Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

23413B

サーバー インフラストラクチャの設計と実装

部品番号 : X18-86896

リリース日 : 07/2013

マイクロソフト ライセンス条項
マイクロソフト インストラクター指導コースウェア

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注意してお読みください。本ライセンス条項は、本ライセンス条項に付属しているコンテンツおよびコンテンツが記録されたメディアのお客様による使用に適用されます。トレーナー コンテンツ、ならびに本許諾コンテンツに関連する更新コンテンツおよび追加コンテンツに、別途固有のライセンス条項が付属していない場合は、それらの製品にも本ライセンス条項が適用されるものとします。それらの製品に固有のライセンス条項が付属している場合は、当該ライセンス条項が適用されるものとします。

本許諾コンテンツにアクセスするか、または本許諾コンテンツをダウンロードもしくは使用することにより、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、本許諾コンテンツにアクセスしたり、本許諾コンテンツをダウンロードまたは使用したりしないでください。

お客様が本ライセンス条項を遵守することを条件として、お客様には取得された各ライセンスについて以下が許諾されます。

1. 定義。

a. 「認定ラーニング センター」とは、マイクロソフト IT Academy プログラム メンバー、マイクロソフト ラーニング コンピテンシー メンバー、またはマイクロソフトが随時指定できるその他同様の法人を意味します。

b. 「認定トレーニング セッション」とは、認定ラーニング センターにおいて、または認定ラーニング センターを通じて、トレーナーがマイクロソフト インストラクター指導コースウェアを使用して実施するインストラクター指導トレーニング クラスを意味します。

c. 「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、認定ラーニング センターのトレーニング施設にある 1 台のセキュリティで保護された専用コンピューターで、特定のマイクロソフト インストラクター指導コースウェア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。

d. 「エンド ユーザー」とは、(i) 認定トレーニング セッションもしくはプライベート 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、(ii) MPN メンバーの従業員、または (iii) マイクロソフトの常勤従業員を意味します。

e. 「本許諾コンテンツ」とは、本ライセンス条項に付属しているコンテンツを意味し、マイクロソフト インストラクター指導コースウェアまたはトレーナー コンテンツが含まれる場合があります。

f. 「マイクロソフト認定トレーナー」または「MCT」とは、(i) 認定ラーニング センターまたは MPN メンバーに代わって、トレーニング セッションにおいてエンド ユーザーを指導するために雇用されており、(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認定されている、個人を意味します。

g. 「マイクロソフト インストラクター指導コースウェア」とは、IT プロフェッショナルおよび開発者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 ブランドのインストラクター指導トレーニング コースを意味します。マイクロソフト インストラクター指導コースウェアのタイトルは、

MOC、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。

h. 「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 メンバーを意味します。

i. 「マイクロソフト ラーニング コンピテンシー メンバー」とは、現在ラーニング コンピテンシー ステータスを保持している、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。

j. 「MOC」とは、IT プロフェッショナルおよび開発者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 オフィシャル コースと呼ばれる「Official Microsoft Learning Product」インストラクター指導コースウェアを意味します。

k. 「MPN メンバー」とは、Microsoft Partner Network プログラムにおけるシルバーまたはゴールド レベルの有効なアクティブ メンバーを意味します。

l. 「個人用デバイス」とは、お客様が個人的に所有または管理する、1 台のパーソナル コンピューター、デバイス、ワークステーション、またはその他のデジタル電子デバイスで、特定のマイクロソフト インストラクター指導コースウェア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。

m. 「プライベート トレーニング セッション」とは、マイクロソフト インストラクター指導コースウェアを使用して事前定義された学習目的に基づいて指導する、MPN メンバーが企業顧客に対して提供するインストラクター指導トレーニング クラスを意味します。これらのクラスは不特定多数の人々に対して広告または宣伝が行われず、クラスの出席者は企業顧客が雇用または契約している個人に限定されます。

n. 「トレーナー」とは、(i) マイクロソフト IT Academy プログラム メンバーが雇用した、認定トレーニング セッションを指導する学問上の認定を受けた教師、または (ii) MCT を意味します。

o. 「トレーナー コンテンツ」とは、マイクロソフト インストラクター指導コースウェアを使用してトレーニング セッションを指導するためにトレーナーのみが使用するよう指定された、トレーナー版のマイクロソフト インストラクター指導コースウェアおよびその他の追加コンテンツを意味します。トレーナー コンテンツには、Microsoft PowerPoint プレゼンテーション、トレーナー準備ガイド、トレーナー育成用資料、Microsoft One Note パック、クラスルーム セットアップ ガイド、およびプレリリース コース フィードバック フォームが含まれる場合があります。言い換えると、トレーナー コンテンツには、いかなるソフトウェア、仮想ハード ディスク、または仮想マシンも含まれません。

2. 使用権。本許諾コンテンツ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。本許諾コンテンツは、**ユーザーごとに複製 1 部が**使用許諾されます。そのため、お客様は、本許諾コンテンツにアクセスする、または本許諾コンテンツを使用する各個人に対して、ライセンスを取得しなければなりません。

2.1 以下は、5 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. **お客様がマイクロソフト IT Academy プログラム メンバーである場合。**
   i. お客様自身に代わって取得された各ライセンスは、お客様に提供された形式でマイクロソフト インストラクター指導コースウェアの複製 1 部を確認するためにのみ使用できます。マイクロソフト インストラクター指導コースウェアがデジタル形式である場合、お客様は最大 3 台の個人用デバイスに複製 1 部をインストールすることができます。お客様が所有または管理していないデバイスに、マイクロソフト インストラクター指導コースウェアをインストールすることはできません。

ii. お客様は、エンド ユーザーまたはトレーナーに代わって取得する各ライセンスについて、以下のいずれかを行うことができます。
    1. マイクロソフト インストラクター指導コースウェアのハード コピー版 1 部を、提供しているマイクロソフト インストラクター指導コースウェアの主題である認定トレーニング セッションの開始直前に限り、かかる認定トレーニング セッションに登録しているエンド ユーザー 1 名に頒布すること。**または**
    2. マイクロソフト インストラクター指導コースウェアのデジタル版 1 部の一意の引き換えコード、および当該コースウェアにアクセスする方法に関する手順を、エンド ユーザー 1 名に提供すること。**または**
    3. トレーナー コンテンツ 1 部の一意の引き換えコード、および当該トレーナー コンテンツにアクセスする方法に関する手順を、トレーナー 1 名に提供すること。

    ただし、以下の条項を遵守することを条件とします。
iii. お客様は、本許諾コンテンツのみへのアクセス権を、本許諾コンテンツの有効なライセンスを取得している個人に提供するものとします。
iv. お客様は、認定トレーニング セッションに出席している各エンド ユーザーが、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 インストラクター指導コースウェアの有効なライセンス取得済みの複製を各自持っていることを確認するものとします。
v. お客様は、マイクロソフト インストラクター指導コースウェアのハード コピー版を提供する各エンド ユーザーに本ライセンス条項の複製 1 部が提示されること、および各エンド ユーザーにマイクロソフト インストラクター指導コースウェアを提供する前に、マイクロソフト インストラクター指導コースウェアのエンド ユーザーによる使用に、本ライセンス条項の条件が適用されることに各エンド ユーザーが同意することを確認するものとします。各個人が、マイクロソフト インストラクター指導コースウェアにアクセスする前に、地域の法律に基づいて強制力を有する方法で、本ライセンス条項に同意する旨を示す必要があります。
vi. お客様は、認定トレーニング セッションを指導する各トレーナーが、かかる認定トレーニング セッションの主題であるトレーナー コンテンツの有効なライセンス取得済みの複製を各自持っていることを確認するものとします。
vii. お客様は、お客様のすべての認定トレーニング セッションに関して、指導しているマイクロソフト インストラクター指導コースウェアの主題であるマイクロソフト テクノロジについて深い知識と経験を有する有資格のトレーナーのみを雇用するものとします。
viii. お客様は、MOC タイトルを使用する各認定トレーニング セッションについて、1 週間に提供するトレーニングは最大 15 時間とするものとします。
ix. お客様は、MCT ではないトレーナーがマイクロソフト インストラクター指導コースウェアのすべてのトレーナー リソースにアクセスできないようにすることに同意するものとします。

b. **お客様がマイクロソフト ラーニング コンピテンシー メンバーである場合。**
i. お客様自身に代わって取得された各ライセンスは、お客様に提供された形式でマイクロソフト インストラクター指導コースウェアの複製 1 部を確認するためにのみ使用できます。マイクロソフト インストラクター指導コースウェアがデジタル形式である場合、お客様は最大 3 台の個人用デバイスに複製 1 部をインストールすることができます。お客様が所有または管理していないデバイスに、マイクロソフト インストラクター指導コースウェアをインストールすることはできません。
ii. お客様は、エンド ユーザーまたはトレーナーに代わって取得する各ライセンスについて、以下のいずれかを行うことができます。
    1. マイクロソフト インストラクター指導コースウェアのハード コピー版 1 部を、提供するマイクロソフト インストラクター指導コースウェアの主題である認定トレーニング セッションの開始直前に限り、かかる認定トレーニング セッションに出席しているエンド ユーザー 1 名に頒布すること。**または**
    2. マイクロソフト インストラクター指導コースウェアのデジタル版 1 部の一意の引き換えコード、および当該コースウェアにアクセスする方法に関する手順を、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 1 名に提供すること。**または**

3. トレーナー コンテンツ 1 部の一意の引き換えコード、および当該トレーナー コンテンツにアクセスする方法に関する手順を、トレーナー 1 名に提供すること。

ただし、以下の条項を遵守することを条件とします。

iii. お客様は、本許諾コンテンツのみへのアクセス権を、本許諾コンテンツの有効なライセンスを取得している個人に提供するものとします。
iv. お客様は、認定トレーニング セッションに出席している各エンド ユーザーが、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 インストラクター指導コースウェアの有効なライセンス取得済みの複製を各自持っていることを確認するものとします。
v. お客様は、マイクロソフト インストラクター指導コースウェアのハード コピー版を提供する各エンド ユーザーに本ライセンス条項の複製 1 部が提示されること、および各エンド ユーザーにマイクロソフト インストラクター指導コースウェアを提供する前に、マイクロソフト インストラクター指導コースウェアのエンド ユーザーによる使用に、本ライセンス条項の条件が適用されることに各エンド ユーザーが同意することを確認するものとします。各個人が、マイクロソフト インストラクター指導コースウェアにアクセスする前に、地域の法律に基づいて強制力を有する方法で、本ライセンス条項に同意する旨を示す必要があります。
vi. お客様は、認定トレーニング セッションを指導する各トレーナーが、かかる認定トレーニング セッションの主題であるトレーナー コンテンツの有効なライセンス取得済みの複製を各自持っていることを確認するものとします。
vii. お客様は、お客様の認定トレーニング セッションに関して、指導しているマイクロソフト インストラクター指導コースウェアの主題である、マイクロソフト認定資格の該当する資格情報を保持する有資格のトレーナーのみを雇用するものとします。
viii. お客様は、MOC を使用するお客様のすべての認定トレーニング セッションに関して、指導している MOC タイトルの主題である、マイクロソフト認定資格の該当する資格情報も保持する有資格の MCT のみを雇用するものとします。
ix. お客様は、マイクロソフト インストラクター指導コースウェアのみへのアクセス権を、エンド ユーザーに提供するものとします。
x. お客様は、トレーナー コンテンツのみへのアクセス権を、トレーナーに提供するものとします。

c. **お客様が MPN メンバーである場合。**

i. お客様自身に代わって取得された各ライセンスは、お客様に提供された形式でマイクロソフト インストラクター指導コースウェアの複製 1 部を確認するためにのみ使用できます。マイクロソフト インストラクター指導コースウェアがデジタル形式である場合、お客様は最大 3 台の個人用デバイスに複製 1 部をインストールすることができます。お客様が所有または管理していないデバイスに、マイクロソフト インストラクター指導コースウェアをインストールすることはできません。
ii. お客様は、エンド ユーザーまたはトレーナーに代わって取得する各ライセンスについて、以下のいずれかを行うことができます。
    1. マイクロソフト インストラクター指導コースウェアのハード コピー版 1 部を、提供しているマイクロソフト インストラクター指導コースウェアの主題であるプライベート トレーニング セッションの開始直前に限り、かかるプライベート トレーニング セッションに出席しているエンド ユーザー 1 名に頒布すること。**または**
    2. マイクロソフト インストラクター指導コースウェアのデジタル版 1 部の一意の引き換えコード、および当該コースウェアにアクセスする方法に関する手順を、プライベート 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 1 名に提供すること。**または**
    3. トレーナー コンテンツ 1 部の一意の引き換えコード、および当該トレーナー コンテンツにアクセスする方法に関する手順を、プライベート トレーニング セッションで指導するトレーナー 1 名に提供すること。

ただし、以下の条項を遵守することを条件とします。

iii. お客様は、本許諾コンテンツのみへのアクセス権を、本許諾コンテンツの有効なライセンスを取得している個人に提供するものとします。

iv. お客様は、プライベート トレーニング セッションに出席している各エンド ユーザーが、かかるプライベート トレーニング セッションの主題であるマイクロソフト インストラクター指導コースウェアの有効なライセンス取得済みの複製を各自持っていることを確認するものとします。
v. お客様は、マイクロソフト インストラクター指導コースウェアのハード コピー版を提供する各エンド ユーザーに本ライセンス条項の複製 1 部が提示されること、および各エンド ユーザーにマイクロソフト インストラクター指導コースウェアを提供する前に、マイクロソフト インストラクター指導コースウェアのエンド ユーザーによる使用に、本ライセンス条項の条件が適用されることに各エンド ユーザーが同意することを確認するものとします。各個人が、マイクロソフト インストラクター指導コースウェアにアクセスする前に、地域の法律に基づいて強制力を有する方法で、本ライセンス条項に同意する旨を示す必要があります。
vi. お客様は、プライベート トレーニング セッションを指導する各トレーナーが、かかるプライベート トレーニング セッションの主題であるトレーナー コンテンツの有効なライセンス取得済みの複製を各自持っていることを確認するものとします。
vii. お客様は、お客様のすべてのプライベート トレーニング セッションに関して、指導しているマイクロソフト インストラクター指導コースウェアの主題である、マイクロソフト認定資格の該当する資格情報を保持する有資格のトレーナーのみを雇用するものとします。
viii. お客様は、MOC を使用するお客様のすべてのプライベート トレーニング セッションに関して、指導している MOC タイトルの主題である、マイクロソフト認定資格の該当する資格情報を保持する有資格の MCT のみを雇用するものとします。
ix. お客様は、マイクロソフト インストラクター指導コースウェアのみへのアクセス権を、エンド ユーザーに提供するものとします。
x. お客様は、トレーナー コンテンツのみへのアクセス権を、トレーナーに提供するものとします。

d. **お客様がエンド ユーザーである場合。**
お客様が取得する各ライセンスについて、お客様は、お客様の個人トレーニングに使用する目的に限り、マイクロソフト インストラクター指導コースウェアを使用することができます。マイクロソフト インストラクター指導コースウェアがデジタル形式である場合、お客様は、トレーニング プロバイダーからお客様に提供された一意の引き換えコードを使用してオンラインでマイクロソフト インストラクター指導コースウェアにアクセスし、かかるマイクロソフト インストラクター指導コースウェアの複製 1 部を最大 3 台の個人用デバイスにインストールして使用することができます。お客様は、マイクロソフト インストラクター指導コースウェアの複製 1 部を印刷することもできます。お客様が所有または管理していないデバイスに、マイクロソフト インストラクター指導コースウェアをインストールすることはできません。

e. **お客様がトレーナーである場合。**
i. お客様が取得する各ライセンスについて、お客様は、認定トレーニング セッションまたはプライベート トレーニング セッションの準備または提供のみを目的として、お客様に提供された形式のトレーナー コンテンツの複製 1 部を 1 台の個人用デバイスにインストールして使用することができます。また、追加の複製 1 部をバックアップ用の複製として別の個人用デバイスにインストールすることができます。かかるバックアップ用の複製は、トレーナー コンテンツの再インストールにのみ使用できます。お客様が所有または管理していないデバイスで、トレーナー コンテンツの複製をインストールまたは使用することはできません。お客様は、認定トレーニング セッションまたはプライベート トレーニング セッションの準備または提供のみを目的として、トレーナー コンテンツの複製 1 部を印刷することもできます。

ii. お客様は、最新バージョンの MCT 契約書に従って、トレーニング セッションの手順に論理的に関連するトレーナー コンテンツの記述部分をカスタマイズすることができます。お客様は、上記の権利を行使することを選択した場合、以下に従うことに同意するものとします。(i) カスタマイズは、認定トレーニング セッションおよびプライベート トレーニング セッションを指導するためにのみ使用できる、および (ii) すべてのカスタマイズは本ライセンス条項に準拠している。言い換えると、「カスタマイズ」の使用とは、スライドとコンテンツの順序の変更、および一部のスライドまたはコンテンツの不使用のみを意味し、スライドまたはコンテンツの変更または改変を意味しないものとします。

2.2 **構成部分の分離。**本許諾コンテンツは 1 つの製品として許諾されており、お客様はそのコンポーネントを分離し、複数のデバイスにインストールすることはできません。

2.3 **本許諾コンテンツの再頒布。**上記の使用権において明示的に規定されている場合を除き、マイクロソフトの書面による許可なく、お客様が第三者に対して、本許諾コンテンツ (および許可される改変) またはその一部を頒布することはできません。

2.4 **第三者のプログラムおよびサービス。**本許諾コンテンツには、第三者によるプログラムまたはサービスが含まれることがあります。お客様によるこれらの第三者によるプログラムまたはサービスの使用には、当該プログラムおよびサービスに別途固有のライセンス条項が付属している場合を除き、本ライセンス条項が適用されます。

2.5 **追加条項。**一部の本許諾コンテンツには、その使用に関して追加の条項、条件、およびライセンスが適用されるコンポーネントが含まれる場合があります。かかる条件およびライセンスにおいて本ライセンス条項と矛盾しない条項は、お客様による個々のコンポーネントの使用にも適用され、本ライセンス条項に規定されている条項を補完するものとします。

3. **プレリリース テクノロジに基づく本許諾コンテンツ。**本許諾コンテンツの主題がマイクロソフト テクノロジのプレリリース版 (以下、「**プレリリース版**」といいます) に基づいている場合は、本ライセンス条項の他の規定に加え、以下の条件も適用されます。

a. **プレリリース版の本許諾コンテンツ。**本許諾コンテンツの主題は、マイクロソフト テクノロジのプレリリース版に関するものです。当該テクノロジは、当該テクノロジの最終版と異なる動作をする場合があり、マイクロソフトは最終版向けに当該テクノロジを変更することがあります。また、最終版がリリースされない場合もあります。当該テクノロジの最終版に基づく本許諾コンテンツには、プレリリース版に基づく本許諾コンテンツと同じ情報が含まれていない場合もあります。マイクロソフトは、当該テクノロジの最終版に基づく本許諾コンテンツを含めて、追加のコンテンツをお客様に提供する義務を負わないものとします。

b. **フィードバック。**お客様は、マイクロソフトに対して本許諾コンテンツに関するフィードバックを提供する場合、直接または第三者の被指名人を介して、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、該当するフィードバックの対象となるマイクロソフト ソフトウェア、マイクロソフト製品、またはサービスの特定部分を使用するためのすべての特許権、またはこの特定部分に関連する第三者の製品、技術、およびサービスに必要とされるすべての特許権を無償で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、テクノロジ、または製品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、テクノロジ、または製品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。

c. **プレリリース版の有効期間。**お客様がマイクロソフト IT Academy プログラム メンバー、マイクロソフ

トラーニング コンピテンシー メンバー、MPN メンバー、またはトレーナーである場合、プレリリース版のテクノロジに関する本許諾コンテンツのすべての複製の使用を、(i) マイクロソフトがお客様に、プレリリース版のテクノロジに関する本許諾コンテンツの使用期限として通知した日付、または (ii) 本許諾コンテンツの主題であるテクノロジの完成版の発売日から 60 日後のうちのいずれか早い方の時点 (以下、「**プレリリース版の有効期間**」) で停止するものとします。お客様は、プレリリース版の有効期間の満了時または終了時に、お客様が所有または管理している本許諾コンテンツのすべての複製を回復できないように削除して破棄するものとします。

4. **ライセンスの適用範囲。**本許諾コンテンツ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、お客様に本許諾コンテンツ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上記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た方法でのみ本許諾コンテンツを使用することができます。お客様は、使用方法を制限するために本許諾コンテンツ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。本ライセンス条項において明示的に許可されている場合を除き、お客様は以下の行為を行うことはできません。
   - 本許諾コンテンツにアクセスするか、または本許諾コンテンツの有効なライセンスを取得していない個人に本許諾コンテンツへのアクセスを許可すること。
   - 本許諾コンテンツに含まれている著作権もしくはその他の保護に関する表示 (透かしを含みます)、ブランド、または識別情報を改変すること、取り除くこと、または不明瞭にすること。
   - 本許諾コンテンツを改変するか、または本許諾コンテンツの派生品を作成すること。
   - 第三者がアクセスまたは使用できるように本許諾コンテンツを公開または提供すること。
   - 本許諾コンテンツを複製、印刷、インストール、販売、公開、送信、貸与、改造、再利用、リンク設定もしくは投稿、または第三者に提供もしくは頒布すること。
   - 本許諾コンテンツの技術的な制限を回避する方法で使用すること。
   - 本許諾コンテンツをリバース エンジニアリング、逆コンパイル、または逆アセンブルすること、あるいは本許諾コンテンツに対する保護を削除またはその他の方法で妨げること。ただし、適用される法令により明示的に認められている場合を除きます。

5. **権利および所有権の留保。**マイクロソフトは、本ライセンス条項においてお客様に明示的に許諾されていない権利をすべて留保します。本許諾コンテンツは、著作権法およびその他の知的財産に関する法律および条約によって保護されています。マイクロソフトまたはそのサプライヤーは、本許諾コンテンツに関する所有権、著作権、およびその他の知的財産権を所有しています。

6. **輸出規制。**本許諾コンテンツ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、本許諾コンテンツに適用される、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/exporting をご参照ください。

7. **サポート サービス。**本許諾コンテンツは現状有姿で提供されます。そのため、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。

8. **解除。**マイクロソフトは、お客様が本ライセンス条項の契約条件を遵守していない場合、他のいかなる権利も制限することなく本ライセンス条項を解除することができます。お客様は、本ライセンス条項の解除時に、お客様が所有または管理している本許諾コンテンツのすべての複製の使用を直ちに停止し、かかるすべての複製を削除して破棄するものとします。

9. **第三者のサイトへのリンク。**お客様は、本許諾コンテンツの使用中に第三者のサイトにリンクすることがあります。第三者のサイトはマイクロソフトの管理が及ばないものであり、第三者のサイトのコンテンツ、第三者のサイトに含まれるリンク、第三者のサイトに対する変更または更新には、マイクロソフトは責任を負いません。マイクロソフトは、いかなる第三者のサイトから受信されたウェブ キャスティングまたは

その他のいかなる形式の送信についても責任を負いません。マイクロソフトは、お客様への便宜を図る目的でのみ、第三者へのリンクを提供しています。リンクが含まれていても、マイクロソフトが第三者のサイトを推奨することを意味しません。

10. 完全合意。本ライセンス条項、ならびにトレーナー コンテンツ、更新コンテンツ、および追加コンテンツに関する追加条項は、本許諾コンテンツ、更新コンテンツ、および追加コンテンツ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。

11. 準拠法。

a. 日本。お客様が本ソフトウェアを日本国内で入手された場合、本ライセンス条項は日本法に準拠するものとします。
b. 米国。お客様が本許諾コンテンツ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、および違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。
c. 日本および米国以外。お客様が本許諾コンテンツ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。

12. 法的効力。本ライセンス条項は、特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。また、お客様が本許諾コンテンツを取得された第三者に関する権利を取得できる場合もあります。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。

13. あらゆる保証の免責。本許諾コンテンツは、提供しうる形で現状有姿のまま提供されます。お客様は、その使用に関するリスクを負うものとします。マイクロソフトおよびその各関連会社は、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マイクロソフトおよびその各関連会社は、法律上許容される最大限において、商品性、特定目的に対する適合性、非侵害性に関する黙示の保証について一切責任を負いません。

14. 救済手段および責任の制限および除外。マイクロソフト、各マイクロソフト関連会社、およびそのサプライヤーの責任は、5.00 米ドルを上限とする直接損害に限定されます。その他の損害 (派生的損害、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。

- 本許諾コンテンツ、サービス、第三者のインターネットの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
- 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派生的損害の免責、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。

2012 年 9 月改訂

第 1 章

サーバーのアップグレードと移行の計画

目次

レッスン 1
アップグレードと移行に関する考慮事項

目次

参考資料

プレインストール要件

参考資料 : Windows サーバー仮想化検証プログラムの詳細については、「Welcome to the Windows Server Virtualization Validation Program」(http://go.microsoft.com/fwlink/?linkid=279917) を参照してください。

インプレース アップグレードとサーバー移行

参考資料 : 移行の詳細については、「Windows Server 移行ツールのインストール、使用、および削除」(http://technet.microsoft.com/ja-jp/library/jj134202.aspx) を参照してください。

アップグレードと移行の計画に役立つツール

参考資料 : Windows Server 2012 用の Microsoft Assessment and Planning Toolkit (MAP) については、http://technet.microsoft.com/ja-jp/solutionaccelerators/dd537573 を参照してください。

レッスン 2
サーバーのアップグレードと移行の計画の作成

目次

質問と解答

討論 : ボリューム ライセンス認証の計画

質問 : 組織の IT インフラストラクチャは、Windows クライアント オペレーティング システムや Windows Server オペレーティング システムのさまざまなエディションが稼働するパーソナル コンピューターとサーバーで構成されています。来月、組織は、500 台の Windows 8 クライアント コンピューターと 20 台の Windows Server 2012 サーバーを展開することを計画しています。財務部門のレガシ アプリケーションに対応するために、Windows 7 が稼働する 10 台のクライアント コンピューターと Windows Server 2008 R2 が稼働する 2 台のサーバーを展開する必要もあります。どの種類のボリューム ライセンス認証を実装する必要がありますか。

解答 : キー管理サービス (KMS) に基づくボリューム ライセンスを実装する必要があります。あなたの組織では、さまざまなエディションの Windows® クライアント オペレーティング システムと Windows Server オペレーティング システムを展開しているためです。

質問 : 組織の IT インフラストラクチャが、さまざまなエディションの Windows クライアント オペレーティング システムや Windows Server オペレーティング システムから Windows 8 と Windows Server 2012 にアップグレードされました。どの種類のボリューム ライセンス認証を実装する必要がありますか。

解答 : Active Directory® ベースのライセンス認証に基づくボリューム ライセンスを実装する必要があります。あなたの組織では Windows 8 と Windows Server 2012 のオペレーティング システムを展開していて、Active Directory ベースのライセンス認証は Windows Server 2012 と Windows 8 を実行するコンピューターでのみサポートされるためです。

参考資料

移行できるサーバーの役割の決定

注 : 以前のエディションの Windows Server でサポートされている役割のみを Windows Server 2012 に移行できます。

参考資料 : 移行する役割および機能を決定する際に役立つ詳細な情報については、「Windows Server 2012 への役割と機能の移行」(http://technet.microsoft.com/ja-jp/library/jj134039) を参照してください。

レッスン 3
仮想化の計画

目次

質問と解答

討論 : 仮想展開と物理展開の選択

質問 : ビジネス アプリケーションやインフラストラクチャ サービスを仮想環境に展開するのはどのような場合ですか。

解答 : さまざまな解答が考えられます。

質問 : 物理環境に現在展開されているサーバーの役割、機能、またはアプリケーション サービスはどれですか。

解答 : さまざまな解答が考えられます。

質問 : 組織で仮想環境を運用している場合、仮想環境に現在展開しているのはどれですか。また、なぜ展開しているのですか。

解答 : さまざまな解答が考えられます。

参考資料

仮想化を実装するための考慮事項

注 : ホスト コンピューターでリソース使用率を計画する場合、ホスト コンピューターでは仮想マシンを実行するために、余分にリソースが必要になることを考慮する必要があります。例えば、仮想マシンが 1GB の RAM を必要とする場合、ホスト コンピューターで仮想マシン用に 32 MB のオーバーヘッドが発生する可能性があります。仮想マシンにさらに 1 GB のメモリを割り当てるごとに、ホスト コンピューターで 8 MB のオーバーヘッドが発生する可能性があります。

注 : 仮想マシンのハードウェア要件を評価する際には、実際の物理ハードウェアでなく、実際のハードウェア使用率を使用する必要があります。現在のハードウェア リソースの 5% しか使用していない物理サーバーを、はるかに少ないハードウェア リソースで構成されている仮想マシンに展開できます。

同梱される仮想ライセンス

注 : このトピックはサーバーのライセンスについての情報のみを提供し、クライアントアクセス ライセンスについては情報を提供していません。ほとんどのサーバーベースのアプリケーションでは、接続するクライアント コンピューターに適切なクライアントアクセス ライセンスが必要になります。

復習とまとめ

ベスト プラクティス

物理または仮想環境での Windows Server 2012 の展開を計画する場合、オペレーティング システム上で実行されるサービスやアプリケーションの可用性、およびバックアップと回復の方法を必ず考慮します。プライベート クラウドでソリューションを実行する場合、System Center 2012 などの IT 環境の効率的な運用を支援するための管理および監視ツールを必ず使用します。さらに、仮想マシンに対して適当なサイズとパフォーマンスを備えた、適切に設計された記憶域ソリューションを確保します。

復習問題

質問 : Windows Server 2012 オペレーティング システムの展開のさまざまなシナリオに関して、あなたの組織の戦略の指針となる重要な留意事項は何ですか。

解答 : ビジネス要件、クラウド コンピューティング、現在のサーバー インフラストラクチャの統合、現在のアプリケーションとインフラストラクチャ ソリューションの Windows Server 2012 へのアップグレードまたは移行など、さまざまな考慮事項が組織の戦略に影響します。

実際の問題とシナリオ

あなたの組織では、仮想化テクノロジはあまり使用されていません。あなたは、2 つのインスタンスの仮想マシンをサポートする Windows Server 2012 Standard エディションのオペレーティング システムを展開しました。管理部門は、将来、仮想環境に新製品を展開する必要があることを心配しています。新製品を展開する際に、追加のライセンスを購入する必要がない、スケーラブルで拡張可能なソリューションを希望しています。

そのため、管理部門では、IT 部門に、Windows Server 2012 Datacenter エディション上で実行できるハードウェア ソリューションを含むサーバー展開戦略の作成を依頼しました。これにより、組織では、仮想環境へのアプリケーションの展開と、ライセンスの追加を必要としない柔軟なスケールアップが可能になります。

ツール

ツール	用途	アクセス方法
Microsoft Assessment and Planning Toolkit (MAP)	組織のサーバー インフラストラクチャのインベントリを分析し、評価し、アップグレードと移行の計画に使用できるレポートを作成。	Microsoft の Web サイト : http://go.microsoft.com/fwlink/?linkid=279918

演習の復習問題と解答

演習 : サーバーのアップグレードと移行の計画

質問と解答

演習の復習

質問 : アップグレードと移行の戦略を立てる際に、なぜ MAP ツールを使用するのですか。

解答 : MAP ツールは、組織のサーバー インフラストラクチャのインベントリを分析し、評価し、アップグレードと移行の計画の作成に使用できるレポートを作成します。このツールが実行する詳細分析は、アップグレードと移行の戦略についての決断を下す際に役立ちます。

質問 : A. Datum 社の内部と境界ネットワークの仮想化と統合に、Windows Server 2012 Datacenter エディションを選択する理由は何ですか。

解答 : Windows Server 2012 Datacenter エディションは、無制限の数の仮想マシンのインスタンスをサポートします。物理サーバーごとの仮想マシンの数が 4 に増えた場合でも、A. Datum 社では、Windows Server 2012 Standard エディションを使用していた場合のように、拡張した分のライセンスを購入する必要がありません。

第 2 章

サーバー展開のインフラストラクチャの計画と実装

目次

レッスン 1
適切なサーバー イメージング戦略の選択

目次

質問と解答

リテール メディアによるハイ タッチ展開の実行

質問 : リテール メディアによるハイ タッチ展開方式の制限事項は何ですか。

解答 : 以下を含めて、さまざまな解答が考えられます。

- IT プロフェッショナルは対話型のインストールを開始する必要があります。
- 個別の応答ファイルがある USB フラッシュ メモリでは不十分です。
- リテール メディアの複数のコピーが必要です。
- この方法の拡張性はそれほど高くありませんが、規模の小さな 1 回限りの展開であれば有効です。

参考資料

ライトタッチによる大量展開の実行

参考資料 : MDT 2012 Update 1 を使用した高度な展開の使用シナリオの詳細については、http://go.microsoft.com/fwlink/?LinkID=277143 を参照してください。

ゼロタッチによる大量展開の実行

注 : ゼロタッチによる大量展開では、ドメイン ネーム システム (DNS) と動的ホスト構成プロトコル (DHCP) のインフラストラクチャ サービスも必要になります。

レッスン 2
自動展開の戦略の選択

目次

質問と解答

討論 : 現在の展開戦略について

質問 : 現在、自分の組織ではどのような方法でオペレーティング システムを展開していますか。

解答 : さまざまな解答が考えられますが、ほとんどの組織はある種のイメージング戦略を実装しており、また、その多くはインフラストラクチャ サービスを使用してイメージを配布します。

質問 : 選択した展開戦略のメリットとデメリットは何ですか。

解答 : 以下を含めて、さまざまな解答が考えられます

- ブランチ オフィスにオンサイトの IT スタッフがいない
- 組織全体に多くのサーバーが展開される
- 組織全体のサーバー構成が類似する

質問 : 使用している展開戦略は、ファイル ベースとバイナリ イメージ ベースのどちらですか。

解答 : バイナリベースのイメージをまだ使用している参加者もいるため、ファイルベースのイメージの利点について、柔軟性およびオフライン保守の観点から比較討論をおこないます。

参考資料

イメージベースの展開戦略の選択

注 : 自動展開のためのテクノロジの詳細については、レッスン 3「自動展開の戦略の実装」を参照してください。

レッスン 3
自動展開の戦略の実装

目次

質問と解答

展開シナリオの選択

質問 : Windows Server 2012 のクリーン インストールを実 行するのは、どのような状況ですか。

解答 : クリーン インストールが唯一の選択肢となることがあります。次の状況が考えられます。

- オペレーティング システムがコンピューターにまったくインストールされていない。
- インストールされているオペレーティング システムが Windows Server 2012 へのアップグレードをサポートしていない。

以前のバージョンの Windows オペレーティング システムでファイル破損や他のパフォーマンス関連の問題が発生している場合は、アップグレードではなくクリーン インストールが推奨されます。以前のバージョンの Windows オペレーティング システムでアプリケーションや設定を引き継ぐ必要がない場合は、アップグレードや移行ではなく、クリーン インストールを選択します。

質問 : Windows Server 2012 のインストール時に発生する可能性のある問題は何ですか。

解答 : さまざまな解答が考えられます。

参考資料

Windows ADK

参考資料 : 有効な検索パスの完全なリストについては、「Windows セットアップの実行方法」の「応答ファイルの暗黙的な検索の順序」セクション (http://technet.microsoft.com/ja-jp/library/cc749415(v=ws.10).aspx) を参照してください。

仮想マシンの展開に使用できるツール

注 : System Center 2012 SP1 では VMM セルフサービス ポータルが削除され、この機能は System Center 2012 App Controller に移行されています。

注 : .vhdx 形式は、ディスクの低密度で動的な表現をサポートしています。そのため、ディスクの全内容を直接格納する場合と比べて、比較的小さいディスク イメージ ファイルを生成します。

デモンストレーション

デモンストレーション : Windows Server 2012 イメージの準備

デモンストレーションの手順

1. LON-SVR1 に切り替えます。
2. タスクバーで [エクスプローラー] 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、[コンピューター] を展開し、[Allfiles (E:)] ドライブをクリックします。詳細ウィンドウで右クリックし、[新規]、[フォルダー] の順にクリックします。
4. [新しいフォルダー] ボックスに「Images」と入力し、Enter キーを押します。
5. エクスプローラーのナビゲーション ウィンドウで、[Images] をダブルクリックし、詳細ウィンドウで右クリックし、[新規]、[フォルダー] の順にクリックします。
6. [新しいフォルダー] ボックスに「Custom Images」と入力し、Enter キーを押します。
7. ホストの 23413B-LON-SVR1 ウィンドウのツールバーで、[メディア] をクリックし、[DVD ドライブ] をポイントして [ディスクの挿入] をクリックします。
8. [開く] ダイアログ ボックスの [ファイル名] ボックスに「C:¥Program Files¥Microsoft Learning¥23413¥Drives¥Windows2012_RTM.iso」と入力し、[開く] をクリックします。
9. D:¥sources¥install.wim を E:¥Images¥Custom Images フォルダーにコピーします。
10. エクスプローラーで、[E:¥Images] を右クリックし、[プロパティ] をクリックします。
11. [共有] タブをクリックし、[詳細な共有] をクリックします。
12. [詳細な共有] ダイアログ ボックスで、[このフォルダーを共有する] チェック ボックスをオンにします。
13. [アクセス許可] をクリックし、[追加] をクリックします。
14. [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 ボックスの [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「Administrator」と入力し、[OK] をクリックします。
15. [Images のアクセス許可] ダイアログ ボックスで、[Administrator (ADATUM¥Administrator)] をクリックし、[許可] で [フル コントロール] チェック ボックスをオンにし、[OK] をクリックします。
16. [詳細な共有] ダイアログ ボックスで、[OK] をクリックし、[閉じる] をクリックします。
17. エクスプローラーで、[コンピューター] を右クリックし、[ネットワーク ドライブの割り当て] をクリックします。
18. [ネットワーク ドライブの割り当て] ダイアログ ボックスの [ドライブ] ボックスにドライブ [Z:] が表示されていることを確認し、[フォルダー] ボックスに「¥¥lon-svr1¥Images」と入力し、[完了] をクリックします。
19. LON-SVR1 で、タスクバーの右下隅にマウスをポイントし、[検索] をクリックし、「cmd.exe」と入力します。
20. [アプリ] リストで、[cmd.exe] を右クリックし、[管理者として実行] をクリックします。
21. 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。

```
Mkdir c:¥mounted
```

22. 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。

```
Dism /get-imageinfo /imagefile:"z:¥Custom Images¥install.wim"
```

23. 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。

```
Dism /mount-wim /wimfile:"z:¥Custom Images¥install.wim" /index:4 /mountdir:c:¥mounted
```

24. 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。

```
Dism /image:c:¥mounted /get-features
```

25. 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。

```
Dism /image:c:¥mounted /get-featureinfo /featurename:IIS-WebServerRole
```

26. 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。

```
Dism /image:c:¥mounted /enable-feature /featurename:IIS-WebServerRole –all
```

27. 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。

```
Dism /unmount-wim /mountdir:c:¥mounted /commit
```

復習とまとめ

ベスト プラクティス

ベスト プラクティス	説明
参照コンピューターには、最新のセキュリティ更新を常にインストールします。	最新状態の参照コンピューターから開始することで、新たにオンラインになったコンピューターの Windows の脆弱性を減らすことができます。
アクセス制御を実装して、起動可能なメディアを保護します。	起動可能なメディアを作成する場合は、必ずパスワードを割り当て、メディアへの物理的なアクセスを制御することを推奨します。
PXE サービス ポイントは、セキュリティ保護されたネットワーク セグメントのみで使用します。	PXE サービス ポイントでは、スイッチとサーバーの UDP ポートを開くことが必要です。
不明なコンピューターにオペレーティング システムを展開する必要がある場合は、アクセス制御を実装して、承認されていないコンピューターがネットワークに接続することを防止します。	不明なコンピューターのプロビジョニングは、必要に応じて複数のコンピューターを立ち上げる便利な方法ですが、悪意のあるユーザーがあなたのネットワークの信頼されたクライアントに化ける可能性もあります。
ブート イメージのサイズを縮小して、TFTP ダウンロードを高速化します。	このイメージが PEIMG.exe /prep を使用して用意されていることを確認します。ベスト プラクティスは、イメージを Windows DS サーバーに追加する前に、ImageX /export コマンドを使用してブート イメージをクリーンな .wim ファイルにエクスポートすることです。

復習問題

質問 : あなたの組織では、さまざまなサーバー展開を使用しており、同一の展開は存在しません。あなたは、展開の支援に、カスタマイズされたイメージを使用することを選択しました。シックまたはシンイメージの使用について考慮する必要はありますか。

解答 : シン イメージが最も適しています。サーバーを展開した後、グループ ポリシーとスクリプトを使用してアプリケーションの展開を自動化します。シック イメージには、このシナリオ用のカスタマイズが多く含まれ過ぎています。

質問 : リテール メディアによるハイ タッチ展開を自動化するためには、どのようなツールが必要ですか。

解答 : リテール メディアによるハイ タッチ展開を自動化するためには、リテール メディア、Windows ADK、リムーバブル メディアを使用することができます。

質問 : あなたの組織では、ライト タッチ展開の実装を望んでいます。MDT 2012 の他に、ライト タッチ展開の実行に役立つツールは何ですか。

解答 : ライト タッチ展開を実行するために使用できるツールを次に示します。

- MAP ツール
- ACT

- ボリュームライセンス メディア
- MDT
- Windows ADK
- 展開作業時にクライアント コンピューターを起動するインストール メディアまたは Windows DS

実際の問題とシナリオ

Windows DS は Windows オペレーティング システムを展開するための 1 つの方法ですが、中規模の企業やエンタープライズでは、より複雑な移行シナリオをカスタマイズするために、MDT の実装を考慮することを推奨します。ゼロ タッチの実装用に、Configuration Manager 2012 は、強力で、スケーラブルかつ管理された展開環境を提供します。Configuration Manager では、Windows オペレーティング システムの展開もできますが、すでにインストールされたコンピューターの管理の継続ができます。

ツール

ツール	使用目的	アクセス方法
Application Compatibility Toolkit	Windows 8 に対するアプリケーションの互換性を検証します。	http://go.microsoft.com/fwlink/?LinkID=277145
Windows ADK	Windows オペレーティング システムの評価と展開をおこないます。	http://go.microsoft.com/fwlink/?LinkID=277146
Windows SIM	応答ファイルの作成と編集をおこないます。	Windows ADK
DISM	WIM ベースのイメージ ファイルの作成、編集、および適用をおこないます。	Windows ADK
USMT	ユーザー設定を移行します。	Windows ADK
DISM	WIM ベースのイメージ ファイルを操作します。	Windows ADK

演習の復習問題と解答

演習 : サーバー展開のインフラストラクチャの計画と実装

質問と解答

演習の復習

質問 : 設計計画にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : あなたの設計計画は提案されているソリューションとは違っていましたか。

解答 : さまざまな解答が考えられます。

質問 : 演習の設計は、あなたの組織の Windows Server 2012 展開方法と比較してどうですか。

解答 : さまざまな解答が考えられます。

質問 : 予算に心配がない場合、それによって設計はどのように変わりますか。

解答 : 予算に心配がない場合、ほとんどの企業が Windows Server 2012 オペレーティング システムの完全なエンド ツー エンド展開に焦点を当てた System Center 2012 Configuration Manager SP1 を使用して実行するゼロタッチ展開を検討するでしょう。Configuration Manager SP1 の実装に要した初期投資費用はすぐに回収できます。Configuration Manager SP1 を使用すると、A. Datum 社が 2 つの新しい会社を買収する際に、Windows Server 2012 の展開にかかる費用を削減できるからです。新しく買収した会社にサーバーを展開する場合、Configuration Manager SP1 でテスト済みのイメージ展開を使用することもできます。この展開のタスク シーケンスでは、マイナー変更があるか、または変更がありません。

第 3 章

IP 構成とアドレス管理のソリューションの設計と保守

目次

レッスン 1
DHCP の設計と実装

目次

質問と解答

討論 : IP アドレス指定方式の選択

質問 : この地域に必要と思われるサブネット数はいくつですか。

解答 : この地域には 300 台のコンピューターがあります。仕様によれば、各サブネットには平均 50 台のコンピューターを展開します。さらに約 25 % の成長に備えるように計画する必要があります。コンピューターをホストするために地域に必要なサブネットは 6 つですが、増加するコンピューターをホストするために各場所に予備のサブネットを計画する必要があります。そのため、合計で 9 つのサブネットが必要です。

質問 : 各サブネットに、いくつのホストを展開しますか。

解答 : 仕様によれば、各サブネットに展開できるホスト コンピューターは最大で 50 台です。

質問 : 各営業所に使用するサブネット マスクはどうなりますか。

解答 : 現在の地域のネットワーク アドレスは、172.16.16.0/20 です。サブネットとホストに割り当てるために 12 ビットが残されています。9 つのサブネットを表示するには、4 ビットが必要です。3 ビットでは 8 つのサブネットまでしか表示できません。4 ビットで実質的に 16 サブネットを表示することができます。これはサブネット数として十分な数です。これは 255.255.255.0 の 10 進表記法マスクです。

質問 : 各営業所のサブネット アドレスはどうなりますか。

解答 : ブランチ 1 :

172.16.16.0/24

172.16.17.0/24

172.16.18.0/24

ブランチ 2 :

172.16.19.0/24

172.16.20.0/24

172.16.21.0/24

ブランチ 3 :

172.16.22.0/24

172.16.23.0/24

172.16.24.0/24

質問 : 各営業所のホスト アドレスの範囲はどうなりますか。

解答 : ブランチ 1 :

172.16.16.1 ～ 172.16.16.254

172.16.17.1 ～ 172.16.17.254

172.16.18.1 ～ 172.16.18.254

ブランチ 2 :

172.16.19.1 ～ 172.16.19.254

172.16.20.1 ～ 172.16.20.254

172.16.21.1 ～ 172.16.21.254

ブランチ 3 :

172.16.22.1 ～ 172.16.22.254

172.16.23.1 ～ 172.16.23.254

172.16.24.1 ～ 172.16.24.254

質問 : このシナリオの場合、パブリック IP アドレスは必要ですか。

解答 : このシナリオでは、パブリック IP アドレスは必要ありません。すべての通信は企業のイントラネット内でおこなわれます。

質問 : 使用できる他のプライベート IP アドレスはどうなりますか。

解答 : 次の表にプライベート アドレスの範囲を示します。

クラス	マスク	範囲
A	10.0.0.0/8	10.0.0.0 ～ 10.255.255.255
B	172.16.0.0/12	172.16.0.0 ～ 172.31.255.255
C	192.168.0.0/16	192.168.0.0 ～ 192.168.255.255

質問 : IP アドレスの割り当てに関して、他にはどんなことが推奨されますか。

解答 : 手動での IP アドレスの割り当ては慎重におこないます。おこなうときには、各サブネットに同一範囲を割り当てます。同じデバイスには常に同じサブネット アドレスを割り当てます。例えば、ルーターには 1 アドレスを割り当て、ドメイン コントローラーには 2 アドレスを割り当てます。この戦略は、インストール プロセスを簡略化し、トラブルシューティングにも役立ちます。

参考資料

注 : 必要なサブネット数を計算するには、ネットワークで必要なサブネット数を判断します。計算式 2n (n はビット数) を使用します。この計算結果が、ネットワークが必要とするサブネット数です。必要なホスト ビット数を計算するには、計算式 2n-2 (n はビット数) を使用します。

DHCP サーバーの可用性の計画

注 : Windows Server® 2012 では、フェールオーバー用に構成できる DHCP サーバーは 2 台のみです。さらに、フェールオーバーを使用できるのは、IPv4 のスコープおよびサブネットに限定されています (IPv6 のスコープおよびサブネットに対しては使用できません)。

デモンストレーション

デモンストレーション : DHCP フェールオーバーの構成

デモンストレーションの手順

1. LON-DC1 で、ユーザー名「adatum¥administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、結果ウィンドウの [役割と機能の追加] をクリックします。
3. [次へ] を 3 回クリックします。
4. [サーバーの役割の選択] ページで、[DHCP サーバー] の役割をクリックし、[機能の追加] をクリックします。
5. [次へ] を 3 回クリックし、[インストール] をクリックします。
6. 役割のインストールが完了したら、[閉じる] をクリックします。
7. サーバー マネージャー コンソールで、[ツール] をクリックし、ドロップダウン リストで [DHCP] をクリックします。
8. [lon-svr1.adatum.com] を展開し、右クリックし、[承認] をクリックします。
9. LON-DC1 に切り替えます。
10. LON-DC1 で、ユーザー名「adatum¥administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
11. サーバー マネージャー コンソールで、[ツール] をクリックし、ドロップダウン リストで [DHCP] をクリックします。
12. DHCP コンソールで、[lon-dc1.adatum.com] を展開し、[IPv4] を選択して右クリックし、[フェールオーバーの構成] をクリックします。
13. フェールオーバーの構成ウィザードで、[次へ] をクリックします。
14. [フェールオーバーに使用するパートナー サーバーを指定します] ページの [パートナー サーバー] フィールドに「172.16.0.21」と入力し、[次へ] をクリックします。
15. [新しいフェールオーバー リレーションシップの作成] ページの [関係名] フィールドに「Adatum DHCP Failover」と入力します。
16. [クライアントの最大リード タイム] フィールドで、時間を「0」、分を「10」に設定します。
17. [モード] フィールドが [負荷分散] に設定されていることを確認します。
18. [負荷分散の割合] がどちらも [50%] に設定されていることを確認します。
19. [状態の切り替えの間隔] チェック ボックスをオンにします。既定値の 60 秒のままにします。
20. [メッセージの認証を有効にする] チェック ボックスをオンにし、[共有シークレット] フィールドに「Pa$$w0rd」と入力し、[次へ] をクリックします。
21. [完了] をクリックし、[閉じる] をクリックします。
22. LON-SVR1 に切り替えます。IPv4 ノードがアクティブであることを確認します。ナビゲーション ウィンドウで [Adatum.com] をクリックし、ツールバーで [最新の情報に更新] をクリックします。
23. [IPv4] ノードを展開し、[スコープ] を展開します。
24. [アドレス プール] をクリックし、アドレス プールが構成されていることを確認します。
25. [スコープ オプション] をクリックし、スコープ オプションが構成されていることを確認します。
26. LON-DC1 と LON-SVR1 の DHCP コンソールを閉じます。

レッスン 2
DHCP スコープの計画と実装

目次

参考資料

DHCP リースの長さの決定

注 : クライアント コンピューターは、起動時にもリースの更新を試みます。

レッスン 3
IPAM のプロビジョニング戦略の計画と実装

目次

デモンストレーション

デモンストレーション : IPAM の実装

デモンストレーションの手順

IPAM をインストールする

1. LON-SVR2 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、結果ウィンドウの [役割と機能の追加] をクリックします。
3. 役割と機能の追加ウィザードで、[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、[次へ] をクリックします。
7. [機能の選択] ページで、[IP アドレス管理 (IPAM) サーバー] チェック ボックスをオンにします。
8. [IP アドレス管理 (IPAM) サーバーに必要な機能を追加しますか] ダイアログ ボックスで、[機能の追加] をクリックし、[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. 役割と機能の追加ウィザードが完了したら、ウィザードを閉じます。

IPAM を構成する

1. サーバー マネージャー コンソールのナビゲーション ウィンドウで、[IPAM] をクリックします。
2. IPAM の概要ウィンドウで、[IPAM サーバーへの接続] をクリックします。[LON-SVR2.Adatum.com] を選択し、[OK] をクリックします。
3. [IPAM サーバーをプロビジョニングする] をクリックします。
4. IPAM のプロビジョニング ウィザードで、[次へ] をクリックします。
5. [プロビジョニング方法の選択] ページで、[グループ ポリシー ベース] が選択されていることを確認し、[GPO 名のプレフィックス] ボックスに「IPAM」と入力し、[次へ] をクリックします。
6. [設定の確認] ページで、[適用] をクリックします。プロビジョニングが完了するまでにしばらくかかります。
7. プロビジョニングが完了したら、[閉じる] をクリックします。
8. IPAM の概要ウィンドウで、[サーバー検出の構成] をクリックします。
9. [サーバー検出の構成] ダイアログ ボックスで [追加] をクリックし、[OK] をクリックします。
10. IPAM の概要ウィンドウで、[サーバー検出を開始する] をクリックします。検出には 5 ～ 10 分かかる場合があります。黄色のバーは、検出がいつ完了するかを示します。
11. IPAM の概要ウィンドウで、[管理するサーバーを選択または追加し、IPAM アクセスを確認する] をクリックします。両方のサーバーの [IPAM アクセスの状態] が [ブロックされている] に設定されていることを確認します。詳細ビューまで下にスクロールし、状態レポートを確認します。IPAM サーバーには、グループ ポリシーで LON-DC1 を管理するためのアクセス許可が与えられていません。
12. タスクバーで、[Windows PowerShell] アイコンを右クリックし、[管理者として実行] をクリックします。
13. Windows PowerShell プロンプトで次のコマンドを入力し、Enter キーを押します。

```
Invoke-IpamGpoProvisioning –Domain Adatum.com
–GpoPrefixName IPAM
–IpamServerFqdn
LON-SVR2.adatum.com
–DelegatedGpoUser Administrator
```

14. 確認を求められた場合は「Y」と入力し、Enter キーを押します。コマンドが完了するまでしばらくかかります。
15. Windows PowerShell を閉じます。
16. サーバー マネージャー コンソールに切り替えます。
17. IPv4 の詳細ウィンドウで、[lon-dc1] を右クリックし、[サーバーの編集] をクリックします。
18. [サーバーの追加または編集] ダイアログ ボックスで、[管理の状態] フィールドを [管理] に設定し、[OK] をクリックします。
19. IPv4 の詳細ウィンドウで、[lon-svr1] を右クリックし、[サーバーの編集] をクリックします。
20. [サーバーの追加または編集] ダイアログ ボックスで、[管理の状態] フィールドを [管理] に設定し、[OK] をクリックします。
21. LON-DC1 に切り替えます。
22. タスクバーで [Windows PowerShell] アイコンをクリックします。
23. Windows PowerShell プロンプトで「Gpupdate /force」と入力し、Enter キーを押します。
24. Windows PowerShell ウィンドウを閉じます。
25. LON-SVR1 に切り替えます。
26. タスクバーで [Windows PowerShell] アイコンをクリックします。
27. コマンド プロンプトで「Gpupdate /force」と入力し、Enter キーを押します。
28. Windows PowerShell ウィンドウを閉じます。
29. LON-SVR2 に切り替えます。
30. サーバー マネージャー コンソールで、[LON-DC1] を右クリックし、[サーバーのアクセス状態の更新] をクリックします。LON-SVR1 に対して、この手順を繰り返します。
31. 完了したら、[更新] アイコンをクリックして、IPv4 を最新の状態に更新します。状態が変更されるまで 5 分ほどかかる場合があります。データの取得状態に完了と表示されたら、次へ進みます。
32. IPAM の概要ウィンドウで、[管理されているサーバーからデータを取得する] をクリックします。操作が完了するまでしばらくかかります。

復習とまとめ

復習問題

質問 : 組織に 2 つのサブネットがあり、両方のサブネットのクライアント コンピューターにアドレスを割り当てるために DHCP を使用する必要があります。展開する DHCP サーバーは 1 つにする必要があります。検討する必要のある要因は何ですか。

解答 : 2 つのサブネットを相互接続するルーターが DHCP リレーをサポートしている必要があります。または、DHCP サーバーをホストしていないサブネットに DHCP リレーを配置する必要があります。さらに、単一の DHCP サーバーに障害が発生したに、サービスの可用性に与える影響についても考慮する必要があります。

質問 : 組織が大きくなり、IPv4 スコープでアドレスが枯渇しつつあります。この場合、何ができますか。

解答 : 既存のスコープと新しいスコープを結合して、スーパースコープを実装することができます。

質問 : DHCP 予約を構成するには、どのような情報が必要ですか。

解答 : 予約をリースするクライアントのメディア アクセス制御 (MAC) アドレスが必要です。

演習の復習問題と解答

演習 : IP 構成と IP アドレス管理のソリューションの設計と保守

質問と解答

演習の復習

質問 : IP 設計と計画の練習では、どのような手法を用いましたか。

解答 : さまざまな解答が考えられます。

質問 : IPAM 展開計画の練習では、どのような手法を用いましたか。

解答 : さまざまな解答が考えられます。

質問 : Contoso 社用の IP アドレス指定のスキーマを、あなたの会社の IP アドレス指定のスキーマを比較してください。

解答 : さまざまな解答が考えられます。

第 4 章
名前解決の設計と実装

目次

レッスン 1
DNS サーバーの実装戦略の設計

目次

参考資料

ネットワーク インフラストラクチャに関する情報の収集

注 : Microsoft ダウンロード センターの Web サイトで、これらの情報を収集するのに役立つ、多くの Solution Accelerator が提供されています。

DNS サーバーの役割の選択

注 : ルート ヒントは、DNS サーバーが、インターネット名前空間の他の場所で、名前解決を要請されたサーバーには権限のないレコードを見つけるためのメカニズムです。

DNS サーバーに関するセキュリティ上の考慮事項

注 : ゾーン転送は、特定のゾーンをサポートする DNS サーバー間で、そのゾーン データがコピーされるメカニズムです。この章の以降のセクションで、ゾーンとゾーン転送の両方について説明します。

注 : Active Directory 統合ゾーンを使用しない場合は、インターネット プロトコル セキュリティ (IPSec) を実装して、サーバー間のゾーン転送トラフィックを暗号化することを検討してください。

デモンストレーション

デモンストレーション : DNS 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

1. LON-SVR1 に切り替えます。
2. ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. サーバー マネージャー コンソールで、[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、[役割ベースまたは機能ベースのインストール] をクリックし、[次へ] をクリックします。
6. [対象サーバーの選択] ページで、[サーバー プールからサーバーを選択] を選択し、[次へ] をクリックします。
7. [サーバーの役割の選択] ページの [役割] リストで、[DNS サーバー] チェック ボックスをオンにし、[機能の追加]、[次へ] の順でクリックします。
8. [機能の選択] ページで、[次へ] をクリックします。
9. [DNS サーバー] ページで、[次へ] をクリックします。
10. [確認] ページで、[インストール] をクリックします。

11. 役割が正常に追加されたら [閉じる] をクリックします。

レッスン 2
DNS 名前空間の設計

目次

参考資料

DNS 名前空間のシナリオ

注 : AD DS 用の名前空間の設計を選択する前に、オプションを十分に考慮します。AD DS の実装後に名前空間を変更することもできますが、時間のかかる複雑なプロセスになります。

注 : ほとんどの場合、AD DS ドメイン内のコンピューターには、DNS ドメイン名と一致するプライマリ DNS サフィックスを使用します。一部の状況では、組織の合併後や買収中などの場合に、これらの名前を変更することが必要な場合があります。名前が異なる場合、これは切り離された名前空間と呼ばれます。切り離された名前空間のシナリオでは、コンピューターのプライマリ DNS サフィックスとコンピューターが存在する DNS ドメイン名が一致しません。切り離されたコンピューターとは、プライマリ DNS サフィックスが一致しないコンピューターです。ドメイン コントローラーの NetBIOS ドメイン名が DNS ドメイン名と一致しない場合も、切り離された名前空間のシナリオが発生します。

名前空間をホストする場合の考慮事項

注 : 小規模な組織は、この二重分割 DNS 方式によりメリットを得る可能性があります。内部 DNS レコードを内部設置型の DNS サーバーに構成し、外部 DNS レコードは組織のインターネット サービス プロバイダー (ISP) でホストされるようにすることを検討してください。

レッスン 3
DNS ゾーンの設計と実装

目次

質問と解答

討論 : DNS ゾーン戦略の設計

質問 : このシナリオで、DNS 設計をどのように変更しますか。

解答 : ブランチ オフィスに追加の DNS サーバーを展開することを検討します。しかし、それは DNS ゾーン転送の構成に影響します。

質問 : ネーム サーバーを追加する場合には、どこに配置しますか。

解答 : WAN リンクに障害が起きた場合の影響を軽減するためには、各場所に、本社の DNS サーバーを使用せずに DNS 解決をおこなう手段があるべきです。各場所に少なくとも 1 台の DNS サーバーを展開し、より大きなサイトにはより多くのサーバーを展開することを検討します。

質問 : どの DNS サーバーの役割を展開するように提案しますか。

解答 : 小規模のブランチでは、キャッシュ専用サーバーを運用することができます。それによって、ゾーン転送を避けることができます。より大きな規模のブランチには、northwindtraders.priv のセカンダリ ゾーンが必要です。しかし、Active Directory 統合ゾーンを検討するならば、すべての DNS サーバーをドメイン コントローラーに昇格することができます。それにより、ネットワークの回復性が向上し、ゾーン転送は AD DS レプリケーションの一部として、自動的に安全におこなわれます。

質問 : すべてのインターネット接続が本社経由で提供される場合、転送の設計をどのように提案しますか。

解答 : すべての DNS サーバーを、本社の DNS サーバーをフォワーダーとして使用するように、構成することができます。それにより、DNS クエリ トラフィックを追跡することも可能になります。

質問 : DNS ゾーンをどのように設計しますか。

解答 : 既存の northwindtraders.priv のゾーンは要件を満たしています。しかし、Active Directory 統合ゾーンへ移行することは有益です。

質問 : Active Directory ゾーンは示されていますか。

解答 : Active Directory ゾーンは、示されていると思われます。

質問 : ゾーン転送をどのようにして設計しますか。

解答 : ゾーン転送を、示された AD DS ゾーンを使用して設計することができます。Active Directory 統合ゾーンを使用する場合には、ブランチ内のすべての DNS サーバーが、AD DS ドメイン コントローラーである必要があります。これにより、ゾーン転送は、通常の AD DS レプリケーションの一部として実行されます。

質問 : Northwind Traders 社は Contoso 社 に買収されたばかりです。これは、DNS 設計の決定に影響を及ぼしますか。

解答 : はい、このことは DNS 設計を決定する際に影響します。Contoso.com ドメインのためには、条件付き転送が有効です。

参考資料

DNS ゾーンの種類

注 : Windows Server 2003 で導入されたスタブ ゾーンは、大規模な DNS 名前空間やマルチ ツリー フォレストで起きる問題のいくつかを解決します。マルチ ツリー フォレストとは、2 つ以上のドメイン名を含む Active Directory フォレストを指します。

NetBIOS 名前解決の考慮事項

注 : NetBIOS は、先頭から 15 文字を特定のコンピューターの名前に使用し、16 番目の文字は、そのコンピューター上にあるリソースまたはサービスを識別するために使用されます。LON-SVR2[20h] は NetBIOS 名の 1 つの例です。これは、LON-SVR2 コンピューター上のサーバー サービスを表します。

注 : WINS サーバー機能によって、WINS サポートを提供します。

デモンストレーション

デモンストレーション : DNS ゾーンの作成

デモンストレーションの手順

プライマリ逆引き参照ゾーンを作成する

1. LON-DC1 に切り替え、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、[ツール]、[DNS] の順にクリックします。
3. DNS コンソールで、[LON-DC1] を展開し、[逆引き参照ゾーン] を展開します。
4. [逆引き参照ゾーン] を右クリックし、[新しいゾーン] をクリックします。
5. 新しいゾーン ウィザードで、[次へ] をクリックします。
6. [ゾーンの種類] ページで、[プライマリ ゾーン] をクリックし、[次へ] をクリックします。
7. [Active Directory ゾーン レプリケーション スコープ] ページで、[次へ] をクリックします。
8. [逆引き参照ゾーン名] ページで、[IPv4 逆引き参照ゾーン] をクリックし、[次へ] をクリックします。
9. [逆引き参照ゾーン名] ページで、[ネットワーク ID] ボックスに「172.16.0」と入力し、[次へ] をクリックします。
10. [動的更新] ページで、[次へ] をクリックします。
11. [新しいゾーン ウィザードの完了] ページで、[完了] をクリックします。

新しいセカンダリ前方参照ゾーンを作成する

1. LON-SVR1 に切り替えます。
2. サーバー マネージャー コンソールで、[ツール]、[DNS] の順にクリックします。
3. DNS コンソールで、[LON-SVR1] を展開し、[前方参照ゾーン] を展開します。

4. [前方参照ゾーン] を右クリックし、[新しいゾーン] をクリックします。
5. 新しいゾーン ウィザードで、[次へ] をクリックします。
6. [ゾーンの種類] ページで、[セカンダリ ゾーン]、[次へ] の順にクリックします。
7. [ゾーン名] ページで、[ゾーン名] ボックスに「Adatum.com」と入力し、[次へ] をクリックします。
8. [マスター DNS サーバー] ページの [マスター サーバー] リストで、「172.16.0.10」と入力して、Enter キーを押し、[次へ] をクリックします。
9. [新しいゾーン ウィザードの完了] ページで、[完了] をクリックします。

レッスン 4
DNS ゾーンのレプリケーションと委任の設計と構成

目次

参考資料

セカンダリ ゾーンを実装する状況

注 : セカンダリ サーバーは、通常、Active Directory 統合ゾーンではないゾーンにのみ実装されます。ゾーンが Active Directory 統合ゾーンの場合、ゾーン転送は、構成に応じて、すべてのドメイン コントローラー間の AD DS レプリケーションの一環として、自動的におこなわれます。

注 : DNS ドメイン training.Contoso.com を、一致する名前を持つ新しいゾーンとして実装できます。この新しいゾーンは、独自のネーム サーバーと管理者を、権限のあるネーム サーバーを識別する親ゾーンの関連するレコードと一緒に持ちます。代替策として、Contoso.com の管理者は、Contoso.com ゾーンに Training という名前のサブドメイン レコードを作成できます。この場合、子ドメインに対するネーム サーバーは存在せず、委任も存在しません。

ゾーン転送とゾーン レプリケーション

注 : DNS 通知は、ゾーン変更時にセカンダリ サーバーへの通知を許容するという、本来の DNS プロトコル仕様を更新したものです。この機能は、データの精度が必要な、時間が重要となる環境で役立ちます。

ゾーン転送のセキュリティの計画

注 : BIND 8.1 は 1998 年にリリースされました。そのため、この DNS 実装のユーザーの多くは、2000 年にリリースされた無償のバージョン 9 にすでにアップグレードしているはずです。

名前空間の統合

注 : DNS サーバー上の再帰と再帰クエリは同一のものではないことを理解する必要があります。DNS サーバー上の再帰は、サーバーがルート ヒントを使用して DNS クエリを解決しようとすることを意味します。

デモンストレーション

デモンストレーション : ゾーン転送の構成

デモンストレーションの手順

ゾーンでゾーン転送を有効にする

1. LON-DC1 に切り替えます。
2. DNS コンソールで、[前方参照ゾーン] を展開し、[Adatum.com] をクリックします。
3. [Adatum.com] を右クリックし、[プロパティ] をクリックします。

4. [Adatum.com のプロパティ] ダイアログ ボックスで、[ゾーンの転送] タブをクリックします。
5. [ゾーン転送を許可するサーバー] チェック ボックスをオンにし、[ネーム サーバー タブの一覧にあるサーバーのみ] をクリックし、[通知] をクリックします。
6. [通知] ダイアログ ボックスの [次のサーバーのみ] リストで、「172.16.0.21」と入力し、Enter キーを押します。
7. [OK] をクリックし、[ネーム サーバー] タブをクリックします。
8. [追加] をクリックし、[新規ネーム サーバー レコード] ダイアログ ボックスの [サーバーの完全修飾ドメイン名 （FQDN)] テキスト ボックスで、「LON-SVR1.Adatum.com」と入力します。[解決] をクリックし、[OK] を 2 回クリックします。

ゾーン転送を実行する

1. LON-SVR1 に切り替え、DNS コンソールを開きます。
2. ナビゲーション ウィンドウで [Adatum.com] をクリックし、ツールバーで [最新の情報に更新] をクリックします。

注 : ゾーン転送はまだ行われていません。そのため、この手順では、ゾーンにレコードはありません。

3. LON-DC1 に切り替えます。
4. DNS コンソールで、[Adatum.com] を右クリックし、[新しいエイリアス (CNAME)] をクリックします。
5. [新しいリソース レコード] ダイアログ ボックスで、[エイリアス名] ボックスに「WWW」と入力します。
6. [ターゲット ホスト用の完全修飾ドメイン名 (FQDN):] ボックスに「LON-SVR1.Adatum.com」と入力し、「OK] をクリックします。
7. LON-SVR1 に切り替えます。
8. DNS コンソールで、[Adatum.com] を右クリックし、[マスターから転送] をクリックします。

注 : 新しいエイリアス レコードが表示されない場合、ナビゲーション ウィンドウで、[前方参照ゾーン] をクリックします。ツールバーで、[最新の情報に更新] をクリックします。[Adatum.com] をクリックし、新しいアイリアス レコードが存在することを確認します。

レッスン 5
DNS サーバーの最適化

目次

参考資料

DNS の再帰の最適化

注 : 再帰を無効にするには、DNS サーバーの [プロパティ] ダイアログ ボックスの [詳細設定] タブで [再帰を無効にする (フォワーダーも無効になります)] チェック ボックスをオンにします。

DNS ルート ヒントの最適化

注 : ルート ヒント ファイル Cache.dns は、%SystemRoot%¥System32¥Dns フォルダーに配置されます。

注 : ルート ヒントは、DNS サーバーの [プロパティ] ダイアログ ボックスの [ルート ヒント] タブで構成できます。

DNS サーバーの機能の最適化

注 : 既定では、DNS サーバーが、プライマリ ゾーンを持つマスター サーバーに接続できない場合、セカンダリ ゾーンのデータは 24 時間経過後に有効期限切れとなります。

Active Directory 統合ゾーンの最適化

注 : _msdcs サブドメインは、すべての AD DS ドメインのレコードを含んでいるので、既定で ForestDNSZones 内にあります。ほとんどの場合、他のゾーンは、ローカル ドメイン内でのみレプリケートされます。

レッスン 6
高可用性とセキュリティのための DNS の設計

目次

質問と解答

討論 : DNS セキュリティを設計するためのガイドライン

質問 : どうすれば、内部 DNS インフラストラクチャのセキュリティを強化できますか。

解答 : Active Directory 統合ゾーンを実装することにより、内部 DNS インフラストラクチャのセキュリティを強化することができます。

質問 : 提案をサポートするには、どのような構成変更が必要ですか。

解答 : ブランチ オフィス 1 に展開されているネーム サーバーを、ドメイン コントローラーに昇格させる必要があります。また、northwindtraders.priv ゾーンを Active Directory 統合ゾーン変換します。さらに、セカンダリ ゾーンとゾーン転送を使用することを避けるために、本社のネーム サーバーを、追加のドメイン コントローラーに置き換えることを検討すべきです。これらのサーバーの役割が変更されたときには、サーバーの名前を変更する必要があることに注意します。

質問 : DNS サーバーで更新を構成するための推奨される方法は何ですか。

解答 : Active Directory 統合を使用する場合、セキュリティで保護された更新のみを構成することができます。

質問 : どの DNS セキュリティ ポリシー レベルを選択しましたか。

解答 : DNS セキュリティ ポリシー レベルに [高] を選択する必要があります。

質問 : DNS 設計に関連する他のセキュリティ上の考慮事項はありませんか。

解答 : 前述の質問の解答により、さまざまな解答が考えられます。

参考資料

DNS セキュリティ戦略の選択

注 : これらのセキュリティ レベルは、単一の構成可能なオプションを表しているのではなく、DNS セキュリティ設定をセキュリティで保護するためのアプローチであることを理解する必要があります。

追加のセキュリティ設定の選択

注 : これらのセキュリティ オプションは、DNS サーバーの [プロパティ] ダイアログ ボックスの [詳細設定] タブで構成できます。

Windows Server 2012 の DNSSEC

注 : ゾーン署名を削除する DNSSEC 管理ユーザー インターフェイスを使用すると、ゾーンの署名を削除することもできます。

注：キー ロールオーバーは、キーの有効期間が終了した際に、1 つのキーの組を別の組に交換する動作です。

復習とまとめ

復習問題

質問 : DNS ゾーンのサブドメインと委任されたゾーンの違いは何ですか。

解答 : DNS ゾーンのサブドメインと委任されたゾーンの違いは、DNS ゾーンのサブドメインは独自のネーム サーバーがないのに対して、委任されたゾーンには独自の権限のあるネーム サーバーがあることです。

質問 : Contoso 社は地域毎に営業部門を設けています。営業スタッフの一部は、コンピューターが 10 台ぐらいしかない地域の営業センターに配属されています。営業スタッフのコンピューターは、Contoso 社の他のスタッフと同じアプリケーションとリソースにアクセスできる必要があります。これらの小規模のブランチには、どのように DNS を実装しますか。

解答 : いくつかの解答が考えられますが、最も論理的なのは、ブランチにキャッシュ専用サーバーを構成することです。

質問 : ブランチ オフィスとサブ サイトの間のリンク障害に耐えるように設計する場合、どのような影響がありますか。

解答 : キャッシュ専用サーバーでは問題があります。リンク障害のイベントでは、ローカルのネーム サーバーのみが、クエリされたレコードに対して、応答を返すことができます。必要なフォールト トレランスを提供するためには、ローカルの DNS サーバーを、セカンダリ ゾーンまたは Active Directory 統合ゾーン (DNS サーバーがドメイン コントローラーでもあると仮定) によって使用します。

質問 : すべての内部の DNS サーバーで再帰を無効にしますか。

解答 : 誤りです。内部の DNS サーバーは通常、再帰が有効である必要があります。一方で、外部 DNS 名前空間をホストしている DNS サーバーは、通常再帰を無効にします。それにより、インターネット クライアントが、DNS 名を解決するためにそのサーバーを使用することを防ぎます。

質問 : すべての DNS サーバーでラウンドロビンを無効にすることが、ベスト プラクティスでないのはなぜですか。

解答 : ラウンドロビンは、ネットワーク リソースの負荷を共有し分散するために DNS サーバーが使用する負荷分散メカニズムです。複数のリソース レコードがある場合、これを使用して、クエリの応答に含まれているすべてのリソース レコードの種類を回転することができます。この機能を無効にすることは、DNS サーバーのプロセッサー上のワークロードを軽減しますが、任意のクエリのためにすべてのクライアントを同一のリソース サーバーにダイレクトします。

質問 : どのような場合にキャッシュ専用サーバーを構成しますか。

解答 : キャッシュ専用サーバーはゾーン データを保持せず、そのため、ゾーン転送に参加しません。このことは、ブランチ オフィスへ接続している WAN リンクが、ゾーン転送トラフィックをサポートするために最小の空間容量しかもたない場合に、役立ちます。

質問 : NetBIOS 名前解決を検討する際に、どのような場合に GNZ ではなく WINS を選択しますか。

解答 : WINS は、NetBIOS 名の登録、登録解除、および解決を、静的な GNZ よりも強力にサポートします。NetBIOS アプリケーションにより依存するエンタープライズ環境のネットワークでは、WINS は論理的な選択です。
しかし、NetBIOS の使用が減少しつつある場合や、クライアントとサーバーが静的な IPv4 構成である場合には、GNZ は、NetBIOS 名前解決をサポートするために必要なすべてを提供することができます。

質問 : ゾーン転送中にネットワークを通過する間のゾーン データのセキュリティ保護について検討しています。すべての DNS サーバーは、ドメイン コントローラーの役割もおこなっています。予測されるセキュリティの脅威を軽減するための戦略を 2 つあげてください。

解答 : 戦略の 1 つは、Active Directory 統合ゾーンを実装することです。それにより、ゾーン転送は、ワイヤ上の標準の Active Directory 暗号化を使用した Active Directory レプリケーションの一部として、おこなわれます。もう 1 つの方法は、接続セキュリティの規則 (IPSec) を実装して、マスター サーバーとセカンダリ ゾーン ホルダーとして構成されたところの間のトラフィックを暗号化します。

演習の復習問題と解答

演習 : 名前解決の設計と実装

質問と解答

演習の復習

質問 : DNS 設計の練習では、どのような手法を用いましたか。

解答 : さまざまな解答が考えられます。

質問 : あなたの設計は提案されているソリューションとは違っていましたか。

解答 : さまざまな解答が考えられます。

質問 : Contoso 社用の DNS 設計と、あなたの会社の DNS 実装を比較してください。

解答 : さまざまな解答が考えられます。

第 5 章

Active Directory ドメイン サービスのフォレストおよびドメインのインフラストラクチャの設計と実装

目次

レッスン 1
AD DS フォレストの設計

目次

質問と解答

討論 : 適切なフォレスト設計の選択

質問 : 2 つの組織を統合するには、フォレストはいくつ必要ですか。

解答 : 2 つのフォレスト、しかも既存のフォレストが必要です。2 つの大きな組織の環境を変えるのは大プロジェクトで、多大な時間と費用を要します。

質問 : 2 つの組織を統合するために、どのような方法を推奨しますか。

解答 : 2 つの組織を統合するには、フォレストの信頼を使用します。

質問 : Tailspin Toys 社のフォレスト内のスキーマ変更は、検討する設計にどのように影響しますか。

解答 : 複数のフォレストを実装する主な理由は、1 つのフォレスト内のすべてのドメイン コントローラーが共通のスキーマを共有しているということです。つまり、2 つのフォレストは、別々の異なったスキーマを持っています。シナリオでは、スキーマの更新が両方の組織に関連する場合を除き、ビジネスに不可欠なアプリケーションをサポートするための変更は 1 つの組織内に配置されることになっているため、スキーマは別々のままにする必要があります。

質問 : 使用される既存の外部ドメイン名は、設計にどのような影響を与えますか。

解答 : これは設計要因ではありません。外部名は、内部の AD DS ドメイン名やフォレスト名と関連している必要はありません。

参考資料

AD DS フォレストとは

注 : AD DS フォレストにはルート ドメインが 1 つだけあります。このルート ドメインには、スキーマ マスターとドメイン名前付けマスターというフォレスト全体の 2 種類の操作マスターが含まれます。

複数フォレストを実装する際の考慮事項

注 : この場合、要件に対応するために、Active Directory ライトウェイト ディレクトリ サービス (AD LDS) を境界ネットワーク上に実装するなどの代替方法を検討します。

レッスン 2
AD DS フォレストの信頼の設計と実装

目次

デモンストレーション

デモンストレーション : フォレストの信頼の作成

デモンストレーションの手順

フォレストの信頼の前提条件を構成する

1. LON-DC1 に切り替え、必要に応じて、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、[ツール]、[DNS] の順にクリックします。
3. DNS のナビゲーション ウィンドウで、[LON-DC1]、[条件付フォワーダー] の順に展開し、[条件付フォワーダー] を右クリックし、[新規条件付フォワーダー] をクリックします。
4. [新規条件付フォワーダー] ダイアログ ボックスの [DNS ドメイン] ボックスに「treyresearch.net」と入力し、[IP アドレス] リストをクリックします。
5. 「172.16.10.10」と入力し、Enter キーを押して、[OK] をクリックします。
6. マウス ポインタでタスクバーの左下隅をポイントして、[Start] をクリックします。
7. 「cmd.exe」と入力し、Enter キーを押します。
8. コマンド プロンプトで「nslookup trey-dc1.treyresearch.net」と入力し、Enter キーを押します。クエリが成功すると、172.16.10.10 という IP アドレスが返されます。
9. TREY-DC1 に切り替えます。
10. 必要に応じて、ユーザー名「Treyresearch¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
11. [スタート] をクリックし、[管理ツール] をポイントして、[DNS] をクリックします。
12. DNS のナビゲーション ウィンドウで、[TREY-DC1]、[条件付フォワーダー] の順に展開し、[条件付フォワーダー] を右クリックし、[新規条件付フォワーダー] をクリックします。
13. [新規条件付フォワーダー] ダイアログ ボックスの [DNS ドメイン] ボックスに「Adatum.com」と入力し、[IP アドレス] リストをクリックします。
14. 「172.16.0.10」と入力し、Enter キーを押して、[OK] をクリックします。
15. [スタート] をクリックし、[検索] ボックスに「cmd.exe」と入力し、Enter キーを押します。
16. コマンド プロンプトで「nslookup lon-svr1.adatum.com」と入力し、Enter キーを押します。クエリが成功すると、172.16.0.21 という IP アドレスが返されます。

フォレストの信頼を作成する

1. LON-DC1 に切り替えます。
2. サーバー マネージャー コンソールで、[ツール] をクリックし、[Active Directory ドメインと信頼関係] をクリックします。
3. Active Directory ドメインと信頼関係コンソールで、[Adatum.com] をクリックして右クリックし、[プロパティ] をクリックします。
4. [Adatum.com のプロパティ] ダイアログ ボックスで [信頼] タブをクリックし、[新しい信頼] をクリックします。
5. [新しい信頼ウィザード] ダイアログ ボックスで、[次へ] をクリックします。
6. [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。
7. [信頼の種類] ページで、[フォレストの信頼]、[次へ] の順にクリックします。

8. [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。
9. [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。
10. [ユーザー名とパスワード] ページで、[ユーザー名] ボックスに「Treyresearch¥Administrator」と入力します。
11. [パスワード] ボックスに「Pa$$w0rd」と入力し、[次へ] をクリックします。
12. [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、[次へ] をクリックします。
13. [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、[次へ] をクリックします。
14. [信頼の選択の完了] ページで、[次へ] をクリックします。
15. [信頼の作成完了] ページで、[次へ] をクリックします。
16. [出力方向の信頼の確認] ページで、[確認する] をクリックし、[次へ] をクリックします。
17. [入力方向の信頼の確認] ページで、[確認する] をクリックし、[次へ] をクリックします。
18. [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。
19. [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。

レッスン 3
AD DS ドメインの設計と実装

目次

参考資料

AD DS ドメイン モデル

注 : フォレスト内のすべてのドメインは相互に信頼し合うので、ドメインはセキュリティ境界を提供しません。さらに、フォレスト ルート ドメインにある Enterprise Admins アカウントには、すべてのフォレスト ドメインに対する管理者特権があります。

注 : ドメイン名は変更できますが、簡単なプロセスではありません。このため、ドメインの展開を開始するときに必ず正確なドメイン名を指定する必要があります。

注 : 細かい設定が可能なパスワード ポリシーおよびアカウント ロックアウト ポリシーも、ドメイン設計モデルの選択に影響を与える場合があります。Windows Server 2008 より前のバージョンの Windows Server では、ドメインの既定のドメイン ポリシーで指定することにより、すべてのドメイン ユーザーに 1 つのパスワード ポリシーと 1 つのアカウント ロックアウト ポリシーだけしか適用できませんでした。そのため、ユーザー セットごとに異なるパスワードとアカウント ロックアウトの設定を作成することはできましたが、パスワード フィルターを作成するか、複数ドメインを展開する必要がありました。Windows Server 2008 の発売以降、細かい設定が可能なパスワード ポリシーを使用して、複数のパスワード ポリシーを指定し、単一のドメイン内の異なるユーザー セットに異なるパスワード制限とアカウント ロックアウト ポリシーを適用できるようになりました。

デモンストレーション

デモンストレーション : AD DS ドメインの実装

デモンストレーションの手順

AD DS サーバーの役割を追加する

1. CON-SVR に切り替えます。
2. ユーザー名「Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. サーバー マネージャー コンソールで、詳細ウィンドウの [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、[役割] リストの [Active Directory ドメイン サービス] チェックボックスをオンにします。
8. [機能の追加] をクリックし、[次へ] をクリックします。
9. [機能の選択] ページで、[次へ] をクリックします。
10. [Active Directory ドメイン サービス] 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. 役割のインストールが完了したら、[閉じる] をクリックします。

既存のフォレストに新しいドメインを作成する

1. サーバー マネージャー コンソールのナビゲーション ウィンドウで、[AD DS] をクリックします。
2. 詳細ウィンドウをクリックします。

3. [すべてのサーバー タスクの詳細と通知] ダイアログ ボックスで、[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。
4. Active Directory ドメイン サービス構成ウィザードの [配置構成] ページで、[新しいドメインを既存のフォレストに追加する] をクリックします。
5. [ドメインの種類の選択] リストで、[ツリー ドメイン] をクリックします。
6. [フォレスト名] ボックスに「adatum.com」と入力します。
7. [新しいドメイン名] ボックスに「contoso.com」と入力し、[変更] 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 [ユーザー名] ボックスに「Adatum¥Administrator」と入力します。[パスワード] ボックスに「Pa$$w0rd」と入力します。
9. [OK] をクリックし、[次へ] をクリックします。
10. [ドメイン コントローラー オプション] ページの [パスワード] および [パスワードの確認入力] ボックスに「Pa$$w0rd」と入力し、[OK] をクリックします。
11. [DNS オプション] ページで、[次へ] をクリックします。
12. [追加オプション] ページで、[次へ] をクリックします。
13. [パス] ページで [次へ] をクリックします。
14. [オプションの確認] ページで、[次へ] をクリックします。
15. 前提条件のチェックが完了したら、[インストール] をクリックします。
16. コンピューターが再起動します。メッセージ ダイアログが表示されたら、ユーザー名「Contoso¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。

レッスン 4
AD DS 環境の DNS 名前空間の設計

目次

参考資料

DNS サーバーを AD DS 環境に実装するためのガイドライン

注 : 内部の DNS レコードをインターネット上に公開するのは、セキュリティ上非常に危険です。攻撃者が、攻撃しようとする内部サーバーを決めるために、この情報を使用する可能性があるからです。例えば、攻撃者はこの情報を使用して、データベース サーバーまたはドメイン コントローラーを識別し、これらのサーバーに対して攻撃を実行する可能性があります。

レッスン 5
AD DS ドメインの信頼の設計

復習とまとめ

復習問題

質問 : リソースのフォレスト モデルの目的は何ですか。

解答 : リソースのフォレスト モデルは、特に重要な、もしくはセキュリティで保護されたアプリケーション、共有フォルダー、その他のシステム リソースがある環境で使用できます。こうしたシナリオでは、管理者は、そのリソースにアクセスする必要のあるユーザーだけを対象とするフォレストを作成します。

質問 : フォレストの信頼を確立するためには、AD DS にどんなフォレストの機能レベルを設定する必要がありますか。

解答 : 2 つのフォレストの間でフォレストの信頼を確立できるようにするには、フォレストの機能レベルを、Windows Server 2003 以降のサーバーに設定する必要があります。さらに、クライアントが別のフォレストの名前を解決できるようにするため、両方のフォレストで DNS を構成する必要もあります。

質問 : 複数の内部名前空間を統合したい場合、どのようなテクノロジを使用しますか。

解答 : スタブ ゾーンと委任レコードを使用します。

質問 : Contoso 社のユーザーが Tailspin Toys ドメイン内の共有フォルダーにアクセスしようとして、アクセス拒否エラーを受信しました。これらの 2 つのドメイン間には信頼関係が存在します。ユーザーにアクセス権を提供するために何をする必要がありますか。

解答 : まず、信頼の方向をチェックして、認証の選択が適用されていることを確認します。その後、共有フォルダーでアクセス制御リスト (ACL) をチェックします。

演習の復習問題と解答

演習 A : Active Directory ドメイン サービス フォレストのインフラストラクチャの設計と実装

質問と解答

演習の復習

質問 : AD DS フォレストの設計の練習にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : あなたの設計は提案されているソリューションとは違っていましたか。

解答 : さまざまな解答が考えられます。

質問 : コストを重要視しないのであれば、あなたの設計はどのようになりますか。

解答 : さまざまな解答が考えられますが、すべての組織を 1 つのフォレストに統合することのメリットに着目してもよいでしょう。これは費用のかかるプロジェクトですが、いくつかの (章内で検討したような) 利点があります。

演習 B : AD DS ドメインのインフラストラクチャの設計と実装

質問と解答

演習の復習

質問 : AD DS ドメインの設計の練習にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : あなたの設計は提案されているソリューションとは違っていましたか。

解答 : さまざまな解答が考えられます。

質問 : このドメインの設計は、組織のドメインの実装と比較してどのようなものですか。

解答 : さまざまな解答が考えられます。

第 6 章

Active Directory の組織単位のインフラストラクチャの設計と実装

目次

レッスン 1
Active Directory 管理タスク委任モデルの計画

目次

参考資料

Active Directory 管理タスク委任モデルとは

参考資料 : Active Directory 管理の委任に関するベスト プラクティスの詳細については、次の 2 つのリンクを参照してください。

- http://go.microsoft.com/fwlink/?linkid=279914
- http://go.microsoft.com/fwlink/?linkid=279915

レッスン 2
OU 構造の設計

目次

質問と解答

OU の設計方式

質問 : あなたの職場で使用しているのは、どのような OU 構造ですか。そのように設計した理由は何ですか。OU モデルに関して、現在直面している問題は何ですか。

これらの質問について、他の受講者および講師と討論してください。

解答 : <解答記入欄>

誤った削除からの OU の保護

質問 : あなたの組織の OU 構造について、どう思いますか。変更したい点はありますか。

解答 : <解答記入欄>

デモンストレーション

デモンストレーション : OU の実装

デモンストレーションの手順

OU を作成する

1. LON-DC1 に切り替え、必要に応じて、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、[ツール]、[Active Directory 管理センター] の順にクリックします。
3. Active Directory 管理センター コンソールのナビゲーション ウィンドウで、[Adatum (local)] をクリックします。
4. タスク ウィンドウの [Adatum (local)] セクションで [新規]、[組織単位] の順にクリックします。
5. [組織単位の作成] ダイアログ ボックスで、[名前] ボックスに「Contoso-IT」と入力します。[説明] ボックスに「アカウントと管理用グループを登録する OU」と入力します。
6. [誤って削除されないように保護する] チェック ボックスがオンになっていることを確認します。
7. OU を作成し、[組織単位の作成 : Contoso-IT] ダイアログ ボックスを閉じるには、[OK] をクリックします。

OU が誤った削除から保護されていることを確認する

1. サーバー マネージャー コンソールで、[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. [Active Directory ユーザーとコンピューター] のメニューで、[表示]、[拡張機能] の順にクリックします。
3. Active Directory ユーザーとコンピューター コンソールで、[Adatum.com] を展開し、[Adatum.com] をクリックします。
4. 詳細ウィンドウで [Contoso-IT] を右クリックし、[プロパティ] をクリックします。

5. [Contoso-IT のプロパティ] ダイアログ ボックスで [オブジェクト] タブをクリックします。[誤って削除されないようにオブジェクトを保護する] チェック ボックスがオンになっていることを確認し、[OK] をクリックします。
6. Active Directory ユーザーとコンピューター コンソールを閉じます。

OU の既定のセキュリティ設定を検査する

1. Active Directory 管理センター コンソールへ切り替えます。
2. Active Directory 管理センターのナビゲーション ウィンドウで、[Adatum (local)] をクリックします。
3. 詳細ウィンドウで、[Contoso-IT] OU をクリックします。
4. タスク ウィンドウの [Contoso-IT] セクションで、[プロパティ] をクリックします。
5. [セキュリティ] タブで、[詳細設定] をクリックします。
6. [Contoso-IT のセキュリティの詳細設定] ダイアログ ボックスで、既定のセキュリティ設定を確認し、[キャンセル] をクリックします。

保護されている OU を削除する

1. [Contoso-IT] ダイアログ ボックスで、[誤って削除されないようにオブジェクトを保護する] チェック ボックスをオフにし、[OK] をクリックします。
2. Active Directory 管理センター コンソールのタスク ウィンドウの [Contoso-IT] セクションで、[削除] をクリックします。
3. [削除の確認] ダイアログ ボックスで、[はい] をクリックします。

レッスン 3
Active Directory グループ戦略の設計と実装

目次

質問と解答

Windows Server 2012 の Active Directory グループ

質問 : あなたの組織のグループ戦略について、クラスで討論してください。グループ戦略に関して、現在あなたの環境で直面している問題は何ですか。

解答 : <解答記入欄>

参考資料

注 : セキュリティ グループと配布グループの間で、グループを変換できます。セキュリティ グループに対して電子メールを有効にすることはできますが、セキュリティのアクセス許可を配布グループに付与することはできません。アクセス許可をセキュリティ グループに付与した後、それを配布グループに変換した場合、アクセス許可は残りますが、有効にはなりません。

デモンストレーション

デモンストレーション : グループの作成と管理

デモンストレーションの手順

OU を作成する

1. LONDC1 で、Active Directory 管理センターに切り替えます。
2. Active Directory 管理センターのナビゲーション ウィンドウで、[Adatum (local)] をクリックします。
3. タスク ウィンドウの [Adatum (local)] セクションで [新規]、[組織単位] の順にクリックします。
4. [組織単位の作成] ダイアログ ボックスで、[名前] ボックスに「SelfService」と入力します。[説明] ボックスに「自己管理するグループの OU」と入力し、[OK] をクリックします。

グループを作成して、グループの管理を構成する

1. Active Directory 管理センター コンソールの詳細ウィンドウで、[SelfService] OU をダブルクリックします。
2. タスク ウィンドウの [SelfService] セクションで、[新規]、[グループ] の順にクリックします。
3. [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「SportsInLondon」と入力します。[電子メール] ボックスに「SportsInLondon@adatum.com」と入力します。
4. [説明] ボックスに「ロンドン コミュニティのスポーツのメンバーを登録する自己管理 DL」と入力します。
5. Active Directory 管理センターの [SelfService OU] で、[SportsInLondon] グループをクリックします。
6. タスク ウィンドウの [SportsInLondon] セクションで、[プロパティ] をクリックします。
7. [SportsInLondon] ダイアログ ボックスの [管理者] セクションで、[編集] をクリックします。
8. [Select User, Contact or Group] 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「SportsInLondon」と入力し、[名前の確認]、[OK] の順にクリックします。

9. [SportsInLondon] ダイアログ ボックスの、[管理者] セクションで、[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、[OK] をクリックします。

ユーザーをグループに追加する

1. Active Directory 管理センターのナビゲーション ウィンドウで、[Adatum (local)] をクリックします。
2. 詳細ウィンドウで、[Marketing] OU をダブル クリックします。
3. 詳細ウィンドウで、[Adam Barr] をクリックします。
4. タスク ウィンドウの [Adam Barr] セクションで、[グループに追加] をクリックします。
5. [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「SportsInLondon」と入力し、[名前の確認]、[OK] の順にクリックします。

コミュニティ グループが自己管理できることを確認する

1. LON-CL1 からサインアウトします。
2. LON-DC1 で、ユーザー名「adatum¥administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. スタート画面で、[管理ツール] タイルをクリックします。
4. [管理ツール] で、[Active Directory 管理センター] をダブル クリックします。
5. Active Directory 管理センターの [概要] ページの [グローバル検索] ボックスに「Pat」と入力し、[検索] をクリックします。
6. 詳細ウィンドウで、[Pat Coleman] をクリックします。
7. タスク ウィンドウの [Pat Coleman] セクションで、[グループに追加] をクリックします。
8. [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「SportsInLondon」と入力し、[名前の確認] をクリックし、[OK] をクリックします。
9. Active Directory 管理センター コンソールのナビゲーション ウィンドウで、[Adatum (local)] をクリックします。
10. 詳細ウィンドウで、[SelfService] OU、[SportsInLondon] グループの順にクリックします。
11. タスク ウィンドウの [SportsInLondon] セクションで、[プロパティ] をクリックします。
12. [SportsInLondon] ダイアログ ボックスの [メンバー] セクションで、Pat Coleman がグループのメンバーであることを確認し、[キャンセル] をクリックします。
13. LON-DC1 からサインアウトします。

復習とまとめ

ベスト プラクティス

グループ戦略を設計する場合は、AG(U)DLP モデルを使用します。アカウントは、ビジネスの役割でグローバル グループにグループ化されます。必要に応じて、ドメインを跨いだこれらのグループを、ユニバーサル グループに統合することができます。役割グループは、特定のリソースへのアクセス権を付与されたドメイン ローカル グループを介して割り当てられます。

Active Directory 管理タスク モデルは、特権をなるべく付与しないことを念頭において設計します。ベスト プラクティスとしては、組織内のタスク一覧を作成し、それぞれのタスクを特定のチームに割り当てます。あるチームがアクセス許可を望む場合は、そのチームがそのタスクを担当することになります。

スクリプトを使用して、あなたの設計を実装します。アクセス許可を設定するための Windows PowerShell コマンドレットと dsacls ツールを確認します。

復習問題

質問 : 管理タスクを委任する際に、特権をなるべく実装しないのが良いのはなぜですか。

解答 : 管理タスクを他の管理グループに委任する際、委任された担当者がユーザー インターフェイスで目にするものを制限します。例えば、ある人が、ユーザー オブジェクトを対象とする OU でユーザー オブジェクトのみを作成する権利を持っている場合、その OU で誤ってコンピューター オブジェクトが作成された場合、ユーザーにはグループ ポリシーが必要になります。また、既定の Account Operators の使用を避ける必要があります。このグループが必要な場合、同じ権利を持つカスタム グループを作成することはできますが、適切なオブジェクト用 (コンピューター OU のコンピューター、ユーザー OU のユーザー、グループ OU のグループ) に限ります。タスクを委任する相手は、そうしたタスクをおこなうスキルを身につけている必要があります。AD DS は、特にスキーマや構成設定など、グローバルな変更になると、非常に複雑になる可能性があります。

質問 : 管理者アカウントを使用し、それらを通常のユーザー アカウントとは異なる場所に格納すべきなのは、なぜですか。

解答 : ユーザーは管理者アカウント特権を持っているため、電子メールのメッセージで、またはインターネットを閲覧している際に受け取るかもしれない悪意のあるコードが、バイナリを実行またはインストールする可能性があります。このため、管理だけを目的とする、専用の個人用管理アカウントの使用を推奨します。また、制限付き管理者アカウントは、委任から保護されています。この保護メカニズムが、携帯電話のメールや FAX などの特定のアプリケーションに予想外の問題を招く可能性があります。さらに、将来、自分の OU 構造内の管理者タスクを委任する可能性があります。そのため、管理者を別の OU 構造に置くことが大切です。それにより、誤って管理者の制御を委任したり、委任された管理者がアカウントを乗っ取り、よりレベルの高いアクセス許可を取得したりできないようにします。

質問 : OU 構造を新しいモデルに移行する際に、考慮しなければならないことは何ですか。

解答 : 新しい OU 構造が既存の構造に損傷を与えてはなりません。オブジェクトを移動する前に、委任が適切に機能していることを確認します。ユーザーやコンピューターを構成するために、GPO が適切にリンクされていることを確認します。さらに、どのポイントでユーザー アカウントの検索をおこなうかを構成するなど、ライトウェイト ディレクトリ アクセス プロトコル (LDAP) 対応のアプリケーションの再構成が必要な場合があります。これは、多機能プリンターや電話システムなど、コンピューターをベースとしないハードウェアにも影響する可能性があります。また、周辺ネットワーク アプリケーションにも影響する可能性があります。例えば、電子メール スキャナーは、電話番号を供給したり、あるいは、電子メールが組織の電子メール システムに入るのを許可する前に、ユーザーが電子メール アカウントを持っていることを確認したりするために、ディレクトリを使用しています。

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
セキュリティの委任ウィザードを使用して、アクセス許可を設定する際、ウィザードが再開した時点で、アクセス許可が表示されません。	共通の委任タスクを構成するには、Active Directory ユーザーとコンピューター コンソールのセキュリティ委任ウィザードを使用します。そこでおこなう設定は、OU の [セキュリティ] のプロパティに書き込まれますが、ウィザードには表示されません。アクセス許可を確かめるには、[セキュリティ] ダイアログ ボックスと [セキュリティの詳細] ダイアログ ボックスを使用して、設定を確認します。
どの属性を委任する必要があるかを、どのようにして判断しますか。	『Best Practices for Delegating Active Directory Administration Whitepaper』 ユーザー オブジェクトの値を変更したり、その値を見つけるために属性エディターを使用したりすることも可能です。LDIFDE.exe を使用して、変更の前後にオブジェクトの属性のテキスト ダンプを作成し、ファイルを比較することもできます。
[セキュリティの詳細] ダイアログ ボックスに表示されない属性のセキュリティ設定をどのようにして変更することができますか。	特定の属性は、[セキュリティの詳細] ダイアログ ボックスに隠されています。ベスト プラクティスは、DSAcls.exe を使用してセキュリティ設定を変更することです。

演習の復習問題と解答

演習 : Active Directory の組織単位 (OU) のインフラストラクチャおよび委任モデルの設計と実装

質問と解答

演習の復習

質問 : あなたはどのような OU の設計を提案しましたか。あなたが設計を決定した理由は何ですか。

解答 : さまざまな解答が考えられます。持ち時間に応じて、受講者はそれぞれの設計について検討します。

質問 : 演習では、Windows PowerShell を使用し、特定の属性に基づいて、ユーザー オブジェクトを移動しましたが、その他の方法でおこなうことができますか。

解答 : Active Directory ユーザーとコンピューター コンソールで、保存されたクエリ機能を使用して、カスタム クエリを作成し、クエリの結果をすべて選択し、それらを移動させることができます。あるいは、Active Directory 管理センター コンソールで、(LDAP フィルター経由で) グローバル検索を実施して、その結果得られるオブジェクトをすべて選択し、それらを一度に移動させることができます。ただし、Windows PowerShell を介するスクリプト、または、コマンド プロンプトで dsquery / dsmove を使用すること、および、それらのスクリプトを実行する前にテスト環境で評価することを推奨します。

質問 : Bill は、特定のグループの自己管理を提案しました。どのようにしてこれを実装しますか。この提案に関する利点とリスクは何ですか。

解答 : セキュリティに関係のないグループの自己管理は良いアイデアです。例えば、ユーザーが好きなときに自由にオプトインやオプトアウトをするコミュニティ グループ、または特定の配布リストを考えてみます。こうしたグループは、グループ自身がその「メンバー」属性を管理できるようにセキュリティ許可が設定されているグループです。グループ オブジェクトのプロパティの [管理者] プロパティを使用することもできます。自己管理を実装すると、グループのメンバーが他のユーザーを追加したり、あるいはメンバー自身を削除したりすることができます。グループに電子メールが有効化されている場合、グループのメンバーは、クライアント コンピューターの管理ツールを使わなくても Office Outlook を使用することができます。

第 7 章
グループ ポリシー オブジェクト戦略の設計と実装

目次

レッスン 1
GPO 設計に必要な情報の収集

目次

質問と解答

質問 : あなたの組織では、グループ ポリシーをどのように使用していますか。組織で、グループ ポリシーに関して直面している、または直面したことがある問題は何ですか。GPO を使って実行したいが、まだ実行できていない設定やタスクについて討論します。

解答 : さまざまな解答が考えられます。

参考資料 :

デスクトップ管理要件に関する情報の収集

注 : マルチドメイン環境では、GPO をサイトに割り当てる際に十分に注意する必要があります。GPO のファイルは SYSVOL に含まれ、必ず、GPO を作成しているドメイン内に作成されます。サイトは必ずしも、ドメインにマップしません。このため、GPO を作成したドメインのドメイン コントローラーがないサイトに GPO を割り当てる可能性があります。サイトのポリシーを作成する場合には、可能な限り、すべてのサイトにまたがるドメインに作成するようにしてください。

レッスン 2
GPO の設計と実装

目次

デモンストレーション

デモンストレーション：GPO の実装

デモンストレーションの手順

DSRM サービス ユーザーを作成する

1. LON-DC1 に切り替え、必要に応じて、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、[ツール]、[Active Directory 管理センター] の順にクリックします。
3. Active Directory 管理センター コンソールのナビゲーション ウィンドウで、[Adatum (ローカル)] をクリックし、[Users] コンテナーをダブルクリックします。
4. タスク ウィンドウの [Users] セクションで [新規] をクリックし、[ユーザー] をクリックします。
5. [ユーザーの作成] ダイアログ ボックスで、[フル ネーム] ボックスに「srv_dsrm」と入力します。
6. [ユーザー SAM アカウント名] テキスト ボックスに「adatum¥srv_dsrm」と入力します。
7. [パスワード] ボックスと [パスワードの確認入力] ボックスに「Pa$$w0rd」と入力します。
8. パスワードのオプションで、[その他のパスワード オプション] を選択し、[パスワードを無期限にする]、[OK] の順にクリックします。
9. Active Directory 管理センター コンソールの、[Users] コンテナーの詳細ウィンドウで、新規ユーザーの [srv_dsrm] をクリックします。
10. タスク ウィンドウの [srv_dsrm] セクションで、[無効] をクリックします。

グループ ポリシーを作成する

1. サーバー マネージャー コンソールで、[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。
3. [グループ ポリシー オブジェクト] ノードを右クリックし、[新規] をクリックします。
4. [新しい GPO] ダイアログ ボックスの [名前] ボックスに「DSRM_Pwd」と入力し、[OK] をクリックします。

グループ ポリシーの基本設定を使用してスケジュールされたタスクを作成する

1. [DSRM_Pwd] を右クリックし、[編集] をクリックします。
2. 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、[スケジュールされたタスク] をクリックします。
3. [スケジュールされたタスク] ノードを右クリックして、[新規] をポイントし、[タスク (Windows 7 以降)] をクリックします。
4. [新しいタスク (Windows 7 以降) のプロパティ] ダイアログ ボックスの [全般] タブの [操作の一覧] で、[作成] をクリックします。
5. [名前] テキスト ボックスに「Sync DSRM Password」と入力します。
6. [セキュリティのオプション] セクションで、[ユーザーまたはグループの変更] をクリックします。
7. [ユーザーまたはグループの変更] 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「System」と入力し、[名前の確認]、[OK] の順にクリックします。

8. [新しいタスク (Windows 7 以降) のプロパティ] ダイアログ ボックスで、[ユーザーがログオンしているかどうかにかかわらず実行する] をクリックします。
9. [タスク スケジューラ (Windows 7)] ダイアログ ボックスで、[キャンセル] をクリックします。
10. [パスワードを保存しない。タスクがアクセスできるのはローカル リソースのみ] チェック ボックスと、[最上位の特権で実行する] チェック ボックスをオンにします。
11. [トリガー] タブで [新規] をクリックします。
12. [新しいトリガー] ダイアログ ボックスの [設定] セクションで、[毎日] オプションを選択し、[詳細設定] セクションで、[繰り返し間隔] チェック ボックスをオンにして、[OK] をクリックします。
13. [新しいタスク (Windows 7 以降) のプロパティ] ダイアログ ボックスの [操作] タブで、[作成] をクリックします。
14. [新しい操作] ダイアログ ボックスの [設定] セクションの [プログラム/スクリプト] テキスト ボックスに「c:¥Windows¥System32¥ntdsutil.exe」と入力します。
15. [引数の追加 (オプション)] テキスト ボックスに「"set dsrm password” “sync from domain account srv_dsrm" quit quit」と入力し、[OK] を 2 回クリックします。

ポリシーを Domain Controllers OU にリンクする

1. グループ ポリシー管理コンソールのナビゲーション ウィンドウで、[Domain Controllers] をクリックします。
2. [Domain Controllers] を右クリックし、[既存の GPO のリンク] をクリックします。
3. [GPO の選択] ダイアログ ボックスの [グループ ポリシー オブジェクト] の下で、[DSRM_Pwd]、[OK] の順にクリックします。

レッスン 3
GPO の処理の設計

目次

質問と解答

質問 : これまでの 3 つのレッスンで説明した内容に基づいて、グループ ポリシー インフラストラクチャをどのように再設計したいですか。その変更を実装するときに生じる可能性のある問題は何ですか。

解答 : さまざまな解答が考えられます。

レッスン 4
グループ ポリシー管理の計画

目次

デモンストレーション

デモンストレーション：GPO の管理

デモンストレーションの手順

すべての GPO のバックアップを作成する

1. LON-DC1 のタスク バーで、Windows PowerShell® を起動します。
2. Windows PowerShell コマンド プロンプトで「New-Item c:¥GPO-Backups –ItemType Directory」と入力し、Enter キーを押します。
3. グループ ポリシー管理コンソールに切り替えます。
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] をクリックします。
5. [グループ ポリシー オブジェクト] を右クリックし、[すべてバックアップ] をクリックします。
6. [グループ ポリシー オブジェクトのバックアップ] ダイアログ ボックスの、「保存先」テキスト ボックスに「C:¥GPO-Backups¥」と入力し、「バックアップ」をクリックします。
7. バックアップが完了したら、[OK] をクリックします。

注：次の Windows PowerShell コマンドレットを使用して GPO をバックアップすることもできます。

```
Backup-GPO –All –Path c:¥GPO-Backups
```

8. GPMC で、[グループ ポリシー オブジェクト] を右クリックし、[バックアップの管理] をクリックします。
9. [バックアップの管理] ダイアログ ボックスで、オプションを確認して [OK] をクリックします。

GPO 設定を文書化する

1. GPMC の [グループ ポリシー オブジェクト] の下で、[DSRM_Pwd] をクリックします。
2. [DSRM_Pwd] を右クリックし、[レポートの保存] をクリックします。
3. [GPO レポートの保存] ダイアログ ボックスのナビゲーション ウィンドウで、[Allfiles (E:)]、[保存] の順にクリックします。
4. タスクバーで [エクスプローラー] をクリックします。
5. ナビゲーション ウィンドウで、[Allfiles (E:)] をクリックします。
6. 詳細ウィンドウで、[DSRM_Pwd.htm] をダブルクリックします。
7. [リンク] セクションおよび [セキュリティ フィルター処理] セクション、[委任]、固有の設定を順に表示します。

注：次の Windows PowerShell コマンドレットを使用して GPO 設定を文書化することもできます。

```
Get-GPOReport –Name GPO-Name –ReportType HTML –Path c:¥GPOReports¥GPOReport1.html
```

復習とまとめ

ベスト プラクティス

グループ ポリシーを編集する複数の管理者が存在し、管理者がさまざまなコンピューターから GPO の編集をおこなう場合、グループ ポリシー管理テンプレートのセントラル ストアを有効化します。

サイトに関連付けられたグループ ポリシーの使用は避けます。

グループ ポリシーのバックアップと回復の戦略を入念に計画します。

GPO を実環境のユーザーとコンピューターに適用する前に、グループ ポリシーのテストを計画します。

ユーザーとコンピューターに適用される GPO の数を制限します。ハイ レベルの GPO を共通の設定に使用し、個々の GPO での個別の設定を制限するように努めます。大量の GPO は、スタートアップとログオンの回数を増加させます。

定期的に、GPO とその設定、GPO が OU 構造の中のどこにリンクされているかを記録 (または更新) する時間をとります。

復習問題

質問 : 特定のユーザーまたはコンピューターに GPO を提供するためのオプションは何ですか。

解答 : Active Directory ドメイン内のドメインやサイト、または OU に、GPO をリンクさせることもできます。セキュリティ フィルターを使用して、グループに基づいてアクセス許可を設定したり、あるいは WMI フィルターを使用して、特定のハードウェアやオペレーティング システムの構成、その他のコンピューター管理上の側面を指定したりすることができます。さらに、継承を強制またはブロックして、GPO をどのように継承するかを調整することができます。

質問 : GPO をサイトに適用する際に何を考慮する必要がありますか。

解答 : GPO は Active Directory オブジェクトにリンクされ、特定の構成オプションは AD DS に格納されています。しかし、グループ ポリシー設定は SYSVOL 内のファイル ベースなので、特定のドメインで自動的にレプリケートされています、AD DS サイトは必ずしも ドメイン構造と一致する必要はありません。例えば、複数のサイトにまたがるドメイン、および複数のドメインのドメイン コントローラーを含むサイトを保有することができます。グループ ポリシーの設定が、ワイド エリア ネットワーク (WAN) に転送されないようにするには、GPO を割り当てたいサイトにおけるユーザーのログオン要求に十分応えられるだけのドメイン コントローラーを保有するドメインで、GPO を作成することが重要です。

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
最近変更したポリシーがまだ適用されません。	コマンド ラインから gpupdate /force を実行するか、または Windows PowerShell で Invoke-GPUpdate –force を実行します。
セキュリティのフィルター処理が期待したように機能しません。	GPMC の [委任] タブの、[セキュリティ] ダイアログ ボックスで [詳細設定] をクリックし、再度 [詳細設定] をクリックします。[セキュリティの詳細] ダイアログ ボックスの [有効なアクセス許可] タブで、特定のユーザーのセキュリティのアクセス許可の問題をトラブルシュートします。

演習の復習問題と解答

演習 : グループ ポリシー オブジェクト戦略の設計と実装

質問と解答

演習の復習

質問 : あなたはどのような GPO の設計を提案しましたか。

解答 : さまざまな解答が考えられます。持ち時間に応じて、受講者はそれぞれの GPO 設計について検討します。

質問 : あなたはアクセス許可の拒否を使用して、特定の GPO が IT 管理者に適用されないようにしています。同じ要件を達成するために使える他の方法はありますか。

解答 : アクセス許可の拒否は、非常に注意深く実装する必要があります。拒否は常にアクセス許可よりも優先され、予想外の結果を招く場合があるからです。とは言え、管理者にとって特定の GPO を拒否することは、一般的で有効なシナリオです。この目標を達成するために、他に考えられる唯一の方法は、その他の部署グループごとにポリシーを適用し、認証されたユーザーを削除することです。ただし、この方法は、まだ部署グループに割り当てられていないユーザー、または、後で追加する新しい部署グループについて、ポリシーに加えるのを忘れるというリスクを招く可能性があります。

第 8 章

Active Directory ドメイン サービス トポロジの設計と実装

目次

レッスン 1
AD DS サイトの設計と実装

目次

デモンストレーション

デモンストレーション : サイト オブジェクトの作成

デモンストレーションの手順

新しい AD DS サイトを作成する

1. LON-DC1 に切り替え、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. サーバー マネージャー コンソールで、[ツール] をクリックし、[Active Directory サイトとサービス] をクリックします。
3. Active Directory サイトとサービス コンソールで、[サイト] 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] をクリックします。
5. 「LondonHQ」と入力して Enter キーを押します。
6. ナビゲーション ウィンドウで、[サイト] を右クリックして、[新しいサイト] をクリックします。
7. [New Object – Site] ダイアログ ボックスで、[名前] ボックスに「Paris」と入力します。
8. [DEFAULTIPSITELINK] を選択し、[OK] をクリックします。
9. [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。

新しい AD DS サブネットを作成する

1. ナビゲーション ウィンドウで、[サブネット] を右クリックして、[新しいサブネット] をクリックします。
2. [新しいオブジェクト - サブネット] ダイアログ ボックスの [プレフィックス] テキスト ボックスに「172.16.0.0/24」と入力します。
3. [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] の下で、[LondonHQ] をクリックし、[OK] をクリックします。
4. ナビゲーション ウィンドウで、[サブネット] を右クリックして、[新しいサブネット] をクリックします。
5. [新しいオブジェクト - サブネット] ダイアログ ボックスの [プレフィックス] テキスト ボックスに「172.16.1.0/24」と入力します。
6. [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、[Paris] をクリックし、[OK] をクリックします。

レッスン 2
AD DS レプリケーションの設計

目次

参考資料

AD DS レプリケーションのコンポーネント

注 : 接続オブジェクトを使用して 2 つのドメイン コントローラー間で強制的にレプリケーションを実行するには、接続オブジェクトを右クリックして、[今すぐレプリケート] を選択します。ただし、前述のとおり、レプリケーションは入力方向のみです。そのため、両方のドメイン コントローラーをレプリケートするには、それぞれのドメイン コントローラーの入力方向の接続オブジェクトをレプリケートする必要があります。

グローバル カタログと RODC レプリケーションの計画

注 : グローバル カタログに含める予定の属性は、グローバル カタログ データのレプリケーションに影響します。

サイト リンク ブリッジを設計する際の検討事項

注 : トランスポート プロトコルの [サイト リンクをすべてブリッジ] オプションをオフにした場合のみ、サイト リンク ブリッジが必要になります。既定では、AD DS ではサイト リンクの推移性は有効で、その場合、サイト リンク ブリッジは何も影響しません。

レッスン 3
ドメイン コントローラーの配置の設計

目次

参考資料

ドメイン コントローラーのハードウェア要件の計画

注 : ドメイン コントローラーの仮想化を検討する際、ほとんどのハードウェア要件は、物理的なマシンでドメイン コントローラーを展開する場合と同じだということを考慮に入れます。

注 : 追加領域に関する要件も、リサイクル中のオブジェクトのサイズと数によって異なります。例えば、180 日という deletedObjectLifetime と recycledObjectLifetime の既定の値を使用して、Windows Server のドメインを作る際、Active Directory のごみ箱の機能は、Active Directory のデータベースのサイズを 20% 増加させていました。

注 : Windows Server 2012 をインストールできるのは、64 ビットのハードウェアのみです。

注 : ドメイン コントローラーの展開を計画する際は、AD DS 関連のソフトウェア以外のソフトウェアをドメイン コントローラーで展開しないようにします。これは、セキュリティとパフォーマンスのためです。追加ソフトウェアをドメイン コントローラーに展開する必要があるシナリオについては、ハードウェア要件が異なる場合があります。

Server Core でドメイン コントローラーを展開する際の考慮事項

注 : Server Core インストールを使用すると、Windows Server 2012 オペレーティング システムが最小構成でインストールされます。Server Core インストールでは、エクスプローラー インターフェイスはインストールされません。つまり、グラフィカル ユーザー インターフェイス (GUI) ツールを使用して、Server Core インストールをリモートで管理することを意味します。サーバーの構成と管理をローカルでおこなうには、コマンドライン ツールを使う必要があります。Windows Server 2012 には、Server Core インストールを管理するために使用できるサーバー構成ツール (sconfig.cmd) が搭載されています。

レッスン 4
ドメイン コントローラーの仮想化に関する考慮事項

目次

参考資料

ドメイン コントローラーを仮想マシンとして展開する際の考慮事項

注 : Windows Server 2012 の AD DS では、仮想マシンや GenerationID を把握しているハイパーバイザーがホストする仮想ドメイン コントローラー向けに、保護対策を導入しています。こうした保護対策は、仮想マシンの状態をロールバックさせるスナップショットを誤って適用して AD DS 環境を壊してしまうのを防ぐのに役立ちます。

レッスン 5
高可用性ドメイン コントローラーの設計

目次

参考資料

高可用性ドメイン コントローラーを設計する際の考慮事項

注 : ベスト プラクティスとして、[TryNextClosestSite] 設定を有効にすると、サイト トポロジやサイト リンク コストを可能な限り簡素化できます。数多くのハブ サイトを保有する組織では、あるサイトのクライアントが別のサイトのドメイン コントローラーにフェールオーバーする必要があるという状況に対応するための計画を簡素化することができます。

注 : 単一サイト環境での高可用性技術は、複数の Active Directory 環境で実装する技術とは異なる場合があります。

AD DS におけるバックアップと回復を設計する際の考慮事項

注 : Windows Server バックアップ MMC は、サーバー マネージャー コンソールのツール リストに表示されますが、その機能を手動で追加するまでは実際にはインストールされていません。

注 : Windows Server バックアップでは、テープへのバックアップのサポートは既に終了しています。

復習とまとめ

復習問題

質問 : マルチサイトの企業で、すべてのサブネットを特定し、サイトと関連付けることが重要なのはなぜですか。

解答 : クライアント コンピューターで、クライアント コンピューターの IP アドレスとサブネットの定義に基づいて正しいサイトを参照すると、ドメイン コントローラーや他のサービスの検索プロセスの効率を上げることができます。クライアント コンピューターの IP アドレスがサイトに属していない場合、クライアント コンピューターは、ドメイン内のすべてのドメイン コントローラーをクエリします。これでは効率が良くありません。実際は、異なるサイトにある複数のドメイン コントローラーにつき 1 台のクライアント コンピューターを実行できます。変更のレプリケートが終わっていないと、望ましくない結果に至る可能性があります。クライアント コンピューターがそれぞれどのサイトに位置するかを知っておくことが重要です。これは、クラアント コンピューターが、ドメイン コントローラーとそれが位置するサイトを特定することにより達成することができます。

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、あるサイトのすべてのドメイン コントローラーを別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、サイト間レプリケーションの管理をおこないます。

質問 : Active Directory レプリケーションの代わりとして使用できるのはどのプロトコルですか。それを使用することのデメリットは何ですか。

解答 : SMTP を使用することはできるが、ドメイン パーティションをレプリケートすることはできないという点です。

演習の復習問題と解答

演習 : Active Directory ドメイン サービスの物理トポロジの設計と実装

質問と解答

演習の復習

質問 : Active Directory サイトとレプリケーションの設計について、あなたの提案はどのようなものでしたか。

解答 : さまざまな解答が考えられます。

質問 : Active Directory ドメイン コントローラーの計画の実施にはどのように取り組みましたか。

解答 : さまざまな解答が考えられます。

質問 : この物理 AD DS 設計は、組織の AD DS の実装と比較してどのようなものですか。

解答 : さまざまな解答が考えられます。

第 9 章
記憶域の計画と実装

目次

レッスン 1
記憶域に関する考慮事項

目次

参考資料

さまざまな種類の記憶域に関する考察

注 : ユーザーがアクセスするドキュメントの大部分がファイル ベースの場合には、最も効率的で低コストなネットワーク記憶域ソリューションは NAS ソリューションです。共有する情報の大部分がデータベース アプリケーションのものである場合には、SAN が最も一般的なソリューションです。ブロック ベースのデータとファイル ベースのデータの両方を共有する必要がある場合は、NAS-SAN 結合ソリューションによって両方のニーズを効果的に満たすことができます。

レッスン 2
iSCSI SAN の計画と実装

目次

参考資料

iSCSI とは

注 : 標準のイーサネット ネットワーク アダプターを使用して、サーバーを iSCSI 記憶装置に接続することができますが、専用の iSCSI HBA を使用することも可能です。

iSCSI ターゲット サーバーと iSCSI イニシエーター

参考資料 : Windows Server 2012 における iSCSI ターゲット導入の詳細については、http://go.microsoft.com/fwlink/?linkid=279916 を参照してください。

デモンストレーション

デモンストレーション : iSCSI の実装

デモンストレーションの手順

iSCSI ターゲット サーバーの役割サービスを追加する

1. サーバー マネージャー コンソールで、[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、[サーバー プールからサーバーを選択] 選択し、[次へ] をクリックします。
5. [サーバーの役割の選択] ページの [ファイル サービスおよび記憶域サービス (インストール済み)] で、[ファイル サービスおよび記憶域サービス (インストール済み)] を展開し、[iSCSI ターゲット サーバー] チェック ボックスを選択したら、[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. [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。
8. インストールが完了したら、[閉じる] をクリックします。
9. コンピューターの再起動を求められた場合は、[今すぐ再起動する] をクリックします。
10. LON-DC1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。

2 つの iSCSI 仮想ディスクと 1 つの iSCSI ターゲットを作成する

1. LON-DC1 のサーバー マネージャー コンソールでナビゲーション ウィンドウの [ファイル サービスおよび記憶域サービス] をクリックします。
2. ファイル サービスおよび記憶域サービスウィンドウの [iSCSI] をクリックします。
3. iSCSI 仮想ディスク ウィンドウで [タスク] をクリックし、[タスク] ドロップダウン リスト ボックスで [iSCSI 仮想ディスクの新規作成] をクリックします。
4. iSCSI 仮想ディスク ウィンドウの新規作成ウィザードで、[iSCSI 仮想ディスクの場所を選択] ページの [記憶域の場所] の下で、ドライブ C をクリックし、[次へ] をクリックします。

5. [iSCSI 仮想ディスク名の指定] ページで「iSCSIDisk1」と入力し、[次へ] をクリックします。
6. [iSCSI 仮想ディスクのサイズの指定] ページの [サイズ] ボックスに「5」と入力し、ドロップダウン リスト ボックスで [GB] を選択し、[次へ] をクリックします。
7. [iSCSI ターゲットの割り当て] ページで、[新しい iSCSI ターゲット] をクリックし、「次へ」をクリックします。
8. [ターゲット名の指定] ページで、[名前] ボックスに「LON-SVR1」と入力し、[次へ] をクリックします。
9. [アクセス サーバーの指定] ページで [追加] をクリックします。
10. [イニシエーターを識別する方法を選択] ダイアログ ボックスで、[選択した種類の値の入力] をクリックし、[種類] ドロップダウン リスト ボックスの [IP アドレス] をクリックします。次に、[値] テキスト ボックスに「172.16.0.21」と入力し、[OK] をクリックします。
11. [アクセス サーバーの指定] ページで、[次へ] をクリックします。
12. [認証を有効にする] ページで、[次へ] をクリックします。
13. [選択内容の確認] ページで、[作成] をクリックします。
14. [結果の表示] ページで、作成が完了するまで待ち、[閉じる] をクリックします。
15. [iSCSI 仮想ディスク] ウィンドウで [タスク] をクリックし、[タスク] ドロップダウン リストの [iSCSI 仮想ディスクの新規作成] をクリックします。
16. iSCSI 仮想ディスク ウィンドウの新規作成ウィザードで、[iSCSI 仮想ディスクの場所を選択] ページの [記憶域の場所] の下にあるドライブ C をクリックし、[次へ] をクリックします。
17. [iSCSI 仮想ディスク名の指定] ページで「iSCSIDisk2」と入力し、[次へ] をクリックします。
18. [iSCSI 仮想ディスクのサイズの指定] ページの [サイズ] ボックスに「5」と入力し、ドロップダウン リスト ボックスで [GB] を選択したら、[次へ] をクリックします。
19. [iSCSI ターゲットの割り当て] ページで、[LON-SVR1] をクリックしたら、[次へ] をクリックします。
20. [選択内容の確認] ページで、[作成] をクリックします。
21. [結果の表示] ページで、作成が完了するまで待ち、[閉じる] をクリックします。

iSCSI ターゲットに接続する

1. LON-SVR1 のサーバー マネージャー コンソールの [ツール] メニューをクリックし、[iSCSI イニシエーター] をクリックします。
2. [Microsoft iSCSI] ダイアログ ボックスで、[はい] をクリックします。
3. [iSCSI イニシエーター プロパティ] ダイアログ ボックスの [ターゲット] タブで「LON-DC1」と入力し、[クイック接続] をクリックします。
4. クイック接続ウィンドウの [検出されたターゲット] セクションで [iqn.1991-05.com.microsoft:lon-dc1-LON-DC1-target] をクリックし、[完了] をクリックします。
5. [iSCSI イニシエーター プロパティ] ダイアログ ボックスで、[OK] をクリックしてダイアログ ボックスを閉じます。

iSCSI ドライブの存在を確認する

1. LON-SVR1 のサーバー マネージャー コンソールを開きます。[ツール] メニューで [コンピューターの管理] をクリックします。
2. コンピューターの管理コンソールで、[記憶域] ノードの下の [ディスクの管理] をクリックします。新しいディスクが追加されていることを確認します。ただし、それらのディスクは現在オフラインで、フォーマットされていません。

3. コンピューターの管理コンソールを閉じます。

レッスン 3
Windows Server 2012 の 記憶域スペース機能

目次

参考資料

記憶域スペースの機能

注 : 記憶域スペース機能では、同一の記憶域プール内に仮想プロビジョニングの仮想ディスクと固定プロビジョニングの仮想ディスクを両方作成することができます。両方のプロビジョニング対応種別を同じ記憶域プールに作成すると、両者が同じワークロードに関係する場合に特に便利です。例えば、仮想プロビジョニング スペースでデータベースをホストし、固定プロビジョニング スペースでそのログをホストすることができます。

記憶域スペース機能に関する考慮事項

注 : すべての有効なスペースを使用する記憶域構成を、固定プロビジョニングといいます。

注 : 3 方向ミラーでは使用可能なスペースは減少しますが、最大 2 台までのディスクの障害に耐えることができます。

復習とまとめ

復習問題

質問 : Tailspin Toys 社は、記憶域インフラストラクチャのさまざまな側面の実装方法を決定しなければなりません。共有ファイルを一元管理できる場所に保存する必要がありますが、今回は完全なファイル サーバーを実装する予定はありません。どのような種類の記憶域を推奨しますか。

解答 : NAS または SAN 記憶域ソリューションなど、さまざまな解答が考えられます。

質問 : Tailspin Toys 社は、複数のデータベース サーバーを実装することを計画しており、データベースのためにディスク領域を提供する予定です。すべてのデータベースのために、単一で集中管理できるディスク アレイを作成したいと考えています。どのような種類の記憶域を推奨しますか。

解答 : NAS または SAN 記憶域ソリューションなど、さまざまな解答が考えられます。

質問 : DAS 記憶域ソリューションに比べて、SAN 記憶域ソリューションの主なメリットは何ですか。

解答 : SAN 記憶域ソリューションの主なメリットは、効率的なリソースの共有が可能であり、記憶域の利用率が高く、ハードウェアの整理統合と可能性を促進することです。

演習の復習問題と解答

演習 : 記憶域の計画と実装

質問と解答

演習の復習

質問 : 記憶域の計画の練習では、どのような手法を用いましたか。

解答 : さまざまな解答が考えられます。

質問 : あなたの組織には、どのように記憶域を実装しますか。

解答 : さまざまな解答が考えられます。

第 10 章
ファイル サービスの計画と実装

目次

レッスン 1
DFS の計画と実装

目次

参考資料

DFS 名前空間を計画する場合の考慮事項

注 : アクセスベースの列挙を使用すると、ユーザーがファイル サーバーの内容を参照するときに、ユーザーにアクセス権が付与されているファイルおよびフォルダーのみが表示されます。これにより、ユーザーがファイル サーバーに接続したときに、アクセスできないファイルやフォルダーが大量に存在することを発見して混乱するのを避けることができます。

注 : スライドの表には、名前空間の各種類の特徴がまとめられています。

DFS レプリケーションを計画する場合の考慮事項

注 : 各レプリケート フォルダーには、自身のステージング フォルダーがあり、既定で、DFS ReplicationPrivate¥Staging フォルダー内のレプリケート フォルダーのローカル パスの下に置かれます。

注 : 競合を解決できないファイルやフォルダーは、「競合して削除されたフォルダー」という名前のフォルダーに移動されます。検索のために、競合して削除されたフォルダーに削除済みファイルやフォルダーを移動するようにサービスを構成することもできます。各レプリケート フォルダーには、それ自身の競合して削除されたフォルダーがあり、DFS ReplicationPrivate¥ConflictandDeleted フォルダー内のレプリケート フォルダーのローカル パスの下に置かれます。

DFS データ記憶域のシナリオ

注 : このシナリオでは、変更がブランチ サーバー全体にレプリケートされるため、ユーザーが一部のファイルの不整合を許容できる場合にのみ推奨されます。また、DFS レプリケーションは、ファイルが閉じられた後にのみ、ファイルをレプリケートすることに注意してください。そのため、長時間開いたままになっているデータベース ファイルや任意のファイルをレプリケートする場合は、DFS レプリケーションは推奨されません。

デモンストレーション

デモンストレーション : DFS の展開と構成

デモンストレーションの手順

DFS の役割をインストールする

1. LON-SVR1 のサーバー マネージャー コンソールで、[管理] をクリックし、[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、[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、[ファイル サービスおよび記憶域サービス]、[ファイル サービスおよび iSCSI サービス] の順に展開し、[DFS 名前空間] チェック ボックスをオンにします。
6. 役割と機能の追加ポップアップ ウィンドウで、[機能の追加] をクリックします。
7. [DFS レプリケーション] 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. [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。

新しい名前空間を作成する

1. LON-SVR1 のサーバー マネージャー コンソールで、[ツール]、[DFS 管理] の順にクリックします。
2. DFS 管理コンソールで、[名前空間] をクリックします。
3. [名前空間] を右クリックし、[新しい名前空間] をクリックします。
4. 新しい名前空間ウィザードの [名前空間サーバー] ページで、[サーバー] の下に「LON-SVR1」と入力し、[次へ] をクリックします。
5. [名前空間の名前と設定] ページで、[名前] の下に「Research」と入力し、[次へ] をクリックします。
6. [名前空間の種類] ページで、[ドメインベースの名前空間] と [Windows Server 2008 モードを有効にする] の両方が選択されていることを確認し、[次へ] をクリックします。
7. [設定の確認と名前空間の作成] ページで、[作成] をクリックします。
8. [確認] ページで、名前領域の作成タスクが正常に完了したことを確認し、[閉じる] をクリックします。
9. コンソールで、[名前空間] ノードを展開し、[¥¥Adatum.com¥Research] をクリックします。受講者と共に、詳細ウィンドウの 4 つのタブを確認します。
10. コンソールで [¥¥Adatum.com¥Research] を右クリックし、[プロパティ] をクリックします。[全般]、[紹介]、[詳細設定] タブのオプションを確認します。
11. [OK] をクリックして、[¥¥Adatum.com¥Research のプロパティ] ダイアログ ボックスを閉じます。

新しいフォルダーとフォルダー ターゲットを作成する

1. LON-SVR1 の DFS 管理コンソールで、[¥¥Adatum.com¥Research] を右クリックし、[新しいフォルダー] をクリックします。
2. [新しいフォルダー] ダイアログ ボックスで、[名前] ボックスに「Proposals」と入力します。
3. [新しいフォルダー] ダイアログ ボックスの [フォルダー] ターゲットの下で、[追加] をクリックします。
4. [フォルダー ターゲットを追加] ダイアログ ボックスに「¥LON-SVR1¥Proposal_docs」と入力し、[OK] をクリックします。
5. [警告] ダイアログ ボックスで、[はい] をクリックします。
6. [共有の作成] ダイアログ ボックスで、次の設定を構成し、[OK] をクリックします。
    i. 共有フォルダーのローカル パス : C:¥Proposal_docs
    ii. 共有フォルダーのアクセス許可 : 管理者はフル アクセス権を、その他のユーザーは読み取り/書き込みアクセス許可を持つ
7. [警告] ダイアログ ボックスで、[はい] をクリックします。
8. [OK] をクリックして、[新しいフォルダー] ダイアログ ボックスを閉じます。

9. コンソールで [¥¥Adatum.com¥Research] を展開し、[プロパティ] をクリックします。現時点でフォルダー ターゲットが 1 つだけであることを確認します。(冗長化するには、DFS レプリケーションを構成して、2 つ目のフォルダー ターゲットを追加します。)
10. 名前空間をテストするには、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。
11. エクスプローラーのアドレス バーに「¥¥Adatum.com¥Research」と入力し、Enter キーを押します。[Proposals] フォルダーが表示されます。

レプリケーション用の新しいフォルダー ターゲットを作成する

1. LON-DC1 に切り替えます。
2. ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. サーバー マネージャー コンソールに切り替えます。
4. サーバー マネージャー コンソールで [管理]、[役割と機能の追加] の順にクリックします。
5. 役割と機能の追加ウィザードで [次へ] をクリックします。
6. [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。
7. [対象サーバーの選択] ページで [次へ] をクリックします。
8. [サーバーの役割の選択] ページで、[ファイル サービスおよび記憶域サービス]、[ファイル サービスおよび iSCSI サービス] の順に展開し、[DFS 名前空間] チェック ボックスをオンにします。
9. [役割と機能の追加ウィザード] ポップアップ ダイアログ ボックスで、[機能の追加] をクリックします。
10. [DFS レプリケーション] チェック ボックスをオンにし、[次へ] をクリックします。
11. [機能の選択] ページで、[次へ] をクリックします。
12. [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。
13. インストールが完了したら、[閉じる] をクリックします。
14. サーバー マネージャー コンソールを閉じます。
15. LON-SVR1 に切り替えます。
16. DFS の管理コンソールで、[Proposals] フォルダーを右クリックし、[フォルダー ターゲットを追加] をクリックします。
17. [新しいフォルダー ターゲット] ダイアログ ボックスに「¥¥LON-DC1¥Proposal_docs」と入力し、[OK] をクリックします。
18. 共有フォルダーを作成するには、[警告] ダイアログ ボックスで、[はい] をクリックします。
19. [共有の作成] ダイアログ ボックスで、[共有フォルダーのローカル パス] フィールドに「C:¥Proposal_docs」と入力します。
20. [共有フォルダーのアクセス許可] フィールドで、[管理者はフル アクセス権を、その他のユーザーは読み取り/書き込みアクセス許可を持つ] を選択し、[OK] をクリックします。
21. [警告] ダイアログ ボックスで、[はい] をクリックします。
22. [レプリケーション] ダイアログ ボックスで、[はい] をクリックします。レプリケート フォルダー ウィザードが起動します。

新しいレプリケーション グループを作成する

1. レプリケート フォルダー ウィザードの [レプリケーション グループおよびレプリケート フォルダーの名前] ページで、既定の設定を受け入れて、[次へ] をクリックします。

2. [レプリケーションの対象] ページで、LON-DC1 と LON-SVR1 がいずれも DFS レプリケーションのメンバーとして適切であることを確認し、[次へ] をクリックします。
3. [プライマリ メンバー] ページで、[LON-SVR1] をプライマリ メンバーとして選択し、[次へ] をクリックします。
4. [トポロジの選択] ページで、既定の [フル メッシュ] を選択したままにします。(これにより、レプリケーション グループのすべてのメンバーの間で、すべてのデータがレプリケートされます。)
5. すべての選択を確認し、[次へ] をクリックします。
6. [レプリケーション グループのスケジュールおよび帯域幅] ページで、[継続的にレプリケートする] という既定の選択にしたままで、[全帯域] を使用するように設定を構成します。特定のスケジュールを選択して、指定した日時の間にレプリケートをおこなうこともできます。
7. [次へ] をクリックします。
8. [設定の確認およびレプリケーション グループの作成] ページで、[作成] をクリックします。
9. [確認] ページで、すべてのタスクが正常に完了したことを確認し、[閉じる] をクリックします。レプリケーションの遅延の警告を確認し、[OK] をクリックします。
10. コンソールで、[Replication] を展開します。
11. [Replication] の下で、[Adatum.com¥research¥proposals] をクリックします。
12. 詳細ウィンドウの各タブをクリックして確認します。

レッスン 2
BranchCache の計画と実装

目次

質問と解答

討論 : DFS レプリケーションまたは BranchCache の選択

質問 : 組織内のブランチ オフィスに勤務するユーザーに対して、本社のサーバーに格納されているファイルへの高速なアクセス方法を提供する必要があります。一部のブランチ オフィスにはファイル サーバーが配置されており、他のブランチ オフィスには配置されていません。ブランチ オフィスには、Windows 7 や Windows 8 などのオペレーティング システムが混在します。DFS レプリケーションと BranchCache のどちらが実装に適していますか。その理由は何でしょうか。

解答 : BranchCache を実装する必要があります。BranchCache の主要機能が、ブランチ オフィスのユーザーに対し、キャッシュを介してリモート ファイルへのより早いアクセスを提供しているからです。ファイル サーバーがないと、DFS レプリケーションの実装に問題が起きます。

質問 : 営業部門は、リモート営業オフィスでファイルを活用しています。これらのファイルは、毎日、その日の終わりに一か所にまとめる必要があります。営業部門のユーザーは、Windows 7 または Windows 8 のどちらかをベースにするノート PC を使用しています。このシナリオでは、DFS レプリケーションと BranchCache のどちらが最適ですか。

解答 : DFS レプリケーションの方が適しています。ただし、DFS レプリケーションはブランチごとにファイル サーバーを必要とします。BranchCache は、ファイルを集中管理された場所に順に並べることはしないため、機能しません。

参考資料

BranchCache モードの選択

注 : BranchCache を使用する際、組織内では両方のモードを使用することができますが、ブランチ オフィス単位では 1 つのモードしか構成できません。

デモンストレーション

デモンストレーション : BranchCache の実装

デモンストレーションの手順

ネットワーク ファイル用 BranchCache の役割サービスを追加する

1. LON-DC1 に切り替え、必要に応じて、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. タスクバーで [サーバー マネージャー] をクリックします。
3. サーバー マネージャー コンソールで、[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、[サーバー プールからサーバーを選択] が選択されていることを確認し、[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、[ファイル サービスおよび記憶域サービス (インストール済み)]、[ファイル サービスおよび iSCSI サービス] の順に展開し、[ネットワーク ファイル用 BranchCache] 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. [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。

ローカル グループ ポリシー エディターで BranchCache を構成する

1. LON-DC1 で、マウス ポインタをタスクバーの左下隅に置き、[スタート] をクリックします。
2. スタート画面で「gpedit.msc」と入力し、Enter キーを押します。
3. [コンピューターの構成]、[管理用テンプレート]、[ネットワーク] の順に展開し、[LAN Manager サーバー] をクリックし、[BranchCache のハッシュの発行] をダブルクリックします。
4. [BranchCache のハッシュの発行] ダイアログ ボックスで、[有効] をクリックします。
5. [オプション] ボックスの [ハッシュの発行の動作] の下で、[ハッシュの発行を BranchCache が有効になっている共有フォルダーにのみ許可する]、[OK] の順にクリックします。
6. ローカル グループ ポリシー エディターを閉じます。

ファイル共有用に BranchCache を有効にする

1. 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. エクスプローラーで、[ローカル ディスク (C:)] をダブルクリックします。
3. ウィンドウの左上にあるクイック アクセス バーで、[新しいフォルダー] をクリックし、「Share 」と入力し、Enter キーを押します。
4. [Share] を右クリックし、[プロパティ] をクリックします。
5. [Share のプロパティ] ダイアログ ボックスで [共有] タブをクリックし、[詳細な共有] をクリックします。
6. [詳細な共有] ダイアログ ボックスで、[このフォルダーを共有する]、[キャッシュ] の順にクリックします。
7. [オフラインの設定] ダイアログ ボックスで、[BranchCache を有効にする] チェック ボックスをオンにし、[OK] をクリックします。
8. [詳細な共有] ダイアログ ボックスで、[OK] をクリックし、[閉じる] をクリックします。
9. 開いているウィンドウをすべて閉じます。

レッスン 3
ダイナミック アクセス制御の計画と実装

目次

参考資料

ID、要求、および集約型アクセス ポリシーとは

注 : 集約型アクセス ポリシーを作成する前に、集約型アクセス規則を少なくとも 1 つは作成する必要があります。集約型アクセス規則では、特定のリソースへのアクセスを制御するパラメータと条件をすべて定義します。集約型アクセス ポリシーには、3 つの構成可能な要素があります。

- **名前 :** それぞれの集約型アクセス規則に対し、わかりやすい名前を付けることを推奨します。
- **ターゲット リソース :** ポリシーの適用先となるデータを定義します。これは、属性とその値を指定することで定義されます。例えば、特別な集約型アクセス規則が、重要と分類したデータに適用される場合があります。
- **アクセス許可 :** だれがデータにアクセスできるかを定義する 1 つ以上のアクセス制御エントリ (ACE) の一覧です。例えば、EmployeeType (従業員の種類) 属性が FTE (フルタイムの社員) に設定されているユーザーに、フル コントロールのアクセス許可を指定することができます。これは、各集約型アクセス規則の重要なコンポーネントです。集約型アクセス規則で課した条件を組み合わせてグループ化することができます。また、アクセス許可は、(ステージングのための) Proposed (提案されたアクセス許可) または Current (現在のアクセス許可) として設定できます。

注 : 集約型アクセス規則を 1 つ以上構成し、その規則を集約型アクセス ポリシーに追加します。これにより、その規則がリソースに適用されます。

デモンストレーション

デモンストレーション : ダイナミック アクセス制御用の集約型アクセス規則と集約型アクセス ポリシーの作成

デモンストレーションの手順

1. LON-DC1 のタスクバーで、[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 コンソールで、[ツール]、[Active Directory 管理センター] の順にクリックします。
3. Active Directory 管理センター コンソールのナビゲーション ウィンドウで、[ダイナミック アクセス制御] をクリックします。
4. [Claim Types] をダブルクリックします。
5. 作業ウィンドウで、[新規]、[要求の種類] の順にクリックします。
6. 要求の種類の作成ウィンドウのソース属性セクションで、[department] 属性をクリックします。
7. [表示名] テキスト ボックスに「Company Department」と入力します。
8. [ユーザー] と [コンピューター] の両方のチェック ボックスをオンにし、[OK] をクリックします。
9. 作業ウィンドウで、[新規]、[要求の種類] の順にクリックします。
10. 要求の種類の作成ウィンドウのソース属性セクションで、[employeetype] 属性をクリックします。
11. [表示名] テキスト ボックスに「Employee Type」と入力します。

12. [ユーザー] と [コンピューター] の両方のチェック ボックスをオンにし、[OK] をクリックします。
13. [ダイナミック アクセス制御] をクリックします。
14. 中央のウィンドウで、[リソース プロパティ] をダブルクリックします。
15. [リソース プロパティ] のリストで、[Department] を右クリックし、[有効にする] をクリックします。
16. Active Directory 管理センター コンソールのナビゲーション ウィンドウで、[ダイナミック アクセス制御] をクリックします。
17. [Central Access Rules] をダブルクリックします。
18. 作業ウィンドウで、[新規]、[集約型アクセス規則] の順にクリックします。
19. [集約型アクセス規則の作成] ダイアログ ボックスで、[名前] ボックスに「Department Match」と入力します。
20. ターゲット リソース セクションで、[編集] をクリックします。
21. 集約型アクセス規則ウィンドウで、[条件の追加] をクリックします。
22. 次のとおりに条件を設定し、[OK] をクリックします。
Resource-Department-Equals-Value-Research and Development.
23. [アクセス許可] セクションで、[次のアクセス許可を現在のアクセス許可として使用する] をクリックし、[編集] をクリックします。
24. [Administrators (ADATUM¥Administrators)] をクリックし、[削除] をクリックします。
25. [アクセス許可のセキュリティの詳細設定] で、[追加] をクリックします。
26. [アクセス許可のアクセス許可エントリ] ダイアログ ボックスで、[プリンシパルの選択] をクリックします。
27. [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 ボックスに「Authenticated Users」と入力し、[名前の確認]、[OK] の順にクリックします。
28. 基本のアクセス許可セクションで、[変更]、[読み取りと実行] および [読み取りと書き込み] をクリックします。
29. [条件を追加] をクリックします。
30. [グループ] ドロップダウン リストで、[Company Department] をクリックします。
31. [値] ドロップダウン リストで [リソース] をクリックします。
32. 最後のドロップダウン ボックスで、[Department] をクリックします。

注：この結果、[User-Company Department-Equals-Resource-Department] が表示されます。

33. [OK] を 3 回クリックします。
34. Active Directory 管理センター コンソールで、[ダイナミック アクセス制御] をクリックし、[Central Access Policies] をダブルクリックします。
35. 作業ウィンドウで、[新規]、[集約型アクセス規則] の順にクリックします。
36. [名前] ボックスに「Department Match」と入力し、[追加] をクリックします。
37. [Department Match] 規則をクリックし、[詳細 (>>)] アイコンをクリックします。
38. [OK] を 2 回クリックします。

復習とまとめ

復習問題

質問 : ドメインベースの DFS 名前空間の主なメリットは何ですか。

解答 : ドメインベースの DFS 名前空間の主なメリットは、ファイル サービスの役割クラスタリングを実装しなくても、名前空間のフォールト トレランスを提供できることです。

質問 : BranchCache と DFS の違いは何ですか。

解答 : BranchCache は、ユーザーがリモートの場所からアクセスしたファイルだけをキャッシュします。DFS は、本社とリモートの場所の間でファイルをレプリケートし、両方の場所にすべてのファイルが存在するようにします。

質問 : BranchCache を、分散キャッシュ モードではなく、ホスト型キャッシュ モードで実装するのはなぜですか。

解答 : 分散キャッシュ モードを使用すると、Windows 8 を実行しているすべてのコンピューターにキャッシュが分散されます。ただし、Windows 8 を実行しているコンピューターまたはノート PC がシャット ダウンされたり、オフィスから撤去されたりする場合があります。これはつまり、キャッシュされたファイルが他のユーザーには利用できないということで、そのファイルを WAN リンクを経由して再度ダウンロードする必要があります。このため、Windows Server 2012 オペレーティング システムを実行しているコンピューターがブランチ オフィスで利用可能なときは、ほとんどの場合ホスト型キャッシュ モードを利用することになります。

質問 : 要求 (クレーム) とは何ですか。

解答 : 要求とは、特定のオブジェクト (通常はユーザーまたはコンピューター) について AD DS が示す情報です。要求は、エンティティに関して、信用できる提供元からの情報を提供します。

質問 : 集約型アクセス ポリシーの目的は何ですか。

解答 : 集約型アクセス ポリシーにより、管理者は、組織内の 1 つ以上のファイル サーバーに適用するポリシーを作成することができます。集約型アクセス ポリシーには、1 つ以上の集約型アクセス ポリシーの規則が含まれています。各規則には、適用性とアクセス許可を決定する設定が含まれています。

演習の復習問題と解答

演習 : ファイル サービスの設計と実装

質問と解答

演習の復習

質問 : データ アクセス設計にどのような手法を用いましたか。

解答 : さまざまな解答が考えられます。

質問 : ダイナミック アクセス制御設計にどのような手法を用いましたか。

解答 : さまざまな解答が考えられます。

質問 : あなたの組織では、ブランチ オフィスに対し、どのようにデータ アクセスを実装しますか。

解答 : さまざまな解答が考えられます。

第 11 章
ネットワーク アクセス サービスの設計と実装

目次

レッスン 1
リモート アクセス サービスの設計と実装

目次

質問と解答

討論 : リモート アクセスの設計

質問 : 営業部門のユーザーのニーズである電子メールへのアクセスに対応するにはどうすればよいでしょうか。

解答 : 既存の VPN を使用して電子メールへのアクセスをサポートすることはできますが、その場合、電子メールへのアクセス用の特定のトラフィックを円滑にするために、ネットワーク ポリシーを変更する必要があります。Exchange Server 2010 および Outlook 2010 では、RPC over HTTPS を使用する接続をサポートしています。この方法は、ユーザーが電子メールサーバーと通信できるもう 1 つの方法です。この方法は、データベース アクセス用に備えることもできる VPN を利用する場合と比べて、いくつかの利点があります。特に、ファイアウォールに対する構成変更の必要がありません。また、ユーザーが内部ネットワーク上にいる場合、ユーザーが電子メールにアクセスする方法は変わりません。ユーザーは、接続のために VPN を起動する必要がありません。

質問 : 設計をサポートするためにその他のネットワーク コンポーネントが必要ですか。必要であれば、それは何ですか。

解答 : 電子メールへのリモート クセスは、選択したソリューションによっては、ファイアウォールの変更が必要な場合があります。また、メール ボックス サーバーを境界ネットワークに配置することは推奨できません。

質問 : データベース アクセスを実現にするには、どの種類の VPN トンネルを推奨しますか。

解答 : どのクライアントの種類も、ファイアウォールの再構成が最小限で済む SSTP をサポートしています。IKEv2 は、Windows 7 および Windows 8 でも使用することができます。

参考資料

適切なトンネリング プロトコルの選択

注 : SSTP は HTTPS に依存するため、他のトンネルの種類を使用できない場所でも、SSTP を使用して VPN 接続を確実に開始できます。例えば、ファイアウォールが HTTP トラフィックおよび HTTPS トラフィックの通過しか許可しないホテルでも、SSTP ベースのトンネルを使用できます。

注 : PPTP、L2TP、SSTP は、本来 PPP 向けに指定された機能によって大きく異なります。PPP は、ダイヤルアップまたは専用の point-to-point 接続でデータを送信するように設計されました。IP の場合、PPP は、PPP フレーム内で IP パケットをカプセル化した上で、カプセル化した PPP パケットを point-to-point リンクを介して送信します。PPP はもともと、ダイヤルアップ クライアントとネットワーク アクセス サーバーとの間で使用するプロトコルとして定義されたものです。

注 : VPN 再接続は、IKEv2 テクノロジを使用して、シームレスで一貫した VPN 接続を提供します。VPN 再接続では、インターネット接続が再度使用可能になると、VPN 接続が自動的に再確立されます。これは、ワイヤレス モバイル ブロードバンドを使用して接続するユーザーに最適な機能です。

注 : IKEv2 VPN 接続では、許容される最長ネットワーク停止時間を設定できます。これは既定では 30 分ですが、5 分～ 8 時間の範囲で設定できます。

ネットワーク アクセス ポリシーの計画

注 : NPS が一致する規則を検出すると、それ以降の規則は無視されます。そのため、ネットワーク ポリシーを適切に順序付けることが重要です。

デモンストレーション

デモンストレーション : VPN の実装

デモンストレーションの手順

VPN サーバーを構成する

1. LON-RTR で、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. 必要に応じて、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。
3. 詳細ウィンドウで、[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、[役割ベースまたは機能ベースのインストール] をクリックし、[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、[ネットワーク ポリシーとアクセス サービス] チェック ボックスをオンにします。
8. [機能の追加] をクリックし、[次へ] を 2 回クリックします。
9. [ネットワーク ポリシーとアクセス 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、[ネットワーク ポリシー サーバー] チェック ボックスがオンになっ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完了したことを確認し、[閉じる] をクリックします。
13. サーバー マネージャー ウィンドウを閉じます。
14. マウス ポインターをタスクバーの左下隅に置き、[スタート] をクリックします。
15. スタート メニューで、[ネットワーク ポリシー サーバー] をクリックします。
16. ネットワーク ポリシー マネージャーのナビゲーション ウィンドウで、[NPS (ローカル)] を右クリックし、[Active Directory にサーバーを登録] をクリックします。
17. [ネットワーク ポリシー サーバー] メッセージ ボックスで、[OK] をクリックします。
18. [ネットワーク ポリシー サーバー] ダイアログ ボックスで、[OK] をクリックします。
19. ネットワーク ポリシー サーバー コンソール ウィンドウを開いたままにします。
20. マウス ポインターをタスクバーの左下隅に置き、[スタート] をクリックします。

21. [スタート] で [管理ツール] をクリックし、[ルーティングとリモート アクセス] をダブルクリックします。[DirectAccess の有効化ウィザード] が開始されたら、[キャンセル]、[OK] の順にクリックします。
22. ルーティングとリモート アクセス コンソールで、[LON-RTR (ローカル)] を右クリックし、[ルーティングとリモート アクセスの無効化] をクリックします。
23. ダイアログ ボックスで、[はい] をクリックします。
24. ルーティングとリモート アクセス コンソールで、[LON-RTR (ローカル)] を右クリックし、[ルーティングとリモート アクセスの構成と有効化] をクリックします。
25. [次へ] をクリックし、[リモート アクセス (ダイヤルアップまたは VPN)]、[次へ] の順にクリックします。
26. [VPN] チェック ボックスをオンにし、[次へ] をクリックします。
27. [ローカル エリア接続 2] のネットワーク インターフェイスをクリックし、[選択したインターフェイスに静的パケット フィルターをセットアップしてセキュリティを有効にする] チェック ボックスをオフにし、[次へ] をクリックします。
28. [IP アドレスの割り当て] ページで、[指定したアドレス範囲] をクリックし、[次へ] をクリックします。
29. [アドレス範囲の割り当て] ページで、[新規] をクリックします。[開始 IP アドレス] フィールドに「172.16.0.100」と入力し、[終了 IP アドレス] フィールドに「172.16.0.110」と入力し、[OK] をクリックします。
30. リモート クライアントに 11 個の IP アドレスが割り当てられていることを確認し、[次へ] をクリックします。
31. [複数のリモート アクセス サーバーの管理] ページで、[次へ] をクリックします。
32. [完了] をクリックします。
33. [ルーティングとリモート アクセス] ダイアログ ボックスで、[OK] をクリックします。
34. 求められたら、再度 [OK] をクリックします。

VPN クライアントを構成する

1. LON-CL2 に切り替えます。
2. ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. スタート画面で「コントロール」と入力します。
4. アプリの一覧で、[コントロール パネル] をクリックします。
5. [コントロール パネル] で [ネットワークとインターネット]、[ネットワークと共有センター]、[新しい接続またはネットワークのセットアップ] の順にクリックします。
6. [接続オプションを選択します] ページで、[職場に接続します]、[次へ] の順にクリックします。
7. [どの方法で接続しますか] ページで、[インターネット接続 (VPN) を使用します] をクリックします。
8. [インターネット接続は後でセットアップします] をクリックします。
9. [接続に使用するインターネット アドレスを入力してください] ページで、[インターネット アドレス] ボックスに「10.10.0.1」と入力します。
10. [接続先の名前] ボックスに「Adatum VPN」と入力します。
11. [他の人がこの接続を使うことを許可する] チェック ボックスをオンにし、[作成] をクリックします。

12. ネットワークと共有センター ウィンドウで、[アダプターの設定の変更] をクリックします。
13. [Adatum VPN] 接続を右クリックして [プロパティ] をクリックし、[セキュリティ] タブをクリックします。
14. [セキュリティ] タブの [VPN の種類] リストで、[Point to Point トンネリング プロトコル (PPTP)] をクリックします。
15. [認証] の下の [次のプロトコルを許可する] をクリックし、[OK] をクリックします。
16. ネットワーク接続ウィンドウで、[Adatum VPN] 接続を右クリックし、[接続/切断] をクリックします。
17. 右にある [ネットワーク] リストで、[Adatum VPN] をクリックし、[接続] をクリックします。
18. ネットワーク認証で、[ユーザー名] テキスト ボックスに「Adatum¥Administrator」と入力します。
19. [パスワード] テキスト ボックスに「Pa$$w0rd」と入力し、[OK] をクリックします。
20. VPN 接続が確立されるまで待ちます。接続に成功しました。認証の問題に関するエラー 812 が表示されます。
21. [閉じる] をクリックします。

Windows グループの条件に基づく VPN ポリシーを作成する

1. LON-RTR に切り替えます。
2. [ネットワーク ポリシー サーバー] に切り替えます。
3. ネットワーク ポリシー サーバーで、[ポリシー] を展開し、[ネットワーク ポリシー] をクリックします。
4. 詳細ウィンドウで、リストの先頭のポリシーを右クリックし、[無効にする] をクリックします。
5. 詳細ウィンドウで、リストの最後のポリシーを右クリックし、[無効にする] をクリックします。
6. ナビゲーション ウィンドウで、[ネットワーク ポリシー] を右クリックし、[新規] をクリックします。
7. 新しいネットワーク ポリシー ウィザードで、[ポリシー名] テキスト ボックスに「Adatum VPN Policy」と入力します。
8. [ネットワーク アクセス サーバーの種類] リストで、[リモート アクセス サーバー (VPN - ダイヤルアップ)] をクリックし、[次へ] をクリックします。
9. [条件の指定] ページで、[追加] をクリックします。
10. [条件の選択] ダイアログ ボックスで、[Windows グループ]、[追加] の順にクリックします。
11. [Windows グループ] ダイアログ ボックスで、[グループの追加] をクリックします。
12. [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)] テキスト ボックスに「Domain Admins 」と入力し、[OK] をクリックします。
13. 再度 [OK] をクリックし、[次へ] をクリックします。
14. [アクセス許可の指定] ページで [アクセスを許可する] をクリックし、[次へ] をクリックします。
15. [認証方法の構成] ページで、[次へ] をクリックします。
16. [制約の構成] ページで、[次へ] をクリックします。
17. [設定の構成] ページで、[次へ] をクリックします。
18. [新しいネットワーク ポリシーの完了] ページで、[完了] をクリックします。

VPN をテストする

1. LON-CL2 に切り替えます。
2. 右にある [ネットワーク] リストで、[Adatum VPN] をクリックし、[接続] をクリックします。
3. ネットワーク認証で、[ユーザー名] テキスト ボックスに「Adatum¥Administrator」と入力します。
4. [パスワード] テキスト ボックスに「Pa$$w0rd」と入力し、[OK] をクリックします。
5. VPN 接続が確立されるまで待ちます。

レッスン 2
NPS による RADIUS 認証の設計

目次

質問と解答

討論 : RADIUS 実装の設計

質問 : 境界ネットワークには 3 台の VPN サーバーがあり、受信リモート アクセス接続に十分な容量を備えています。ネットワーク ポリシーの管理と適用を簡素化するにはどのようにしますか。

解答 : NPS の役割を展開し、そのサーバーを RADIUS サーバーとして構成することを検討します。次に、RRAS を実行している VPN サーバーを、RADIUS サーバーとして構成します。最後に、NPS サーバーで、ネットワーク ポリシーを構成します。

質問 : VPN を使うことなくすべてのユーザーに電子メール アクセスを提供することはできますか。

解答 : はい、技術的には、RPC over HTTPS を実装できます。ただし、他のリソースへのアクセスを望むユーザーの要求により、VPN の使用は避けられません。このため、実用上の見地から考えると、他の種類のアクセス向けの VPN が必要になるでしょう。ユーザーが自宅のコンピューターを使用しているのであれば、構成は未定です（かつコンピューターは管理されていません）。したがって、VPN ソリューションは理にかなっていると考えられます。

質問 : すべてのユーザーがリモート接続できるようにするには、ネットワーク ポリシーをどのように変更しますか。

解答 : ユーザーを特定し、またユーザーが何にアクセスできるかについてフィルター処理をおこなうネットワーク ポリシーを、RADIUS サーバーで追加構成する必要があります。部門ごとに異なったポリシーが必要な場合もあります。これを決定するためには、どの部門がどのリソースへのアクセスを必要としているかを判定する分析をおこなう必要があります。ネットワーク ポリシーが正しい処理順序で構成されるようにすることが大切です。

質問 : どの種類の VPN を推奨しますか。

解答 : SSTP または IKEv2 が適切な VPN ソリューションです。

質問 : 接続要求ポリシーは必要ですか。

解答 : 実行中の RADIUS サーバーは 1 台のみのため、接続要求ポリシーは必要ありません。接続要求ポリシーとは、NPS サーバーが RADIUS クライアントから受信する接続要求の認証と承認を RADIUS サーバーで実行するように指定することが可能な条件と設定のセットです。

質問 : RADIUS プロキシは必要ですか。

解答 : 前述のとおり、RADIUS サーバーは 1 台だけです。RADIUS プロキシとして NPS を使用する際は、接続要求ポリシーを構成します。これらのポリシーは、NPS サーバーが他の RADIUS サーバーに転送する接続要求、および、接続要求を転送しようとしている転送先の RADIUS サーバーを示します。リモートの RADIUS サーバー グループ内の 1 台以上のコンピューターでログインする際、アカウンティング データを転送するように NPS を構成することもできます。このシナリオでは、RADIUS プロキシは不要です。

参考資料

RADIUS ソリューションのコンポーネント

注 : クライアントオペレーティング システムを実行するワイヤレスのノート PC や他のコンピューターなどのクライント コンピューターは、RADIUS クライアントではありません。

RADIUS クライアントは、NPS サーバーなどの RADIUS サーバーとの通信に RADIUS プロトコルを使用するため、ネットワーク アクセス サーバー (ワイヤレス アクセス ポイント、802.1X 認証スイッチ、VPN サーバー、ダイヤルアップ サーバーなど) になります。

接続要求ポリシー

注 : 接続要求ポリシーは、接続試行が許可されるかどうかの判断に使用するのではなく、その判断をおこなう RADIUS サーバーを特定するために使用することを理解しておく必要があります。

注 : PEAP (Protected Extensible Authentication Protocol) 認証による VPN または 802.1X 強制方式を使用して NAP を展開する場合は、接続要求がローカルで処理されていても、接続要求ポリシーで PEAP 認証を構成する必要があります。

注 : NPS と RRAS を同じコンピューターにインストールし、Windows 認証とアカウンティングに対して RRAS を構成する場合は、RRAS 認証要求とアカウンティング要求を RADIUS サーバーに転送できます。これは、RRAS 認証要求とアカウンティング要求が、リモート RADIUS サーバー グループに転送するように構成された接続要求ポリシーと一致する場合に発生することがあります。

レッスン 3
境界ネットワークの設計

目次

質問と解答

討論 : インターネット接続の設計

質問 : 現在の構成ではどのような問題がありますか。

解答 : ドメイン コントローラーはセキュリティで保護されていないため、境界ネットワークはドメイン コントローラーを保有するべきではありません。ディレクトリ サービスが必要な場合は、AD LDS を実装し、AD LDS サーバーに対して必要な AD DS のデータ サブセットのレプリケーションを構成することを検討します。例えば、Exchange Server 2010 のエッジ サービスをサポートするために、AD LDS サーバーを境界に展開して、Exchange エッジ トランスポート サーバーの役割をサポートすることができます。さらに、RADIUS サーバーを境界ネットワークに移動させ、追加セキュリティを提供する必要があります。RADIUS クライアント (VPN サーバー) を構成し、内部のファイアウォールで構成可能な、定義済みのトラフィック特性を使用して、RADIUS サーバーに接続することができます。

質問 : 電子メール送信をサポートするためには、どのような追加のサーバーを境界ネットワークに展開する必要がありますか。または、サーバーの追加は必要ないですか。

解答 : ベスト プラクティスとして、ネットワークの境界にエッジ サーバー (または他の SMTP リレー) を実装して、メッセージ検疫を向上させることを推奨します。ただし、このシナリオで使われる特定のトラフィックをサポートするために、内部ファイアウォールを変更する必要があります。

質問 : 以前に設計した VPN インフラストラクチャをサポートするために、どのようなファイアウォール変更をおこなう必要がありますか。

解答 : Northwind Traders には、L2TP/IPsec と SSTP VPN の実装が必要です。SSTP VPN は、すべての通信に TCP ポート 443 を使用していますが、これは通常、ファイアウォール経由で既に許容されています。ただし、インターネットからの L2TP トラフィックをサポートするために、ファイアウォールの変更が必要になります。両方の VPN に対して、想定されるトラフィックの種類を許容できるように、内部ファイアウォールを変更する必要があります。

参考資料

境界ネットワークで必要なサービス

注 : 特定の TCP ポートを使用するようにアプリケーションを構成することができます。実際、多くのアプリケーションは HTTP または HTTPS のみを使用するように構成できます。つまり、インターネットに接続しているファイアウォールを、受信 TCP ポート 80/443 のみを許可するように構成できます。

レッスン 4
DirectAccess の計画と実装

目次

参考資料

DirectAccess のコンポーネント

注 : 社外設置型のプロビジョニングでは、クライアント コンピューターを社内で接続しなくてもドメインに参加させることができます。

注 : NLS の URL は、グループ ポリシー オブジェクト (GPO) を使用して配布されます。

注 : 今までと同様に、この機能は Microsoft Forefront® 統合アクセス ゲートウェイでも実現できます。旧バージョンと同様に、変換サービスは、内部デバイスから開始されたセッションをサポートしません。IPv6 DirectAccess クライアントから送信された要求のみをサポートします。

DirectAccess の設計プロセス

注 : DirectAccess は 1 つのユニットとしてインストールして管理するように設計されています。これらの機能を分割すると、複雑さが増し、構成の問題が発生する可能性があります。

注 : DirectAccess サーバーは AD DS ドメインのメンバーにする必要がありますが、ドメイン コントローラーにすることはできません。

注 : DirectAccess クライアントに証明書をインストールする一番簡単な方法は、自動登録により PKI 経由でコンピューター証明書を発行することです。自動登録により、すべてのドメイン メンバーがエンタープライズ CA からコンピューター証明書を確実に取得できます。

デモンストレーション

デモンストレーション : 作業の開始ウィザードによる DirectAccess サーバーの構成

デモンストレーションの手順

Active Directory に DirectAccess クライアント コンピューターのセキュリティ グループを作成する

1. LON-DC1 で、サーバー マネージャー コンソールが自動的に開きます。サーバー マネージャー コンソールの右上隅で [ツール] をクリックし、[Active Directory ユーザーとコンピューター] をクリックします。
2. Active Directory ユーザーとコンピューター コンソール ツリーで、[Adatum.com] を右クリックし、[新規]、[組織単位] の順にクリックします。
3. 新しいオブジェクト - 組織単位ウィンドウで、[名前] ボックスに「DA_Clients OU」と入力し、[OK] をクリックします。
4. Active Directory ユーザーとコンピューター コンソール ツリーで、[Adatum.com] を展開し、[DA_Clients OU] を右クリックし、[新規]、[グループ] の順にクリックします。
5. [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] ボックスに「DA_Clients」と入力します。

6. [グループのスコープ] の下で、[グローバル] が選択されていることを確認し、さらに、[グループの種類] の下で、[セキュリティ] が選択されていることを確認し、[OK] をクリックします。
7. 詳細ウィンドウで [DA_Clients] を右クリックし、[プロパティ] をクリックします。
8. [DA_Clients のプロパティ] ダイアログ ボックスで、[メンバー] タブをクリックし、[追加] をクリックします。
9. [ユーザー、アドレス帳、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、[オブジェクトの種類] をクリックし、[コンピューター] チェック ボックスをオンにし、[OK] をクリックします。
10. [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「LON-CL1」と入力し、[OK] をクリックします。
11. [メンバー] の下に [LON-CL1] が表示されていることを確認し、[OK] をクリックします。
12. Active Directory ユーザーとコンピューター コンソールを閉じます。

DirectAccess を構成する

1. LON-RTR に切り替えます。
2. マウス ポインターを画面の左下隅に置き、[スタート] をクリックします。
3. [コントロール パネル] をクリックします。
4. コントロール パネルで、[ネットワークとインターネット] をクリックします。
5. [ネットワークとインターネット] で、[ネットワークと共有センター] をクリックします。
6. [ネットワークと共有センター] で、[アダプターの設定の変更] をクリックします。
7. [ローカル エリア接続 2] を右クリックし、[プロパティ] をクリックします。
8. [ローカル エリア接続 2 のプロパティ] ダイアログ ボックスで、[インターネット プロトコル バージョン 4 (TCP/IPv4)] をダブル クリックします。
9. [IP アドレス] ボックスに「131.107.0.21」と入力します。
10. [サブネット マスク] ボックスに「255.255.0.0」と入力し、[OK] をクリックします。
11. [ローカル エリア接続 2 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。
12. マウス ポインターをデスクトップの右下隅に合わせ、[設定] をクリックし、[電源]、[再起動] の順にクリックします。
13. [続行] をクリックします。
14. サーバーが再起動したら、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
15. サーバー マネージャー コンソールで、[ツール]、[リモート アクセス管理] の順にクリックします。
16. リモート アクセス管理コンソールで、[作業の開始ウィザードを実行する] をクリックします。
17. [リモート アクセスの構成] ページで、[DirectAccess のみを展開します] をクリックします。
18. エッジが選択されていることを確認し、[クライアントからリモート アクセス サーバーへの接続に使用するパブリック名または IPv4 アドレスを入力してください] に「131.107.0.21」と入力し、[次へ] をクリックします。
19. 作業の開始ウィザードで、[ここ] のリンクをクリックします。
20. [リモート アクセスの確認] ページの、[リモート クライアント] の隣で、[変更] リンクをクリックします。

21. [ドメイン コンピューター (Adatum¥Domain Computers)] をクリックし、[削除] をクリックします。
22. [追加] をクリックし、ボックスに「DA_Clients」と入力し、[OK] をクリックします。
23. [モバイル コンピューターに対してのみ DirectAccess を有効にする] チェック ボックスをオフにし、[次へ] をクリックします。
24. [Network Connectivity Assistant] で、[完了] をクリックします。
25. [リモート アクセスの確認] ページで [OK] をクリックします。
26. リモート アクセスの構成で、[完了] をクリックして DirectAccess ウィザードを終了します。
27. [作業の開始ウィザードの設定を適用しています] ボックスで、[閉じる] をクリックします。

復習とまとめ

復習問題

質問 : ネットワーク接続の試行が成功するかどうかの判定にどの種類のポリシーを使用することができますか。

解答 : 接続要求ポリシーは使用できませんが、ネットワーク ポリシーを使用することができます。

質問 : 自宅のコンピューターで会社の電子メールにアクセスできるように構成する場合、リモート アクセスを有効にする方法として、RPC over HTTPS と VPN のどちらが一般的に優れていますか。

解答 : 家庭のコンピューターは管理されておらず、また多くの場合構成が異なるので、このシナリオの VPN の方が優れた方法です。また、コンピューターに Outlook 2010 がインストールされていない場合もよくあります。多くの家庭のコンピューターで、Outlook 2010 以外の電子メールアプリケーションが使われているからです。

質問 : 高レベルのセキュリティが必要な、クライアントが混在する環境では、VPN トンネルの種類として、PPTP、L2TP/IPsec、SSTP、または IKEv2 のどれを選択しますか。

解答 : L2TP/IPsec は強固な認証と暗号化を提供しており、クライアントの種類の大半がサポートしています。IKEv2 をサポートしているのは Windows 7 と Windows 8 のみ、SSTP をサポートしているのは Windows Vista®、Windows 7、Windows 8 のみです。

質問 :「NPS サーバーの役割は、RADIUS クライアントとして機能することができる」は正しいですか、それとも誤りですか。

解答 : 誤りです。RRAS はこの機能を提供できますが、NPS を構成できるのは、RADIUS プロキシとして、または RADIUS サーバーとしてのいずれかに限ります。

質問 : 要塞ホスト、マルチホーム ファイアウォール、バックツーバック ファイアウォールの中で、ファイアウォールのソリューションとして、セキュリティがより強化されているのはどれですか。

解答 : バックツーバック ファイアウォールが最もセキュリティが強化されたソリューションです。

質問 : DirectAccess ソリューションにおいて、NLS はどのような機能を持っていますか。

解答 : DirectAccess クライアントは、NLS を使用して、クライアント自身の場所を判断します。クライアントが HTTPS で接続できる場合は、クライアントは自身がイントラネット上にいると想定し、DirectAccess コンポーネントを無効化します。NLS と通信できない場合、クライアントは自身がインターネット上にいると想定します。NLS サーバーは、Web サーバーの役割を使用してインストールします。

質問 : DirectAccess クライアントは、どのようにしてネットワーク リソースに接続できますか。

解答 : DirectAccess クライアントは、次に示す方法で、ネットワーク リソースに接続できます。

- IPv6 インターネットを介してダイレクト接続
- 6to4 を使用して接続
- Teredo を使用して接続
- IP-HTTPS を使用して接続

演習の復習問題と解答

演習 : ネットワーク アクセス サービスの設計と実装

質問と解答

演習の復習

質問 : VPN 設計にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : DirectAccess 設計にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : 組織ではリモート ユーザーをどのようにサポートしていますか。

解答 : さまざまな解答が考えられます。

第 12 章
ネットワーク保護の設計と実装

目次

レッスン 1
ネットワーク セキュリティ設計の概要

目次

質問と解答

討論 : 組織が直面するネットワークの脅威とは

質問 : 組織が直面する最も一般的な 10 個のネットワーク セキュリティの脅威は何か。

解答 : さまざまな解答が考えられます。次の解答はその一例です。

- ウイルスやワーム
- トロイの木馬
- スパム
- フィッシング
- パケット盗聴
- 悪意のあるコードを含む Web サイト
- パスワード攻撃
- ディスクの損失によるデータ侵害
- 共有コンピューターの使用
- いくつかの攻撃を起動する未検出のゾンビ コンピューター

質問 : これらの脅威に対処するために考えられる軽減策または解決策は何か。

解答 : さまざまな解答が考えられます。次の解答はその一例です。

- ウイルスやワームへの対応策。電子メール メッセージと添付ファイルの取り扱いについてユーザーに教育し、クリーン メッセージを提供するウイルス対策ソフトウェアなどのテクノロジを実装するようにしてください。
- トロイの木馬への対応策。トロイの木馬に感染するリスクを軽減するのに役立つオンライン プラクティスについてユーザー教育をしてください。しかしながらこれでは不十分です。トロイの木馬に感染するリスクを軽減するのに役立つ 安全かつブロックされた Web サイトの一覧を実装する必要があります。
- スパムへの対応策。クリーン メッセージ ストリームを提供するテクノロジを実装し、電子メール使用のベスト プラクティスについてユーザー教育をしてください。
- フィッシングへの対応策。クリーン メッセージ ストリームを提供するテクノロジを実装し、電子メール使用のベスト プラクティスについてユーザー教育をしてください。
- パケット盗聴への対応策。物理ネットワークへのアクセスを制限し、ハッカーがネットワーク盗聴用のデバイスに接続できないようにします。ワイヤレス ネットワークのセキュリティで保護された設定を実装します。セキュリティで保護されていないパブリック ワイヤレス ホットスポットへの接続についてユーザー教育をしてください。
- 悪意のあるコードを含む Web サイトへの対応策。悪意のあるコードを特定し、スパイウェア、アドウェア、およびクロスサイト スクリプティングを防ぐことができる Internet Explorer® 10 などの Web ブラウザーを実装します。
- パスワード攻撃への対応策。パスワード攻撃には、トロイの木馬またはネットワークへの物理アクセスが必要です。トロイの木馬への感染を防止し、物理ネットワークを保護することで、パスワード攻撃を減らすことができます。パスワードを複雑にすることで、卑劣なパスワード攻撃から身を守ることができるかもしれません。

- ディスクの物理的損失によるデータ侵害への対応策。コンピューターや USB 記憶デバイスの保護の重要性についてユーザー教育をしてください。Windows BitLocker® ドライブ暗号化や Windows BitLocker to Go® などの暗号化テクノロジの実装も検討してください。
- 共有コンピューターの使用への対応策。キオスク コンピューターなどの共有コンピューターの使用を許可する必要が場合は、制約のあるポリシーを実装し、特定のタスクだけを実行できるようにします。先行する数多くのソリューションを実装することで、共有コンピューターを保護することができます。
- いくつかの攻撃を起動する未検出のゾンビ コンピューターへの対応策。これらのコンピューターは、トロイの木馬、ウイルス、ワームに感染しており、フィッシング、またはスパム攻撃を実装することが可能です。先行する数多くのソリューションを実装することで、コンピューターへの感染や、攻撃を防ぐことができます。

通常のネットワーク攻撃に対処するために役立つソリューション

- オンラインでのベストプラクティスについてユーザー教育をしてください。
- 電子メールメッセージの安全性を保つためのテクノロジを実装します。
- ネットワークへの物理アクセスを制限します。
- 記憶デバイスの暗号化を実装します。

参考資料

多層防御モデルとは

注：非常に機微なデータは、隔離されたネットワークに接続するサーバーに配置できます。ただし、このアプローチは、ネットワーク上に格納されたさまざまなデータに対して、常に適切であるとは限りません。

注：ネットワーク侵入者検出機能を、ネットワークに実装することを検討します。この機能により、データが漏えいしたり、サービスが中断されたりする前に、不適切なネットワーク アクセスを識別できます。

レッスン 2
一般的なネットワーク セキュリティの脅威の識別と軽減

目次

参考資料

リスク評価と影響

注 : リスク管理計画には、プロアクティブ (事前的) な要素とリアクティブ (事後的) な要素の両方を含めることが重要です。つまり、セキュリティの脅威を軽減するためのプロアクティブな計画と、万一セキュリティ問題が発生した場合にはすばやく対処できる計画の両方を策定します。

MOF リスク管理プロセス

注 : MOF は、効率的で費用対効果の高い IT サービスを作成、実装、および管理するためのガイダンスを提供するドキュメントのコレクションです。情報技術インフラストラクチャ ライブラリ (ITIL) の代わりに使用できます。

レッスン 3
Windows ファイアウォール戦略の設計と実装

目次

質問と解答

討論 : Windows ファイアウォールによる対応のシナリオ

質問 : Windows ファイアウォールは、どのようなシナリオに対応できますか。

解答 : さまざまな解答が考えられます。次の解答はその一例です。

- IP アドレスの特定の範囲または特定のポートに受信通信を制限することで、内部脅威からサーバーを保護します。
- 特定のポートまたは特定のアプリケーションに送信通信を制限することで、悪意のあるソフトウェア (マルウェア) が伝播しないようにします。
- ネットワーク トラフィックの認証に IPSec を提供します。
- IPSec を使用し、トランジットのデータを暗号化します。

参考資料

IPSec の利点と使用法

注 : IPSec は、セキュリティで保護された接続の確立を IP アドレスに依存するため、動的 IP アドレスを指定することはできません。サーバーが、IPSec ポリシー フィルターの静的 IP アドレスを持っていることが必要な場合があります。大規模なネットワーク展開の場合、および一部のモバイル ユーザーの場合には、接続の両端で動的 IP アドレスを使用すると、IPSec ポリシーの設計が複雑になる可能性があります。

認証オプションと認証方法

注 : グループ ポリシーを使用すると、組織全体に証明書を配布できます。これにより、接続セキュリティ規則の証明書を簡単に管理できます。

注 : 高度な認証方法を指定して、複数の方法とそれを試行する順番を決定することもできます。

ネットワーク セキュリティ規則を設計するためのベスト プラクティス

注 : ドメイン コントローラーに関連する接続セキュリティ規則に対して Kerberos V5 認証を使用すると、ドメインが機能しなくなる可能性があります。

注 : 接続セキュリティ規則を通じて適用される IPSec ポリシーは、グループ ポリシーを通じて適用される IPSec ポリシーよりも優先されます。グループ ポリシーの IPSec ポリシーは、Windows XP や Windows Server 2003 など、接続セキュリティ規則をサポートしないクライアントの下位互換性のためにのみ提供されます。

デモンストレーション

デモンストレーション : 接続セキュリティの規則の構成

デモンストレーションの手順

LON-SVR1 で ICMP トラフィックを有効にする

1. LON-SVR1 に切り替えます。
2. ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. サーバー マネージャーで、[ツール] をクリックし、[セキュリティが強化された Windows ファイアウォール] をクリックします。
4. [セキュリティが強化された Windows ファイアウォール] で、[受信の規則] をクリックし、[新しい規則] をクリックします。
5. [新規の受信の規則ウィザード] ダイアログ ボックスで [カスタム] をクリックし、[次へ] をクリックします。
6. [プログラム] ページで [次へ] をクリックします。
7. [プロトコルおよびポート] ページの [プロトコルの種類] リストで [ICMPv4] をクリックし、[次へ] をクリックします。
8. [スコープ] ページで [次へ] をクリックします。
9. [操作] ページで [キュリティで保護されている場合、接続を許可する] をクリックし、[次へ] をクリックします。
10. [ユーザー] ページで、[次へ] をクリックします。
11. [コンピューター] ページで、[次へ] をクリックします。
12. [プロファイル] ページで、[次へ] をクリックします。
13. [名前] ページの [名前] ボックスに「ICMPv4 allowed」と入力し、[完了] をクリックします。

接続するサーバーでサーバー間規則を作成する

1. LON-SVR1 のセキュリティが強化された Windows ファイアウォールで、[接続セキュリティ規則] を右クリックし、[新しい規則] をクリックします。
2. 新規の接続セキュリティの規則ウィザードで、[サーバー間規則] をクリックし、[次へ] をクリックします。
3. [エンドポイント] ページで、[次へ] をクリックします。
4. [要件] ページで、[Require authentication for inbound and outbound connections] をクリックし、[次へ] をクリックします。
5. [認証方法] ページで、[詳細設定] をクリックし、[カスタマイズ] をクリックします。
6. [詳細な認証方法のカスタマイズ] ダイアログ ボックスの [1 番目の認証方法] の下で、[追加] をクリックします。
7. [1 番目の認証方法の追加] ダイアログ ボックスで、[事前共有キー] をクリックして「secret」と入力し、[OK] をクリックします。
8. [詳細な認証方法のカスタマイズ] ダイアログ ボックスで、[OK] をクリックします。
9. [認証方法] ページで、[次へ] をクリックします。
10. [プロファイル] ページで、[次へ] をクリックします。
11. [名前] ページの [名前] ボックスに「Adatum-Server-to-Server」と入力し、[完了] をクリックします。

LON-CL1 でサーバー間規則を作成する

1. LON-CL1 に切り替えます。
2. ユーザー名「Adatum¥administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
3. スタート画面で「Windows Firewall」と入力し、[設定] をクリックします。
4. [設定] リストで、[Windows ファイアウォール] をクリックします。
5. Windows ファイアウォールで、[詳細設定] をクリックします。
6. クリックし、[接続セキュリティの規則] を右クリックして [新しい規則] をクリックします。
7. 新規の接続セキュリティの規則ウィザードで、[サーバー間規則] をクリックし、[次へ] をクリックします。
8. [エンドポイント] ページで、[次へ] をクリックします。
9. [要件] ページで、[Require authentication for inbound and outbound connections] をクリックし、[次へ] をクリックします。
10. [認証方法] ページで、[詳細設定] をクリックし、[カスタマイズ] をクリックします。
11. [詳細な認証方法のカスタマイズ] ダイアログ ボックスの [1 番目の認証方法] の下で、[追加] をクリックします。
12. [1 番目の認証方法の追加] ダイアログ ボックスで、[事前共有キー] をクリックし、「secret」と入力して [OK] をクリックします。
13. [詳細な認証方法のカスタマイズ] ダイアログ ボックスで、[OK] をクリックします。
14. [認証方法] ページで、[次へ] をクリックします。
15. [プロファイル] ページで、[次へ] をクリックします。
16. [名前] ページの [名前] ボックスに「Adatum-Server-to-Server」と入力し、[完了] をクリックします。

規則をテストする

1. ポインターをタスクバーの左下隅に置き、[スタート] をクリックします。
2. スタート画面で「cmd.exe」と入力し、Enter キーを押します。
3. コマンド プロンプトで、「ping 172.16.0.21」と入力し、Enter キーを押します。
4. セキュリティが強化された Windows ファイアウォールに切り替えます。
5. [監視]、[セキュリティ アソシエーション] の順に展開し、[メイン モード] をクリックします。
6. 右側のウィンドウで、リストされた項目をダブルクリックします。
7. [メイン モード] で情報を表示し、[OK] をクリックします。
8. [クイック モード] をクリックします。
9. 右側のウィンドウで、リストされた項目をダブルクリックします。
10. [クイック モード] で情報を表示し、[OK] をクリックします。

レッスン 4
NAP インフラストラクチャの設計と実装

目次

参考資料

SHV 設定を定義する際の考慮事項

注 : Windows SHA は、ウイルス対策アプリケーションが有効かどうか、およびそれが最新かどうかを判定できます。他のベンダーの SHA は、その他の特性を判定できる可能性があります。

デモンストレーション

デモンストレーション : NAP の実装

デモンストレーションの手順

NPS のサーバーの役割をインストールする

1. LON-DC1 に切り替え、ユーザー名「Adatum¥administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
2. 必要に応じて、タスクバーで、[サーバー マネージャー] をクリックします。
3. サーバー マネージャー コンソールの詳細ウィンドウで、[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、[役割ベースまたは機能ベースのインストール] をクリックし、[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、[ネットワーク ポリシーとアクセス サービス] チェック ボックスをオンにします。
8. [機能の追加] をクリックし、[次へ] を 2 回クリックします。
9. [ネットワーク ポリシーとアクセス 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、[ネットワーク ポリシー サーバー] チェック ボックスがオンになっ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完了したことを確認し、[閉じる] をクリックします。

NPS を NAP 正常性ポリシー サーバーとして構成する

1. サーバー マネージャー コンソールで、[ツール] をクリックし、[ネットワーク ポリシー サーバー] をクリックします。
2. ナビゲーション ウィンドウで、[ネットワーク アクセス保護]、[システム正常性検証ツール]、[Windows セキュリティ正常性検証ツール] の順に展開し、[設定] をクリックします。
3. 右側のウィンドウで、[名前] の下の [既定の構成] をダブルクリックします。
4. ナビゲーション ウィンドウで、[Windows 8/Windows 7/Windows Vista] をクリックします。
5. 詳細ウィンドウで、[ネットワーク接続に対してファイアウォールが有効] を除くすべてのチェック ボックスをオフにします。
6. [OK] をクリックして、[Windows セキュリティ正常性検証ツール] ダイアログ ボックスを閉じます。

正常性ポリシーを構成する

1. ナビゲーション ウィンドウで、[ポリシー] を展開します。
2. [正常性ポリシー] を右クリックし、[新規] をクリックします。
3. [新しい正常性ポリシーの作成] ダイアログ ボックスの [ポリシー名] の下に「Compliant」と入力します。
4. [クライアント SHV (システム正常性検証ツール) のチェック対象] の下で、[すべての SHV チェックにパスしたクライアント] が選択されていることを確認します。
5. [この正常性ポリシーで使用されている SHV :] の下で、[Windows セキュリティ正常性検証ツール] チェック ボックスをオンにし、[OK] をクリックします。
6. [正常性ポリシー] を右クリックし、[新規] をクリックします。
7. [新しい正常性ポリシーの作成] ダイアログ ボックスの [ポリシー名] ボックスに「Noncompliant」と入力します。
8. [クライアント SHV (システム正常性検証ツール) のチェック対象 :] の下で、[1 つ以上の SHV チェックに失敗したクライアント] をクリックします。
9. [この正常性ポリシーで使用されている SHV :] で、[Windows セキュリティ正常性検証ツール] チェック ボックスをオンにし、[OK] をクリックします。

準拠するコンピューター用ネットワーク ポリシーを構成する

1. ナビゲーション ウィンドウで、[ポリシー] の下の [ネットワーク ポリシー] をクリックします。
2. [ポリシー] を右クリックして、[ポリシー名] の下にある 2 つの既定ポリシーを無効にし、[無効] をクリックします。
3. [ネットワーク ポリシー] を右クリックし、[新規] をクリックします。
4. [ネットワーク ポリシー名と接続の種類の指定] ページで、[ポリシー名] の下に「Compliant-Full-Access」と入力し、[次へ] をクリックします。
5. [条件の指定] ページで、[追加] をクリックします。
6. [条件の選択] ダイアログ ボックスで、[正常性ポリシー] をダブルクリックします。
7. [正常性ポリシー] ダイアログ ボックスの [正常性ポリシー] の下で [準拠] をクリックし、[OK] をクリックします。
8. [条件の指定] ページで、[次へ] をクリックします。
9. [アクセス許可の指定] ページで、[次へ] をクリックします。
10. [認証方法の構成] ページで、[コンピューターの正常性チェックのみを実行する] を除くすべてのチェック ボックスをオフにし、[次へ] をクリックします。
11. もう一度 [次へ] をクリックします。
12. [設定の構成] ページで、[NAP 強制] をクリックします。[完全なネットワーク アクセスを許可する] が選択されていることを確認し、[次へ] をクリックします。
13. [新しいネットワーク ポリシーの完了] ページで、[完了] をクリックします。

非準拠のコンピューター用ネットワーク ポリシーを構成する

1. [ネットワーク ポリシー] を右クリックし、[新規] をクリックします。
2. [ネットワーク ポリシー名と接続の種類の指定] ページで、[ポリシー名] に「Noncompliant-Restricted」と入力し、[次へ] をクリックします。
3. [条件の指定] ページで、[追加] をクリックします。

4. [条件の選択] ダイアログ ボックスで、[正常性ポリシー] をダブルクリックします。
5. [正常性ポリシー] ダイアログ ボックスの [正常性ポリシー] の下で [非準拠] をクリックし、[OK] をクリックします。
6. [条件の指定] ページで、[次へ] をクリックします。
7. [アクセス許可の指定] ページで、[アクセスを許可する] が選択されていることを確認し、[次へ] をクリックします。
8. [認証方法の構成] ページで、[コンピューターの正常性チェックのみを実行する] を除くすべてのチェック ボックスをオフにし、[次へ] をクリックします。
9. もう一度 [次へ] をクリックします。
10. [設定の構成] ページで、[NAP 強制]、[制限付きアクセスを許可する] の順にクリックします。[クライアント コンピューターの自動修復を有効にする] チェック ボックスをオフにし、[次へ] をクリックし、[完了] をクリックします。

動的ホスト構成プロトコル (DHCP) サーバーの役割を NAP に構成する

1. サーバー マネージャー コンソールで、[ツール]、[DHCP] の順にクリックします。
2. DHCP コンソールで、[LON-DC1.Adatum.com]、[IPv4] の順に展開し、[Scope [172.16.0.0] Adatum] を右クリックし、[プロパティ] をクリックします。
3. [Scope [172.16.0.0] Adatum のプロパティ] ダイアログ ボックスで、[ネットワーク アクセス保護] タブをクリックし、[このスコープに対して有効にする] をクリックし、[OK] をクリックします。
4. ナビゲーション ウィンドウで、[Scope [172.16.0.0] Adatum] の下の [ポリシー] をクリックします。
5. [ポリシー] を右クリックし、[新しいポリシー] をクリックします。
6. DHCP ポリシーの構成ウィザードで、[ポリシー名] ボックスに「NAP Policy」と入力し、[次へ] をクリックします。
7. [ポリシーの条件を構成] ページで、[追加] をクリックします。
8. [条件の追加/編集] ダイアログ ボックスの [条件] のリストで、[ユーザー クラス] をクリックします。
9. [Operator] リストで、[Equals] をクリックします。
10. [値] リストで、[既定のネットワーク アクセス保護クラス] をクリックし、[追加] をクリックします。
11. [OK] をクリックし、[次へ] をクリックします。
12. [ポリシーの設定を構成] ページで、[いいえ] をクリックし、[次へ] をクリックします。
13. [ポリシーの設定を構成] ページの [ベンダー クラス] リストで、[DHCP 標準オプション] をクリックします。
14. [利用可能なオプション] リストで、[[006] DNS サーバー] チェック ボックスをオンにします。
15. [IP アドレス] ボックスに「172.16.0.10」と入力し、[追加] をクリックします。
16. [利用可能なオプション] リストで、[[015] DNS ドメイン名] チェック ボックスをオンにします。
17. [文字列値] ボックスに「restricted.adatum.com」と入力し、[次へ] をクリックします。
18. [サマリー] ページで、[完了] をクリックします。
19. DHCP コンソールを閉じます。

クライアントの NAP 設定を構成する

1. LON-CL1 に切り替え、ユーザー名「Adatum¥administrator」、パスワード「Pa$$w0rd」を使用してサインインします。

2. スタート画面で「napclcfg.msc」と入力し、Enter キーを押します。
3. [NAPCLCFG – NAP クライアントの構成 (ローカル コンピューター)] のナビゲーション ウィンドウで、[強制クライアント] をクリックします。
4. 結果ウィンドウで、[HCP 検疫強制クライアント] を右クリックし、[有効] をクリックします。
5. [NAPCLCFG – NAP クライアントの構成 (ローカル コンピューター)] を閉じます。
6. ポインターをタスクバーの左下隅に置き、[スタート] をクリックします。
7. スタート画面で「Services.msc」と入力し、Enter キーを押します。
8. サービスの結果ウィンドウで、[ネットワーク アクセス保護エージェント] をダブルクリックします。
9. [ネットワーク アクセス保護エージェントのプロパティ (ローカル コンピューター)] ダイアログ ボックスで、[スタートアップの種類] リストの [自動] をクリックします。
10. [スタート] をクリックし、[OK] をクリックします。
11. ポインターをタスクバーの左下隅に置き、[スタート] をクリックします。
12. スタート画面で「gpedit.msc」と入力し、Enter キーを押します。
13. コンソール ツリーで、[ローカル コンピューター ポリシー]、[コンピューターの構成]、[管理用テンプレート]、[Windows コンポーネント] の順に展開し、[セキュリティ センター] をクリックします。
14. [セキュリティ センターをオンにする (ドメイン上のコンピューターのみ)] をダブルクリックし、[有効] をクリックし、[OK] をクリックします。
15. コンソール ウィンドウを閉じます。
16. ポインターをタスクバーの左下隅に置き、[設定] をクリックします。
17. [設定] リストで、[コントロール パネル] をクリックします。
18. コントロール パネルで、[ネットワークとインターネット] をクリックします。
19. [ネットワークとインターネット] で、[ネットワークと共有センター] をクリックします。
20. [ネットワークと共有センター] の左側のウィンドウで、[アダプターの設定の変更] をクリックします。
21. [ローカル エリア接続] を右クリックし、[プロパティ] をクリックします。
22. [ローカル エリアの接続プロパティ] ダイアログ ボックスで、[インターネット プロトコル バージョン 4 (TCP/IPv4)] をダブル クリックします。
23. [インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティ] ダイアログ ボックスで、[IP アドレスを自動的に取得する] をクリックします。
24. [DNS サーバーのアドレスを自動的に取得する] をクリックし、[OK] をクリックします。
25. [ローカル エリア接続のプロパティ] ダイアログ ボックスで、[OK] をクリックします。

NAP をテストする

1. ポインターをタスクバーの左下隅に置き、[スタート] をクリックします。
2. スタート画面で「cmd.exe」と入力し、Enter キーを押します。
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。

```
Ipconfig
```

4. サービスに切り替えます。
5. サービスの結果ウィンドウで、[Windows ファイアウォール] をダブルクリックします。

6. [Windows ファイアウォールのプロパティ (ローカル コンピューター)] ダイアログ ボックスで、[スタートアップの種類] リストの [無効] をクリックします。
7. [停止] をクリックし、[OK] をクリックします。
8. [システム トレイ] エリアで、[ネットワーク アクセス保護] のポップアップ警告をクリックします。[ネットワーク アクセス保護] ダイアログ ボックスの情報を確認し、[閉じる] をクリックします。

注：ポップアップ警告が表示されない場合は、デモンストレーションを続行してください。

9. 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。

```
Ipconfig
```

10. コンピューターのサブネット マスクが 255.255.255.255 で、DNS サフィックスが restricted.Adatum.com であることを確認します。すべてのウィンドウを開いたままにします。

復習とまとめ

復習問題

質問 : Windows SHV は、ファイアウォールの状態 (有効または無効) の両方の状態、および最新になっているかどうかを判定することができます。
( ) はい
( ) いいえ

解答 :
(√) はい
( ) いいえ

質問 : ネットワーク攻撃に共通するいくつかの形態は何ですか。

解答 : 盗聴、データの改ざん、ID スプーフィング、パスワードによる攻撃、サービス拒否攻撃、Man-in-the-middle 攻撃、キーの漏えい、アプリケーション層攻撃などがあります。

質問 : NAP をサポートするためにはどのようなサーバーの役割を展開する必要がありますか。

解答 : NPS の役割、また、必要に応じて Active Directory® Certificate Services (AD CS) も展開する必要があります。動的ホスト構成プロトコル (DHCP) 強制を実装している場合は、DHCP サーバーを展開する必要があります。VPN 強制には、ルーティングとリモート アクセスの役割サービス (NPS の役割の一部) が必要です。

質問 : IPSec にはどのような利用を推奨しますか。

解答 : 次のとおりです。

- パケットのフィルター処理
- ホスト間トラフィックのセキュリティ保護
- サーバーへのトラフィックのセキュリティ保護
- レイヤー 2 トンネリング プロトコル (L2TP)
- サイト間 (ゲートウェイ間) のトンネリング
- 論理ネットワークの強制

実際の問題とシナリオ

シナリオ : Tailspin Toys 社は、そのセキュリティ インフラストラクチャ全体の一環として、NAP の実装を計画しています。同社では、接続方法にかかわらず、すべてのネットワーク クライアントに適用できる強制方法を希望しています。PKI の準備は整っています。どのような強制方法を推奨しますか。

解答 : IPSec 強制が最適です。また、スイッチとアクセスポイントによって 802.1X 認証がサポートされている場合は、802.1X 強制も推奨されます。手動で IP 構成を割り当てられたクライアントが NAP をバイパスする可能性があるため、DHCP 強制は適していません。また、すべてのクライアントが VPN に接続されているわけではないため、VPN 強制も適していません。

シナリオ : Wingtip Toys 社では、IPSec NAP 強制の実装を希望しています。この方法をサポートするためには、どのインフラストラクチャ コンポーネントを準備する必要がありますか。

解答 : IPSec では、NAP の一般的要件に加えて、正常性証明書の正常性登録機関 (HRA) や公開キーのインフラストラクチャ (PKI) の展開が要求されます。

演習の復習問題と解答

演習 : ネットワーク保護の設計と実装

質問と解答

演習の復習

質問 : ファイアウォールの設計の練習にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : NAP の設計の練習にはどのように取り組みますか。

解答 : さまざまな解答が考えられます。

質問 : ネットワーク アクセスの設計は、あなたの組織におけるネットワーク アクセスの実装と比較してどうですか。

解答 : さまざまな解答が考えられます。

ご意見をお寄せください

ご意見を送付する前に、既知の問題については、Microsoft ヘルプとサポートの Microsoft サポート技術情報で検索することができます。コース番号、リビジョン、またはコース タイトルを使用して、検索してください。

注 : すべてのトレーニングの製品が Microsoft ヘルプとサポートの記事にはなりません。そのような場合は、既存のエラー ログのエントリがあるかどうかを講師にお問い合わせください。

コースウェアへのご意見

コースウェアへのご意見は、support@mscourseware.com にお送りください。時間と労力をかけていただき心から感謝します。私たちは受信した電子メールをすべて確認し、その情報を適切なチームに転送します。たくさんのご意見を受信するため、残念ながら返信をすることができませんが、ご意見を Microsoft のラーニング プロダクトの改善に役立てていきます。

エラーの報告

ご意見を送信される際、電子メールの件名に、トレーニング製品名と番号をご記入ください。コメントまたはバグの報告を送信される場合は、次の項目をご記入ください。

1. ドキュメントまたは CD の品番
2. ページ番号または場所
3. エラーまたは変更の提案についての詳細な説明

問題の確認に必要と思われる詳細をすべてご記入してください。

重要 : すべてのエラーとご提案が審査されますが、有効なもののみ製品の Microsoft サポート技術情報の記事に追加されます。