を展開したいと考えています。同社では、PKI のプラットフォームとして Windows Server 2016 の AD CS を使用することにしました。証明書は主に、EFS、デジタル署名、Web サーバーに使用されます。暗号化されるドキュメントは重要なので、万一のキー損失に備えて、障害復旧策を用意することが大切です。また、会社の Web サイトの保護された部分にアクセスしようとするクライアントが、ブラウザーで警告を受けるようなことはあってはなりません。

- Contoso 社はどのような種類の展開を選択するべきですか。
- Contoso 社は、EFS やデジタル署名に対し、どのような種類の証明書を使用するべきですか。
- Contoso 社は、Web サイトに対し、どのような種類の証明書を使用するべきですか。
- ユーザーが証明書を失っても EFS で暗号化されたデータが失われていないことを、Contoso 社はどのように確認しますか。

復習問題

質問 : 証明書の自動登録を使用するための要件を挙げてください。

解答 : 証明書の自動登録を使用するには、エンタープライズ CA を所有し、グループ ポリシーのオプションを構成する必要があります。また、必要な証明書テンプレートの自動登録を有効にし、グループ ポリシー オブジェクトを構成する必要もあります。

質問 : 仮想スマート カードはどのようにして機能しますか。

解答 : 仮想スマート カードは、従来のスマート カードの機能を模倣していますが、追加のハードウェアの購入を要求するのではなく、ユーザーがすでに所有しているテクノロジや、常に使用する可能性が高いテクノロジを使用します。

ツール

- CA の管理コンソール
- 証明書テンプレート コンソール
- 証明書コンソール
- Certutil.exe

第 10 章

AD FS の実装と管理

目次

レッスン 1
AD DS の概要

目次

質問と解答

質問 : フェデレーションによる信頼は、組織が AD DS フォレスト間に構成できるフォレストの信頼と同じです。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

フェデレーションによる信頼は、組織が AD DS フォレスト間で構成可能なフォレストの信頼とは異なります。フェデレーションによる信頼では、2 つの組織間で AD FS サーバーが相互に直接通信する必要がありません。さらに、フェデレーションの展開におけるすべての通信は HTTPS 上でおこなわれるため、フェデレーションを可能にするためにファイアウォールでポートをいくつも開く必要はありません。

レッスン 2
AD FS の要件と計画

目次

質問と解答

質問 : Windows Server 2016 では、フェデレーション サーバー プロキシの機能は、Web アプリケーション プロキシの役割の一部となります。

( ) 正

( ) 誤

解答 :

(√) 正

( ) 誤

フィードバック :

フェデレーション サーバー プロキシは、通常、境界ネットワークに展開する省略可能なコンポーネントです。インターネットからフェデレーション サーバーへの接続に対して、セキュリティを強化するために展開されます。Windows Server 2016 では、フェデレーション サーバー プロキシの機能は、Web アプリケーション プロキシの一部となります。

参考資料

オンライン サービスのための AD FS 展開の計画

参考資料 : ツールは、次の URL から実行することができます。
Microsoft Office 365 展開準備ツール
http://aka.ms/D9vmqf

参考資料 : これらの手順についての追加情報は、次のサイトを参照してください。
チェックリスト : AD FS を使用してシングル サインオンを実装および管理する
https://msdn.microsoft.com/ja-jp/library/azure/jj205462.aspx

高可用性 AD FS 展開の計画

参考資料 : SQL Server の高可用性ソリューションについては、次のサイトを参照してください。
高可用性ソリューション (SQL Server)
https://technet.microsoft.com/ja-JP/Library/ms190202.aspx

キャパシティ プランニング

参考資料 : AD FS キャパシティ プランニング スプレッドシートの詳細、またはダウンロードについては、次のサイトを参照してください。
AD FS サーバーの容量計画
https://technet.microsoft.com/ja-jp/library/gg749899.aspx

デモンストレーション : AD FS サーバーの役割のインストール

デモンストレーションの手順

AD FS をインストールする

1. LON-DC1 で、[スタート]、[Windows PowerShell] の順にクリックします。
2. 次のコマンドレットを入力し、Enter キーを押します。

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
```

   このコマンドレットは、Microsoft グループ キー配布サービスのルート キーを作成し、この演習の後半で使用されるアカウント用のグループ管理サービス アカウント (gMSA) のパスワードを生成します。このコマンドレットへの応答として、グローバルー意識別子 (GUID) が表示されます。

3. LON-DC1 のサーバー マネージャーで、[管理]、[役割と機能の追加] の順にクリックします。
4. 役割と機能の追加ウィザードの [開始する前に] ページで、[次へ] をクリックします。
5. [インストールの種類の選択] ページで、[次へ] をクリックします。
6. [対象サーバーの選択] ページで、[次へ] をクリックします。
7. [サーバーの役割の選択] ページで、[Active Directory Federation Services] チェック ボックスをオンにし、[次へ] をクリックします。
8. [機能の選択] ページで、[次へ] をクリックします。
9. [Active Directory フェデレーション サービス (AD FS)] ページで、[次へ] をクリックします。
10. [インストール オプションの確認] ページで、[インストール] をクリックします。
11. インストールが完了するまで待ち、[閉じる] をクリックします。

AD FS 用の DNS レコードを追加する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[DNS] の順にクリックします。
2. DNS マネージャーで、[LON-DC1]、[前方参照ゾーン] の順に展開し、[Adatum.com] をクリックします。
3. [Adatum.com] を右クリックし、[新しいホスト (A または AAAA)] をクリックします。
4. 新しいホスト ウィンドウの [名前] ボックスに「adfs」と入力します。
5. [IP アドレス] ボックスに「172.16.0.10」と入力し、[ホストの追加] をクリックします。
6. DNS ウィンドウで、[OK]、[完了] の順にクリックします。
7. DNS マネージャーを閉じます。

AD FS を構成する

1. LON-DC1 のサーバー マネージャーで、[通知] アイコンをクリックし、[このサーバーにフェデレーション サービスを構成します] をクリックします。
2. Active Directory フェデレーション サービス構成ウィザードの [ようこそ] ページで、[フェデレーション サーバー ファームに最初のフェデレーション サーバーを作成します] をクリックし、[次へ] をクリックします。
3. [Active Directory ドメイン サービスへの接続] ページで、[次へ] をクリックし、Adatum¥Administrator を使用して構成を実行します。
4. [サービスのプロパティの指定] ページで、[SSL 証明書] の一覧から [adfs.adatum.com] を選択します。

5. [フェデレーション サービスの表示名] ボックスに「A. Datum Corporation」と入力し、[次へ] をクリックします。
6. [サービス アカウントの指定] ページで、[グループ管理サービス アカウントを作成します] をクリックします。
7. [アカウント名] ボックスに「ADFSService」と入力し、[次へ] をクリックします。
8. [構成データベースの指定] ページで、[Windows Internal Database を使用してサーバーにデータベースを作成します] をクリックし、[次へ] をクリックします。
9. [オプションの確認] ページで、[次へ] をクリックします。
10. [前提条件の確認] ページで、[構成] をクリックします。
11. [結果] ページで、[閉じる] をクリックします。

レッスン 3
AD FS の展開と構成

目次

質問と解答

質問 : 要求規則とは何かを説明してください。要求規則は何に使用できますか。

解答 : 要求規則は、どのように要求が送信され、AD FS サーバーで処理されるかを定義します。要求規則は、要求プロバイダーが発行し、証明書利用者が受け入れる要求に適用されるビジネス ロジックを定義します。次の要求規則を使用できます。

- どの入力方向の要求が、1 つ以上の要求プロバイダーから受け入れられるかを定義します。
- どの出力方法の要求が、1 つ以上の証明書利用者に提供されるかを定義します。
- 1 つ以上のユーザーまたはユーザー グループに対して、特定の証明書利用者へのアクセスを有効にする承認規則を適用します。

参考資料

AD FS のインストールと構成

参考資料 : 詳細については、次のサイトを参照してください。
SQL Server を使用するフェデレーション サーバー ファーム
https://technet.microsoft.com/ja-jp/library/dn554242.aspx

参考資料 : AD FS で使用可能なすべての更新プログラムについては、次のサイトを参照してください。
Active Directory フェデレーション サービス (AD FS) 用更新プログラム
https://technet.microsoft.com/ja-jp/js-jp/library/mt126278.aspx

ホーム領域検出のしくみ

参考資料 : RelayState については、次のサイトを参照してください。
Supporting Identity Provider Initiated RelayState
http://aka.ms/Df8hqs

AD FS 展開の管理

参考資料 : Office 365 Federation Metadata Update Automation Installation Tool の詳細とダウンロードについては、次のサイトを参照してください。
Microsoft Office 365 Federation Metadata Update Automation Installation Tool
http://aka.ms/i1hw8d

デモンストレーション : 要求プロバイダー信頼と証明書利用者信頼の構成

デモンストレーションの手順

要求プロバイダー信頼を構成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[AD FS の管理] の順にクリックします。
2. AD FS コンソールで、[要求プロバイダー信頼] をクリックします。
3. [Active Directory] を右クリックし、[要求規則の編集] をクリックします。
4. Active Directory の要求規則の編集ウィンドウの [受け入れ変換規則] タブで、[規則の追加] をクリックします。
5. 変換要求規則の追加ウィザードの [規則テンプレートの選択] ページで、[要求規則テンプレート] の一覧から [LDAP 属性を要求として送信] を選択し、[次へ] をクリックします。
6. [規則の構成] ページで、[要求規則名] ボックスに「Outbound LDAP Attributes Rule」と入力します。
7. [属性ストア] の一覧で、[Active Directory] をクリックします。
8. [LDAP 属性の出力方向の要求の種類への関連付け] セクションで、[LDAP 属性] と [出力方向の要求の種類] に次の値を選択します。
   - E-Mail-Addresses : 電子メール アドレス
   - User-Principal-Name : UPN
9. [完了]、[OK] の順にクリックします。

AD FS 用に WIF アプリケーションを構成する

1. LON-SVR1 で、サーバー マネージャーを開き、[ツール]、[Windows Identity Foundation Federation Utility] の順にクリックします。
2. [フェデレーション ユーティリティ ウィザードの開始] ページで、[アプリケーション構成の場所] ボックスに、「C:¥inetpub¥wwwroot¥AdatumTestApp¥web.config」(サンプルの web.config ファイルの場所) と入力します。
3. [アプリケーション URI] ボックスに「https://lon-svr1.adatum.com/AdatumTestApp/」と入力し、フェデレーション サーバーからの入力方向の要求を信頼するサンプル アプリケーションへのパスを指定して、[次へ] をクリックします。
4. [Security Token Service] ページで、[既存の STS を使う] をクリックし、[STS WS-Federation メタデータのドキュメントの場所] ボックスに「https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml」と入力します。[次へ] をクリックします。
5. [STS 署名証明書のチェーンの検証エラー] ページで、[証明書チェーンの検証を無効にする] をクリックし、[次へ] をクリックします。
6. [セキュリティ トークンの暗号化] ページで、[暗号化しない] をクリックし、[次へ] をクリックします。
7. [提供されたクレーム] ページで、フェデレーション サーバーから提供されるクレームを確認し、[次へ] をクリックします。
8. [概要] ページで、フェデレーション ユーティリティ ウィザードによってサンプル アプリケーションに加えられる変更を確認し、[完了] をクリックします。
9. [成功] ダイアログ ボックスで、[OK] をクリックします。

証明書利用者信頼を構成する

1. LON-DC1 の AD FS コンソールで、[証明書利用者信頼] をクリックします。

2. 操作ウィンドウで、[証明書利用者信頼の追加] をクリックします。
3. 証明書利用者信頼の追加ウィザードの [ようこそ] ページで、[開始] をクリックします。
4. [データ ソースの選択] ページで、[オンラインまたはローカル ネットワークで公開されている証明書利用者についてのデータをインポートする] をクリックします。
5. [フェデレーション メタデータのアドレス (ホスト名または URL)] ボックスに「https://lon-svr1.adatum.com/adatumtestapp/」と入力し、[次へ] をクリックします。これにより、前の作業で構成されたメタデータがダウンロードされます。
6. [表示名の指定] ページで、[表示名] ボックスに「A. Datum Corporation Test App」と入力し、[次へ] をクリックします。
7. [アクセス制御ポリシーの選択] ページで、[すべてのユーザーを許可] をクリックし、[次へ] をクリックします。
8. [信頼の追加の準備完了] ページで、証明書利用者信頼の設定を確認し、[次へ] をクリックします。
9. [完了] ページで、[閉じる] をクリックします。
10. [証明書利用者信頼] の一覧で、[A. Datum Corporation Test App] をクリックし、[要求発行ポリシーの編集] をクリックします。
11. A. Datum Corporation Test App の要求発行ポリシーの編集ウィンドウの [発行変換規則] タブで、[規則の追加] をクリックします。
12. [要求規則テンプレート] ボックスで、[入力方向の要求をパス スルーまたはフィルター処理] を選択し、[次へ] をクリックします。
13. [要求規則名] ボックスに「Pass through Windows account name」と入力します。
14. [入力方向の要求の種類] の一覧で、[Windows アカウント名] をクリックし、[完了] をクリックします。
15. [発行変換規則] タブで、[規則の追加] をクリックします。
16. [要求規則テンプレート] ボックスで、[入力方向の要求をパス スルーまたはフィルター処理] を選択し、[次へ] をクリックします。
17. [要求規則名] ボックスに「Pass through E-Mail Address」と入力します。
18. [入力方向の要求の種類] の一覧で、[電子メール アドレス] をクリックし、[完了] をクリックします。
19. [発行変換規則] タブで、[規則の追加] をクリックします。
20. [要求規則テンプレート] ボックスで、[入力方向の要求をパス スルーまたはフィルター処理] を選択し、[次へ] をクリックします。
21. [要求規則名] ボックスに「Pass through UPN」と入力します。
22. [入力方向の要求の種類] の一覧で、[UPN] をクリックし、[完了] をクリックします。
23. [発行変換規則] タブで、[規則の追加] をクリックします。
24. [要求規則テンプレート] ボックスで、[入力方向の要求をパス スルーまたはフィルター処理] を選択し、[次へ] をクリックします。
25. [要求規則名] ボックスに「Pass through Name」と入力します。
26. [入力方向の要求の種類] の一覧で、[名前] をクリックし、[完了] をクリックします。
27. [発行変換規則] タブで、[OK] をクリックします。

デモンストレーション : 要求規則の構成

デモンストレーションの手順

1. LON-DC1 の AD FS コンソールで、[証明書利用者信頼] をクリックし、[A. Datum Corporation Test App] をクリックして、[要求発行ポリシーの編集] を選択します。
2. A. Datum Corporation Test App の要求発行ポリシーの編集ウィンドウの [発行変換規則] タブで、[規則の追加] をクリックします。
3. [要求規則テンプレート] ボックスで、[入力方向の要求をパス スルーまたはフィルター処理] を選択し、[次へ] をクリックします。
4. [要求規則名] ボックスに「Send Group Name Rule」と入力します。
5. [入力方向の要求の種類] の一覧で、[グループ] をクリックし、[完了] をクリックします。
6. [OK] をクリックします。
7. [A. Datum Corporation Test App] を右クリックし、[アクセス制御ポリシーの編集] をクリックします。
8. A. Datum Corporation Test App のアクセス制御ポリシーの編集ウィンドウの [アクセス制御ポリシー] タブで、[特定のグループを許可] をクリックします。
9. [ポリシー] の下で、<パラメーター> リンクをクリックします。
10. [追加] をクリックし、[グループの選択] ボックスに「Research」と入力して、[OK] をクリックします。再び [OK] をクリックし、[グループの選択] ダイアログ ボックスを閉じます。
11. [OK] をクリックし、[アクセス制御ポリシー] ダイアログ ボックスを閉じます。
12. [A. Datum Corporation Test App] を右クリックし、[要求発行ポリシーの編集] をクリックします。
13. [発行変換規則] タブで、[Pass through UPN] をクリックし、[規則の編集] をクリックします。
14. [入力方向の要求の種類] の一覧で、[UPN] が選択されていることを確認します。
15. [特定の要求値だけをパス スルーする] をクリックします。
16. [入力方向の要求の値] ボックスに「@adatum.com」と入力します。
17. [規則言語の表示] をクリックします。
18. [OK] を 2 回クリックします。
19. A. Datum Corporation Test App の要求発行ポリシーの編集ウィンドウで、[OK] をクリックします。

レッスン 4
Web アプリケーション プロキシの概要

目次

質問と解答

質問 : Web アプリケーション プロキシの構成に関する文章のうち、正しいものを次から選んでください (該当するものをすべて選択してください)。

( ) Web アプリケーション プロキシをインストールするには、組織内に AD FS が実装済みである必要があります。

( ) Web アプリケーション プロキシをインストールするには、組織内に AD FS が実装済みである必要はありません。

( ) 公開する各アプリケーションについて、外部 URL と内部 URL を構成する必要があります。

( ) 外部 URL を定義する際、内部 URL のホスト名を含む証明書も選択する必要があります。

( ) 外部 URL を定義する際、外部 URL のホスト名を含む証明書も選択する必要があります。

解答 :

(√) Web アプリケーション プロキシをインストールするには、組織内に AD FS が実装済みである必要があります。

( ) Web アプリケーション プロキシをインストールするには、組織内に AD FS が実装済みである必要はありません。

(√) 公開する各アプリケーションについて、外部 URL と内部 URL を構成する必要があります。

( ) 外部 URL を定義する際、内部 URL のホスト名を含む証明書も選択する必要があります。

(√) 外部 URL を定義する際、外部 URL のホスト名を含む証明書も選択する必要があります。

フィードバック :

2 番目の選択肢は誤りです。Web アプリケーション プロキシをインストールするには、組織内に AD FS が実装されている必要があります。

4 番目の選択肢は誤りです。証明書は、外部 URL のホスト名を含む必要があります。

参考資料

Web アプリケーション プロキシを使用するシナリオ

参考資料 : IWA と Kerberos の制約付き委任を使用するための Web サイトの構成については、次のサイトを参照してください。
Configure a site to use Integrated Windows authentication
http://aka.ms/Nbsbll

参考資料 : 負荷分散された Exchange Server の Kerberos 認証の構成については、次のサイトを参照してください。
負荷分散されたクライアント アクセス サーバーの Kerberos 認証の構成
https://technet.microsoft.com/ja-jp/library/ff808312(v=exchg.150).aspx

参考資料 : Web アプリケーション プロキシを介した RD ゲートウェイの公開については、次のサイトを参照してください。
Publishing Applications with SharePoint, Exchange and RDG
http://aka.ms/C7f0wn

Web アプリケーション プロキシのインストールと構成

参考資料 : AD FS で使用可能なすべての更新プログラムについては、次のサイトを参照してください。
Active Directory フェデレーション サービス (AD FS) 用更新プログラム
https://technet.microsoft.com/ja-jp/library/mt126278.aspx

デモンストレーション : Web アプリケーション プロキシのインストールと構成

デモンストレーションの手順

Web アプリケーション プロキシをインストールする

1. LON-SVR2 で、サーバー マネージャーを開き、[管理]、[役割と機能の追加] の順にクリックします。
2. 役割と機能の追加ウィザードの [開始する前に] ページで、[次へ] をクリックします。
3. [インストールの種類の選択] ページで、[次へ] をクリックします。
4. [対象サーバーの選択] ページで、[次へ] をクリックします。
5. [サーバーの役割の選択] ページで、[リモート アクセス] チェック ボックスをオンにし、[次へ] をクリックします。
6. [機能の選択] ページで、[次へ] をクリックします。
7. [リモート アクセス] ページで、[次へ] をクリックします。
8. [役割サービスの選択] ページで、[Web アプリケーション プロキシ] をクリックします。
9. 役割と機能の追加ウィザードで、[機能の追加] をクリックします。
10. [役割サービスの選択] ページで、[次へ] をクリックします。
11. [インストール オプションの確認] ページで、[インストール] をクリックします。
12. [インストールの進行状況] ページで、[閉じる] をクリックします。

AD FS サーバーから証明書をエクスポートする

1. LON-DC1 の スタート画面で「mmc」と入力し、Enter キーを押します。
2. Microsoft 管理コンソールで、[ファイル]、[スナップインの追加と削除] の順にクリックします。
3. スナップインの追加と削除ウィンドウで、[利用できるスナップイン] 列の [証明書] をダブルクリックします。
4. 証明書スナップイン ウィンドウで、[コンピューター アカウント]、[次へ] の順にクリックします。
5. コンピューターの選択ウィンドウで、[ローカル コンピューター (このコンソールを実行しているコンピューター)]、[完了] の順にクリックします。
6. スナップインの追加と削除ウィンドウで、[OK] をクリックします。
7. Microsoft 管理コンソールで、[証明書 (ローカル コンピューター)]、[個人] の順に展開し、[証明書] をクリックします。
8. [adfs.adatum.com] を右クリックし、[すべてのタスク] をポイントして、[エクスポート] をクリックします。
9. 証明書のエクスポート ウィザードで、[次へ] をクリックします。

10. [秘密キーのエクスポート] ページで、[はい、秘密キーをエクスポートします]、[次へ] の順にクリックします。
11. [エクスポート ファイルの形式] ページで、[次へ] をクリックします。
12. [セキュリティ] ページで、[パスワード] チェック ボックスをオンにします。
13. [パスワード] の [パスワードの確認入力] ボックスに「Pa55w.rd」と入力し、[次へ] をクリックします。
14. [エクスポートするファイル] ページで、[ファイル名] ボックスに「C:¥adfs.pfx」と入力し、[次へ] をクリックします。
15. [証明書のエクスポート ウィザードの完了] ページで、[完了] をクリックし、[OK] をクリックして成功のメッセージを閉じます。
16. 変更を保存せずに Microsoft 管理コンソールを閉じます。

Web アプリケーション プロキシ サーバーへ証明書をインポートする

1. LON-SVR2 の スタート画面で「mmc」と入力し、Enter キーを押します。
2. Microsoft 管理コンソールで、[ファイル]、[スナップインの追加と削除] の順にクリックします。
3. スナップインの追加と削除ウィンドウで、[利用できるスナップイン] 列の [証明書] をダブルクリックします。
4. 証明書スナップイン ウィンドウで、[コンピューター アカウント]、[次へ] の順にクリックします。
5. コンピューターの選択ウィンドウで、[ローカル コンピューター (このコンソールを実行しているコンピューター)]、[完了] の順にクリックします。
6. スナップインの追加と削除ウィンドウで、[OK] をクリックします。
7. Microsoft 管理コンソールで、[証明書 (ローカル コンピューター)] を展開し、[個人] をクリックします。
8. [個人] を右クリックし、[すべてのタスク] をポイントして、[インポート] をクリックします。
9. 証明書のインポート ウィザードで、[次へ] をクリックします。
10. [インポートするファイル] ページで、[ファイル名] ボックスに「¥¥LON-DC1¥c$¥adfs.pfx」と入力し、[次へ] をクリックします。
11. [秘密キーの保護] ページで、[パスワード] ボックスに「Pa55w.rd」と入力します。
12. [このキーをエクスポート可能にする] チェック ボックスをオンにして、[次へ] をクリックします。
13. [証明書ストア] ページで、[証明書をすべて次のストアに配置する] をクリックします。
14. [証明書ストア] ボックスで、[個人] を選択し、[次へ] をクリックします。
15. [証明書のインポート ウィザードの完了] ページで、[完了] をクリックします。
16. [OK] をクリックし、成功のメッセージを閉じます。
17. 変更を保存せずに Microsoft 管理コンソールを閉じます。

Web アプリケーション プロキシを構成する

1. LON-SVR2 のサーバー マネージャーで、[通知] アイコンをクリックし、[Web アプリケーション プロキシ ウィザードを表示する] をクリックします。
2. Web アプリケーション プロキシの構成ウィザードの [ようこそ] ページで、[次へ] をクリックします。
3. [フェデレーション サーバー] ページで、次の情報を入力し、[次へ] をクリックします。
    - フェデレーション サービス名 : adfs.adatum.com

- ユーザー名 : Adatum¥Administrator
- パスワード : Pa55w.rd

4. [AD FS プロキシ証明書] ページの [AD FS プロキシにより使用される証明書を選択してください] ダイアログ ボックスで、[adfs.adatum.com] を選択し、[次へ] をクリックします。
5. [確認] ページで、[構成] をクリックします。
6. [結果] ページで、[閉じる] をクリックします。

演習の復習の質問と解答

演習 : AD FS の実装

質問と解答

質問 : AD FS サービスのホスト名として使用するために、adfs.adatum.com を構成することが重要な理由は何ですか。

解答 : AD FS サーバーに既存のサーバーのホスト名を使用すると、サーバー ファームにそれ以外のサーバーを追加できません。サーバー ファーム内のすべてのサーバーは、AD FS サービスを提供する際、同一のホスト名を共有する必要があります。AD FS プロキシ サーバーも、AD FS サーバーのホスト名を使用します。

質問 : AD FS が適切に機能しているかどうかを、どのようにしてテストできますか。

解答 : AD FS サーバーの https://hostname/federationmetadata/2007-06/federationmetadata.xml に正常にアクセスできる場合、AD FS は適切に機能しています。

復習とまとめ

ベスト プラクティス

以前のバージョンの AD FS では、セキュリティ構成ウィザード (SCW) を使用して、AD FS 固有のセキュリティのベスト プラクティスをフェデレーション サーバーとフェデレーション サーバー プロキシのコンピューターに適用するのが一般的でした。Windows Server 2016 では、既定で機能のセキュリティが強化されているため、SCW は削除されました。そのため、特定のセキュリティ設定を制御する必要がある場合は、グループ ポリシーまたは Security Compliance Manager (http://aka.ms/Ncq8jm を参照) を使用することができます。

復習問題

質問 : 組織は AD FS を実装しようと計画しています。これは、内部クライアントのみが AD FS を使用して内部アプリケーションにアクセスすることを意味します。ただし、後で、自宅にいるユーザーに対して、AD FS によりセキュリティが強化された Web ベースのアプリケーションへのアクセスを提供する必要があります。サード パーティ CA から証明書をいくつ取得する必要がありますか。

解答 : 信頼される必要がある AD FS 証明書は、サービス通信証明書のみであるため、サード パーティ CA から 1 つだけ証明書を取得する必要があります。トークン署名証明書とトークン暗号化解除証明書は、自己署名証明書の使用を続けることができます。

質問 : あなたの組織では、単一の AD FS サーバーと単一の Web アプリケーション プロキシを実装しました。AD FS は、最初は単一のアプリケーションに対してのみ使用されていましたが、今は複数の業務に不可欠なアプリケーションに使用されています。可用性の高い AD FS を構成する必要があります。

AD FS のインストール時に、WID の使用を選択しました。このデータベースを高可用性構成で使用できますか。

解答 : はい、Windows Internal Database (WID) を使用して、最大 5 台の AD FS サーバーをサポートできます。最初の AD FS サーバーは、プライマリ サーバーとなり、そこですべての構成変更がおこなわれます。プライマリ サーバーでの変更は、他の AD FS サーバーへレプリケートされます。

第 11 章

AD RMS の実装と管理

目次

レッスン 1
AD RMS の概要

目次

質問と解答

質問 : ユーザーが RAC を受け取るのはいつですか。

解答 : ユーザーが初めて AD RMS で保護されたコンテンツにアクセスするか、保護されたドキュメントを作成するなどの AD RMS タスクを実行すると発行されます。

質問 : Azure RMS は、サーバーにローカルに展開されます。

(　) 正

(　) 誤

解答 :

(　) 正

(√) 誤

フィードバック :

Azure RMS はクラウド ベースのサービスであり、ローカルに展開する必要はありません。

参考資料

Azure RMS とは

参考資料 : 無料の RMS 共有アプリケーションを Microsoft からダウンロードするには、次のサイトを参照してください。
ダウンロード センター
https://www.microsoft.com/ja-jp/download/details.aspx?id=40857

AD RMS、Azure RMS、および Azure RMS for Office 365 の比較

参考資料 : 詳細については、次のサイトを参照してください。
Azure Information Protection と AD RMS の比較
http://aka.ms/sndlw0

レッスン 2
AD RMS インフラストラクチャの展開および管理

目次

質問と解答

質問 : AD RMS クラスターを実装するために必要なコンポーネントは何ですか。

( ) Office

( ) サービス アカウント

( ) データベース

( ) AD FS (Active Directory フェデレーション サービス)

( ) SSL (Secure Sockets Layer) 証明書

解答 :

( ) Office

(√) サービス アカウント

(√) データベース

( ) AD FS (Active Directory フェデレーション サービス)

( ) SSL (Secure Sockets Layer) 証明書

フィードバック :

AD RMS を実装するために作成されたサービス アカウント、WID データベースまたは SQL Server データベースが必要です。

質問 : AD DS から AD RMS クラスターを削除する際に、最初におこなう必要があることは何ですか。

解答 : AD RMS サーバーを削除する前に、そのサーバーを使用停止にする必要があります。

参考資料

AD RMS の監視

参考資料 : 詳細については、次のサイトを参照してください。
Monitoring Scenarios
http://aka.ms/Pyumg7

デモンストレーション : AD RMS クラスターの最初のサーバーのインストール

デモンストレーションの手順

サービス アカウントを構成する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. [Adatum (ローカル)] を選択して右クリックし、[新規] をクリックして、[組織単位] をクリックします。
3. [組織単位の作成] ダイアログ ボックスで、[名前] ボックスに「ServiceAccounts」と入力し、[OK] をクリックします。

4. [Service Accounts] 組織単位 (OU) を右クリックし、[新規] をクリックして、[ユーザー] をクリックします。
5. [ユーザーの作成] ダイアログ ボックスで、次の詳細情報を入力し、[OK] をクリックします。
   - 名 : ADRMSSVC
   - ユーザー UPN ログオン : ADRMSSVC
   - ユーザー SAM アカウント名ログオン : Adatum¥ADRMSSVC
   - パスワード : Pa55w.rd
   - パスワードの確認入力 : Pa55w.rd
   - その他のパスワード

     パスワードを無期限にする : 有効
     ユーザーはパスワードを変更できない : 有効

ドメイン ネーム システム (DNS) を準備する

1. サーバー マネージャーで、[ツール]、[DNS] の順にクリックします。
2. DNS マネージャー コンソールで、[LON-DC1]、[前方参照ゾーン] の順に展開します。
3. [Adatum.com] を右クリックし、[新しいホスト (A または AAAA)] をクリックします。
4. [新しいホスト] ダイアログ ボックスで、次の情報を入力し、[ホストの追加] をクリックします。
   - 名前 : adrms
   - IP アドレス : 172.16.0.21

   [OK] をクリックし、[完了] をクリックします。
5. DNS マネージャー コンソールを閉じます。

AD RMS の役割をインストールする

1. LON-SVR1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. [スタート]、[サーバー マネージャー] の順にクリックします。
3. サーバー マネージャーで、[管理]、[役割と機能の追加] の順にクリックします。
4. 役割と機能の追加ウィザードで、[次へ] を 3 回クリックします。
5. [サーバーの役割の選択] ページで、[Active Directory Rights Management サービス] をクリックします。
6. [役割と機能の追加ウィザード] ダイアログ ボックスで、[機能の追加]、[次へ] を 4 回、[インストール] の順にクリックし、インストールが完了したら、[閉じる] をクリックします。

AD RMS を構成する

1. LON-SVR1 のサーバー マネージャーで、[AD RMS] ノードをクリックします。
2. [LON-SVR1 で Active Directory Rights Management サービスの構成が必要です] の [その他] をクリックします。
3. [すべてのサーバー タスクの詳細と通知] ページで、[追加の構成を行います] をクリックします。
4. [AD RMS] ページの AD RMS 構成 : LON-SVR1.adatum.com ウィンドウで、[次へ] をクリックします。
5. [AD RMS クラスター] ページで、[新しい AD RMS ルート クラスターを作成する]、[次へ] の順にクリックします。

6. [構成データベース] ページで、[このサーバーの Windows Internal Database を使用する]、[次へ] の順にクリックします。
7. [サービス アカウント] ページで、[指定] をクリックします。
8. [Windows セキュリティ] ダイアログ ボックスで、次の詳細情報を入力し、[OK]、[次へ] の順にクリックします。
   - ユーザー名 : ADRMSSVC
   - パスワード : Pa55w.rd

注 : ADRMSSVC サービス アカウントを使用しようとするとエラーが発生する場合は、LON-DC1 と LON-DC2 の間でレプリケーションを強制的におこない、もう一度この手順を実行します。

9. [暗号化モード] ページで、[暗号化モード 2]、[次へ] の順にクリックします。
10. [クラスター キーの格納] ページで、[AD RMS の一元管理型のキーの格納を使用する]、[次へ] の順にクリックします。
11. [クラスター キー パスワード] ページで「Pa55w.rd」と 2 回入力し、[次へ] をクリックします。
12. [クラスター Web サイト] ページで、[Default Web Site] が選択されていることを確認し、[次へ] をクリックします。
13. [クラスター アドレス] ページで、次の情報を入力し、[次へ] をクリックします。
    - 接続の種類 : 暗号化されない接続 (http://) を使用する
    - 完全修飾ドメイン名 : adrms.adatum.com
    - ポート : 80
14. [ライセンサー証明書] ページで「AdatumADRMS」と入力し、[次へ] をクリックします。
15. [SCP の登録] ページで、[SCP をすぐに登録する]、[次へ] の順にクリックします。
16. [確認] ページで、[インストール] をクリックし、インストールが完了したら、[閉じる] をクリックします。
17. スタート画面で、[Administrator] をクリックし、[サインアウト] をクリックします。

注 : AD RMS を管理する前に、サインアウトする必要があります。

レッスン 3
AD RMS のコンテンツ保護の構成

目次

質問と解答

質問 : スーパー ユーザー グループが保有するアクセス許可の種類は何ですか。

解答 : スーパー ユーザー グループのメンバーには、スーパー ユーザー グループが構成されている AD RMS クラスターで発行されるすべての使用ライセンスに対する完全な所有者権限が与えられます。

参考資料

除外ポリシーとは

参考資料 : 詳細については、次のサイトを参照してください。
除外ポリシーを有効にする
https://technet.microsoft.com/ja-jp/library/cc730687.aspx

デモンストレーション : 権利ポリシー テンプレートの作成

デモンストレーションの手順

1. LON-SVR1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. サーバー マネージャーを開き、[ツール]、[Active Directory Rights Management サービス] の順にクリックします。
3. AD RMS コンソールで、[LON-SVR1]、[権利ポリシー テンプレート] ノードの順にクリックします。
4. 操作ウィンドウで、[配布権利ポリシー テンプレートの作成] をクリックします。
5. 配布権利ポリシー テンプレートの作成ウィザードの [テンプレート識別情報の追加] ページで、[追加] をクリックします。
6. [新しいテンプレート識別情報の追加] ページで、次の情報を入力し、[追加]、[次へ] の順にクリックします。
   - 言語 : 日本語 (日本)
   - 名前 : ReadOnly
   - 説明 : 読み取り専用アクセス。コピーまたは印刷はできない。
7. [ユーザー権利の追加] ページで、[追加] をクリックします。
8. [ユーザーまたはグループの追加] ページで「executives@adatum.com」と入力し、[OK] をクリックします。
9. [executives@adatum.com] を選択し、[executives@adatum.com の権利] の一覧にある [表示] を選択します。
10. [所有者 (作成者) に無期限のフル コントロールの権利を付与する] が選択されていることを確認し、[次へ] をクリックします。
11. [有効期限ポリシーの指定] ページで、次の設定を選択し、[次へ] をクリックします。
    - コンテンツの有効期限 : 有効期間 (日数) を指定する : 7
    - 使用ライセンスの有効期限 : 有効期間 (日数) を指定する : 7

12. [拡張ポリシーの指定] ページで、[コンテンツを利用するたびに新しい使用ライセンスを要求する (クライアント側のキャッシュを無効にする)]、[次へ]、[完了] の順にクリックします。

デモンストレーション : アプリを除外する除外ポリシーの作成

デモンストレーションの手順

1. LON-SVR1 で、AD RMS コンソールに切り替え、[除外ポリシー] ノードをクリックして、[アプリケーションの除外一覧の管理] をクリックします。
2. 操作ウィンドウで、[アプリケーションの除外を有効にする] をクリックします。
3. 操作ウィンドウで、[アプリケーションの除外] をクリックします。
4. [アプリケーションの除外] ダイアログ ボックスで、次の情報を入力し、[完了] をクリックします。
    - アプリケーション ファイル名 : Powerpnt.exe
    - 最小バージョン : 14.0.0.0
    - 最大バージョン : 16.0.0.0

演習の復習の質問と解答

演習 : AD RMS インフラストラクチャの実装

質問と解答

質問 : IRM サービスと AD RMS の役割を併用できるようにするために、どのような手順をおこないますか。

解答 : AD RMS を展開する前に、AD RMS サーバーのサーバー証明書を構成する必要があります。

復習とまとめ

ベスト プラクティス

- AD RMS を展開する前に、組織のビジネス要件を分析し、必要なテンプレートを作成します。ユーザーとミーティングし、AD RMS 機能を説明し、ユーザーがどのような種類のテンプレートを必要としているかを調査します。
- スーパー ユーザー グループのメンバーは厳密に管理します。このグループのユーザーはすべての保護されたコンテンツにアクセスできます。

復習問題

質問 : AD RMS を構成する際、AD RMS サーバーにインストールされた SSL 証明書を保有する利点は何ですか。

解答 : SSL により、クライアントと AD RMS サーバー間の接続を保護することができます。

質問 : 組織のメンバーではない外部の契約者である 5 人のユーザーに、AD RMS で保護されたコンテンツへのアクセス許可を付与する必要があります。このアクセス許可を提供するためには、どのような手段を使いますか。

解答 : 外部の契約者に RAC を提供するためには、Microsoft アカウントを使用します。

質問 : ユーザーが AD RMS テンプレートを使用して PowerPoint のコンテンツを保護することを防ぎたいと考えています。それを実現するためには、どのような手順をおこないますか。

解答 : PowerPoint のアプリケーションの除外を構成する必要があります。

第 12 章

AD DS と Microsoft Azure AD の同期の実装

目次

レッスン 1
ディレクトリ同期の計画と準備

目次

質問と解答

質問 : ディレクトリ同期を実装すると、ユーザー アカウントとグループは、ローカル AD DS から Azure AD へ移動します。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

ディレクトリ同期では、オブジェクトを移動しません。ローカルの AD DS から、属性のサブセットを含めてオブジェクトをコピーし、Azure AD に新しいオブジェクトを作成します。

参考資料

ディレクトリ同期の計画

参考資料 : 詳細については、次のサイトを参照してください。
Azure Hybrid Identity Design Considerations Guide
http://aka.ms/ibuqek

ディレクトリ同期の前提と準備

参考資料 : 詳細については、次のサイトを参照してください。
Office 365 で "会社の同期可能なオブジェクト数を超えました。" というエラー メッセージを受け取った場合に、ディレクトリ サービスの割当値を拡張する方法
http://aka.ms/r4x1q4

レッスン 2
Azure AD Connect によるディレクトリ同期の実装

目次

質問と解答

質問 : AD DS と Azure AD 間の同期を実装すると、AD DS オブジェクトはどこでマスター化されますか。

解答 : Active Directory 同期のために Azure AD Connect を展開した場合、Active Directory ユーザーとコンピューターや Windows PowerShell などのツールを使用してオンプレミス AD DS 内のオブジェクトをマスター化します。権限ソースはオンプレミス AD DS となります。

参考資料

Azure AD Connect のカスタム同期

参考資料 : 詳細については、次のサイトを参照してください。
代替ログイン ID を構成します
http://aka.ms/nqh5gc

Azure AD Connect の監視機能

参考資料 : 詳細については、次のサイトを参照してください。
クラウド内のオンプレミスの ID インフラストラクチャと同期サービスの監視
https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-aadconnect-health/

デモンストレーション : Azure AD Connect のインストールと構成

デモンストレーションの手順

1. LON-SVR1 で、Internet Explorer を開き、http://www.microsoft.com/en-us/download/details.aspx?id=47594 を参照します。
2. [Microsoft Azure Active Directory Connect] ページで、[Download] をクリックします。
3. [実行] をクリックします。ダウンロードが完了するまで、数分待ちます。

注 : ダウンロードの開始で問題が発生した場合は、https://download.microsoft.com の Web サイトを信頼済みサイトに追加してください。

4. Microsoft Azure Active Directory Connect ウィザードの [Azure AD Connect へようこそ] ページで、[ライセンス条項とプライバシーに関する声明に同意します] チェック ボックスをオンにし、[続行] をクリックします。
5. [簡単設定] ページで、[カスタマイズ] をクリックします。
6. [必須コンポーネントのインストール] ページで、使用可能なオプションを確認します。ただし、変更せずに、[インストール] をクリックします。
7. [ユーザー サインイン] ページで、[パスワード同期] を選択し、[次へ] をクリックします。

8. [Azure AD に接続] ページで、[ユーザー名] ボックスにアカウント ユーザー名として「SYNC@yourdomain.onmicrosoft.com」、[パスワード] ボックスに「Pa55w.rd」と入力して、[次へ] をクリックします。接続が確立されるまでに数分かかる場合があります。
9. [ディレクトリの接続] ページで、[ユーザー名] ボックスにアカウント ユーザー名として「Adatum¥Administrator」、[パスワード] ボックスに「Pa55w.rd」と入力します。[ディレクトリの追加]、[次へ] の順にクリックします。
10. [Azure AD サインインの構成] ページで、[検証済みのドメインなしで続行する] チェック ボックスをオンにし、[次へ] をクリックします。
11. [ドメインと OU のフィルタリング] ページで、[次へ] をクリックします。
12. [一意のユーザー識別] ページで、使用可能なオプションを確認し、説明します。ただし、変更はしないでください。
13. [次へ] をクリックします。
14. [ユーザーおよびデバイスのフィルタリング] ページで、[選択した項目の同期] をクリックします。[グループ] ボックスに「Research」と入力し、[解決] をクリックします。[解決] をクリックした後、緑色のチェック マークが表示されることを確認します。
15. [次へ] をクリックします。
16. [オプション機能] ページで、[パスワードの書き戻し] を選択し、その他のオプションを説明して、[次へ] をクリックします。
17. [構成の準備完了] ページで、[インストール] をクリックし、インストールが完了したら、[終了] をクリックします。
18. ローカルの AD DS と Azure AD のオブジェクトの同期が開始されます。このプロセスが完了するまで 5 分ほど待ちます。
19. ホスト コンピューターで Internet Explorer を開き、https://manage.windowsazure.com を参照して、Azure クラシック ポータルを開きます。
20. 試用版サブスクリプションに関連付けられている Microsoft アカウントを使用して、Azure にサインインします。Azure クラシック ポータルが開いたら、[Adatum] ディレクトリをクリックします。
21. [adatum] ページで、[ユーザー] タブをクリックします。

注 : ローカルの AD DS からユーザー アカウントを参照できることを確認します。ローカルの adatum.com ドメインから、Research ユーザーを参照することができます。

22. ホスト コンピューターで、Internet Explorer を最小化します。
23. LON-SVR1 で、[スタート] をクリックし「Synchronization」と入力します。
24. 検索ウィンドウで、[Synchronization Service] をクリックします。
25. LON-SVR1 の Synchronization Service Manager ウィンドウで、[Operations] タブをクリックします。
26. [Export]、[Delta Synchronization]、[Delta Import] のタスクが表示されることを確認します。すべてのタスクの [Start Time] と [End Time] の列に現在の時刻と日付が表示されていることを確認します。また、[Status] 列で最新のタスクが成功 (success) していることを確認します。
27. Synchronization Service Manager を閉じます。

レッスン 3
ディレクトリ同期による ID の管理

目次

質問と解答

質問 : クラウド ベースとオンプレミスのサービスの両方のための SSO を実現する場合、何を展開する必要がありますか。該当するものをすべて選択してください。

(　) Azure AD Connect Health

(　) AD FS (Active Directory フェデレーション サービス)

(　) Azure AD Connect

(　) Office 365

(　) Azure AD

解答 :

(　) Azure AD Connect Health

(√) AD FS (Active Directory フェデレーション サービス)

(√) Azure AD Connect

(　) Office 365

(　) Azure AD

質問 : ローカルに展開された AD DS と Azure AD 間のフェデレーション、および AD FS を実装している場合は、Azure AD Connect を使用する必要はありません。

(　) 正

(　) 誤

解答 :

(　) 正

(√) 誤

フィードバック :

オンプレミス AD DS では、認証を実行し、その情報を Azure AD に渡します。Azure AD のパスワードは使用されません。ただし、両方のディレクトリ サービスのアカウントが一致している必要があります。そのため、Azure AD Connect と AD FS の両方を使用する必要があります。

参考資料

ディレクトリ同期の変更

参考資料 : 詳細については、次のサイトを参照してください。
Azure AD Connect Sync: フィルター処理の構成
https://azure.microsoft.com/ja-jp/documentation/articles/active-directory-aadconnectsync-configure-filtering/

ディレクトリ同期の監視

参考資料 : 詳細については、次のサイトを参照してください。
Azure Active Directory Cmdlets
http://aka.ms/pfsm1x

ディレクトリ同期のトラブルシューティング

参考資料 : 詳細については、次のサイトを参照してください。
オンプレミス ID と Azure Active Directory の統合
http://aka.ms/cdm2kk

参考資料 : 詳細については、次のサイトを参照してください。
Azure Active Directory 同期ツールのインストールと構成ウィザードのエラー メッセージをトラブルシューティングする方法
https://support.microsoft.com/ja-jp/kb/2684395

演習の復習の質問と解答

演習 : ディレクトリ同期の構成

質問と解答

質問 : Azure AD Connect を構成する前に何をする必要がありますか。

解答 : Azure AD で同期アカウントを作成してから、ドメインを Azure AD テナントに追加する必要があります。

質問 : Azure AD Connect の同期スケジュールを変更するには、どのコマンドレットを使用する必要がありますか。

解答 : Azure AD Connect をインストールするコンピューターで、Set-ADSyncScheduler コマンドレットを使用する必要があります。

復習とまとめ

ベスト プラクティス

- より簡単な環境では、Azure AD Connect の簡単設定を使用します。
- ユーザーが、少なくとも 2 つの認証方法で、パスワードのセルフサービスによるリセット機能を使用できるようにします。
- 書き戻し機能の使用を検討します。
- Azure AD Premium サブスクリプションをお持ちの場合は、Azure AD Connect Health を実装します。

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
ディレクトリ同期のフィルター処理が機能していない。	ディレクトリ同期ツールの最新バージョンを使用することが重要です。ただし、ツールを新しいバージョンにアップグレードする際、既存のフィルターとその他の管理エージェントのカスタマイズがすべて、自動的に新しいインストールへインポートされる訳ではありません。新しいバージョンにアップグレードする場合、アップグレードしてから最初の同期サイクルを実行する前に、必ず、フィルター処理の構成を手動で再適用する必要があります。
Azure AD Connect をインストールした後、Synchronization Service Manager を開くと、「Unable to connect to the Synchronization Service」というエラー メッセージが表示される。	適切な Azure AD Connect のドメイン ユーザー アカウントを ADSyncAdmins グループに追加し、サインアウトしてから、再度サインインします。 Azure AD Connect のインストール中に、サインインに使用されたドメイン ユーザー アカウントが、自動的に ADSyncAdmins グループに追加されます。ただし、Synchronization Service Manager を正常に開くためには、サインアウトしてから、再度サインインする必要があります。

実際の問題とシナリオ

ディレクトリ同期は、オンプレミス AD DS オブジェクトと Azure AD のサービス間とのリンクです。そのため、運用環境を展開した後で、Azure AD Connect または Synchronization Service Manager に変更を加える場合は注意が必要です。例えば、フィルター処理の小さなミスであっても、Office 365 のすべてのユーザー メールボックスが誤って削除される事態を招くことがあります。

例えば、テスト環境では、別の Azure AD テナント (試用版) に接続されている別のディレクトリ同期サーバーで加えられたすべての変更をテストすることができます。さらに、Synchronization Service Manager で各管理エージェントに対して手動で実行プロファイルを開始し、Azure AD にエクスポートする前の保留中の操作を監視する必要があります。場合によっては、削除可能回数の上限を含む Azure AD にエクスポートするための実行プロファイルを新しく作成することが推奨されます。

復習問題

質問 : Azure AD からオンプレミス AD DS へオブジェクトを同期するには、どの機能を構成する必要がありますか。

解答 : 書き戻し機能を展開する必要があります。現在、パスワードの書き戻し、グループの書き戻し、およびデバイスの書き戻しを使用することができます。

ツール

次の表に、この章で参照しているツールを一覧表示します。

ツール	用途	アクセス方法
Azure AD Connect	AD DS と Azure AD 間の信頼を確立します。	Microsoft ダウンロード センター
Azure AD Connect Health	AD DS の Azure AD 同期の正常性を監視します。	Azure クラシック ポータル
Azure クラシック ポータル	Azure AD を管理します。	http://aka.ms/n2l3cb

第 13 章

AD DS の監視、管理、および回復

目次

レッスン 1
AD DS の監視

目次

参考資料

監視ツールの概要

参考資料 : 詳細については、次のサイトを参照してください。
Using PowerShell To Gather Performance Data
http://aka.ms/F8mxnr

デモンストレーション : AD DS の監視

デモンストレーションの手順

パフォーマンス モニターを構成して AD DS を監視する

1. LON-DC1 に切り替えます
2. サーバー マネージャーで、[ツール]、[パフォーマンス モニター] の順にクリックします。
3. [モニター ツール] ノードの下で、[パフォーマンス モニター] をクリックします。
4. ツール バーで [追加] (緑色の「+」) をクリックし、オブジェクトとカウンターを追加します。
5. [カウンターの追加] ダイアログ ボックスで、[使用可能なカウンター] リストで、[Directory Services] オブジェクトを展開します。
6. DRA Inbound Bytes Total/sec カウンターをクリックし、[追加] をクリックします。
7. 手順 6 を繰り返し、次のカウンターも追加します。
   - DirectoryServices¥DRA Outbound Bytes Total/sec
   - DirectoryServices¥DS Threads In Use
   - DirectoryServices¥DS Directory Reads/sec
   - DirectoryServices¥DS Directory Writes/sec
   - DirectoryServices¥DS Directory Searches/sec
   - NTDS¥DRA Inbound Objects/sec
   - NTDS¥DRA Pending Replication Synchronizations
   - Security System-Wide Statistics¥NTLM Authentications
   - Security System-Wide Statistics¥Kerberos Authentications
8. [OK] をクリックます。
9. グラフの下のカウンター リストで、[DS Directory Searches/sec] を選択します。
10. ツール バーの [ハイライト] をクリックします。選択されたカウンターがハイライトされ、カウンターのパフォーマンスを簡単に観察できるようになります。
11. 再度ツール バーの [ハイライト] をクリックし、ハイライトをオフにします。

データ コレクター セットを作成する

1. コンソール ツリーで、[パフォーマンス]、[モニター ツール] の順に展開し、[パフォーマンス モニター] をクリックします。[パフォーマンス モニター] を右クリックし、[新規作成] をポイントして、[データ コレクター セット] をクリックします。
2. [新しいデータ コレクター セットを作成します。] ダイアログ ボックスで、[名前] ボックスに「Custom ADDS Performance Counters」と入力し、[次へ] をクリックします。
3. データ コレクター セットを保存する既定のルート ディレクトリを確認し、[次へ]、[完了] の順にクリックします。

データ コレクター セットを開始する

1. コンソール ツリーで、[データ コレクター セット]、[ユーザー定義] の順に展開し、[ユーザー定義] をクリックします。
2. [Custom ADDS Performance Counters] を右クリックし、[開始] をクリックします。[Custom ADDS Performance Counters] ノードが自動的に選択されることを確認します。

注 : データ コレクター セット内の個々のデータ コレクターを特定できることを確認してください。この場合、データ コレクター セットには 1 つのデータ コレクター ([システム モニター ログ] パフォーマンス カウンター) のみが含まれています。また、データ コレクターからの出力が保存されている場所を確認することもできます。

3. コンソール ツリーで [Custom ADDS Performance Counters] データ コレクター セットを右クリックし、[停止] をクリックします。

レポートの結果データを分析する

1. コンソール ツリーで、[レポート]、[ユーザー定義]、[Custom ADDS Performance Counters] の順に展開し、[システム モニター ログ.blg] をダブルクリックします。
2. ログのパフォーマンス カウンターのグラフを確認します。

レッスン 2
Active Directory データベースの管理

目次

デモンストレーション : データベース管理の実行

デモンストレーションの手順

AD DS を停止する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[サービス] の順にクリックします。
2. サービス コンソールで、[Active Directory Domain Services] を右クリックし、[停止] をクリックします。
3. [別のサービスの停止] ダイアログ ボックスで、[はい] をクリックします。

Active Directory データベースのオフライン最適化を実行する

1. LON-DC1 で、[スタート]、[Windows PowerShell] の順にクリックします。
2. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
Ntdsutil.exe
```

3. 次のコマンドを入力し、Enter キーを押します。

```
activate instance NTDS
```

4. 次のコマンドを入力し、Enter キーを押します。

```
files
```

5. 次のコマンドを入力し、Enter キーを押します。

```
compact to C:¥
```

オフラインの Active Directory データベースの整合性をチェックする

1. 次のコマンドを入力し、Enter キーを押します。

```
Integrity
```

2. 次のコマンドを入力し、Enter キーを押します。

```
quit
```

3. 次のコマンドを入力し、Enter キーを押します。

```
quit
```

4. Windows PowerShell ウィンドウを閉じます。

AD DS を開始する

1. タスク バーで [サーバー マネージャー] アイコンをクリックします。
2. サーバー マネージャーで、[ツール]、[サービス] の順にクリックします。
3. サービス コンソールで、[Active Directory Domain Services] を右クリックし、[開始] をクリックします。
4. Active Directory ドメイン サービスの [状態] 列に [実行中] と表示されていることを確認します。

レッスン 3

AD DS の Active Directory バックアップと回復のオプションおよびその他の ID とアクセスのソリューション

目次

デモンストレーション : Active Directory のごみ箱の実装

デモンストレーションの手順

Active Directory のごみ箱を有効にする

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory サイトとサービス] の順にクリックします。
2. [Sites]、[Default-First-Site-Name]、[Servers]、[LON-DC1] の順に展開し、[NTDS Settings] をクリックします。
3. [<自動生成>] を右クリックし、[今すぐレプリケート]、[OK] の順にクリックします。
4. [LON-DC2] を展開し、[NDTS Settings] をクリックします。
5. [<自動生成>] を右クリックし、[今すぐレプリケート]、[OK] の順にクリックします。
6. サーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
7. [Adatum (ローカル)] をクリックします。
8. タスク ウィンドウで、[ごみ箱の有効化] をクリックします。警告メッセージ ボックスが表示されたら、[OK] をクリックし、Active Directory 管理センターのメッセージを最新の状態にするために、もう一度 [OK] をクリックします。
9. F5 キーを押して、Active Directory 管理センターを最新の状態にします。

テスト アカウントを作成してから削除する

1. Active Directory 管理センターで、[Research] OU をダブルクリックします。
2. タスク ウィンドウで、[新規]、[ユーザー] の順にクリックします。
3. アカウントで、次の情報を入力し、[OK] をクリックします。
   - フル ネーム : Test1
   - ユーザー UPN ログオン : Test1
   - パスワード : Pa55w.rd
   - パスワードの確認入力 : Pa55w.rd
4. 前の手順を繰り返し、2 つ目のユーザーの Test2 を作成します。
5. [アカウント] ボックスで、[Test1] と [Test2] の両方を選択し、選択したものを右クリックし、[削除] をクリックします。
6. 確認ウィンドウで、[はい] をクリックします。

削除したアカウントを復元する

1. Active Directory 管理センターで、[Adatum (ローカル)] をクリックし、[Deleted Objects] をダブルクリックします。
2. [Test1] を右クリックし、[復元] をクリックします。
3. [Test2] を右クリックし、[復元先] をクリックします。
4. 復元先ウィンドウで、[IT] OU、[OK] の順にクリックします。
5. Test1 が Research OU にあり、Test2 が IT OU にあることを確認します。

演習の復習の質問と解答

演習 : AD DS でのオブジェクトの回復

質問と解答

質問 : 削除されたユーザーやユーザー オブジェクトを含む OU を、権限のある復元で復元すると、復元前とオブジェクトは全く同じになりますか。どの属性が同じではない可能性がありますか。

解答 : 解答はさまざまですが、グループ メンバーシップについての議論を構成するために、このような質問が出されました。ユーザーのグループ メンバーシップは、ユーザー オブジェクトの属性ではなく、グループ オブジェクトの属性です。ユーザーに対して権限のある復元を実行する場合、グループ内のユーザーのメンバーシップを復元しません。ユーザーが削除されると、グループのメンバー属性からも削除されるため、ユーザーが復元されても、ユーザーのプライマリ グループ以外のグループのメンバーにはなりません。グループ メンバーシップを復元するには、グループに対して権限のある復元を実行することを検討する必要があります。グループに対して権限のある復元を実行すると、メンバーシップをバックアップ作成日まで戻す場合に、望ましくないことがあります。

質問 : 演習では、Active Directory のごみ箱が有効にされる前にオブジェクトが削除された場合、それらのオブジェクトを復元することはできましたか。

解答 : はい。ただし、ほとんどの属性を持たない廃棄済み (Tombstone) オブジェクトとしてのみ、または AD DS の権限のある復元を使用して、復元することができます。

復習とまとめ

ベスト プラクティス

- ドメイン コントローラーを定期的にバックアップします。
- AD DS データベースの回復を、ドメイン コントローラーを復元するシナリオの 1 つとして検討します。
- Active Directory のごみ箱を有効にして、削除されたオブジェクトの回復を簡略化します。
- データベースの保守作業を実行する際、再起動可能な AD DS を使用します。

復習問題

質問 : AD DS により、どのような種類の復元をおこなうことができますか。

解答 : Active Directory のごみ箱により、権限のある復元、権限のない復元、単一オブジェクトの復元をおこなうことができます。