Microsoft

OFFICIAL MICROSOFT LEARNING PRODUCT

23744B

Windows Server 2016 のセキュリティ

製品番号 : 23744B

リリース日 : 10/2017

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。

Please note: As this Licensed Content is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce le contenu sous licence étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le contenu sous licence visé par une licence est offert « tel quel ». Toute utilisation de ce contenu sous licence est à votre seule risque et péril. Microsoft n'accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d'adéquation à un usage particulier et d'absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.
Cette limitation concerne:

- tout ce qui est relié au le contenu sous licence, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers; et.
- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles-ci ne le permettent pas.

2013 年 7 月改訂

第 1 章

攻撃と侵害の検出と Sysinternals ツール

目次

レッスン 1
攻撃の理解

目次

質問と解答

質問 : 受講者の組織が経験した攻撃について、説明してください。

解答 : 解答はさまざまです。この質問は、受講者の組織が経験した攻撃に関する討論を引き出すことを目的としています。

レッスン 2
セキュリティ侵害の検出

目次

質問と解答

質問 : 侵害の検出の体験について、話し合います。環境内で侵害が起きたと疑われる場合、何を探しますか。

解答 : 解答はさまざまです。ここでおこなう討論は、レッスン 1 の討論に基づいています。

レッスン 3
Sysinternals ツールによるアクティビティの検証

目次

質問と解答

質問 : Sysinternals ツールのいずれかを使用したことがあるかどうか、どのように使用したかについて、話し合います。

解答 : 受講者の経験により、解答はさまざまです。この質問により、講師は、受講者がこれらのツールについてどれくらい理解しているのかをさらに知ることができます。

参考資料

System Monitor

 **参考資料 :** Sysmon については、次のサイトを参照してください。
Sysmon v6.03
https://technet.microsoft.com/ja-jp/sysinternals/sysmon

AccessChk

 **参考資料 :** AccessChk の詳細については、次のサイトを参照してください。
AccessChk v6.1
http://aka.ms/V9l243

Autoruns

 **参考資料 :** Autoruns ツールについては、次のサイトを参照してください。
Autoruns for Windows
http://aka.ms/Xnt6os

LogonSessions

 **参考資料 :** LogonSessions ツールについては、次のサイトを参照してください。
LogonSessions v1.4
http://aka.ms/Ugnyh8

Process Explorer

 **参考資料 :** Process Explorer ツールについては、次のサイトを参照してください。
Process Explorer v16.21
http://aka.ms/usw7c8

Process Monitor

参考資料 : Process Monitor については、次のサイトを参照してください。
Process Monitor v3.33
http://aka.ms/Qc19u6

Sigcheck

参考資料 : Sigcheck については、次のサイトを参照してください。
Sigcheck v2.55
http://aka.ms/Lsef33

デモンストレーション : Sysinternals ツール

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 を起動します。
2. LON-SVR1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
3. タスク バーで [エクスプローラー] をクリックします。
4. エクスプローラーで、[Allfiles (E:)] ボリュームをダブルクリックします。
5. [Labfiles] フォルダーをダブルクリックします。
6. [Mod01] フォルダーをダブルクリックします。
7. Mod01 フォルダーで、[LogonSessions.zip] を右クリックし、[すべて展開] をクリックします。
8. [圧縮 (ZIP 形式) フォルダーの展開] ダイアログ ボックスで、[完了時に展開されたファイルを表示する] チェック ボックスをオフにし、[展開] をクリックします。
9. ProcessExplorer.zip と ProcessMonitor.zip に対して、手順 7 ～ 8 を繰り返します。
10. エクスプローラーを閉じます。
11. [スタート] を右クリックし、[コンピューターの管理] をクリックします。
12. コンピューターの管理コンソールで、[ローカル ユーザーとグループ] を展開し、[ユーザー] を右クリックして、[新しいユーザー] をクリックします。
13. [新しいユーザー] ダイアログ ボックスで、[ユーザー名] ボックスに「Attacker」と入力します。
14. [パスワード] ボックスと [パスワードの確認入力] ボックスに「Pa55w.rd」と入力します。
15. [ユーザーは次回ログオン時にパスワード変更が必要] チェック ボックスをオフにし、[作成]、[閉じる] の順にクリックします。
16. [ユーザー] リストで、[Attacker] を右クリックし、[プロパティ] をクリックします。
17. [Attacker のプロパティ] ダイアログ ボックスで [所属するグループ] タブをクリックし、[追加] をクリックします。
18. [グループの選択] ダイアログ ボックスに「Administrators」と入力し、[OK] をクリックします。
19. [Attacker のプロパティ] ダイアログ ボックスを閉じるには、[OK] をクリックします。
20. コンピューターの管理コンソールを閉じます。

21. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
22. [ファイル名を指定して実行] ダイアログ ボックスに「cmd.exe」と入力し、[OK] をクリックします。
23. 管理者 : C:¥Windows¥system32¥cmd.exe ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
runas /user:Attacker cmd.exe
```

24. [Attacker のパスワードを入力してください] と表示されたら、「Pa55w.rd」と入力し、Enter キーを押します。
25. cmd.exe (LON-SVR1¥Attacker として実行中) ウィンドウを画面の右側に移動します。
26. 管理者 : C:¥Windows¥system32¥cmd.exe ウィンドウを画面の左側に移動します。
27. 画面の右側にある LON-SVR1¥Attacker 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。

```
ftp.exe
```

28. 画面の左側にある管理者 : ウィンドウで、次のコマンドを入力し、各コマンドの最後で Enter キーを押します。

```
E:
Cd labfiles¥Mod01¥LogonSessions
Logonsessions -p
```

29. [LogonSessions License Agreement] ダイアログ ボックスで、[Agree] をクリックします。
30. Logonsessions ツールの出力を確認します。

注 : Adatum¥Administrator のログオン セッションで実行されているプロセスと、LON-SVR1¥Attacker のログオン セッションで実行されているプロセスを確認します。LON-SVR1¥Attacker のログオン セッションで ftp.exe が実行中であることを確認します。

31. 画面の左側にある管理者 : コマンド プロンプトで、次のコマンドを入力し、各コマンドの最後で Enter キーを押します。

```
Cd E:¥Labfiles¥Mod01¥ProcessExplorer
procexp
```

32. [Process Explorer License Agreement] ダイアログ ボックスで、[Agree] をクリックします。
33. Process Explorer を画面の左側に移動します。
34. Process Explorer で、cmd.exe プロセスの下にある ftp.exe プロセスを見つけます。
35. 右側の cmd.exe ウィンドウの ftp> プロンプトで「bye」と入力し、Enter キーを押して、ftp セッションを閉じます。

注 : Process Explorer から ftp.exe 項目が削除されます。

36. 右側の cmd.exe ウィンドウで、「notepad newfile1.txt」と入力し、Enter キーを押して、[はい] をクリックします。

注 : 新しい notepad.exe 項目が Process Explorer に表示されます。

37. メモ帳で、ランダムなテキストを入力し、保存せずにウィンドウを閉じ、Process Explorer ウィンドウの変更に注意します。
38. 画面の左側にある管理者で実行しているコマンド プロンプトで、次のコマンドを入力し、各コマンドの最後で Enter キーを押します。

```
Cd E:¥Labfiles¥Mod01¥ProcessMonitor
Procmon
```

39. [Process Monitor License Agreement] ダイアログ ボックスで、[Agree] をクリックし、Process Monitor ウィンドウを画面の左側にスナップします。
40. 右側の cmd.exe ウィンドウで「ftp.exe」と入力し、Enter キーを押します。
41. Process Monitor ウィンドウ全体をスクロールして、ftp.exe のプロセス名を見つけます。
42. ftp.exe のプロセス名を右クリックし、[Highlight ‘ftp.exe’] をクリックします。
43. Process Monitor ウィンドウ全体をスクロールして、ftp.exe のプロセス名のインスタンスがすべて強調表示されていることを確認します。
44. Process Monitor のツール バーで、[Filter] アイコンをクリックします。
45. [Process Monitor Filter] ダイアログ ボックスで、[Architecture] ドロップダウン リストをクリックし、[Process Name] をクリックします。
46. ボックスに「ftp.exe」と入力し、[Add]、[OK] の順にクリックします。
47. 右側の cmd.exe ウィンドウの ftp> プロンプトに「bye」と入力し、Enter キーを押します。
48. Process Monitor のツール バーで、[Filter] アイコンをクリックします。
49. フィルターのリストで、[Process Name is ftp.exe] チェック ボックスをオフにし、[Architecture] ドロップダウン リストで [Process Name] をクリックします。
50. ボックスに「cmd.exe」と入力し、[Add]、[OK] の順にクリックします。
51. 右側の cmd.exe ウィンドウで、「notepad newfile2.txt」と入力し、Enter キーを押して、[はい] をクリックします。ランダムなテキストを入力し、ファイルを保存せずに閉じます。
52. cmd.exe フィルターに基づき、Process Monitor に記録された追加のアクティビティを確認します。
53. Process Monitor の [File] メニューで、[Save] をクリックします。
54. [ファイルに保存] ダイアログ ボックスで、既定を受け入れ、[OK] をクリックします。

演習の復習の質問と解答

演習 : 基本的な侵害の検出とインシデント対応戦略

質問と解答

質問 : 各セッションで使用されているプロセスを表示するには、LogonSessions でどのスイッチを使用しますか。

解答 : 各セッションで使用されているプロセスを表示するには、-p スイッチを使用します。

質問 : Process Explorer と Process Monitor の間の主要な違いは何ですか。

解答 : Process Explorer は、アクティビティをリアルタイムに表示できるように設計されており、Process Monitor は、後で分析するためにアクティビティを記録します。

復習とまとめ

復習問題

質問 : あなたの環境で目にしたことがあるのは、この章で説明したどの攻撃の種類ですか。

解答 : 解答はさまざまです。受講者の環境や経験に依存します。

第 2 章

資格情報の保護と特権アクセス

目次

レッスン 1
ユーザー権利の理解

目次

質問と解答

質問 : 管理アカウントに特権を割り当てるモデルについて、受講者に質問します。Exchange や Configuration Manager などの複数の個別のシステムに対して特権を持つアカウントがありますか。また各管理タスク セットに個別のアカウントがありますか。

解答 : 解答はさまざまです。受講者の組織のプラクティスによって異なります。

参考資料

最低限の特権の原則

参考資料 : 詳細については、次のサイトを参照してください。
最低限の権限管理モデルを実装します。
http://aka.ms/Hw2tr3

Protected Users、認証ポリシー、および認証ポリシー サイロ

参考資料 : 詳細については、次のサイトを参照してください。
認証ポリシーと認証ポリシー サイロ
https://technet.microsoft.com/ja-jp/library/dn486813(v=ws.11).aspx

デモンストレーション : ユーザー権利とアカウント セキュリティ オプションの構成

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 と LON-SVR2 を起動します。
2. LON-DC1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
3. 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。
4. Active Directory 管理センター コンソールで、[Adatum (ローカル)] をクリックし、[IT] OU をダブルクリックします。
5. [IT] OU で [Dante Dabney] をダブルクリックします。
6. [Dante Dabney] ダイアログ ボックスで、[ログオン先] をクリックします。
7. [ログオン先] ダイアログ ボックスで、[次のコンピューター] をクリックして「LON-SVR2」と入力し、[追加] をクリックします。
8. [OK] をクリックし、[ログオン先] ダイアログ ボックスを閉じます。
9. [OK] をクリックし、[Dante Dabney] ダイアログ ボックスを閉じます。
10. LON-SVR1 に切り替え、ユーザー名「Adatum¥Dante」、パスワード「Pa55w.rd」を使用してサインインを試みます。

11. [このアカウントでは、この PC を利用できません。別の PC を使ってください。] というメッセージを確認し、[OK] をクリックします。
12. LON-SVR2 に切り替え、ユーザー名「Adatum¥Dante」、パスワード「Pa55w.rd」を使用してサインインを試みます。
13. サインインが成功したら、[スタート]、[Dante Dabney] (左端にある人のアイコン)、[サインアウト] の順にクリックします。
14. LON-SVR2 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
15. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
16. [ファイル名を指定して実行] ダイアログ ボックスに「gpedit.msc」と入力し、[OK] をクリックします。
17. ローカル グループ ポリシー エディターで、[コンピューターの構成]、[Windows の設定]、[セキュリティの設定]、[ローカル ポリシー] の順に展開し、[ユーザー権利の割り当て] を選択します。
18. [ローカル ログオンを拒否] ポリシーをダブルクリックします。
19. [ローカル ログオンを拒否のプロパティ] ダイアログ ボックスで、[ユーザーまたはグループの追加] をクリックします。
20. [ユーザー、コンピューター、サービス アカウントまたはグループの選択] ダイアログ ボックスで「Dante」と入力し、[名前の確認] をクリックして、[OK] を 2 回クリックします。
21. ローカル グループ ポリシー エディターを閉じます。
22. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
23. [ファイル名を指定して実行] ダイアログ ボックスに「gpupdate /force」と入力し、[OK] をクリックします。
24. [スタート]、[Administrator] (左端にある人のアイコン)、[サインアウト] の順にクリックします。
25. LON-SVR2 で、ユーザー名「Adatum¥Dante」、パスワード「Pa55w.rd」を使用してサインインを試みます。サインインが許可されないことを確認します。

デモンストレーション : 特権の委任

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「Pa55w.rd」を使用してサインインしていることを確認します。
2. サーバー マネージャー コンソールで、[ツール]、[Active Directory ユーザーとコンピューター] の順にクリックします。
3. [Marketing] OU を右クリックし、[制御の委任] をクリックします。
4. [オブジェクト制御の委任ウィザードの開始] ページで、[次へ] をクリックします。
5. [ユーザーまたはグループ] ページで、[追加] をクリックします。
6. [ユーザー、コンピューターまたはグループの選択] ページで「IT」と入力し、[名前の確認]、[OK]、[次へ] の順にクリックします。
7. [委任するタスク] ページで、[ユーザーのパスワードをリセットして次回ログオン時にパスワードの変更を要求する] を選択し、[次へ] をクリックします。
8. [完了] をクリックし、オブジェクト制御の委任ウィザードを閉じます。

9. LON-SVR1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
10. [スタート] をクリックし、[サーバー マネージャー] をクリックします。サーバー マネージャー 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。
11. 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。
12. [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]、[次へ] の順にクリックします。
13. [対象サーバーの選択] ページで、[次へ] をクリックします。
14. [サーバーの役割の選択] ページで、[次へ] をクリックします。
15. [機能の選択] ページで、[リモート サーバー管理ツール]、[役割管理ツール] の順に展開し、[AD DS および AD LDS ツール] を選択して、[次へ]、[インストール] の順にクリックします。
16. インストイールが完了したら、[閉じる] をクリックします。
17. [スタート] を右クリックし、[シャットダウンまたはサインアウト]、[サインアウト] の順にクリックします。
18. LON-SVR1 で、ユーザー名「Adatum¥Beth」、パスワード「Pa55w.rd」を使用してサインインします。
19. [スタート] をクリックし、[サーバー マネージャー] をクリックします。
20. 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。
21. [Adatum.com] の下で、[Marketing] OU をクリックします。[Ada Russell] を右クリックし、[パスワードのリセット] をクリックします。
22. [パスワードのリセット] ダイアログ ボックスに「Pa55w.rd2」と 2 回入力し、[OK] を 2 回クリックします。これにより、Beth のアカウントを使用して [Marketing] OU のパスワードをリセットすることができることを確認できます。
23. [Managers] OU をクリックし、[Art Odum] ユーザー アカウントを右クリックして、[パスワードのリセット] をクリックします。
24. [パスワードのリセット] ダイアログ ボックスに「Pa55w.rd2」と 2 回入力し、[OK] を 2 回クリックします。
25. アクセスが拒否されているため、Art Odum のパスワード変更を完了できないことを確認します。

レッスン 2
コンピューター アカウントおよびサービス アカウント

目次

質問と解答

質問 : 自分の組織でサービス アカウントをどのように管理しているかを受講者に尋ねます。

解答 : 解答はさまざまです。受講者の組織でサービス アカウントをどのように管理しているかによって異なります。

デモンストレーション : グループ管理サービス アカウントの作成と管理

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「Pa55w.rd」を使用してサインインしていることを確認します。
2. [スタート] をクリックし、[Windows PowerShell] をクリックします。
3. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

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

4. 「LON-SVRS-GMSA」という名前のグループ管理サービス アカウントを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
New-ADServiceAccount LON-SVRS-GMSA -DNSHOSTNAME LON-SVRS-GMSA.adatum.com
```

5. LON-SVR1 に切り替え、Beth のアカウントからサインアウトし、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
6. [スタート] をクリックし、[Windows PowerShell] をクリックします。
7. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Install-WindowsFeature RSAT-AD-PowerShell
Set-ADServiceAccount -Identity LON-SVRS-GMSA -PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$
Install-ADServiceAccount LON-SVRS-GMSA
```

8. [スタート] を右クリックし、[コンピューターの管理] をクリックします。
9. [サービスとアプリケーション] を展開し、[サービス] をクリックします。
10. [Windows Internal Database] サービスを右クリックし、[プロパティ] をクリックします。
11. [ログオン] タブで、[アカウント]、[参照] の順にクリックします。
12. [ユーザーの選択] ダイアログ ボックスで、[場所] をクリックします。
13. [場所] ダイアログ ボックスで、[ディレクトリ全体]、[OK] の順にクリックします。
14. [ユーザーまたはサービス アカウントの選択] ダイアログ ボックスに「ADATUM¥LON-SVRS-GMSA$」と入力し、[OK] をクリックします。
15. [パスワード] と [パスワードの確認入力] ボックスを空欄にし、[OK] をクリックします。
16. サービスとしてログオンする権利がアカウントに付与されたというメッセージが表示されたら、[OK] をクリックします。

レッスン 3
資格情報の保護

目次

質問と解答

質問 : 組織で NTLM のブロックを実施する前に何をする必要がありますか。

解答 : 組織は、認証プロトコルを無効にする前に、NTLM の使用状況を監査する必要があります。

参考資料

Credential Guard の構成

参考資料 : 詳細については、次のサイトを参照してください。
Credential Guard によるドメインの派生資格情報の保護
http://aka.ms/Vwpgdp

NTLM のブロック

参考資料 : 詳細については、次のサイトを参照してください。
Introducing the Restriction of NTLM Authentication
http://aka.ms/Ynbr7l

デモンストレーション : 問題のあるアカウントの特定

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「Pa55w.rd」を使用してサインインしていることを確認します。
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 ウィンドウを最大化し、[グローバル検索] をクリックします。
4. 中央のウィンドウの右上にある、円の中の下矢印をクリックし、[条件の追加] をクリックします。
5. [有効期限のある (または無期限の) パスワードが設定されているユーザー] を選択し、[追加] をクリックします。
6. [検索] をクリックします。255 個のアイテムが見つかったことを確認します。
7. [すべてクリア] をクリックします。
8. [条件の追加] をクリックします。
9. [有効なアカウントを持ち、指定日数を過ぎる間ログオンしていないユーザー] を選択し、[追加] をクリックします。
10. 下線のついた設定および [有効なアカウントを持ち、次の日数を過ぎる間ログオンしていないユーザー : 15] をクリックし、[90] をクリックします。
11. [検索] をクリックします。
12. 250 のアイテムが見つかったことを確認します。

レッスン 4
Privileged Access Workstation とジャンプ サーバー

目次

質問と解答

質問 : 自分の環境で Privileged Access Workstation またはジャンプ サーバーを使用するかどうか、またその理由を受講者に尋ねます。

解答 : 解答はさまざまです。受講者の環境によって異なります。

参考資料

ジャンプ サーバー

参考資料 : 詳細については、次のサイトを参照してください。
特権アクセス ワークステーション
http://aka.ms/Rd5xkn

ドメイン コントローラーのセキュリティ保護

参考資料 : 詳細については、次のサイトを参照してください。
攻撃からドメイン コントローラーをセキュリティで保護します
http://aka.ms/H84erd

レッスン 5
Local Administrator Password Solution

目次

質問と解答

質問 : 自分の組織でローカル管理者アカウントのパスワードをどのようにして管理していますか。

解答 : 解答はさまざまです。自身の組織にそのようなテクノロジがないことを伝えてくる受講者もいれば、LAPS を使用する受講者など、ソリューションを持っている受講者もいます。

デモンストレーション : LAPS の構成と展開

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「Pa55w.rd」を使用してサインインしていることを確認します。
2. サーバー マネージャー コンソールで、[ツール]、[Active Directory ユーザーとコンピューター] 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] ドメインを右クリックし、[新規作成]、[組織単位] の順にクリックします。
4. [新しいオブジェクト - 組織単位] ダイアログ ボックスに「Sydney_Computers」と入力し、[OK] をクリックします。
5. [Adatum.com] の下で [Computers] コンテナーをクリックし、[LON-SVR2] を右クリックして、[移動] をクリックします。
6. [移動] ダイアログ ボックスで、[Sydney_Computers] をクリックし、[OK] をクリックします。
7. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
8. [ファイル名を指定して実行] ダイアログ ボックスに「¥¥LON-SVR1¥e$¥Labfiles¥Mod02¥」と入力し、[OK] をクリックします。
9. Mod02 ウィンドウで、[LAPSx64.msi] をダブルクリックします。
10. Local Administrator Password Solution Setup ウィザードの [Welcome] ページで、[Next] をクリックします。
11. [End-User License Agreement] ページで、[I accept the terms in the License Agreement] をクリックし、[Next] をクリックします。
12. [Custom Setup] ページで、[AdmPwd GPO Extension] をクリックし、[Entire feature will be unavailable] を選択します。
13. [Management Tools] の下にある [Fat client UI] をクリックし、[Will be installed on local hard drive] を選択します。
14. 同様に、[Management Tools] の下にある [PowerShell module]、および [GPO Editor templates] をそれぞれクリックし、[Will be installed on local hard drive] を選択します。
15. [Next]、[Install] の順にクリックします。
16. インストールが完了したら、[Finish] をクリックします。
17. [スタート] をクリックし、[Windows PowerShell] をクリックします。
18. 管理者 : Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各行の最後で Enter キーを押します。

```
Import-Module admpwd.ps
Update-AdmPwdADSchema
Set-AdmPwdComputerSelfPermission -Identity "Sydney_Computers"
```

19. 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。
20. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[Sydney_Computers] OU を右クリックして、[このドメインに GPO を作成し、このコンテナーにリンクする] をクリックします。
21. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「LAPS_GPO」と入力し、[OK] をクリックします。
22. グループ ポリシーの管理コンソールで、[Sydney_Computers] の下の [LAPS_GPO] を右クリックし、[編集] をクリックします。
23. 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]、[ポリシー]、[管理用テンプレート] ノードの順に展開し、[LAPS] を選択します。
24. [Enable local admin password management] ポリシーをダブルクリックします。
25. Enable local admin password management ウィンドウで、[有効]、[OK] の順にクリックします。
26. [Password Settings] ポリシーをダブルクリックします。
27. [Password Settings] ポリシー ダイアログ ボックスで [有効] をクリックし、[Password Length] を [20] に設定します。
28. [Password Age] が [30] に設定されていることを確認し、[OK] をクリックします。
29. グループ ポリシー管理エディターを閉じます。
30. LON-SVR2 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
31. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
32. [ファイル名を指定して実行] ダイアログ ボックスに「¥¥LON-SVR1¥e$¥Labfiles¥Mod02¥」と入力し、[OK] をクリックします。
33. Mod02 ウィンドウで、[LAPSx64.msi] をダブルクリックします。
34. Local Administrator Password Solution Setup ウィザードの [Welcome] ページで、[Next] をクリックします。
35. [End-User License Agreement] ページで、[I accept the terms of the License Agreement] をクリックし、[Next]、[Install] の順にクリックします。
36. [Finish] をクリックし、Local Administrator Password Solution Setup ウィザードを閉じます。
37. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
38. [ファイル名を指定して実行] ダイアログ ボックスに「gpupdate /force」と入力し、[OK] をクリックします。
39. LON-SVR2 を再起動します。
40. LON-DC1 に切り替えます。
41. [スタート]、[LAPS]、[LAPS UI] の順にクリックします。
42. [LAPS UI] ダイアログ ボックスで、[Computer Name] ボックスに「LON-SVR2」と入力し、[Search] をクリックします。
43. [Password] と [Password expires] の値を確認し、[Exit] をクリックします。
44. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Get-AdmPwdPassword LON-SVR2 | Out-Gridview
```

45. LON-SVR2 に割り当てられたパスワードを確認します。

演習の復習の質問と解答

演習 A : ユーザーの権利、セキュリティ オプション、およびグループ管理サービス アカウントの実装

質問と解答

質問 : 特定のグループのユーザーが重要なサーバーにサインインできないように、どのようにしてブロックしますか。

解答 : 特定のグループのユーザーが重要なサーバーにサインインできないようにするには、ローカル ログオンを拒否するポリシーを使用してブロックします。

質問 : 組織内の特定のチームにグループの作成、削除、および管理を許可したい場合、どの特権を委任しますか。

解答 : 組織内の特定のチームにグループの作成、削除、および管理を許可したい場合は、制御の委任ウィザードを使用します。

演習 B : LAPS の構成と展開

質問と解答

質問 : OU を構成し、その OU 内のコンピューターが LAPS を使用できるようにするには、どの Windows PowerShell コマンドレットを使用しますか。

解答 : OU を構成し、その OU 内のコンピューターが LAPS を使用できるようにするには、Set-AdmPwdComputerSelfPermission コマンドレットを使用します。

質問 : コンピューターが LAPS を使用するように構成されている場合、AD DS からローカル管理者のパスワードを取得するには、どの Windows PowerShell コマンドレットを使用しますか。

解答 : コンピューターが LAPS を使用するように構成されている場合、AD DS からローカル管理者のパスワードを取得するには、Get-AdmPwdPassword コマンドレットを使用します。

復習とまとめ

復習問題

質問 : LAPS ユーザー インターフェイス (UI) アプリまたは Windows PowerShell を使用して、LAPS を使用するように構成されたコンピューターのローカル管理者のパスワードを既定で取得できるのは、どのセキュリティ グループのメンバーですか。

解答 : LAPS ユーザー インターフェイス (UI) アプリまたは Windows PowerShell を使用して、LAPS を使用するように構成されたコンピューターのローカル管理者のパスワードを取得できるのは、Domain Admins グループおよび Enterprise Admins グループのメンバーです。

第 3 章

Just Enough Administration による管理者権限の制限

目次

レッスン 1
JEA の理解

目次

質問と解答

質問 : JEA 役割機能ファイルで使用されるファイル名拡張子はどれですか。

(　) .psrc

(　) .psd1

(　) .pssc

解答 :

(√) .psrc

(　) .psd1

(　) .pssc

フィードバック :

JEA 役割機能ファイルは、ファイル拡張子として .psrc を使用します。ファイル拡張子の .pssc は、セッション構成ファイルに使用されます。ファイル拡張子の .psd1 は、モジュール マニフェストに使用されます。

デモンストレーション : 役割機能ファイルの作成

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 と LON-SVR2 を起動します。
2. Active Directory ユーザーとコンピューターを使用して、[IT] OU に「DNSOps」という名前のグローバル グループを作成します。
3. ユーザー Beth Burke を DNSOps グループのメンバーに登録します。
4. LON-DC1 で [スタート] をクリックし、[Windows PowerShell ISE] をクリックします。
5. Windows PowerShell ISE ウィンドウを最大化します。
6. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Cd 'c:¥Program Files¥WindowsPowerShell¥Modules'
Mkdir DNSOps
Cd DNSOps
New-ModuleManifest .¥DNSOps.psd1
Mkdir RoleCapabilities
Cd RoleCapabilities
New-PSRoleCapabilityFile -Path .¥DNSOps.psrc
Ise DNSOps.psrc
```

7. Windows PowerShell ISE の DNSOps.psrc スクリプト ウィンドウで、[# VisibleCmdlets =] で始まる行に移動して、その下にカーソルを置き、次を入力します。

```
VisibleCmdlets = @{ Name = ‘Restart-Service’; Parameters = @{ Name=’Name’; ValidateSet = ‘DNS’}}
```

8. [# VisibleFunctions =] で始まる行に移動して、その下にカーソルを置き、次を入力します。

```
VisibleFunctions = 'Add-DNSServerResourceRecord', 'Clear-DNSServerCache','Get-DNSServerResourceRecord','Remove-DNSServerResourceRecord'
```

9. # VisibleExternalCommands = で始まる行に移動して、その下にカーソルを置き、次を入力します。

```
VisibleExternalCommands = ‘C:¥Windows¥System32¥whoami.exe’
```

10. [保存] をクリックします。

デモンストレーション : セッション構成ファイルの作成

デモンストレーションの手順

1. LON-DC1 の Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
New-PSSessionConfigurationFile -Path .¥DNSOps.pssc -Full
Ise DNSOps.pssc
```

2. Windows PowerShell ISE の DNSOps.psrc スクリプト ウィンドウで、SessionType = ‘Default’ 行に移動し、次のように変更します。

```
SessionType = 'RestrictedRemoteServer'
```

3. [#RunAsVirtualAccount = $true] 行に移動し、# を削除して「RunAsVirtualAccount = $true」にします。
4. [# RoleDefinitions] で始まる行に移動し、その下にカーソルを置き、次を入力します。

```
RoleDefinitions = @{ 'ADATUM¥DNSOps' = @{ RoleCapabilities = 'DNSOps' };}
```

5. [保存] をクリックします。

デモンストレーション : JEA エンドポイントの作成

デモンストレーションの手順

1. LON-DC1 の Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Register-PSSessionConfiguration -Name DNSOps -Path .¥DNSOps.pssc
Restart-Service WinRM
Get-PSSessionConfiguration
```

2. DNSOps が Windows PowerShell のエンドポイントとして表示されることを確認します。

レッスン 2
JEA の検証と展開

目次

質問と解答

質問 : 複数の役割機能を持つ 1 つの JEA エンドポイントを作成する方法と、それぞれに異なる役割機能を持つ複数の JEA エンドポイントを作成する方法とでは、どちらが適切ですか。

解答 : 解答はさまざまです。受講者の考えによって異なります。

フィードバック : 個別の JEA エンドポイントを作成することで、個別の操作タスクを異なるユーザーに簡単に委任することができます。単一の JEA エンドポイントを作成し、複数の役割機能にリンクすると、1 つ以上のユーザー グループに、必要ではない管理特権を不注意に割り当てる可能性があります。

デモンストレーション : JEA エンドポイントへの接続

デモンストレーションの手順

1. サインインしていない場合は、LON-SVR1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. [スタート] をクリックし、[Windows PowerShell] をクリックします。
3. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Enter-PSSession -ComputerName LON-DC1
(get-command).count
Whoami
Exit-PSSession
```

4. LON-SVR1 からサインアウトします。
5. LON-SVR1 で、ユーザー名「Adatum¥Beth」、パスワード「Pa55w.rd」を使用してサインインします。
6. [スタート] をクリックし、[Windows PowerShell] をクリックします。
7. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Enter-PSSession -ComputerName LON-DC1 -ConfigurationName DNSOps
(Get-Command).count
WhoAmI
Get-DNSServerResourceRecord -zonename Adatum.com
Add-DNSServerResourceRecord -zonename “Adatum.com” -A -Name “MEL-SVR1” -IPv4Address “172.16.0.101”
Get-DNSServerResourceRecord -zonename Adatum.com
Restart-Service DNS
Restart-Service WinRM
```

注 : Restart-Service WinRM を実行して WinRM サービスを再起動すると、JEA エンドポイントはこれを許可するように構成されていないため、エラーメッセージが表示されます。また、Get-Service を実行してコンピューターの現在のサービスを表示しても、JEA エンドポイントはこれを許可するように構成されていないため、エラーメッセージが表示されます。

```
Exit-PSsession
```

デモンストレーション : 別のコンピューターへの JEA 構成の展開

デモンストレーションの手順

1. サインインしていない場合は、LON-SVR2 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. [スタート] を右クリックし、[ファイル名を指定して実行] をクリックします。
3. [ファイル名を指定して実行] ダイアログ ボックスに「¥¥LON-DC1¥c$」と入力し、[OK] をクリックします。
4. エクスプローラーで、Program Files¥WindowsPowerShell¥Modules フォルダーに移動します。
5. DNSOps フォルダーをローカルの C:¥Program Files¥WindowsPowerShell¥Modules フォルダーにコピーします。
6. [スタート] をクリックし、[Windows PowerShell] をクリックします。
7. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Cd ‘c:¥Program Files¥WindowsPowerShell¥Modules¥DNSOps¥RoleCapabilities’
Register-PSSessionConfiguration -Name DNSOps -Path .¥DNSOps.pssc
Restart-Service WinRM
Get-PSSessionConfiguration
```

8. DNSOps が Windows PowerShell のエンドポイントとして表示されることを確認します。

演習の復習の質問と解答

演習 : JEA による管理者権限の制限

質問と解答

質問 : どのような方法で、追加の DNS サーバーの保守機能を JEA 構成に追加しますか。

解答 : 役割機能ファイルを変更して、追加の DNS サーバーの保守機能を JEA 構成に追加します。

質問 : JEA セッションで仮想アカウントが使用されているかどうかを、どのコマンドで確認できますか。

解答 : whoami.exe コマンドを使用して、JEA セッションで仮想アカウントが使用されているかどうかを確認できます。

復習とまとめ

復習問題

質問：JEA 構成のどの要素により、JEA エンドポイントに接続中に実行できるタスクを指定できますか。

解答：役割機能ファイルにより、JEA エンドポイントに接続中に実行できるタスクを指定できます。

第 4 章

特権アクセス管理と管理フォレスト

目次

レッスン 1
ESAE フォレスト

目次

質問と解答

質問 : 管理タスク用のアカウントをセキュリティで保護する方法として、現在の環境で ESAE フォレストの展開を検討する必要がありますか。

解答 : 解答はさまざまです。環境により異なります。

レッスン 2
Microsoft Identity Manager の概要

目次

質問と解答

質問 : 現在の環境で ID を管理するために、MIM または Forefront Identity Manager (FIM) を展開しているどうかを、受講者に質問します。

解答 : 解答はさまざまです。受講者の環境により異なります。

参考資料

MIM の要件

参考資料 : MIM の要件については、次のサイトを参照してください。
MIM 2016 でサポートされるプラットフォーム
http://aka.ms/Armxl4

レッスン 3
JIT 管理と PAM の概要

目次

質問と解答

質問 : ホスト サーバーのオペレーティング システム以外で、MIM 2016 を展開する前に展開しておく必要がある 2 つの Microsoft 製品は何ですか。

解答 : MIM 2016 を展開する前に SharePoint と SQL Server を展開する必要があります。

デモンストレーション : PAM 信頼関係の構成

デモンストレーションの手順

1. SYD-DC1 と MEL-DC1 を起動します。これらの仮想マシンが起動したら、SYD-MIM と MEL-SVR1 を起動します
2. SYD-MIM で、ユーザー名「Adatumadmin¥MIMAdmin」、パスワード「Pa$$w0rd」を使用してサインインし、Windows PowerShell ウィンドウを開きます。
3. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
$ca = get-credential -UserName Adatum¥Administrator -Message "Adatum forest domain admin credentials"
```

4. メッセージ ダイアログが表示されたら、パスワード「Pa$$w0rd」を使用してサインインし、[OK] をクリックします。
5. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します (仮想マシンの速度に応じて、一部のコマンドレットは実行の完了に数分かかる場合があります)。

```
New-PAMTrust -SourceForest "adatum.com" -Credentials $ca
New-PAMDomainConfiguration -SourceDomain "adatum" -Credentials $ca
Test-PAMTrust -SourceForest "adatum.com" -CorpCredentials $ca
Test-PAMDomainConfiguration -SourceDomain "adatum" -Credentials $ca
```

6. MEL-DC1 に切り替え、ユーザー名「Adatum¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインします。
7. サーバー マネージャー コンソールで、[Tools]、[Active Directory Users and Computers] の順にクリックします。
8. Active Directory ユーザーとコンピューター コンソールで、[Adatum.com] を右クリックし、[Delegate Control] をクリックします。
9. オブジェクト制御の委任ウィザードの [Welcome to the Delegation of Control Wizard] ページで、[Next] をクリックします。
10. [Users or Groups] ページで、[Add] をクリックします。
11. [Select this object type] ページで、[Locations] をクリックします。
12. [Locations] ダイアログ ボックスで、[ADATUMADMIN.COM] をクリックし、[OK] をクリックします。
13. [Select Users, Computers, or Groups] ダイアログ ボックスに「Domain Admins」と入力し、[Check Names] をクリックします。
14. [Enter Network Credentials] ダイアログ ボックスで、次の資格情報を入力し、[OK] をクリックします。
    - Username : ADATUMADMIN¥Administrator
    - Password : Pa$$w0rd

15. [Select Users, Computers, or Groups] ダイアログ ボックスで、[Domain Admins;] の後ろに「Mimmonitor」と入力し、[Check Names]、[OK] の順にクリックします。
16. [Users or Groups] ページで、[Next] をクリックします。
17. [Tasks to Delegate] ページで、[Read all user information] チェック ボックスをオンにし、[Next]、[Finish] の順にクリックします。

デモンストレーション : ユーザーとシャドウ プリンシパルの作成

デモンストレーションの手順

1. MEL-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ていることを確認します。
2. タスク バーで、[Windows PowerShell] アイコンをクリックします。
3. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
New-ADGroup -name CorpAdmins -GroupCategory Security -GroupScope Global -SamAccountName CorpAdmins
New-ADUser -SamAccountName Wayne -name Wayne
$jp = ConvertTo-SecureString 'Pa$$w0rd' -asplaintext -force
Set-ADAccountPassword -identity Wayne -NewPassword $jp
Set-ADUser -identity Wayne -Enabled 1 -DisplayName "Wayne"
```

注 : これにより、CorpAdmins という名前の新しいグループと Wayne という名前の新しいユーザーが作成され、後で PAM のデモンストレーションのために使用されます。

4. SYD-MIM に切り替えます。ユーザー名「adatumadmin¥mimadmin」、パスワード「Pa$$w0rd」を使用してサインインします。
5. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
$sj = New-PAMUser -SourceDomain adatum.com -SourceAccountName Wayne
$jp = ConvertTo-SecureString 'Pa$$w0rd' -asplaintext -force
Set-ADAccountPassword -identity priv.Wayne -NewPassword $jp
Set-ADUser -identity priv.Wayne -Enabled 1
$ca = get-credential -UserName Adatum¥Administrator -Message "Adatum forest domain admin credentials"
```

6. ダイアログ ボックスで、パスワード「Pa$$w0rd」を使用してサインインし、[OK] をクリックします。
7. Windows PowerShell ウィンドウで、次のコマンドを入力し、各コマンドの最後で Enter キーを押します。

```
$pg = New-PAMGroup -SourceGroupName "CorpAdmins" -SourceDomain adatum.com -SourceDC mel-dc1.adatum.com -Credentials $ca
$pr = New-PAMRole -DisplayName "CorpAdmins" -Privileges $pg -Candidates $sj
```

8. SYD-DC1 に切り替えます。ユーザー名「adatumadmin¥Administrator」、パスワード「Pa$$w0rd」を使用してサインインしま。
9. サーバー マネージャーで、[Tools]、[Active Directory Users and Computers] の順にクリックします。
10. [PAM Objects] コンテナーを開き、Adatum.CorpAdmins グループと PRIV.Wayne ユーザーが存在することを確認します。

11. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Get-ADGroup -identity Adatum.corpadmins -properties SIDHistory
Get-ADGroup -server mel-dc1.adatum.com -identity corpadmins
```

注 : Adatum グループの SID 値と ADATUMADMINS グループの SID 履歴値は同じです。

デモンストレーション : 特権アクセスの構成と要求

デモンストレーションの手順

1. ユーザー名「Adatum¥administrator」、パスワード「Pa$$w0rd」を使用して MEL-SVR1 にサインインしていることを確認します。
2. Hyper-V コンソールを使用して MEL-SVR1 仮想マシンに、MIM2016_EVAL.iso を挿入します。
3. MEL-SVR1 で「Adatum¥administrator」を使用してサインインし、[DVD ドライブ (D:) MIM2016-EVAL] を開きます。
4. タスク バーで [エクスプローラー] アイコンをクリックし、[DVD ドライブ (D:) MIM2016-EVAL] をダブルクリックします。
5. [Microsoft Identity Manager] ページで、[Install Add-ins and Extensions, 64-bit] をクリックします。
6. [Do you want to run or save setup.exe?] ダイアログ ボックスで、[Run] をクリックします。
7. Microsoft Identity Manager 2016 ウィザードの [Welcome to the Microsoft Identity Manager Add-ins and Extensions Setup Wizard] ページで、[Next] をクリックします。
8. [End-User License Agreement] ページで、[I accept the terms in the License Agreement] をクリックし、[Next] をクリックします。
9. [カスタマー エクスペリエンス向上プログラム] ページで、[I don’t want to join the program at this time]、[Next] の順にクリックします。
10. [Custom Setup] ページで、[MIM Add-in for Outlook]、[Entire feature will be unavailable] の順にクリックします。
11. [Custom Setup] ページで、MIM Password and Authentication]、[Entire feature will be unavailable] の順にクリックします。
12. [Custom Setup] ページで、[PAM Client]、[Entire Feature Will Be Installed On Local Hard Drive] をクリックし、[Next] をクリックします。
13. [Configure MIM PAM Service Address] ページで、次の設定を構成し、[Next] をクリックします。
    - PAM Server Address : syd-mim.adatumadmin.com
    - Port : 5725
14. [Install] をクリックし、インストールが完了したら、[Finish] をクリックします。
15. [Start] を右クリックし、[Computer Management] をクリックします。
16. Computer Management コンソールで、[Local Users and Groups] を展開し、[Groups] をクリックし、[Administrators] グループをダブル クリックします。
17. [Administrators Properties] ダイアログ ボックスで、[Add] をクリックします。

18. [Select Users, Computers, Service Accounts, or Groups] ダイアログ ボックスに「Adatumadmin¥Adatum.corpadmins」と入力し、[Check Names] をクリックします。
19. 資格情報「Adatumadmin¥Administrator」、パスワード「Pa$$w0rd」を入力し、[OK] を 3 回クリックします。
20. [Start] を右クリックし、[Shut Down or Sign Out] を選択して、[Restart] をクリックし、[Continue] をクリックします。
21. MEL-SVR1 で、ユーザー名「Adatum¥Wayne」、パスワード「Pa$$w0rd」を使用してサインインします。
22. タスク バーの [Windows PowerShell] をクリックします。Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
Whoami /groups
```

23. Wayne アカウントが Adatum.CorpAdmins グループのメンバーではないことを確認します。
24. タスク バーの [サーバー マネージャー] をクリックします。
25. サーバー マネージャー コンソールで、[Manage]、[Add Roles and Features] の順にクリックします。
26. [Before you begin] ページで、[Next] を 4 回クリックします。
27. [Select Features] ページで、[WINS Server] をクリックします。
28. [Add Roles and Features Wizard] ダイアログ ボックスで、[Add Features]、[Next]、[Install] の順にクリックします。
29. [you do not have adequate user rights to make changes to the target computer] というメッセージを確認し、[Close] をクリックします。
30. [Start] を右クリックし、[Shut Down or Sign Out]、[Sign out] の順にクリックします。
31. ユーザー名「Adatumadmin¥priv.Wayne」、パスワード「Pa$$w0rd」を使用して MEL-SVR1 にサインインします。
32. タスク バーの [Windows PowerShell] をクリックします。Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
Whoami /groups
```

33. アカウントが Adatum.CorpAdmins グループのメンバーではないことを確認します。
34. タスク バーの [サーバー マネージャー] をクリックします。
35. サーバー マネージャー コンソールで、[Manage]、[Add Roles and Features] の順にクリックします。
36. [Before you begin] ページで、[Next] を 4 回クリックします。
37. [Select Features] ページで、[WINS Server] をクリックします。
38. [Add Roles and Features Wizard] ダイアログ ボックスで、[Add Features]、[Next]、[Install] の順にクリックします。
39. [you do not have adequate user rights to make changes to the target computer] というメッセージを確認し、[Close] をクリックします。
40. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Import-Module MIMPAM
Get-PAMRoleForRequest
```

注 : これにより、priv.Wayne アカウントに適用できるロールのリストが表示されます。一覧されたロールの TTL を確認します。

41. 次のコマンドレットを入力します。

```
New-PamRequest -RoleDisplayName CorpAdmins
```

注 : 要求のステータスは [Processing] (処理中) に設定されています。

42. [Start] を右クリックし、[Shut Down or Sign Out]、[Sign out] の順にクリックします。
43. MEL-SVR1 で、ユーザー名「Adatumadmin¥priv.Wayne」、パスワード「Pa$$w0rd」を使用してサインインします。
44. タスク バーの [Windows PowerShell] をクリックします。Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
Whoami /groups
```

45. アカウントが Adatum.CorpAdmins グループのメンバーであることを確認します。
46. サーバー マネージャー コンソールで、[Manage]、[Add Roles and Features] の順にクリックします。
47. [Before you begin] ページで、[Next] を 4 回クリックします。
48. [Select Features] ページで、[WINS Server] をクリックします。
49. [Add Roles and Features Wizard] ダイアログ ボックスで、[Add Features]、[Next]、[Install] の順にクリックします。
50. インストールが完了したら、[Close] をクリックします。

デモンストレーション : PAM ロールの管理

デモンストレーションの手順

1. MEL-DC1 に切り替えて、ADATUM¥Administrator としてサインインしていることを確認します。
2. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
New-ADUser -SamAccountName Gavin -name Gavin
$jp = ConvertTo-SecureString 'Pa$$w0rd' -asplaintext -force
Set-ADAccountPassword -identity Gavin -NewPassword $jp
Set-ADUser -identity Gavin -Enabled 1 -DisplayName "Gavin"
```

注 : この一連のコマンドレットにより、PAM で使用可能な Gavin という名前の新しいユーザーを作成できます。

3. SYD-MIM に切り替え、ADATUMADMIN¥MIMAdmin としてサインインしていることを確認します。

4. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
$sj = New-PAMUser -SourceDomain adatum.com -SourceAccountName Gavin
$jp = ConvertTo-SecureString 'Pa$$w0rd' -asplaintext -force
Set-ADAccountPassword -identity priv.Gavin -NewPassword $jp
Set-ADUser -identity priv.Gavin -Enabled 1
```

5. SYD-MIM で Internet Explorer を起動し、http://syd-mim.adatumadmin.com:82/IdentityManagement/default.aspx に移動します。この操作が完了するまでに数分かかる場合があります。
6. Microsoft Identity Manager コンソールの [Privileged Access Management] で [PAM Roles] をクリックします。
7. [Privileged Access Management] 役割のリストで、[CorpAdmins] をクリックします。
8. [Corpadmins] ダイアログ ボックスの [General] タブで、[PAM Role TTL(sec)] を 3600 から 600 に変更し、[OK]、[Submit] の順にクリックします。

注 : このデモンストレーションを実施する際、他のフィールドの機能を説明することもできます。

9. [Privileged Access Management] 役割のリストで、[Corpadmins] をクリックします。
10. [Corpadmins] ダイアログ ボックスの [Candidates] タブで、[Browse] (文書のアイコン) をクリックします。
11. [Select Users] ダイアログ ボックスで、検索ボックスの横にある虫眼鏡をクリックします。Wayne と Adatum.Wayne はすでに選択されていることを確認します。ADATUM.Gavin と Gavin を選択し、[OK] を 2 回クリックして、[Submit] をクリックします。
12. [OK] をクリックし、[CorpAdmins] ダイアログ ボックスを閉じます。
13. [Privileged Access Management] の [PAM Requests] をクリックします。
14. [PAM Requests] を確認します。
15. [PRIV.Wayne] をクリックし、要求がいつ実行されたか、要求がいつ期限切れになるかを確認します。

演習の復習の質問と解答

演習 : PAM による管理者権限の制限

質問と解答

質問 : PAM ロールを要求しているユーザーが、そのロールにアクセスするのに 1 時間ではなく 2 時間かかっていることを確認するためには、どのような手順をおこないますか。

解答 : ロールの TTL を 2 時間に変更します。

質問 : PAM ロールが付与されているユーザーをどこで確認できますか。

解答 : MIM コンソールで、特権アクセス管理領域の下で PAM 要求セクションを使用することができます。

復習とまとめ

復習問題

質問 : PAM の展開に必要なフォレストの最小数はいくつですか。

解答 : PAM の展開には、PAM と運用フォレストを展開する管理フォレストを含め、少なくとも 2 つのフォレストが必要です。

第 5 章

マルウェアおよび脅威の軽減

目次

レッスン 1
Windows Defender の構成と管理

目次

質問と解答

質問 : Windows Defender で利用できるスキャン オプションを列挙してください。

解答 : 次の表で、スキャン オプションについて説明します。

スキャン オプション	説明
クイック	ウイルス、スパイウェア、望ましくないソフトウェアなどのマルウェアが最も感染する可能性のある領域をチェックします。
フル	ハード ディスク上のすべてのファイルと実行中のプログラムのすべてをチェックします。
カスタム	ユーザーが特定のドライブおよびフォルダーを選択してスキャンできます。

デモンストレーション : Windows Defender の使用

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-CL1 を起動します
2. LON-CL1 に切り替え、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
3. [スタート] を右クリックし、[コントロール パネル] をクリックします。
4. [表示方法] リストで、[大きいアイコン] を選択し、[Windows Defender] をクリックします。
5. [新機能] ダイアログ ボックスで、[閉じる] をクリックします。
6. Windows Defender の [ホーム] タブで、[クイック] スキャンが選択されていることを確認します。
7. [今すぐスキャン] をクリックし、結果を確認します。
8. Windows Defender を閉じます。
9. エクスプローラーを開き、C:¥Files に移動します。
10. [ファイル] フォルダーの sample.txt をメモ帳で開きます。sample.txt ファイルには、マルウェア検出をテストするためのテキスト文字列が含まれています。
11. sample.txt で <remove> インスタンスを両方ともかっこを含めて削除します。また、余分な行または空白も削除します。
12. ファイルを保存して閉じます。この後すぐに、Windows Defender により潜在的な脅威が検出されます。
13. Windows Defender により、sample.txt が Files フォルダーから削除されます。
14. [スタート] を右クリックし、[コントロール パネル] をクリックします。
15. [Windows Defender] をクリックします。
16. Windows Defender で、[履歴] タブをクリックします。
17. [詳細の表示] をクリックし、結果を確認します。
18. 検疫されているすべてのファイルを削除します。
19. 開いているウィンドウをすべて閉じます。

レッスン 2
ソフトウェアの制限

目次

参考資料

AppLocker とは

参考資料 : AppLocker の詳細については、次のサイトを参照してください。
AppLocker の概要
http://technet.microsoft.com/ja-jp/library/hh831409.aspx

デモンストレーション : AppLocker 規則の作成

デモンストレーションの手順

GPO を作成して実行可能ファイルに対する AppLocker の既定の規則を実施する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. グループ ポリシーの管理コンソール (GPMC) で、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に参照します。
3. [グループ ポリシー オブジェクト] を右クリックし、[新規] をクリックします。
4. [新しい GPO] ウィンドウで、[名前] ボックスに「WordPad Restriction Policy」と入力し、[OK] をクリックします。
5. [WordPad Restriction Policy] を右クリックし、[編集] をクリックします。
6. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[アプリケーション制御ポリシー]、[AppLocker] の順に参照します。
7. [実行可能ファイルの規則] を右クリックし、[新しい規則の作成] をクリックします。
8. [開始する前に] ページで、[次へ] をクリックします。
9. [アクセス許可] ページで、[拒否] を選択し、[次へ] をクリックします。
10. [条件] ページで、[発行元] を選択し、[次へ] をクリックします。
11. [発行元] ページで、[参照] をクリックし、[PC] をクリックします。
12. [開く] ページで、[ローカル ディスク (C:)] をダブルクリックします。
13. [開く] ページで、[Program Files]、[Windows NT]、[Accessories] の順に展開し、[wordpad.exe] をクリックし、[開く] をクリックします。
14. スライダーを [ファイル名] の位置まで上に移動し、[次へ] をクリックします。
15. 再度 [次へ] をクリックし、[作成] をクリックします。
16. 既定の規則を作成するように求められた場合は、[はい] をクリックします。
17. 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]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に参照します。
18. [アプリケーション制御ポリシー] を展開し、[AppLocker] を右クリックして、[プロパティ] をクリックします。
19. [強制] タブの [実行可能ファイルの規則] で [構成済み] チェック ボックスをオンにして、[規則の実施] をクリックし、[OK] をクリックします。

20. 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]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に参照します。
21. [システム サービス] をクリックし、[Application Identity] をダブルクリックします。
22. [Application Identity] のプロパティで、[このポリシーの設定を定義する] チェック ボックスをオンにします。
23. [サービスのスタートアップ モードを選択してください] の [自動] をクリックし、[OK] をクリックします。
24. グループ ポリシー管理エディターを閉じます。

GPO をドメインに適用する

1. GPMC 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] を展開します。
2. GPMC で、[Adatum.com] を右クリックし、[既存の GPO のリンク] をクリックします。
3. GPO の選択ウィンドウのグループ ポリシー オブジェクト ウィンドウで [WordPad Restriction Policy] をクリックし、[OK] をクリックします。
4. GPMC を閉じます。
5. スタート画面に切り替え、「cmd」と入力し、Enter キーを押します。
6. コマンド プロンプトで「gpupdate /force」と入力し、Enter キーを押します。ポリシーが更新されるのを待ちます。

AppLocker 規則をテストする

1. LON-CL1 で、ユーザー名「Adatum¥Beth」、パスワード「Pa55w.rd」を使用してサインインします。
2. [検索] ボックスに「cmd」と入力し、Enter キーを押します。
3. コマンド プロンプトで「gpupdate /force」と入力し、Enter キーを押します。ポリシーが更新されるのを待ちます。
4. [検索] ボックスに「WordPad」と入力し、Enter キーを押します。ワードパッドが起動しないことを確認します。

 **注 :** gpupdate が有効になるまでに数分かかる場合があります。ワードパッドが起動する場合は、数分待ってから再試行します。

レッスン 3
Device Guard 機能の構成と使用

目次

参考資料

Device Guard ポリシーの実装

 **参考資料 :** 詳細については次のサイトを参照してください。
ConfigCI Module
http://aka.ms/U0nker

コードの整合性ファイルの規則

 **参考資料 :** 詳細については次のサイトを参照してください。
署名されていないアプリをコード整合性ポリシーに追加する
http://aka.ms/Tkie2j

 **参考資料 :** signtool.exe をダウンロードするには、次のサイトを参照してください。
SignTool
http://aka.ms/S4ihkk

デモンストレーション : コードの整合性ファイルの規則の作成

デモンストレーションの手順

1. LON-DC1 で、スタート画面を開き、[Windows PowerShell] を選択します。
2. Windows PowerShell ウィンドウで、次のコマンドを入力し、各行の最後で Enter キーを押します。

```
$CIPolicyPath=$env:userprofile+"¥Desktop¥"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
```

3. インストールされているアプリケーションについて、デバイスをスキャンします。コードの整合性ポリシーを作成するために、次のコマンドレットを入力して、Enter キーを押します。

```
New-CIPolicy -Audit -Level Hash -FilePath $InitialCIPolicy -UserPEs -Fallback Hash 3> Warningslog.txt
```

4. コードの整合性ポリシーをバイナリ形式に変換するために、次のコマンドレットを入力して、Enter キーを押します。

```
ConvertFrom-CIPolicy $InitialCIPolicy $CIPolicyBin
```

5. 手順が完了したら、Windows PowerShell ウィンドウを閉じます。Device Guard ポリシー ファイル (DeviceGuardPolicy.bin) と元の .xml ファイル (InitialScan.xml) が、デスクトップ上に作成されます。
6. タスク バーの [エクスプローラー] アイコンをクリックし、[クイック アクセス] ボックスに「C:¥Users¥Administrator¥Desktop¥Initialscan.xml」と入力し、Enter キーを押して、デスクトップにある InitalScan.xml ファイルを開きます。

   SIPolicy の現在の規則が、監査モードが有効として設定されていることがわかります。
7. [スタート] をクリックし、[Windows PowerShell] をクリックします。

8. 規則のオプションを確認するために、Windows PowerShell ウィンドウで、次のコマンドレットを入力します。

```
Set-RuleOption -Help
```

9. コマンドの出力で、規則 3 で [監査モード] が有効 (Enabled : Audit Mode) になっていることを確認します。

10. 次のコマンドレットを入力し、各行の最後で Enter キーを押します。

```
# 使用する変数を初期化します
$CIPolicyPath=$env:userprofile+"¥Desktop¥"
$InitialCIPolicy=$CIPolicyPath+"InitialScan.xml"
$CIPolicyBin=$CIPolicyPath+"DeviceGuardPolicy.bin"
$EnforcedCIPolicy=$CIPolicyPath+"EnforcedPolicy.xml"
$CIEnforceBin = $CIPolicyPath + “EnforceDeviceGuardPolicy.bin"
# 元のコピーを維持するために初期ファイルをコピーします
cp $InitialCIPolicy $EnforcedCIPolicy
# 監査モードを削除します
Set-RuleOption -Option 3 -FilePath $EnforcedCIPolicy -Delete
# 新しいコードポリシーをバイナリ形式に変換します
ConvertFrom-CIPolicy $EnforcedCIPolicy $CIEnforceBin
```

11. デスクトップにある EnforcedPolicy.xml ファイルを開き、[監査モード] の記述 (Enabled : Audit Mode) がないことを確認します。

レッスン 4
EMET の展開と使用

目次

デモンストレーション : EMET によるアプリケーションの保護

デモンストレーションの手順

1. 23744B-LON-DC1 で、E:¥Labfiles¥Mod05 にある EMET Setup.msi をインストールします。
2. インストールが完了したら、[Configure Manually Later] を選択し、[Finish]、[Close] の順にクリックします。
3. 右下隅の通知領域で、[EMET Notification] アイコンを右クリックし、[Open EMET] を選択します。
4. 上部のメニュー バーで [Apps] をクリックし、EMET で構成されているアプリケーションのリストが空白になっていることを確認して、Application Configuration ウィンドウを閉じます。
5. EMET の左上隅で、[Import] をクリックします。
6. [Recommended Software.xml] 選択し、[開く] をクリックします。
7. 上部のメニュー バーで [Apps] をクリックし、EMET で構成されているアプリケーションのリストが登録されたことを確認します。
8. Windows PowerShell の実行可能ファイルをアプリケーション構成に追加するために、[Add Application] をクリックし、[ファイル名] ボックスに「C:¥Windows¥System32¥WindowsPowerShell¥v1.0¥powershell.exe」と入力します。
9. [開く]、[OK] の順にクリックします。
10. [スタート] をクリックし、[Windows PowerShell] アイコンをクリックします。Windows PowerShell が起動したら、Windows PowerShell ウィンドウを最小化します。
11. [Enhanced Mitigation Experience Toolkit] ページで、[Refresh] をクリックします。[Running Processes] の下に [PowerShell - Windows PowerShell] が表示されることを確認します。

演習の復習の質問と解答

演習 : AppLocker、Windows Defender、Device Guard 規則、および EMET によるアプリケーションのセキュリティ保護

質問と解答

質問 : 演習には、マルウェアの防止に使用できるいくつかのオプションが含まれていました。どのソリューションが、脆弱性の悪用を可能な限り困難にするセキュリティ緩和策テクノロジを使用していますか。

解答 : EMET です。EMET は、悪用を非常に困難にします。ただし、セキュリティ緩和策テクノロジにより、悪意のあるハッカーが脆弱性を悪用できないと保証することはできません。

質問 : この章で紹介されたどのテクノロジを組み合わせて、マルウェアを防ぐことができますか。

解答 : Windows Defender、AppLocker、EMET、および Device Guard は、連携して Windows システム上のマルウェアを阻止するように設計されています。

復習とまとめ

ベスト プラクティス

組織で EMET を使用する際、GPO を使用して、環境全体で一貫した構成を展開する必要があります。

復習問題

質問 : 大規模なエンタープライズ環境で EMET を展開するためには、どのような方法が最良ですか。

解答 : グループ ポリシーまたは System Center Configuration Manager を使用します。現在のバージョンは、グループ ポリシーと System Center Configuration Manager に既定で対応しています。

実際の問題とシナリオ

世界中の組織で、マルウェアを使用して脆弱性が悪用されているという新たな報告があります。最新の Microsoft セキュリティ情報を確認して、システムにどのような脆弱性が存在する可能性があるか、およびマルウェア対策テクノロジと更新プログラムについて最新情報を取得する方法を理解します。

ツール

Windows システムの脆弱性の検出に使用できるツールが多数あります。Kali Linux には、Windows 管理者がシステムのセキュリティのテストに使用できる複数のツールが含まれ、無料で配布されています。

第 6 章

詳細な監査とログ分析によるアクティビティの分析

目次

レッスン 1
監査の概要

目次

デモンストレーション : セキュリティ ログのイベントの検索

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 を起動します。
2. LON-SVR1 のタスク バーで、[エクスプローラー] をクリックします。
3. ナビゲーション ウィンドウで、[PC] をクリックします。
4. [Allfiles (D:)] をダブルクリックします。
5. [Labfiles] を右クリックし、[プロパティ] をクリックし、[セキュリティ] タブをクリックして、[詳細設定] をクリックします。
6. [監査] タブをクリックし、[追加] をクリックします。
7. [プリンシパルの選択] をクリックします。ボックスに「Everyone」と入力し、[OK] をクリックします。
8. [種類] で、[すべて] を選択し、[OK] をクリックします。
9. [OK] を 2 回クリックします。
10. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
11. [フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[Default Domain Policy] を右クリックして、[編集] をクリックします。
12. [コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に展開し、[ローカル ポリシー] を展開します。
13. [監査ポリシー] をクリックします。
14. [オブジェクト アクセスの監査] をダブルクリックし、[これらのポリシーの設定を定義する] チェック ボックスをオンにします。
15. [成功] チェック ボックスと [失敗] チェック ボックスの両方をオンにし、[OK] をクリックします。
16. コマンド プロンプトを開き、次のコマンドを入力して、Enter キーを押します。

```
gpupdate /force
```

注 : 監査ポリシーは、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[詳細な監査ポリシー] の下の [監査ポリシーの詳細な構成] で構成することもできます。

レッスン 2
詳細な監査

目次

参考資料

監査コレクション サービス

参考資料 : ACS についての詳細は、次のサイトを参照してください。
サービス (ACS) コレクターとデータベースの監査コレクションをインストールする方法
https://msdn.microsoft.com/ja-jp/library/hh284670(v=sc.12).aspx

デモンストレーション : 詳細な監査の構成

デモンストレーションの手順

1. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
2. グループ ポリシーの管理で、[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] を右クリックし、[新規作成] をクリックします。
3. 新しい GPO ウィンドウの [名前] ボックスに「File Audit」と入力し、Enter キーを押します。
4. [グループ ポリシー オブジェクト] をダブルクリックし、[File Audit] を右クリックして、[編集] をクリックします。
5. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[監査ポリシーの詳細な構成]、[監査ポリシー] の順に展開し、[オブジェクト アクセス] をクリックします。
6. [詳細なファイル共有の監査] をダブルクリックします。
7. [詳細なファイル共有の監査のプロパティ] ダイアログ ボックスで、[次の監査イベントを構成する] チェック ボックスをオンにします。
8. [成功] チェック ボックスと [失敗] チェック ボックスをオンにし、[OK] をクリックします。
9. [リムーバブル記憶域の監査] をダブルクリックします。
10. [プロパティ] ダイアログ ボックスで、[次の監査イベントを構成する] チェック ボックスをオンにします。
11. [成功] チェック ボックスと [失敗] チェック ボックスをオンにし、[OK] をクリックします。
12. グループ ポリシー管理エディターを閉じます。
13. グループ ポリシーの管理を閉じます。

デモンストレーション : イベント ログの転送

デモンストレーションの手順

1. LON-SVR1 で [スタート] をクリックし、[Windows PowerShell] をクリックします。
2. 次のコマンドを入力し、Enter キーを押します。

```
winrm quickconfig
```

3. LON-DC1 に接続し、[スタート] をクリックします。

4. [Windows PowerShell] をクリックし、次のコマンドを入力して、Enter キーを押します。

```
wecutil qc
```

5. [サービスのスタートアップ モードは Delay-Start に変更されます。続行しますか] と表示されたら「Y」と入力します。
6. 次のコマンドを入力し、各コマンドの最後で Enter キーを押します。

```
Winrm id -remote:lon-svr1
Winrm enumerate winrm/config/listener
```

7. LON-SVR1 に接続し、Windows PowerShell ウィンドウを選択し、次のコマンドを入力して、各コマンドの最後で Enter キーを押します。

```
Winrm id -remote:lon-dc1
Winrm enumerate winrm/config/listener
shutdown -r
```

8. LON-DC1 に切り替えて、続けて Windows PowerShell を使用し、次のコマンドを入力して、各コマンドの最後で Enter キーを押します。

```
net localgroup "event log readers" LON-DC1$ /add
shutdown -r
```

9. LON-SVR1 の再起動後、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用して再度サインインします。
10. LON-DC1 の再起動後、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用して再度サインインします。
11. LON-DC1 で、サーバー マネージャーが開くのを待ちます。
12. [ツール] をクリックし、[イベント ビューアー] を選択します。
13. コンソール ツリーで [サブスクリプション] をクリックし、ダイアログが表示されたら [はい] をクリックします。
14. [操作] メニューで、[サブスクリプションの作成] をクリックします。
15. [サブスクリプション名] ボックスにサブスクリプションの名前として「LogDemo」と入力します。
16. [説明] ボックスにオプションの説明を入力します。
17. [宛先ログ] ボックスで、ログ ファイルとして既定の [転送されたイベント ログ] が指定されていることを確認します。
18. [コンピューターの選択] をクリックします。
19. [ドメイン コンピューターの追加] をクリックし、「LON-SVR1」と入力して [名前の確認] をクリックし、[OK] を 2 回クリックします。
20. [イベントの選択] をクリックし、[クエリ フィルター] ダイアログ ボックスを表示します。
21. [イベントレベル] で、[重大]、[警告]、[エラー] チェックボックスをオンにして、[イベント ログ] の横で、[Application] と [セキュリティ] を選択します。[OK] をクリックします。
22. [サブスクリプションのプロパティ] ダイアログ ボックスで [OK] をクリックします。サブスクリプションがサブスクリプション ウィンドウに追加され、操作が正常に終了すると、サブスクリプションのステータスが [アクティブ] になります。
23. LON-SVR1 で、[スタート] をクリックし、[Windows PowerShell] をクリックします。

24. 次のコマンドを入力し、Enter キーを押します。

```
Eventcreate /id 999 /t error /l application /d “Error test event”
```

25. 数分経ったら LON-DC1 に戻り、LON-SVR1 からイベントが転送されていることを確認します。[Windows ログ] ノードの [転送されたイベント] でイベントを確認できます。

注 : イベントが LON-DC1 で表示されるまでに 15 ～ 20 分かかる場合があります。

レッスン 3
Windows PowerShell の監査とログ

目次

デモンストレーション : Windows PowerShell をによる監査の管理

デモンストレーションの手順

1. サーバー マネージャーで、[ツール]、[イベント ビューアー] の順にクリックします。
2. [Windows ログ] の [システム] を確認します。
3. [スタート] をクリックし、[Windows PowerShell] をクリックします。
4. 次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Get-EventLog Security -newest 20
Get-EventLog System -newest 20 | Format-List
Get-EventLog "Windows PowerShell" | Group-Object eventid | Sort-Object Name
```

デモンストレーション : トランスクリプト ログ、モジュール ログ、およびスクリプト ブロックのログ記録の構成

デモンストレーションの手順

1. 必要に応じて、LON-DC1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. Windows PowerShell ウィンドウに切り替えます。
3. 次のコマンドレットを入力し、Enter キーを押します。

```
Get-Module Microsoft.*| Select Name, LogPipelineExecutionDetails
```

4. 出力をチェックし、LogPipelineExecutionDetails のステータスを確認します。
5. 次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Get-Module Microsoft.*| ForEach {$_.LogPipelineExecutionDetails = $True}
Get-Module Microsoft.*| Select Name, LogPipelineExecutionDetails
```

6. 出力を確認した後、次のコマンドレットを入力し、各コマンドレットの最後で Enter キーを押します。

```
Get-EventLog Security -Newest 100
Get-ChildItem -Path C:¥inetpub¥wwwroot
```

7. イベント ログを確認します。
8. Windows PowerShell に戻り、次のコマンドレットを入力して、Enter キーを押します。

```
Get-WinEvent -FilterHashtable @{LogName='Windows PowerShell';Id ='800'} -MaxEvents 1 | Select -Expand Message
```

9. サーバー マネージャーを開き、[ツール]、[グループ ポリシーの管理] の順に選択します。
10. [Default Domain Policy] を右クリックし、[編集] をクリックします。
11. グループ ポリシー管理エディターを閉じます。
12. [コンピューターの構成]、[ポリシー]、[管理用テンプレート]、[Windows コンポーネント] の順に展開し、[Windows PowerShell] をクリックして、メイン画面に表示される GPO の設定を確認します。
13. GPO ノードを折りたたみます。
14. [コンピューターの構成]、[基本設定]、[Windows の設定] の順に展開し、[環境] を右クリックし、[新規作成] をポイントして、[環境変数] を選択します。次の情報を入力します。

- 名前 : PSLogScriptBlockExecution
- 値 : 0

15. [OK] をクリックし、[環境] を右クリックし、[新規作成] をポイントして、[環境変数] をクリックします。次の情報を入力して、[OK] をクリックします。
    - 名前 : PSLogScriptBlockExecutionVerbose
    - 値 : 0
16. グループ ポリシー管理エディターを閉じます。
17. [スタート] をクリックし、[サーバー マネージャー] を選択して、[ツール]、[イベント ビューアー] の順にクリックします。
18. [Windows ログ] の [システム] を確認します。
19. 次のファイル パスで、イベント トレーシング (ETW) ログを確認します。
    [アプリケーションとサービス]、[Microsoft]、[Windows]、[PowerShell]、[Operational]
20. 開いているウィンドウをすべて閉じます。

演習の復習の質問と解答

演習 : 詳細な監査の構成

質問と解答

質問 : 監査ポリシーを組織全体に適用する理由は何ですか。

解答 : 全般的な問題を正確に特定しようとする場合や、特定のイベントがどこで発生しているか確かでない場合、イベントをキャプチャするためには、大規模なサーバーのグループを対象にする必要があります。この場合、イベントのフィルター処理を使用して、特定の監査イベントを見つけることができます。問題の場所を正確に特定してから、監査のスコープを絞り込んだり、監査を無効化したりして、生成されるログ数を削減し、コンピューターのパフォーマンスへの影響を抑え、定期的に収集するログの読み取りを容易にすることがベスト プラクティスです。

復習とまとめ

ベスト プラクティス

Windows Server 2016 では、セキュリティ監査ログのレベルを詳細化し、監査ポリシーの展開と管理を簡略化する監査機能の強化がおこなわれています。

監査は、ネットワークで継続されるアクティビティで、組織における重要なセキュリティ プラクティスの 1 つです。セキュリティ関連のイベントを監査することで、潜在的に悪意のあるアクティビティについて早期に通知を受け取ったり、侵害が発生した場合に証拠を得たりすることができます。

復習問題

質問 : グループ ポリシーを使用して、組織のすべてのファイル サーバーに適用するために、監査ポリシーを構成しました。ポリシーを有効化し、グループ ポリシー設定が適用されていることを確認した後、監査イベントがイベントログに記録されていないことがわかりました。最も可能性の高い原因は何ですか。

解答 : ファイル アクセスを監査するには、ファイルまたはフォルダーを構成して、特定のイベントを監査する必要があります。それをおこなわないと、監査イベントは記録されません。

実際の問題とシナリオ

転送されたイベントのログを確認すると、イベント ログ リーダーの許可がスキップされると、コレクターが次のメッセージを表示する場合があります。

ソース Microsoft-Windows-EventForwarder からのイベント ID 111 の説明が見つかりません。このイベントを発生させるコンポーネントがローカル コンピューターにインストールされていないか、インストールが壊れています。ローカル コンピューターにコンポーネントをインストールするか、コンポーネントを修復してください。イベントが別のコンピューターから発生している場合、イベントと共に表示情報を保存する必要があります。

第 7 章

Microsoft Advanced Threat Analytics と Microsoft Operations Management Suite の展開と構成

目次

レッスン 1
ATA の展開と構成

目次

質問と解答

質問 : ATA Lightweight Gateway を構成する場合、ポート ミラーリングを構成する必要があります。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック :

ATA Lightweight Gateway をドメイン コントローラーにインストールすることで、ポート ミラーリングを構成する必要がなくなります。

質問 : ドメイン シンクロナイザーの候補として、どの ATA ゲートウェイを構成する必要がありますか。

( ) すべての ATA ゲートウェイ

( ) リモート サイトの ATA ゲートウェイ

( ) 読み取り専用のドメイン コントローラーにインストールされた ATA ゲートウェイ

( ) 読み取り専用のドメイン コントローラーおよび、リモート サイトの ATA ゲートウェイではない、その他すべての ATA ゲートウェイ

解答 :

( ) すべての ATA ゲートウェイ

( ) リモート サイトの ATA ゲートウェイ

( ) 読み取り専用のドメイン コントローラーにインストールされた ATA ゲートウェイ

(√) 読み取り専用でなく、リモート サイトの ATA ゲートウェイでない、その他すべての ATA ゲートウェイ

フィードバック :

既定では、ATA ゲートウェイのみがドメイン シンクロナイザー候補として設定されます。すべてのリモート サイトの ATA ゲートウェイを、ドメイン シンクロナイザー候補から外すことを推奨します。ドメイン コントローラーが読み取り専用の場合、ドメイン シンクロナイザー候補として設定しないでください。

参考資料

ATA の理解

参考資料 : 詳細については、次のサイトでデータシートを参照してください。
Microsoft Advanced Threat Analytics
https://www.microsoft.com/ja-jp/cloud-platform/products-Microsoft-Advanced-Threat-Analytics.aspx

ATA の展開要件

参考資料 : ディレクトリ オブジェクトのアクセス許可については、次のサイトを参照してください。
View or Set Permissions on a Directory Object
http://aka.ms/Bgxyha

デモンストレーション : ATA の展開と構成

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 と LON-CL1 を起動します。
2. LON-DC1 Active Directory ユーザーとコンピューターを開きます。
3. IT OU に次のユーザーを作成します。
   - 姓 : ATA
   - 名 : Read
   - ユーザー ログオン名 : ataread
   - パスワード : Pa55w.rd
   - パスワードの確認入力 : Pa55w.rd
   - [ユーザーは次回ログオン時にパスワード変更が必要] チェック ボックスをオフにします。
4. Active Directory ユーザーとコンピューターを閉じます。
5. LON-SVR1 で、タスク バーの [ネットワーク] アイコンを右クリックし、[ネットワークと共有センターを開く] をクリックします。
6. [アダプターの設定の変更] をクリックし、[イーサネット] を右クリックし、[プロパティ] をクリックします。
7. [インターネット プロトコル バージョン 4 (TCP/IPv4)] を選択し、[プロパティ] をクリックします。
8. [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、[詳細設定] をクリックします。
9. [TCP/IP 詳細設定] ダイアログ ボックスの [IP 設定] タブで、[IP アドレス] の下の [追加] をクリックします。
10. [IP アドレス] ボックスに「172.16.0.13」と入力します。[サブネット マスク] の既定値が [255.255.0.0] であることを確認します。[追加] をクリックし、[OK] を 2 回クリックし、[閉じる] をクリックします。
11. LON-SVR1 のタスク バーで、[エクスプローラー] アイコンをクリックします。
12. E:¥LabFiles¥Mod07¥ に移動し、[ATA1.7.iso] を右クリックし、[マウント] を選択します。
13. Microsoft ATA Center Setup.exe を含む新しい DVD ドライブが表示されることを確認します。
14. [Microsoft ATA Center Setup.exe] を右クリックし、[管理者として実行] をクリックします。
15. 最初のページで、言語の選択が求められます。[日本語] を選択し、[次へ] をクリックします。
16. マイクロソフト ソフトウェア ライセンス条項を確認し、[マイクロソフト ソフトウェア ライセンス条項に同意します] チェック ボックスをオンにし、[次へ] をクリックします。

17. Microsoft Update オプションを選択できる次のページで、既定のままで、[次へ] をクリックします。
18. [センター サービスの IP アドレス] と [コンソールの IP アドレス] に異なる IP アドレスが設定されていることを確認します。[センター サービスの IP アドレス] は [172.16.0.26]、[コンソールの IP アドレス] は [172.16.0.13] となります。
19. [インストール] をクリックします。インストール後は、起動を指示されるまで、[起動] をクリックしないでください。
20. [サーバー マネージャー] を開き、[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。
21. [システム ツール] の下で、[ローカル ユーザーとグループ] を展開し、[グループ] を選択します。
22. [Microsoft Advanced Threat Analytics Administrators] を右クリックし、[グループに追加] をクリックします。
23. [追加] をクリックし、ボックスに「Beth」と入力し、[名前の確認]、[OK] をクリックします。
24. [追加] をクリックし、ボックスに「ATARead」と入力し、[名前の確認]、[OK] をクリックします。
25. [OK] をクリックして、[Microsoft Advanced Threat Analytics Administrators のプロパティ] ダイアログボックスを閉じます。
26. コンピューターの管理を閉じます。
27. インストールが完了したら、[起動] をクリックします。
28. セキュリティ通知で、[このサイトの閲覧を続行する] をクリックします。
29. サインイン ページが表示されたら、ユーザー名「Beth」、パスワード「Pa55w.rd」を使用して、[サインイン] をクリックします。

    ※ サインイン ページが表示されない場合は、Internet Explorer の画面で Alt キーを押し、[表示] メニューから、[エンコード]、[その他]、[Unicode (UTF-8)] の順にクリックします。
30. 右上隅で、[省略 (...)] をクリックし、[構成] をクリックします。
31. 左側の [データ ソース] の下で、[ディレクトリ サービス] をクリックします。
32. ユーザー名に「ATARead」と入力します。
33. パスワードに「Pa55w.rd」と入力します。
34. ドメインに「adatum.com」と入力し、[接続のテスト] をクリックし、[接続できました] と表示されたら、[保存] をクリックします。
35. 画面上部にある [ゲートウェイ セットアップをダウンロードし、最初のゲートウェイをインストールします] をクリックします。
36. [ゲートウェイ セットアップのダウンロード] をクリックします。
37. ファイルを E:¥Labfiles¥Mod07 に保存します。

注 : 上述のダウンロードの手順には、インターネット接続は必要ありません。ダウンロードは、サーバー上に存在するデータから作成されます。

38. エクスプローラーを開き、E:¥Labfiles¥Mod07 を参照します。
39. Microsoft ATA Gateway Setup.zip ファイルをコピーして、¥¥LON-DC1¥E$¥Labfiles¥Mod07 に貼り付けます。
40. エクスプローラーを閉じます。
41. LON-DC1 でエクスプローラーを開き、E:¥Labfiles¥Mod07¥ を参照します。

42. [Microsoft ATA Gateway Setup.zip] を右クリックし、[すべて展開] をクリックします。
43. [ファイルを下のフォルダーに展開する] ボックスに「E:¥Labfiles¥Mod07¥Gateway」と入力し、[展開] をクリックします。
44. E:¥Labfiles¥Mod07¥Gateway で、[Microsoft ATA Gateway Setup.exe] を右クリックし、[管理者として実行] を選択します。
45. 最初のページで、言語の選択が求められます。[日本語] を選択し、[次へ] をクリックします。
46. ATA ゲートウェイの展開の種類を確認します。これはドメイン コントローラーであるため、[ライトウェイト ゲートウェイ] がすでに選択されています。[次へ] をクリックします。
47. [ユーザー名] ボックスに「ATARead」と入力します。[パスワード] ボックスに「Pa55w.rd」と入力し、[インストール] をクリックします。
48. インストールが完了したら、[完了] をクリックします。

レッスン 2
Microsoft Operations Management Suite の展開と構成

目次

質問と解答

質問 : Microsoft 以外の製品で、Microsoft Operations Management Suite の管理と保護の対象となるのは何ですか。

( ) AWS

( ) VMware

( ) Linux

( ) OpenStack

解答 :

(√) AWS

(√) VMware

(√) Linux

(√) OpenStack

フィードバック

Microsoft Operations Management Suite により、Azure、AWS、Windows Server、Linux、VMware、OpenStack などを管理し、保護することができます。

質問 : クラウドおよびオンプレミスの環境内のリソースが生成するデータの収集と分析に役立つ Microsoft Operations Management Suite サービスはどれですか。

( ) Activity Log 分析

( ) Data Analytics

( ) Microsoft Operations Management Suite data connectors

( ) Network data connectors

解答 :

(√) Activity Log 分析

( ) Data Analytics

( ) Microsoft Operations Management Suite data connectors

( ) Network data connectors

フィードバック

Activity Log 分析は、クラウドおよびオンプレミスの環境内のリソースが生成するデータの収集と分析に役立つ Operations Management Suite サービスです。

質問 : Activity Log 分析には、収集データを分析するローカル リソースが必要です。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック

Activity Log 分析の展開の要件は、Azure が中心となるコンポーネントをホストするため、最小限で済みます。コンポーネントには、収集データの関連付けと分析を可能にするリポジトリとサービスが含まれます。Microsoft Operations Management Suite ポータルには、あらゆるブラウザーでアクセスできるため、クライアント ソフトウェアの要件はありません。

参考資料

Microsoft Operations Management Suite の使用と展開のシナリオ

 **参考資料：**Runbook による Azure Automation については、次のサイトを参照してください。
Getting Started With Azure Automation – Runbook Management
http://aka.ms/Cz3zbw

デモンストレーション : Microsoft Operations Management Suite の展開と構成

デモンストレーションの手順

1. 必要に応じて、この章の練習 2、作業 1 および作業 2 で説明されているように、Microsoft アカウントと Azure アカウントを作成します。
2. LON-CL1 で、ユーザー名「LON-CL1¥Admin」、パスワード「Pa55w.rd」を使用してサインインし、Microsoft Edge を起動します。
3. 次の URL を入力し、Enter キーを押します。
   https://www.microsoft.com/ja-jp/cloud-platform/operations-management-suite
4. [無料アカウントの作成] をクリックします。
5. [サインアップして体験する] をクリックします。
6. サインインしていない場合は、あなたの Microsoft アカウントを使用してサインインします。
7. あなたの Microsoft アカウントを作成するために使用した電子メールを [新しいワークスペースの作成] フォームに入力し、[作成] をクリックします。
8. 使用する Azure サブスクリプションを選択し、[リンク] をクリックします。
9. [Microsoft Operations Management Suite] ページが表示されることを確認します。
10. Microsoft Operations Management Suite ホームページで、[ソリューション ギャラリー] をクリックします。
11. 使用可能なソリューションを確認します。
12. 左側の家のアイコンをクリックします。
13. [概要] ページで、[設定] をクリックします。
14. [Connected Sources] をクリックし、[Windows Servers] が選択されていることを確認します。
15. Windows の [スタート] をクリックします。
16. 「notepad」と入力し、Enter キーを押します。
17. Microsoft Edge に切り替え、右側のウィンドウで、[ワークスペース ID] と [主キー] を見つけます。

18. [ワークスペース ID] と [主キー] の両方をコピーし、メモ帳に貼り付けます。
19. 後で必要になる場合に備えて、メモ帳のファイルをデスクトップに WorkspaceID.txt として保存します。
20. [Windows エージェントのダウンロード (64 ビット)] をクリックし、MMASetup-AMD64.exe をダウンロードします。
21. [保存]、[実行] の順にクリックします。
22. [ユーザー アカウント制御] ダイアログ ボックスが表示されたら、[はい] をクリックします。
23. [Microsoft Monitoring Agent セットアップ ウィザードへようこそ] ページで、[次へ] をクリックします。
24. マイクロソフト ソフトウェア ライセンス条項を確認し、[同意します] をクリックします。
25. [次へ] をクリックし、既定の解凍先フォルダーを受け入れます
26. [Azure ログ分析 (OMS) にエージェントを接続する] を選択し、[次へ] をクリックします。
27. メモ帳にコピーしたワークスペース ID と主キーを入力し、[次へ] をクリックします。
28. Microsoft 更新プログラムのインストールを促すメッセージが表示されたら、[次へ] をクリックします。
29. [インストール] をクリックし、[完了] をクリックします。
30. LON-CL1 で、コントロール パネルを開きます。
31. コントロール パネルで、[システムとセキュリティ]、[Microsoft Monitoring Agent] の順にクリックします。
32. [ユーザー アカウント制御] ダイアログ ボックスが表示されたら、[はい] をクリックします。
33. [Azure Log Analytics (OMS)] タブをクリックし、一覧表示された項目から選択し、[編集] をクリックします。これにより、必要に応じて、ワークスペース キーを更新できます。[キャンセル] をクリックします。
34. [キャンセル] をクリックします。
35. Microsoft Operations Management Suite の概要ページに戻り、ブラウザーを更新します。[使用状況] を表示し、LON-CL1 のデータを確認します。

 　**注 :** 使用状況のデータが表示されるまでにしばらくかかる場合があります。Microsoft Operations Management Suite の演習を始める前に説明しておくとよいでしょう。

演習の復習の質問と解答

演習 : ATA と Microsoft Operations Management Suite の展開

質問と解答

質問 : ATA Lightweight Gateway を使用するメリットは何ですか。

解答 : ATA Lightweight Gateway では、ポート ミラーリングを構成する必要がありません。

質問 : ATA をインストールするための要件は何ですか。

解答 : 要件には、ドメイン ユーザー アカウント、TTL が短いサブネットの一覧、ハニートークン アカウント、Wireshark、Microsoft Message Analyzer などがあります。

復習とまとめ

ベスト プラクティス

大規模な環境では、スケールアウトと複数の ATA ゲートウェイの使用を検討する必要があります。

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
一部のユーザーが、ATA センターの ATA イベント ログでイベント ID 1013 が表示されたと報告しています。	この問題はシステムのバックアップに関連する場合があり、バックアップ プロセス中にディスクが十分な IOPS を提供できていない可能性があります。

復習問題

質問 : Microsoft Operations Management Suite で検証できるセキュリティ ドメインは何ですか。

解答 : Microsoft Operations Management Suite で、次のドメインを検証できます。

- マルウェア対策評価
- 更新の管理
- ID およびアクセス

質問 : ATA を使用してセキュリティを強化する方法を説明してください。

解答 : ATA には、次の利点があります。

- **動作分析により、脅威を検出 :** 規則の作成、エージェントの展開、セキュリティ レポートのオーバーフローの微調整や監視が必要ありません。
- **悪意のあるユーザーと同じ速さで適応 :** ATA は、継続して、組織のエンティティの動作 (ユーザー、デバイス、およびリソース) を学習し、適応し、急速に進化する企業内の変化を反映します。
- **単純な攻撃タイムラインにより、重要な事柄に焦点を絞りこみ :** 攻撃タイムラインは、適切な事柄を時系列に表示し、企業内の誰が、何を、いつ、どのように実行したかを見通す力を与える、明確で効率的で便利な取り込み装置です。
- **誤検知の減少 :** 疑わしいアクティビティが前後関係から検出された場合のみ、警告を発します。
- **次の手順の優先順位を付け、計画 :** それぞれの特定された疑わしいアクティビティまたは既知の攻撃に対して、ATA は推奨される調査および修復を提案します。

ATA の主な機能には次のものがあります。

- **モビリティをサポート :** ATA は、組織の境界内またはモバイル デバイス上の組織のリソースに対するすべての認証と承認を証明します。
- **SIEM との統合 :** ATA は、SIEM と連携し、SIEM にセキュリティの警告を転送、または特定の人々に電子メールを送信するオプションを提供します。
- **シームレスな展開 :** ATA は、アプリケーションとして機能し、ポート ミラーリングを使用してシームレスな展開が可能です。

質問 : Microsoft Operations Management Suite を使用して、セキュリティを強化する方法を説明してください。

解答 : Microsoft Operations Management Suite のセキュリティとコンプライアンス機能は、インフラストラクチャのセキュリティ リスクの特定、評価、および軽減に役立ちます。これらの機能は、ログ データとエージェント システムの構成を分析して、環境のセキュリティの維持を支援する複数のソリューションにより、実装されます。

- セキュリティおよび監査ソリューションは、管理されたシステムでのセキュリティ イベントを収集し、分析して、疑わしいアクティビティを特定します。
- マルウェア対策評価ソリューションは、管理されたシステムでのマルウェア対策による保護の状態を報告します。
- 更新の管理は、管理されたシステムでのセキュリティ更新プログラムとその他の更新プログラムを分析し、更新が必要なシステムを簡単に特定することができます。

実際の問題とシナリオ

ATA センターの容量計画

- ATA データベースに必要なディスク領域は、ドメイン コントローラーごとに異なります。
- 複数のドメイン コントローラーがある場合、各ドメイン コントローラーの必要なディスク領域を合計し、ATA データベースに必要な総ディスク領域を計算します。
- 要件に基づいて、ATA センターのサイズを正確に計算するには、次のサイトを参照してください。
  ATA 容量計画
  https://docs.microsoft.com/ja-jp/advanced-threat-analytics/ata-capacity-planning

ツール

Wireshark は、精密なレベルでネットワークを検証できるネットワーク プロトコル アナライザーです。Wireshark は大変役立ちますが、ATA ゲートウェイまたは ATA センターに使用するサーバーにインストールしてはいけません。

第 8 章

仮想化インフラストラクチャのセキュリティ保護

目次

レッスン 1
保護されたファブリック

目次

質問と解答

質問 : シールドされた VM をロック解除し、正常であることが検証されている Hyper-V ホストで実行させるために必要なトランスポート キーを提供するサービスはどれですか。

解答 : KPS です。

参考資料

TPM 構成証明付き保護されたホストとしての Nano Server

参考資料 : 詳細については、次のサイトを参照してください。
Prepare Nano Server Script for Guarded Fabric
http://aka.ms/V2thr5

レッスン 2
シールドされた仮想マシンおよび暗号化サポート仮想マシン

目次

質問と解答

質問 : 暗号化サポート VM とシールドされた VM の違いは何ですか。

解答 : シールドされた VM と同様に、暗号化サポート VM は、セキュア ブート、仮想トラステッド プラットフォーム モジュール (vTPM)、および VM 状態の暗号化を使用します。ただし、暗号化サポート VM では、これらの設定を構成することができます。シールドされた VM では、これらの設定が強制されます。さらに、暗号化サポート VM では仮想マシン接続コンソールがオンに設定されているのに対し、シールドされた VM ではオフにされています。シールドされた VM では、COM/シリアル ポートが無効化されているため、VM プロセスにデバッガーを接続できません。

参考資料

シールドされた VM および暗号化サポート VM のトラブルシューティング

参考資料 : 詳細については、次のサイトを参照してください。
Shielded VMs and Guarded Fabric Troubleshooting Guide for Windows Server 2016
https://aka.ms/ehnloq

演習の復習の質問と解答

演習 : 管理者が信頼する構成証明およびシールドされた仮想マシンにより保護されたファブリック

質問と解答

質問 : 保護されたファブリックに不可欠なコンポーネントを説明してください。

解答 : シールドされた VM と保護されたファブリックを採用することにより、クラウド サービス プロバイダーまたは企業のプライベート クラウド管理者は、安全性のより高い環境をテナント VM 用に提供できます。保護されたファブリックは、通常は 3 ノードのクラスターで構成される 1 つの HGS、1 つ以上の保護されたホスト、および一連のシールドされた VM で構成されます。

質問 : 演習では、HGS と保護されたホストから構成される環境を作成し、その企業ドメインに HGS グループを追加しました。これらの役割の中で、物理サーバーのものはどれですか。

解答 : 保護されたホストです。保護されたホストは、仮想化環境では実行できません。

復習とまとめ

ベスト プラクティス

1 つのドメインを使用して、保護されたファブリックを構成することも可能ですが、HGS ごとに一意のフォレストを構成することを推奨します。

一般的な問題とトラブルシューティングのヒント

一般的な問題	トラブルシューティングのヒント
vTPM をオンにしても、シールドされた VM が起動できません。	保護されたホストが適切なセキュリティ グループに属していることを確認します。

復習問題

質問 : ドメイン間にはどのような信頼が必要ですか。保護されたホストはどのドメインのメンバーである必要がありますか。

解答 : HGS サーバーには、組織のドメインとの一方向の信頼が必要です。保護されたホストは、HGS フォレストのメンバーではなく、組織のドメインのメンバーである必要があります。

第 9 章

アプリケーション開発およびサーバー ワークロード インフラストラクチャのセキュリティ保護

目次

レッスン 1
SCM の使用

目次

質問と解答

質問 : SCM 4.0 は、次の既定の製品ベースラインのうちどれを保有していますか。

(　) Internet Explorer 6 および Internet Explorer 7

(　) Exchange Server 2007 SP1

(　) Windows 8

(　) Windows Server 2008 SP1

(　) Windows Server 2012

解答 :

(　) Internet Explorer 6 および Internet Explorer 7

(　) Exchange Server 2007 SP1

(√) Windows 8

(　) Windows Server 2008 SP1

(√) Windows Server 2012

フィードバック

SCM 4.0 には、Windows Server 2012、Internet Explorer 8、および Exchange Server 2010 よりも前に作成されたシステム向けのベースライン テンプレートはありません。

参考資料

セキュリティ ベースラインの管理

参考資料 : 詳細については、次のサイトを参照してください。
Security baseline for Windows 10 v1607 (“Anniversary edition”) and Windows Server 2016
https://aka.ms/hhsdmo

セキュリティ構成の展開

参考資料 : スタンドアロンの LGPO.EXE ツールは、次のサイトでダウンロードできます。
LGPO.exe - Local Group Policy Object Utility, v1.0
https://aka.ms/kkvmk5

デモンストレーション : SCM のインストール

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 を起動します。
2. LON-SVR1 のタスク バーで、[エクスプローラー] をクリックします。
3. エクスプローラーで E:¥Labfiles¥Mod09 フォルダーに移動します。

4. [Security_Compliance_Manager_Setup.exe] をダブルクリックします。コマンド プロンプトが開き、さまざまな SCM 前提条件が起動します。
5. Microsoft Visual C++ 2010 x86 Redistributable Setup ウィンドウが表示されたら、[同意する] を選択し、[インストール] をクリックします。
6. [インストールが完了しました] ページが表示されたら、[完了] をクリックします。
7. Microsoft Security Compliance Manager Setup ウィザードが起動します。[Welcome] ページで、[Always check for SCM and baseline updates] チェック ボックスをオフにし、[Next] をクリックします。
8. [License Agreement] ページで、[I accept the terms of the license agreement] をクリックし、[Next] をクリックします。
9. [Installation Folder] ページで、[Next] をクリックします。
10. [SQL Instances found] ページで、[Create a new SQL express instance] を選択し、[Next] をクリックします。
11. [Microsoft SQL Server 2008 Express] ページで、[Next] をクリックします。
12. [SQL Server 2008 Express License Agreement] ページで、[I accept the terms of the license agreement] をクリックし、[Next] をクリックします。
13. [Ready to Install] ページで、[Install] をクリックします。
14. [Installation Successful] ページが開いたら、[Finish] をクリックします。

注 : Windows 10、Windows Server 2016、Internet Explorer 11 などには新しいベースラインがいくつか用意されていますが、それらは個別にダウンロードしてインポートする必要があります。このコースの仮想マシンではインターネット アクセスができないので、これらのベースラインをダウンロードすることはできません。これが、[Always check for SCM and baseline updates] チェック ボックスをオフにした理由です。

15. SCM コンソールが開き、複数のベースラインが自動的にインポートされます。次のデモンストレーションのために、SCM コンソールを開いたままにします。

デモンストレーション : セキュリティ ベースラインの構成および管理

デモンストレーションの手順

Windows Server 2016 の GPO をインストールする

1. LON-SVR1 の SCM コンソールの操作ウィンドウで、[Import - GPO Backup (folder)] をクリックします。
2. Browse for folder ウィンドウで、E:¥Labfiles¥Mod09¥Windows 10 RS1 and Server 2016 Security Baseline¥GPOs¥ に移動し、最初にリストされた GPO GUID を選択し、[OK] をクリックします。
3. GPO Name ウィンドウで、GPO の名前を確認し、[OK] をクリックします。
4. SCM Log ウィンドウで、[OK] をクリックします。
5. GPO フォルダー内に残っているすべての GPO GUID に対して、手順 1 ～ 4 を繰り返します。

Windows Server 2016 の GPO を Windows Server 2012 Member Server Baseline に関連付けて結合する

1. SCM コンソールのコンソール ツリーで、[Custom baselines] が展開されていない場合はそれを展開し、[GPO import] を展開します。

2. ベースラインのリストから、[SCM Windows Server 2016 - Member Server Baseline - Computer 0.0] を選択します。
3. 操作ウィンドウの [Baseline] の下で、[Associate] ハイパーリンクをクリックします。
4. Associate Product with GPO ウィンドウで、リストから [Windows Server 2012] を選択し、[Associate] をクリックします。
5. Baseline name ウィンドウで、「Associated Server 2012-2016」と入力し、[OK] をクリックします。
6. SCM コンソール ツリーで、[Custom baselines] の下の [Associated Server 2012-2016] を選択し、操作ウィンドウで、[Baseline] の下の [Compare/Merge] ハイパーリンクをクリックします。
7. Compare Baselines ウィンドウで、[Windows Server 2012] を展開し、展開されたリストから、[WS2012 Member Server Security Compliance 1.0] を選択し、[OK] をクリックします。
8. Compare Baselines ウィンドウに表示される情報に注意します。[Settings that differ] 領域と [Settings that match] 領域の両方の設定を確認します。
9. Compare Baselines ウィンドウで、[Merge Baselines] をクリックします。
10. Merge Baselines ウィンドウで [Merge conflicts to resolve] 項目を確認し、[OK] をクリックします。
11. [Specify a name for the merged baseline] ボックスに「Member Server Merged 2012-2016」と入力し、[OK] をクリックします。
12. 詳細ウィンドウで、[Name] 列の下の [Session Configuration] まで下にスクロールします。
13. [Interactive Logon: Message title for users attempting to log on] という名前の項目をクリックします。
14. [Not Defined] チェック ボックスをオフにし、[Customize setting value] ボックスに「Welcome to A. Datum Corporation!」と入力し、[Collapse] をクリックします。
15. [Interactive Logon: Message text for users attempting to log on] という名前の項目をクリックします。
16. [Not Defined] チェック ボックスをオフにし、[Customize setting value] ボックスに「This device uses the Member Server Merged 2012-2016 Baseline.」と入力して、[Collapse] をクリックします。
17. 操作ウィンドウの [Export] の下で、[GPO Backup (folder)] ハイパーリンクをクリックします。
18. Browse For Folder ウィンドウで [Allfiles (E:)]、[Labfiles] の順に展開し、[Mod09] を選択して、[OK] をクリックします。
19. エクスプローラーを閉じます。

デモンストレーション : セキュリティ ベースラインのリモート サーバーへの展開

デモンストレーションの手順

SCM GPO のバックアップをグループ ポリシーの管理コンソールにインポートする

1. LON-DC1 のタスク バーで、[エクスプローラー] をクリックします。
2. エクスプローラーの URL ボックスに「¥¥LON-SVR1¥E$¥Labfiles¥Mod09」と入力し、Enter キーを押します。
3. [<GUID>] フォルダーを右クリックしてコピーします (例 : {bed88c04-5ffe-4857-aff6-be595c53ad41})。
4. LON-DC1 のエクスプローラーで、Allfiles (E:¥)¥Labfiles に移動します。

   詳細ウィンドウで、空白部分を右クリックし、[貼り付け] をクリックします。エクスプローラーを閉じます。

5. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
6. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] を選択します。
7. 詳細ウィンドウの何も表示されていない場所を右クリックし、[新規作成] をクリックします。
8. 新しい GPO ウィンドウで、[名前] ボックスに「Member Server 2012-2016 Baseline」と入力し、[OK] をクリックします。
9. 詳細ウィンドウで、[Member Server 2012-2016 Baseline] を右クリックし、[設定のインポート] をクリックします。
10. 設定のインポート ウィザードの [ようこそ] ページで、[次へ] をクリックします。
11. [GPO のバックアップ] ページで、[次へ] をクリックします。
12. [バックアップの場所] ページで、[バックアップ フォルダー] ボックスに「E:¥Labfiles」と入力し、[次へ] をクリックします。
13. [ソース GPO] ページで、[Member Server Merged 2012-2016] 項目が選択されていることを確認し、[次へ] をクリックします。
14. [バックアップをスキャン中] ページで、[次へ] をクリックします。
15. [参照の移行] ページで、移行テーブルを使用して、設定を移行先 GPO にマップする方法を確認します。ただし、移行テーブルが存在しないため、既定の設定を受け入れ、[次へ] をクリックする必要があります。
16. [設定のインポート ウィザードの完了] ページで、[完了] をクリックし、インポートが成功したら、[OK] をクリックします。
17. 詳細ウィンドウで、[Member Server 2012-2016 Baseline] を右クリックし、[編集] をクリックします。
18. グループ ポリシー管理エディター ウィンドウを最大化します。
19. 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]、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[ローカル ポリシー] の順に展開します。
20. [ローカル ポリシー] で、[セキュリティ オプション] を選択します。
21. [セキュリティ オプション] の詳細ウィンドウで、[対話型ログオン : ログオン時のユーザーへのメッセージのタイトル] という設定項目まで下にスクロールし、ダブルクリックします。
22. [Welcome to A. Datum Corporation!] に設定されていることを確認します。
23. [対話型ログオン : ログオン時のユーザーへのメッセージのテキスト] 項目に対しても同じ操作をおこないます。ここで、[This device uses the Member Server Merged 2012-2016 Baseline] に設定されていることを確認します。
24. グループ ポリシー管理エディターを閉じ、グループ ポリシーの管理コンソールを最小化します。

Member Servers OU を作成して LON-SVR2 を移動し、Member Server 2012-2016 Baseline GPO をその OU にリンクする

1. LON-DC1 のサーバー マネージャーで、[ツール]、[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コンソール ツリーで [Adatum.com] を展開します。
3. [Adatum.com] を右クリックし、[新規作成] をポイントして、[組織単位] をクリックします。
4. 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「Member Servers」と入力し、[OK] をクリックします。
5. コンソール ツリーで、[Computers] ノードを選択します。

6. 詳細ウィンドウで、[LON-SVR2] を右クリックし、[移動] をクリックします。
7. 移動ウィンドウで、[Member Servers] OU を選択し、[OK] をクリックします。
8. コンソール ツリーで、[Member Servers] を選択し、この OU に LON-SVR2 があることを確認します。
9. Active Directory ユーザーとコンピューターを閉じます。
10. グループ ポリシーの管理コンソールを最大化します。
11. コンソール ツリーで [Adatum.com] を選択し、[最新の情報に更新] アイコンをクリックします。
12. Adatum.com の下に Member Servers OU が表示されます。[Member Servers] OU を選択します。
13. [Member Servers] を右クリックし、[既存の GPO のリンク] をクリックします。
14. GPO の選択ウィンドウで、[Member Server 2012-2016 Baseline] GPO を選択し、[OK] をクリックします。
15. グループ ポリシーの管理コンソールを閉じます。

LON-SVR2 を起動し、対話型ログオン メッセージのタイトルとテキストを確認する

1. ホスト コンピューターの Hyper-V マネージャーで、[23744B-LON-SVR2] をダブルクリックし、仮想マシン接続ウィンドウで、[起動] をクリックします。
2. 仮想マシンが起動すると、サインイン画面が表示される前に、対話型ログオン画面が表示されます。
3. この画面で [OK] をクリックし、LON-SVR2 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
4. 開いているウィンドウをすべて閉じ、すべての仮想マシンからサインアウトします。

レッスン 2
Nano Server の紹介

目次

質問と解答

活動の順序

質問 : 次に示しているのは、DSC を Nano Server に適用する手順です。これらの手順を正しい順序に並べてください。

	手順
	Nano Server で DSC 用構成スクリプトを作成します。
	構成スクリプトを Nano Server にコピーします。
	必要な DSC リソースがインポートされ使用できることを確認します。
	Nano Server で構成スクリプトを実行し、MOF ファイルを作成します。
	Windows PowerShell で Start-DscConfiguration コマンドレットを使用し、MOF ファイルに基づいて DSC を展開します。
	DSC が展開され、構成が期待どおりに設定されていることを確認します。

解答 :

	手順
1	Nano Server で DSC 用構成スクリプトを作成します。
2	構成スクリプトを Nano Server にコピーします。
3	必要な DSC リソースがインポートされ使用できることを確認します。
4	Nano Server で構成スクリプトを実行し、MOF ファイルを作成します。
5	Windows PowerShell で Start-DscConfiguration コマンドレットを使用し、MOF ファイルに基づいて DSC を展開します。
6	DSC が展開され、構成が期待どおりに設定されていることを確認します。

参考資料

Nano Server がより安全な理由

参考資料 : 詳細については、次のサイトを参照してください。
Introducing Server management tools
https://aka.ms/mwe46x

Nano Server の準備、展開、および管理

参考資料 : Nano Server Image Builder は、次のサイトでダウンロードできます。
Download Center
http://aka.ms/NanoServerImageBuilder

デモンストレーション : Nano Server の展開と管理

デモンストレーションの手順

必要な Windows PowerShell スクリプトをコピーする

1. 23744B-LON-HOST1 を起動します。
2. エクスプローラーを開き、E:¥Program Files¥Microsoft Learning¥23744¥Drives に移動して、[WinServer2016_1607-JP.iso] を右クリックします。

注 : 23744B-LON-HOST1 からブートした後、ドライブ文字の順序が変わる場合があります。[Program Files¥Microsoft Learning¥23744¥Drives] へのパスを含むドライブ文字を選択してください。

3. [マウント] をクリックします。
4. ドライブ文字をメモします。これは、以降のメディア ソースの作業で使用します
5. LON-HOST1 で、[スタート] をクリックし、[Windows PowerShell] をクリックします。
6. Windows PowerShell ウィンドウで「cd ¥」と入力し、Enter キーを押します。
7. 「md Nano」と入力し、Enter キーを押します。
8. 次のコマンドを入力し、Enter キーを押します。

```
copy X:¥NanoServer¥NanoServerImageGenerator¥*.ps* c:¥nano
```

注 : 上記の手順 7 の X は、マウントされた .iso ファイルに割り当てられたドライブ文字に置き換えます。

Windows PowerShell モジュールをインポートする

1. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Import-Module c:¥nano¥NanoServerImageGenerator.psm1
```

2. 次のコマンドレットを入力し、Enter キーを押します。

```
New-NanoServerImage -Edition Standard -mediapath X:¥-Basepath c:¥nano -targetpath c:¥nano¥nano-svr1.vhdx -
DeploymentType Guest -computername NANO-SVR1 -storage -package Microsoft-NanoServer-DSC-Package -Compute
```

注 : 上記の手順 2 の X は、マウントされた .iso ファイルに割り当てられたドライブ文字に置き換えます。

3. [AdministratorPassword] ダイアログ ボックスで、パスワード「Pa55w.rd」を入力し、Enter キーを押して、サインインします。
4. プロセスが完了したら、タスク バーの [エクスプローラー] をクリックし、C:¥Nano に移動して、一覧表示されているファイルを調べます。nano-svr1.vhdx が存在することを確認します。

仮想マシンから Hyper-V VM を作成する

1. LON-HOST1 で、Hyper-V マネージャーを開きます。

2. Hyper-V マネージャー コンソールの操作ウィンドウで、[新規]、[仮想マシン] の順にクリックします。
3. 仮想マシンの新規作成ウィザードの [ようこそ] ページで、[次へ] をクリックします。
4. [名前と場所の指定] ページで、[名前] ボックスに「NANO-SVR1」と入力し、[仮想マシンを別の場所に格納する] チェック ボックスをオンにして、[参照] をクリックします。
5. フォルダーの選択ウィンドウで、「C:¥nano」と入力し、Enter キーを押して、[フォルダーの選択] をクリックします。
6. [名前と場所の指定] ページで、[次へ] をクリックします。
7. [世代の指定] ページで、[第 2 世代] を選択し、[次へ] をクリックします。
8. [メモリの割り当て] ページで、[次へ] をクリックします。
9. [ネットワークの構成] ページで、[接続] ドロップダウン リストから [Internal Network] を選択し、[次へ] をクリックします。
10. [仮想ハード ディスクの接続] ページで、[既存の仮想ハード ディスクを使用する]、[参照] の順にクリックします。
11. 開くウィンドウで、「C:¥nano」と入力し、Enter キーを押し、[nano-svr1.vhdx] を選択して、[開く] をクリックします。
12. [仮想ハード ディスクの接続] ページで、[次へ] をクリックします。
13. [仮想マシンの新規作成ウィザードの完了] ページで、[完了] をクリックします。
14. LON-HOST1 の Hyper-V マネージャーで、仮想マシン ウィンドウの [NANO-SVR1] をダブルクリックします。
15. LON-HOST1 上の NANO-SVR1 - 仮想マシン接続ウィンドウで、[起動] をクリックします。

Nano Server にサインインし基本設定を表示する

1. NANO-SVR1 で、[ユーザー名] ボックスに「Administrator」と入力し、Tab キーを押します。
2. [パスワード] ボックスにパスワード「Pa55w.rd」を入力し、Enter キーを押して、サインインします。
3. NANO-SVR1 の Nano Server Recovery Console で、コンピューター名が [NANO-SVR1] で、そのコンピューターがワークグループ内にあることを確認します。
4. [Network] が選択されるまで Tab キーを押し、Enter キーを押します。
5. [イーサネット] ダイアログ ボックスで、Enter キーを押します。
6. [Network Adapter Setting] で、IP 構成が DHCP から提供されていることを確認します。
7. IP アドレスを書き留めます。
8. Esc キーを 2 回押します。

Nano Server をドメインに追加する

1. LON-DC1 に切り替えます。
2. [スタート] をクリックし、[Windows PowerShell] をクリックします。
3. Windows PowerShell ウィンドウで次のコマンドを入力し、Enter キーを押します。

```
djoin.exe /provision /domain adatum /machine nano-svr1 /savefile C:¥odjblob
```

注 : 次のコマンドの IP アドレス 172.16.0.X を、Nano Server のインストール中に記録した IP アドレスに置き換えます。

4. Windows PowerShell リモート処理を有効にするために、次のコマンドレットを入力し、Enter キーを押します。

```
Enable-PSRemoting -Force
```

5. IP アドレスを置き換えるために、次のコマンドレットを入力し、Enter キーを押します。

```
Set-Item WSMan:¥localhost¥Client¥TrustedHosts "172.16.0.X"
```

6. 「Y」と入力し、Enter キーを押します。
7. IP アドレスを置き換えるために、次のコマンドを入力し、Enter キーを押します。

```
$ip = "172.16.0.X"
```

8. 次のコマンドレットを入力し、Enter キーを押します。

```
Enter-PSSession -ComputerName $ip -Credential $ip¥Administrator
```

9. [Windows PowerShell 資格情報の要求] ダイアログ ボックスで、[パスワード] ボックスに「Pa55w.rd」と入力し、[OK] をクリックします。
10. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
netsh advfirewall firewall set rule group="ファイルとプリンターの共有" new enable=yes
```

11. 次のコマンドレットを入力し、Enter キーを押します。

```
Exit-PSSession
```

12. ネットワーク ドライブを Nano Server の C ドライブにマップするために、次のコマンドを入力し、各行の最後で Enter キーを押します。

```
net use z:¥¥172.16.0.X¥c$
Z:
```

13. 次のコマンドを入力し、Enter キーを押します。

```
copy c:¥odjblob
```

14. 次のコマンドレットを入力し、Enter キーを押します。

```
Enter-PSSession -ComputerName $ip -Credential $ip¥Administrator
```

15. [Windows PowerShell 資格情報の要求] ダイアログ ボックスで、[パスワード] ボックスに「Pa55w.rd」と入力し、[OK] をクリックします。
16. Windows PowerShell ウィンドウで、「cd¥」と入力し、Enter キーを押します。
17. 次のコマンドを入力し、Enter キーを押します。

```
djoin /requestodj /loadfile c:¥odjblob /windowspath c:¥windows /localos
```

18. 次のコマンドを入力し、Enter キーを押して、Nano Server を強制的に再起動します。

```
shutdown /r /t 5
```

19. Windows PowerShell ウィンドウを閉じないでください。次のデモンストレーションで使用します。
20. NANO-SVR1 に切り替えます。
21. [ユーザー名] ボックスに「Administrator」と入力し、Tab キーを押します。
22. [パスワード] ボックスに「Pa55w.rd」と入力し、Tab キーを押します。
23. [ドメイン] ボックスに「Adatum」と入力し、Enter キーを押します。
24. Nano Server Recovery Console で、コンピューターが Adatum.com ドメインに属していることを確認します。

デモンストレーション : DSC による Nano Server のセキュリティの構成

デモンストレーションの手順

DSC スクリプトを確認する

1. LON-DC1-B のタスク バーで、[エクスプローラー] をクリックします。
2. エクスプローラーのコンソール ツリーで、[PC] を選択し、C:¥Labfiles¥Mod09 を展開します。
3. [Demo2DscNanoConfig.ps1] ファイルを右クリックし、[編集] をクリックします。Windows PowerShell Integrated Scripting Environment (ISE) でスクリプトが開きます。
4. スクリプトの主要な部分を簡単に確認します。該当する部分は、サービスを呼び出すブロックです。Hyper-V 仮想マシン管理サービス (vmms) が稼働しているかどうかをチェックしています。
5. スクリプトを変更または保存せずに Windows PowerShell ISE を閉じます。エクスプローラーは閉じないでください。

DSC スクリプトを NANO-SVR1 に展開する

1. LON-DC1-B の Windows PowerShell ウィンドウに戻ります。
2. 前のデモンストレーションでマップしたドライブ Z がそのままマップされている必要があります。マップされていない場合は、前のデモンストレーションで使用した値で X を置き換えて、次のコマンドを入力し、Enter キーを押します。

```
net use z:¥¥172.16.0.X¥c$
```

注 : [コマンド 'z:' を実行するセッションが閉じられたか切断されたため、このコマンドは実行されませんでした] というメッセージは無視することができます。ドライブは正しくマップされたままになります。

3. Windows PowerShell ウィンドウで、次のコマンドを入力し、各行の最後で Enter キーを押します。

```
z:
md demo
cd demo
copy c:¥Labfiles¥Mod09¥Demo2DscNanoConfig.ps1
```

4. 次のコマンドレットを入力し、Enter キーを押します。

```
Get-Command -Module PSDesiredStateConfiguration
```

この出力は、前のデモンストレーションで DSC パッケージがモジュールとして正常にインストールされたことを示します。また、このモジュールで使用できるコマンドもすべて示します。

5. 次のコマンドレットを入力し、Enter キーを押します。

```
Get-DscResource
```

このコマンドレットの出力は、Nano Server で DSC が操作できるさまざまなリソースを示します。

6. 次のコマンドを入力し、Enter キーを押します。X は Nano Server の IP アドレスに置き換えます。

```
$ip = "172.16.0.X"
```

7. 次のコマンドを入力し、Enter キーを押します。

```
$cred = Get-Credential
```

8. Windows PowerShell 資格情報の要求ウィンドウで、[ユーザー名] ボックスに「Adatum¥Administrator」、[パスワード] ボックスに「Pa55w.rd」と入力し、[OK] をクリックします。

9. 次のコマンドレットを入力し、Enter キーを押します。

```
Enter-PSSession -ComputerName $ip -Credential $Cred
```

10. 次のコマンドを入力し、Enter キーを押します。

```
Cd C:¥demo
```

11. 次のコマンドレットを入力し、Enter キーを押します。

```
Install-Module -Name xsmbshare -Force
```

12. NuGet プロバイダーのメッセージ ダイアログ ボックスに「Y」と入力し、Enter キーを押します。

13. 次のコマンドを入力し、Enter キーを押します。

```
.¥Demo2DscNanoConfig.ps1 -nodes localhost
```

スクリプトは Localhost.MOF という名前の .MOF ファイルを作成します。

14. 次のコマンドレットを入力し、Enter キーを押します。

```
Start-DscConfiguration -ComputerName "NANO-SVR1" -Wait -Force -Verbose -Path .¥NanoConfig
```

15. Wait パラメーターは、このコマンドが実行されるまで、コンソールへの入力を数秒間停止します。このコマンドが正常に実行されると、NANO-SVR1 で vmms サービスが実行されていることを確認できます。

16. 次のコマンドレットを入力し、Enter キーを押します。

```
Exit-PSSession
```

17. 開いているウィンドウをすべて閉じ、LON-DC1 からサインアウトします。

レッスン 3
コンテナーの理解

目次

質問と解答

活動の分類

質問 : 次の各項目を分類してください。

項目	
1	オペレーティング システム環境を提供する
2	ユーザー モードのみを備えている
3	オペレーティング システム バイナリの独自のコピーを保有する、追加の分離境界を提供する
4	ユーザー インターフェイス、アプリケーション スタック、および従来の .NET Framework の多くが削除されている
5	このイメージを複数回使用して、基本レイヤーを変更することなくアプリを展開できる
6	基本イメージを使用して、自動的に Hyper-V 仮想マシンを作成する
7	Windows コンテナーのプラットフォームとして使用できる
8	共有されたカーネルを使用する
9	信頼できないアプリを同じホストで実行するために、必要となる分離を提供する

カテゴリ 1		カテゴリ 2		カテゴリ 3
Nano Server		Windows Server コンテナー		Hyper-V コンテナー

解答 :

カテゴリ 1		カテゴリ 2		カテゴリ 3
Nano Server		Windows Server コンテナー		Hyper-V コンテナー
オペレーティング システム環境を提供する ユーザー インターフェイス、アプリケーション スタック、および従来の .NET Framework の多くが削除されている Windows コンテナーのプラットフォームとして使用できる		ユーザー モードのみを備えている このイメージを複数回使用して、基本レイヤーを変更することなくアプリを展開できる 共有されたカーネルを使用する		オペレーティング システム バイナリの独自のコピーを保有する、追加の分離境界を提供する 基本イメージを使用して、自動的に Hyper-V 仮想マシンを作成する 信頼できないアプリを同じホストで実行するために、必要となる分離を提供する

デモンストレーション : Windows Server コンテナーの展開と管理

デモンストレーションの手順

Microsoft Docker イメージ リポジトリを調査する

1. LON-HOST1 で、必要に応じて、[スタート] をクリックし、[Windows PowerShell] をクリックします。
2. ダウンロードされたイメージを確認するために、Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
docker search Microsoft
```

事前構築済みの Microsoft/IIS Docker イメージをダウンロードする

1. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
docker run hello-world:nanoserver
```

このコマンドレットが完了するには約 1 ～ 2 分かかり、Docker により実行されるプロセス全体の手順が表示されます。

注 : このコマンドレットの実行には約 2 分かかります。完了すると、次の行が返されます。

```
Hello from Docker!
This message shows that your installation appears to be working correctly.
To generate this message, Docker took the following steps:
1. The Docker client contacted the Docker daemon.
2. The Docker daemon pulled the "hello-world" image from the Docker Hub.
3. The Docker daemon created a new container from that image which runs the
   executable that produces the output you are currently reading.
4. The Docker daemon streamed that output to the Docker client, which sent it
   to your terminal.
```

2. ダウンロードされたイメージを確認するために、次のコマンドを入力し、Enter キーを押します。

```
docker images
```

事前構築済みのイメージを使用して新しいコンテナーを展開する

1. IIS コンテナーを展開するために、Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
docker run -d --name MyIIS -p 80:80 microsoft/iis cmd
```

注 : このコマンドは、IIS イメージをバックグラウンド サービス (-d) として実行し、コンテナー ホストのポート 80 がコンテナーのポート 80 にマップするようにネットワークを構成します。

Docker を使用してコンテナーを管理する

1. 実行中のコンテナーを確認するために、Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
docker ps
```

2. [Container ID] という見出しの下にある最初の列のデータ (fd85c4dbffba などの長い文字列) を確認します。これを使用して、そのコンテナーを停止できます。実行中のコンテナーを確認するために、次のコマンドを入力し、Enter キーを押します。

```
docker stop <ContainerID>
```

注 : 上記の <ContainerID> を、手順 1 で実行した Docker ps コマンドで返された文字列に置き換えます。

デモンストレーション : Hyper-V コンテナーの展開

デモンストレーションの手順

1. LON-HOST1 の Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
ipconfig
hostname
```

2. この IP アドレスとホスト名は、LON-HOST1 のものであることに注意してください。
3. 次のコマンドを入力し、Enter キーを押します。

```
docker run -it --isolation=hyperv microsoft/nanoserver cmd
```

4. 上記のコマンドの終了後、Windows PowerShell ウィンドウ内に、背景が黒のコマンド プロンプトが開くことに注意してください。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
hostname
```

5. IP アドレスが、手順 2 で確認したものとは異なること、ホスト名が長い文字列であることに注意します。これは、作成した Nano Server のものです。
6. LON-HOST1 で、[スタート] をクリックし、[Windows PowerShell] をクリックします。もう 1 つの Windows PowerShell ウィンドウが開きます。
7. 実行中のコンテナーを確認するために、新しい Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
docker ps
```

8. [Container ID] という見出しの下にある最初の列のデータ (fd85c4dbffba などの長い文字列) を確認します。実行中のコンテナーを停止するために、新しい Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
docker stop <ContainerID>
```

9. <ContainerID> を、手順 7 の docker ps コマンドで返されたコンテナー ID に置き換えます。
10. 開いているウィンドウをすべて閉じます。

演習の復習の質問と解答

演習 A : SCM の使用

質問と解答

質問 : LON-SVR2 がワークグループのスタンドアロン サーバーの場合、[Member Server Merged 2012-2016] ベースラインで作成したセキュリティ設定を適用するには、何をする必要がありますか。

解答 : LGPO.exe コマンド ライン ツールを使用できます。それ以外の方法としては、セキュリティの設定を手動で追加する必要があります。

質問 : SCM で 2 つの異なる製品ベースラインを結合するには、何をおこなう必要がありますか。

解答 : まず、2 つの製品を関連付ける必要があります。

演習 B : Nano Server の展開と構成

質問と解答

質問 : 次の Windows PowerShell コマンドは、何を実行しますか。

```
docker search Microsoft
```

解答 : Microsoft により作成された Windows コンテナーの事前構築済みの機能と役割をすべて一覧表示します。

質問 : 次の Windows PowerShell コマンドレットは、何を実行しますか。

```
Get-Command -Module PSDesiredStateConfiguration
```

解答 : DSC パッケージがモジュールとして正常にインストールされたことを示します。また、このモジュールで使用できるコマンドもすべて示します。

復習とまとめ

ベスト プラクティス

- メインのクライアント コンピューターまたはサーバーに SCM をインストールした後、スタンドアロンおよびワークグループ デバイスが簡単にアクセスできるように、LocalGPO フォルダーを共有します。
- 完全なグラフィック エクスペリエンスのために、GUI 機能を備えたリモート システムから、Nano Server の Docker を管理します。
- コンテナー間で永続的なデータを共有する場合、または非永続的なコンテナーのデータを使用する場合は、Data Volume Container という名前のコンテナーを作成し、そこからデータをマウントします。

ツール

ツール	目的	アクセス方法
SCM	さまざまな Windows 製品とオペレーティング システムのセキュリティ ベースラインを作成、管理、および展開します。	Microsoft.com からの無料ダウンロード
Windows Server 2016 用の Docker Enterprise Edition	Docker により、オペレーティング システムに関わらず、ホスト オペレーティング システム上のユーザー スペースで分離されたプロセスとして、コンテナーを実行することができます。	https://aka.ms/y6lgzc
GitHub	Windows Server に Hyper-V コンテナーを展開します。	https://aka.ms/puavgj

復習問題

質問 : Nano Server、Windows Server コンテナー、または Hyper-V コンテナーの中で、あなたが実現できる最も保護された処理環境はどれですか。

解答 : Windows Server コンテナーは、従来から展開されているサーバー オペレーティング システムよりも安全ですが、Hyper-V コンテナーは Windows Server コンテナーよりもさらに安全です。Nano Server でコンテナーをホストすることで、コンテナーをすばやく簡単に展開できます。Nano Server で Hyper-V コンテナーを使用することで、3 つの選択肢の中で最も高いセキュリティを確保できます。

第 10 章

データの保護と計画

目次

レッスン 1
暗号化の計画と実装

目次

質問と解答

EFS の概要

質問 : EFS では、対称暗号化または公開キー暗号化のどちらを使用しますか。

解答 : EFS では、両方の暗号化方式の組み合わせを使用しています。対称暗号化を使用してファイルの内容を暗号化し、公開キー暗号化を使用してファイルの暗号化に使用する対称キーを暗号化し保護します。

質問 : EFS を使用して暗号化されたファイルを開くことができるのは、どのようなユーザーですか。

解答 : EFS で暗号化されたファイルを開くには、ユーザーはファイルへのアクセス許可を持つ必要があります。ただし、ユーザーは、対称キーの暗号化解除をおこなう適切な秘密キーを持つ必要もあります。その後、ユーザーは対称キーを使用して、暗号化されたファイルの暗号化を解除し、それを開きます。ユーザーが適切な秘密キーを持っている場合は、このプロセスは透過的で、暗号化されていないかのようにファイルを開くことができます。ユーザーが適切な秘密キーを持っていない場合は、ユーザーに対してアクセス拒否エラーが表示されます。

EFS と証明書

質問 : EFS を使用してファイルを暗号化する前に、ユーザーは証明書を所有している必要があるのは、なぜですか。

解答 : EFS は、ユーザーの公開キーを使用して、ファイルをそれぞれ暗号化するためにランダムに生成された対称キーを暗号化します。ユーザーが公開キーを持っていない場合、EFS は対称キーを暗号化して保護することができません。このシナリオでは、EFS はユーザー証明書を取得してから暗号化を実行します。

質問 : EFS で暗号化されたファイルを他のユーザーと共有できますか。

解答 : はい。EFS で暗号化されたファイルは他のユーザーと共有できます。ただし、そのためには、ユーザーの公開キーを使用できる必要があります。これは、EFS が公開キーを使って対称キーを暗号化するためです。

EFS で暗号化されたファイルの回復

質問 : データ回復エージェントは、EFS で暗号化された任意のファイルをどのようにして暗号化解除しますか。

解答 : 環境内でデータ回復エージェントを構成した場合、EFS は、回復エージェントの公開キーを使用して対称キーのコピーを暗号化し、暗号化中にファイルに追加します。データ回復エージェントは、秘密キーを使用して対称キーのコピーの暗号化を解除し、それを使用してファイルの暗号化を解除します。

質問 : ファイルの暗号化を解除する適切な秘密キーを持たない場合、ファイルを暗号化したデバイスから、データ回復エージェントの専用コンピューターへ、EFS で暗号化されたファイルをコピーできますか。

解答 : いいえ。ファイルの暗号化を解除する適切な秘密キーを持たない場合、EFS で暗号化されたファイルをコンピューター間でコピーすることはできません。コピー操作には、ソース ファイルの読み取りが含まれます。適切な秘密鍵キーを持っていない場合は、ファイルを開いて読むことはできません。ユーザーは、暗号化されたファイルのバックアップをおこない、それらをデータ回復エージェントの専用コンピューターで復元する必要があります。

一般的な EFS の問題の解決

質問 : 自身の秘密キーを失ったユーザーは、どのようにして暗号化されたファイルをデータ回復エージェントの専用コンピューターにコピーできますか。

解答 : 秘密キーを失ったユーザーは、暗号化されたファイルをコピーすることはできませんが、ユーザーは、暗号化されたファイルのバックアップをおこない、それらをデータ回復エージェントの専用コンピューターに転送することができます。

質問 : 新しいデータ回復エージェントを追加した後、それらのデータ回復エージェントがファイルを暗号化解除できるまでに、どれだけ待つ必要がありますか。

解答 : 暗号化されたファイルの Data Recovery Field (DRF) は自動的に更新されませんが、適切な秘密キーを持つユーザーがファイルのプロパティを表示するか、または cipher /U コマンドを実行すると更新されます。

質問 : EFS により暗号化されたファイルを暗号化解除するためには、公開キーが必要です。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック

公開キーは、ファイルを暗号化するためのものです。ファイルの暗号化を解除するには秘密キーが必要です。

質問 : ユーザーが適切な秘密キーを持っている場合、EFS により暗号化されたファイルを必ず暗号化解除できます。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック

ユーザーはファイルにアクセスできる場合にのみ暗号化を解除できます。ファイルへのアクセス許可がない場合、そのファイルの暗号化を解除することはできません。

質問 : EFS を使用して、ファイルを暗号化するには、ネットワーク内に CA が必要です。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック

EFS は CA を使用する必要はありません。CA により発行された証明書を EFS に使用することが推奨されますが、自己署名証明書を使用することもできます。

参考資料

EFS の概要

参考資料 : 詳細については、次のサイトを参照してください。
How EFS Works
http://aka.ms/Uw9drx

EFS で暗号化されたファイルの回復

参考資料 : 詳細については、次のサイトを参照してください。
Key Recovery vs Data Recovery Differences
http://aka.ms/Frtdxi

デモンストレーション : EFS によるデータの保護

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-CL1 と LON-CL2 を起動します。
2. LON-CL1 で、ユーザー名「Adatum¥Adam」、パスワード「Pa55w.rd」を使用してサインインします。
3. LON-CL1 のタスク バーで [スタート] をクリックし、「certmgr.msc」と入力して、Enter キーを押します。
4. 証明書 - 現在のユーザー コンソールのナビゲーション ウィンドウで、[個人] をクリックし、詳細ウィンドウに項目が何も表示されていないことを確認します。
5. タスク バーで [エクスプローラー] アイコンをクリックします。

6. エクスプローラーのナビゲーション ウィンドウで、[PC]、[ローカル ディスク (C:)]、[Labfiles] の順に展開し、[Mod10] を選択します。詳細ウィンドウで、[Adam1] を右クリックし、[プロパティ] を選択し、[詳細設定] をクリックします。
7. [属性の詳細] ダイアログ ボックスで、[詳細] が選択不可になっていることを確認します。
8. [内容を暗号化してデータをセキュリティで保護する] チェック ボックスをオンにし、[OK] をクリックします。
9. [適用] をクリックし、[ファイルだけを暗号化] を選択して、[OK] をクリックします。

   EFS はファイルを暗号化する前にユーザー証明書を取得する必要があるため、ユーザーの最初のファイルの暗号化に数秒かかる場合があります。
10. [Adam1 のプロパティ] ダイアログ ボックスで、[詳細設定]、[詳細] の順にクリックします。Adam Hobbs がこのファイルにアクセスでき、Administrator がこのファイルの回復証明書を持っていることを確認します。
11. [追加] をクリックし、[暗号化ファイル システム] ダイアログ ボックスに、現在公開キーを持っているユーザーである Adam Hobbs のみが表示されることを確認します。[キャンセル] を 4 回クリックします。
12. エクスプローラーで、[Adam1] のファイルに小さな鍵のアイコンがあることを確認します。フォルダー内の他のファイルには鍵のアイコンがないことを確認します。
13. 証明書 - 現在のユーザー コンソールで、F5 キーを押して最新情報に更新します。
14. ナビゲーション ウィンドウで、[個人] を展開し、[証明書] をクリックします。
15. 詳細ウィンドウで、Adam Hobbs 用に発行された、ファイル システムを暗号化するための証明書が 1 つのみ表示されていることを確認します。
16. タスク バーで [スタート] をクリックし、[Adam Hobbs]、[アカウントの切り替え] の順にクリックします。
17. LON-CL1 で、ユーザー名「Adatum¥Dawn」、パスワード「Pa55w.rd」を使用してサインインします。
18. 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。
19. エクスプローラーのナビゲーション ウィンドウで、[PC]、[ローカル ディスク (C:)]、[Labfiles] の順に展開し、[Mod10] を選択します。
20. 詳細ウィンドウで [Adam1] をダブルクリックし、Dawn はファイルの暗号化解除をおこなう Adam の秘密キーを持っていないため、「アクセスが拒否されました」というエラー メッセージが表示されることを確認します。
21. [OK] をクリックしてメモ帳を閉じます。
22. エクスプローラーの詳細ウィンドウで [Don1] を右クリックし、[プロパティ] を選択します。
23. [プロパティ] ダイアログ ボックスで、[詳細設定] をクリックします。[内容を暗号化してデータをセキュリティで保護する] チェック ボックスをオンにし、[OK] をクリックします。[ファイルだけを暗号化] を選択し、[常にファイルだけを暗号化] チェック ボックスをオンにして、[OK] をクリックします。
24. 数秒待ち、Dawn が暗号化している最初のファイルであることを確認します。そのため、EFS はユーザー証明書を取得する必要があり、ユーザーがすでに EFS 証明書を取得している場合よりも時間がかかります。
25. [Don1 のプロパティ] ダイアログ ボックスで、[詳細設定]、[詳細] の順にクリックします。Dawn Williamson がこのファイルにアクセスできること、また、Administrator がこのファイルの回復証明書を持っていることを確認します。

26. [追加] をクリックし、[Adam Hobbs] を選択して、[OK] をクリックします。Adam Hobbs と Dawn Williamson がこのファイルにアクセスできることを確認し、[OK] を 3 回クリックします。
27. タスク バーで [スタート] をクリックし、[Dawn Williamson] をクリックして、[ADATUM¥Adam] を選択します。
28. LON-CL1 で、ユーザー名「Adatum¥Adam」、パスワード「Pa55w.rd」を使用してサインインします。
29. エクスプローラーで、[Don1] をダブルクリックします。ファイルを開き、コンテンツを読むことができることを確認します。Dawn は Adam に暗号化されたファイルへのアクセス権を付与することを説明します。
30. メモ帳を閉じます。

レッスン 2
BitLocker の計画と実装

目次

質問と解答

BitLocker の概要

質問 : BitLocker を使用して、ボリューム上の機密データのみを、同じボリューム上のその他のデータは暗号化せずに、暗号化できますか。

解答 : いいえ。各ボリュームで BitLocker を有効にすると、すべてのボリューム データが暗号化されます。

質問 : BitLocker を使用して、Windows デバイスのすべてのボリュームを暗号化できますか。

解答 : BitLocker を使用しても、システム ボリュームは暗号化できません。ただし、ファイル システムに関係なく、他のすべてのボリュームを暗号化できます。

BitLocker と TPM

質問 : どのようにして、TPM 非搭載のデバイスで BitLocker が機能するように構成できますか。

解答 : BitLocker は、既定で TPM を必要とします。デバイスに TPM が搭載されていない場合、グループ ポリシーを使用して BitLocker が TPM なしで機能するように構成します。そのような場合は、ボリュームを暗号化するために BitLocker の USB スタートアップ キーを提供する必要があります。

質問 : TPM 非搭載の Windows デバイスで BitLocker を実行するデメリットは何ですか。

解答 : TPM がなくても、Windows デバイス上のボリュームを暗号化することができます。ただし、TPM 非搭載の Windows デバイスでは、スタートアップ中にシステム整合性の検証を使用できません。

BitLocker の構成と管理

質問 : BitLocker の構成と管理に使用できるツールを挙げてください。

解答 : 会社が、MDOP のライセンスを取得している場合、コントロール パネルの BitLocker ドライブ暗号化ツール、Windows PowerShell コマンドレット、BitLocker ドライブ暗号化の構成ツール (Manage-bde.exe)、MBAM ツールを使用できます。

質問 : Windows 10 デバイスで、[Active Directory ドメイン サービスに BitLocker 回復情報を保存する (Windows Server 2008 および Windows Vista)] グループ ポリシー設定を有効にしました。BitLocker を有効にすると、BitLocker 回復情報は、AD DS に格納されますか。

解答 : いいえ。このグループ ポリシー設定は Windows Server 2008 と Windows Vista にのみ適用されており、Windows 10 には適用されていません。Windows 10 デバイスに BitLocker 回復キーを格納する場合は、[BitLocker で保護されているオペレーティング システム ドライブの回復方法を選択する]、[BitLocker で保護されている固定ドライブの回復方法を選択する]、または [BitLocker で保護されているリムーバブル ドライブの回復方法を選択する] のグループ ポリシー オプションを有効にする必要があります。

BitLocker で暗号化されたドライブの回復

質問 : TPM 搭載のデバイスで BitLocker を有効にする場合、回復パスワードの保存の目的は何ですか。

解答 : TPM が変更されアクセスできなくなった場合、主要なシステム ファイルが変更された場合、または誰かがオペレーティング システムを迂回しようとしてスタートアップ メディアからデバイスを起動した場合に、デバイスは回復モードに切り替わり、回復パスワードを入力するまでそのままの状態となります。回復パスワードを入力することで、ユーザーはアクセスできるようになり、スタートアップ プロセスを完了させることができるようになります。

質問 : 回復パスワードとパスワード ID の違いは何ですか。

解答 : 回復パスワードは、BitLocker で保護されたドライブのロック解除をおこなうため 48 桁の数字です。特定の BitLocker で暗号化されるボリュームごとに一意で、AD DS、USB フラッシュ ドライブ、またはファイルなどに格納できます。パスワード ID は、暗号化されるドライブごとに一意の 32 桁の文字列です。Active Directory ユーザーとコンピューターのコンピューター オブジェクトの [プロパティ] ページにある [BitLocker 回復] タブで確認できます。

Microsoft BitLocker Administration and Monitoring による BitLocker の管理

質問 : どのように MBAM を使用して、ヘルプ デスクがリモート ユーザーの BitLocker ロック解除キーの回復に費やしている時間を削減できますか。

解答 : 管理者は MBAM セルフサービス ポータルを有効にすると、ヘルプ デスクに電話をしなくても BitLocker 回復パスワードを回復することができます。

質問 : 会社では、BitLocker で保護され、Microsoft Intune で管理される Windows 10 デバイスのみが使用されています。この環境に MBAM を展開することができますか。

解答 : MBAM には AD DS と SQL Server が必要です。会社では Windows 10 デバイスのみが使用されており、前提条件を満たしていないため、MBAM を展開することはできません。

質問 : BitLocker を使用するためには、デバイスに TPM が搭載されている必要があります。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック

Windows 10 では、TPM なしで BitLocker を使用できます。

質問 : BitLocker で保護された Windows 8.1 のドライブを、Windows 10 でロック解除できます。

( ) 正

( ) 誤

解答 :

(√) 正

( ) 誤

フィードバック

以前のバージョンの Windows の BitLocker は Windows 10 と互換性があります。Windows 10 バージョン 1511 以降は、下位互換性のない新しい BitLocker 暗号化モードを使用できます。

質問 : C ドライブで BitLocker を有効にした場合、回復キーを AD DS に格納するように指定することもできます。

( ) 正

( ) 誤

解答 :

( ) 正

(√) 誤

フィードバック

ドライブで BitLocker を有効にすると、回復ドライブを格納する場所を指定できますが、USB フラッシュ ドライブ、ファイル、Microsoft アカウントのみを選択したり、印刷したりすることができます。ウィザードで BitLocker 回復キーを AD DS に格納することはできません。この操作はグループ ポリシーを使用することによってのみ実行できます。

参考資料

BitLocker の概要

参考資料 : 詳細については、次のサイトを参照してください。
BitLocker の概要
https://msdn.microsoft.com/ja-jp/library/hh831713(v=ws.11).aspx

BitLocker の構成と管理

参考資料 : 詳細については、次のサイトを参照してください。
BitLocker:BitLocker ドライブ暗号化ツールを使用して、BitLocker を管理するには
https://technet.microsoft.com/ja-jp/library/jj647767.aspx

参考資料 : 詳細については、次のサイトを参照してください。
BitLocker グループ ポリシーの設定
https://technet.microsoft.com/ja-jp/library/jj679890.aspx

Microsoft BitLocker Administration and Monitoring による BitLocker の管理

参考資料 : 詳細については、次のサイトを参照してください。
Microsoft BitLocker Administration and Monitoring
https://technet.microsoft.com/ja-jp/windows/hh826072.aspx

デモンストレーション : BitLocker の使用

デモンストレーションの手順

1. LON-CL1 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
2. LON-CL1 仮想マシン接続ウィンドウで、[ファイル] メニュー、[設定] の順にクリックします。
3. [23744B-LON-CL1 の設定] ダイアログ ボックスのナビゲーション ウィンドウで、[SCSI コントローラー] をクリックし、詳細ウィンドウで、[ハード ドライブ]、[追加]、[参照] の順にクリックして、C:¥Program Files¥Microsoft Learning¥23744¥Drives に移動します。
4. [Disk1.vhd]、[開く]、[適用] の順にクリックします。
5. [23744B-LON-CL1 の設定] ダイアログ ボックスのナビゲーション ウィンドウで、[フロッピー ディスク ドライブ] をクリックし、詳細ウィンドウで、[仮想フロッピー ディスク (.vfd) ファイル] を選択します。
6. C:¥Program Files¥Microsoft Learning¥23744¥Drives¥Floppy.vfd を参照し、[開く]、[OK] の順にクリックします。
7. LON-CL1 のタスク バーで [スタート] をクリックし、「gpedit.msc」と入力して、Enter キーを押します。
8. ローカル グループ ポリシー エディターのナビゲーション ウィンドウで、[コンピューターの構成]、[管理用テンプレート]、[Windows コンポーネント]、[BitLocker ドライブ暗号化] の順に展開します。
9. ナビゲーション ウィンドウで、[オペレーティング システムのドライブ] をクリックし、詳細ウィンドウで、[スタートアップ時に追加の認証を要求する] をダブルクリックします。
10. [スタートアップ時に追加の認証を要求する] ダイアログ ボックスで、[有効] をクリックします。[互換性のある TPM が装備されていない BitLocker を許可する] 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。

注 : この構成は、デバイスに TPM が搭載されていない場合にのみ必要であることを説明します。

11. ナビゲーション ウィンドウで、[固定データ ドライブ] ノードをクリックし、詳細ウィンドウで、[BitLocker で保護されている固定ドライブの回復方法を選択する] をダブルクリックします。
12. [BitLocker で保護されている固定ドライブの回復方法を選択する] ダイアログ ボックスで、[有効]、[OK] の順にクリックします。
13. LON-CL1 のタスク バーで、[エクスプローラー] アイコンをクリックします。
14. エクスプローラーのナビゲーション ウィンドウで、[PC] を展開し、[Data (E:)] をクリックし、詳細ウィンドウの何も表示されていない場所を右クリックして [新規作成] を選択し、[テキスト ドキュメント] をクリックして、ファイル名を自分の名前に変更します

15. エクスプローラーのナビゲーション ウィンドウで、[Data (E:)] を右クリックし、[BitLocker を有効にする] をクリックします。
16. [BitLocker ドライブ暗号化 (E:)] ダイアログ ボックスで、[パスワードを使用してドライブのロックを解除する] チェック ボックスをオンにし、[パスワードを入力してください] ボックスと [パスワードをもう一度入力してください] ボックスに「Pa55w.rd」と入力して、[次へ] をクリックします。
17. [回復キーのバックアップ方法を指定してください。] ページで、[ファイルに保存する] をクリックします。
18. [BitLocker 回復キーに名前を付けて保存] ダイアログ ボックスのナビゲーション ウィンドウで、[PC] をクリックし、詳細ウィンドウで、[フロッピー ディスク ドライブ (A:)] をダブルクリックして、[保存]、[次へ] の順にクリックします。
19. [使用する暗号化モードを選ぶ] ページで、[次へ]、[暗号化の開始] の順にクリックします。
20. エクスプローラーのナビゲーション ウィンドウで、ローカル ディスク (E:) のみに小さな鍵アイコンがあることを確認します。
21. 23744B-LON-CL1 仮想マシン接続ウィンドウで、[ファイル] メニュー、[設定] の順にクリックします。
22. [23744B-LON-CL1 の設定] ダイアログ ボックスのナビゲーション ウィンドウで、[SCSI コントローラー] の下の [ハード ドライブ Disk1.vhd] をクリックし、詳細ウィンドウで、[削除]、[OK] の順にクリックします。
23. LON-CL2 で、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
24. 23744B-LON-CL2 仮想マシン接続ウィンドウで、[ファイル] メニュー、[設定] の順にクリックします。
25. [23744B-LON-CL2 の設定] ダイアログ ボックスのナビゲーション ウィンドウで、[SCSI コントローラー] をクリックし、詳細ウィンドウで、[ハード ドライブ]、[追加]、[参照] の順にクリックして、C:¥Program Files¥Microsoft Learning¥23744¥Drives に移動します。[Disk1.vhd]、[開く]、[OK] の順にクリックします。
26. 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。ナビゲーション ウィンドウで、ドライブ E: が、小さな鍵アイコンと共に [ローカル ディスク (E:)] として表示されることを確認します。
27. エクスプローラーのナビゲーション ウィンドウで、[ローカル ディスク (E:)] をクリックします。[BitLocker (E:)] ダイアログ ボックスが開きます。
28. [BitLocker (E:)] ダイアログ ボックスで、ボックスに「Pa55w.rd」と入力し、[ロック解除] をクリックします。
29. エクスプローラーのナビゲーション ウィンドウで、E ドライブが [Data (E:)] と表示され、[ローカル ディスク (E:)] と表示されないことを確認します。

注 : 詳細ウィンドウで、自分の名前のファイルが表示されていることを確認します。

30. LON-DC1 で Windows PowerShell を起動します。
31. BitLocker 回復パスワード ビューアーをインストールするために、Windows PowerShell ウィンドウで、次のコマンドレットを 1 行で入力し、Enter キーを押します。

```
Install-WindowsFeature RSAT-Feature-Tools-BitLocker-BdeAducExt
```

32. Active Directory ユーザーとコンピューターで、[Adatum.com] を展開し、[Computers] をクリックします。
33. 詳細ウィンドウで、[LON-CL1] を右クリックし、[プロパティ] をクリックします。
34. [LON-CL1 のプロパティ] ダイアログ ボックスで、[BitLocker 回復] タブをクリックし、BitLocker 回復パスワードが表示されていることを確認します。

注 : LON-CL1 の暗号化されたディスクの BitLocker 回復パスワードが表示されていることを示します。

演習の復習の質問と解答

演習 : 暗号化と BitLocker によるデータの保護

質問と解答

質問 : Administrator はデータ回復エージェントであるにも関わらず、LON-CL2 で Administrator が Adam1.txt ファイルを開くことができないのはなぜですか。

解答 : 既定では、管理者のデータ回復証明書は、最初のドメイン コントローラーにのみ格納されます。管理者は LON-CL2 上にデータ回復証明書を持っていなかったため、ファイルを開くことができませんでした。データ回復証明書をインポートした後は、ファイルを開くことができます。

質問 : LON-CL1 を TPM 非搭載で BitLocker を許容するように構成しなければならなかった理由は何ですか。

解答 : 仮想マシンに TPM が搭載されていないためです。既定で BitLocker には TPM が必要で、この要件を変更することなく、LON-CL1 で BitLocker を使用することはできません。

復習とまとめ

復習問題

質問 : EFS ファイル暗号化を使用して、ボリューム全体を暗号化できますか。

解答 : EFS は、ファイルまたはフォルダー レベルでは有効化できますが、ボリューム レベルでは有効化できません。ただし、EFS は、ボリュームのルート フォルダー内のすべてのフォルダーとファイルでは有効化できます。これにより、そのボリューム上のすべてのファイルが暗号化されます。

質問 : EFS を使用して、Windows システム ファイルを暗号化できますか。

解答 : いいえ。EFS ファイル暗号化を使用して、システム属性が設定されているファイルを暗号化することはできません。

質問 : 紛失した Windows デバイスの完全なワイプを実行できますか。

解答 : いいえ。Windows デバイスは選択的なワイプのみをサポートします。紛失したデバイスが Microsoft Intune、Microsoft System Center Configuration Manager、またはその他のモバイル デバイス管理ソリューションによって管理されている場合は、Windows デバイスの選択的なワイプのみ実行することができます。

第 11 章

ファイル サービスの最適化およびセキュリティ保護

目次

レッスン 1
ファイル サーバー リソース マネージャー

目次

質問と解答

質問 : クォータは、すべてのデータ全体に実装するものですか、あるいは選択した場所内にのみ実装するものですか。

解答 : 解答はさまざまです。ただし、クォータをすべてのデータに適用すると、意図しない結果になる可能性があります。クォータを実装する前に、クォータの設定について十分な計画を立てる必要があります。

質問 : ご使用の環境では、ファイル スクリーン処理を実装しますか。

解答 : 解答はさまざまです。ただし、ファイル スクリーン処理を展開する前に、その影響を十分に検討する必要があります。

デモンストレーション : FSRM のインストールと構成

デモンストレーションの手順

FSRM をインストールする

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 を起動します。
2. LON-SVR1 で、[スタート]、[サーバー マネージャー]、[管理]、[役割と機能の追加] の順にクリックします。
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、[役割ベースまたは機能ベースのインストール] が選択されていることを確認し、[次へ] をクリックします。
5. [対象サーバーの選択] ページで、[LON-SVR1.Adatum.com] が選択されていることを確認し、[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、[ファイル サービスおよび記憶域サービス (2/12 個をインストール済み)]、[ファイル サービスおよび iSCSI サービス (1/11 個をインストール済み)] の順に展開し、[ファイル サーバー リソース マネージャー] チェック ボックスをオンにします。
7. 役割と機能の追加ウィザードで [機能の追加] をクリックします。
8. [次へ] を 2 回クリックして、役割サービスと機能の選択を確認します。
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。

FSRM を構成する

1. サーバー マネージャーで、[ツール]、[ファイル サーバー リソース マネージャー] の順にクリックします。
2. ファイル サーバー リソース 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、[ファイル サーバー リソース マネージャー (ローカル)] を右クリックし、[オプションの構成] をクリックします。
3. [ファイル サーバー リソース マネージャーのオプション] ダイアログ ボックスで、[ファイル スクリーンの監査] タブをクリックし、[監査データベースにファイル スクリーン処理の動作状況を記録する] チェック ボックスをオンにします。
4. [OK] をクリックし、[ファイル サーバー リソース マネージャーのオプション] ダイアログ ボックスを閉じます。ファイル サーバー リソース マネージャー コンソールを閉じます。

Windows PowerShell を使用して FSRM を管理する

1. サーバー マネージャーで、[ツール]、[Windows PowerShell] の順にクリックします。
2. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
Set-FSRMSetting -SMTPServer "SMTPServer" -AdminEmailAddress "fileadmin@adatum.com" -FromEmailAddress "Lon-SVR1@adatum.com"
```

3. Windows PowerShell ウィンドウを閉じます。
4. ファイル サーバー リソース マネージャー コンソールを開きます。
5. ファイル サーバー リソース 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、[ファイル サーバー リソース マネージャー (ローカル)] を右クリックし、[オプションの構成] をクリックします。
6. [電子メールの通知] タブで、構成済みのオプションを確認し、Set-FSRMSetting コマンドで設定したオプションと同じであることを確かめます。
7. 開いているウィンドウをすべて閉じます。

デモンストレーション : クォータの使用率の監視

デモンストレーションの手順

クォータを作成する

1. サインインしていない場合は、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用して LON-SVR1 にサインインします。
2. [スタート] をクリックし、[サーバー マネージャー] をクリックします。
3. サーバー マネージャーで、[ツール]、[ファイル サーバー リソース マネージャー] の順にクリックします。
4. ファイル サーバー リソース マネージャー コンソールで、[クォータ管理] を展開し、[クォータ テンプレート] をクリックします。
5. [100 MB 制限] テンプレートを右クリックし、[テンプレートからのクォータを作成] をクリックします。
6. クォータの作成ウィンドウで、[参照] をクリックします。
7. フォルダーの参照ウィンドウで [Allfiles (E:)]、[Labfiles]、[Mod11] の順に展開し、[Data] をクリックして、[OK] をクリックします。
8. クォータの作成ウィンドウで、[作成] をクリックします。
9. ファイル サーバー リソース マネージャー コンソールで、[クォータ] をクリックし、新しく作成したクォータを表示します。

クォータをテストする

1. [スタート] をクリックし、[Windows PowerShell] アイコンをクリックします。
2. Windows PowerShell ウィンドウで、次のコマンドを入力し、各コマンドの最後に Enter キーを押します。

```
cd E:¥labfiles¥Mod11¥Data
fsutil file createnew largefile.txt 130000000
```

3. 次のメッセージが表示されることを確認します。
   エラー : ディスクに十分な空き領域がありません。
4. Windows PowerShell ウィンドウを閉じます。

デモンストレーション : ファイル スクリーンの実装

デモンストレーションの手順

ファイル スクリーンを作成する

1. LON-SVR1 のファイル サーバー リソース マネージャー コンソールで、[ファイル スクリーンの管理] を展開し、[ファイル スクリーン テンプレート] をクリックします。
2. [イメージ ファイルのブロック] テンプレートを右クリックし、[テンプレートからファイル スクリーンを作成] をクリックします。
3. ファイル スクリーンの作成ウィンドウで、[参照] をクリックします。
4. フォルダーの参照ウィンドウで [Allfiles (E:)]、[Labfiles]、[Mod11] の順に展開し、[Data] をクリックして、[OK] をクリックします。
5. ファイル スクリーンの作成ウィンドウで、[作成] をクリックします。

ファイル スクリーンをテストする

1. エクスプローラーを開きます。
2. エクスプローラーで、[PC]、[Allfiles (E:)]、[Labfiles] の順に展開し、[Mod11] フォルダーをクリックします。
3. エクスプローラーで、[ホーム] タブ、[新しい項目]、[ビットマップ イメージ] の順にクリックします。
4. 「testimage」と入力し、Enter キーを押します。
5. ファイルが作成できたことを確認します。
6. [testimage] を右クリックし、[コピー] をクリックします。
7. [Data] を右クリックし、[貼り付け] をクリックします。
8. この操作を実行するアクセス許可が必要であるというメッセージが表示されます。[キャンセル] をクリックし、メッセージを閉じます。
9. エクスプローラーを閉じます。

デモンストレーション : オンデマンドでの記憶領域レポートの生成

デモンストレーションの手順

記憶域レポートを生成する

1. LON-SVR1 のファイル サーバー リソース マネージャーのナビゲーション ウィンドウで、[記憶域レポートの管理] を右クリックし、[レポートを今すぐ生成する] をクリックします。
2. [記憶域レポート タスクのプロパティ] ダイアログ ボックスで、[大きいサイズのファイル] チェックボックスをオンにします。
3. [スコープ] タブをクリックし、[追加] をクリックします。
4. フォルダーの参照ウィンドウで、[Allfiles (E:)] をクリックし、[OK] をクリックします。

5. [記憶域レポート タスクのプロパティ] ダイアログ ボックスで [OK] をクリックします。
6. [記憶域レポートの生成] ダイアログ ボックスで、[レポートが生成され、表示されるのを待つ] が選択されていることを確認し、[OK] をクリックして、レポートを生成します。
7. エクスプローラーで、Interactive フォルダー内の html ファイルを右クリックし、[プログラムから開く]、[Internet Explorer]、[OK] の順にクリックし、レポートを確認します。
8. レポート ウィンドウを閉じます。
9. エクスプローラーを閉じます。
10. ファイル サーバー リソース マネージャーを閉じます。
11. サーバー マネージャーを閉じます。

レッスン 2
分類およびファイル管理タスクの実装

目次

質問と解答

質問 : あなたの環境では、自動分類をどのように使用できますか。

解答 : 解答はさまざまです。自動分類と AD RMS を結び付けて、基本的なデータ損失防止ソリューションを実現したいと考える受講者もいるでしょう。

デモンストレーション : ファイル分類の構成

デモンストレーションの手順

分類プロパティを作成する

1. LON-SVR1 で [スタート] をクリックし、[サーバー マネージャー] をクリックします。
2. サーバー マネージャーで、[ツール]、[ファイル サーバー リソース マネージャー] の順にクリックします。
3. ファイル サーバー リソース マネージャーで、[分類管理] を展開し、[分類プロパティ] を右クリックして、[ローカル プロパティの作成] をクリックします。
4. ローカル分類プロパティの作成ウィンドウで、[名前] ボックスに「Documents」と入力し、[プロパティの種類] ドロップダウン リストで、[はい/いいえ] が選択されていることを確認して、[OK] をクリックします。

分類規則を作成する

1. ファイル サーバー リソース マネージャーで、[分類管理] を展開し、[分類規則] をクリックし、操作ウィンドウで [分類規則の作成] をクリックします。
2. 分類規則の作成ウィンドウの [全般] タブで、[規則名] ボックスに「Corporate Documents Rule」と入力し、[有効] チェック ボックスがオンであることを確認します。
3. 分類規則の作成ウィンドウの [スコープ] タブで、[追加] をクリックします。
4. フォルダーの参照ウィンドウで [Allfiles (E:)]、[Labfiles]、[Mod11] の順に展開し、[Documents] フォルダーをクリックして、[OK] をクリックします。
5. 分類規則の作成ウィンドウの [分類] タブで、[分類方法] ドロップダウン リストの [フォルダー分類子] をクリックします。[プロパティ - ファイルに割り当てるプロパティを選択してください] ドロップダウン リストで、[Documents] をクリックし、[プロパティ - 値の指定] ドロップダウン リストで [はい] をクリックします。
6. 分類規則の作成ウィンドウの [評価の種類] タブで、[既存のプロパティ値を再評価する] をクリックし、[値を統合する] が選択されていることを確認し、[OK] をクリックします。
7. ファイル サーバー リソース マネージャーの操作ウィンドウで、[すべての規則で今すぐ分類を実行する] をクリックします。
8. [分類の実行] ダイアログ ボックスで、[分類の完了を待つ] をクリックし、[OK] をクリックします。
9. Internet Explorer に表示された自動分類レポートを調べて、レポートで表示された分類されたファイル数と Documents フォルダー内のファイル数が一致していることを確認します。3 つのファイルがあります。
10. Internet Explorer を閉じます。

デモンストレーション : ファイル管理タスクの構成

デモンストレーションの手順

ファイルを作成する

1. LON-SVR1 のタスク バーで、[エクスプローラー] アイコンをクリックします。
2. E:¥Labfiles¥Mod11¥Documents に移動し、[Strategy1.txt] を右クリックして、[コピー] をクリックします。右側のウィンドウで何も表示されていない場所を右クリックし、[貼り付け] をクリックして、「Strategy1 - コピー.txt」という名前を付けます。

ファイル管理タスクを作成する

1. LON-SVR1 で [スタート] をクリックし、[サーバー マネージャー] をクリックします。
2. サーバー マネージャーで、[ツール]、[ファイル サーバー リソース マネージャー] の順にクリックします。
3. ファイル サーバー リソース マネージャーで、[ファイル管理タスク] を右クリックし、[ファイル管理タスクの作成] をクリックします。
4. [タスク名] ボックスに「Expire Documents」と入力します。
5. [説明] ボックスに「Move old documents to another folder」と入力します。
6. [スコープ] タブをクリックします。
7. [スコープ] セクションで、[追加] をクリックします。
8. [Allfiles (E:)]、[Labfiles]、[Mod11] の順に展開し、[Documents] をクリックして、[OK] をクリックします。

ドキュメントを有効期限切れにするようにファイル管理タスクを構成する

1. ファイル管理タスクの作成ウィンドウで、[アクション] タブをクリックします。
2. [アクション] タブで、[種類] の [ファイルの有効期限] を選択します。
3. [有効期限切れのディレクトリ] に「E:¥Labfiles¥Mod11¥Data」と入力します。
4. ファイル管理タスクの作成ウィンドウで、[条件] タブをクリックします。
5. [条件] タブで、[ファイル名のパターン] チェック ボックスをオンにし、ボックスに「*コピー*」と入力します。
6. ファイル管理タスクの作成ウィンドウで、[スケジュール] タブをクリックします。
7. [毎月] を選択し、[最終] チェック ボックスをオンにします。
8. ファイル管理タスクの作成ウィンドウで、[OK] をクリックします。
9. [Expire Documents] タスクを右クリックし、[ファイル管理タスクを今すぐ実行する] をクリックします。
10. ファイル管理タスクの実行ウィンドウで、[タスクの実行の完了を待つ] を選択し、[OK] をクリックします。
11. 生成されたレポートを表示し、1 つのファイルが移動されたことを確認します。
12. レポート ヘッダーにある有効期限切れのディレクトリへのリンクをクリックし、そのディレクトリを展開して、有効期限切れのファイルを表示します。
13. E:¥Labfiles¥Mod11¥Documents フォルダーを開いて、内容を確認します。Strategy1 - コピー.txt ファイルがないことを確認します。
14. 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

目次

質問と解答

質問 : ダイナミック アクセス制御を使用する場合、要件となるのはどのテクノロジですか。

( ) Active Directory ドメイン サービス

( ) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

解答 :

(√) Active Directory ドメイン サービス

(√) Kerberos

( ) AD CS

( ) AD RMS

( ) AD FS

フィードバック

ファイル分類では AD RMS を使用する場合がありますが、ダイナミック アクセス制御の要件は、AD DS と Kerberos のみです。

質問 : Windows Server 2016 のダイナミック アクセス制御は、ユーザー要求とコンピューター要求の両方をサポートします。

( ) 正

( ) 誤

解答 :

(√) 正

( ) 誤

フィードバック :

ダイナミック アクセス制御は、ユーザー要求とコンピューター要求をサポートします。要求は、AD DS の属性とこれらの属性の値に基づきます。

参考資料

ダイナミック アクセス制御の基盤テクノロジ

参考資料 : Kerberos v5 における Kerberos 防御の変更については、次のサイトを参照してください。
Kerberos 認証の新機能
https://technet.microsoft.com/ja-jp/ja-jp/library/hh831747.aspx

集約型アクセス ポリシーの実装と構成

参考資料 : Microsoft Data Classification Toolkit は、次のサイトからダウンロードすることができます。
Microsoft Data Classification Toolkit
http://aka.ms/alw15o

参考資料 : ユーザーに適切なアクセス権が付与されない場合にダイナミック アクセス制御のトラブルシューティングをおこなうには、次のサイトからドキュメントをダウンロードしてください。
Understand and Troubleshoot Dynamic Access Control in Windows Server 2012
http://aka.ms/w2d2fo

デモンストレーション : ダイナミック アクセス制御の構成

デモンストレーションの手順

ダイナミック アクセス制御用に AD DS を準備する

1. LON-DC1 のサーバー マネージャーで、[ツール]、[Active Directory ユーザーとコンピューター] の順にクリックします。
2. Active Directory ユーザーとコンピューター ウィンドウで、[Adatum.com] ドメインを右クリックし、[新規作成]、[組織単位] の順にクリックします。
3. [組織単位の作成] ダイアログ ボックスで、[名前] ボックスに「DAC-Protected computers」と入力し、[OK] をクリックします。
4. 中央のウィンドウで、[Computers] コンテナーをダブルクリックし、[LON-SVR1] を右クリックして、[移動] をクリックします。
5. 移動ウィンドウで、[DAC-Protected computers] をクリックし、[OK] をクリックします。
6. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
7. [フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[グループ ポリシー オブジェクト] コンテナーをクリックします。
8. 結果ウィンドウで、[Default Domain Controllers Policy] を右クリックし、[編集] をクリックします。
9. グループ ポリシー管理エディターの [コンピューターの構成] で、[ポリシー]、[管理用テンプレート]、[システム] を展開し、[KDC] をクリックします。
10. 詳細ウィンドウで、[KDC で信頼性情報、複合認証、および Kerberos 防御をサポートする] をダブルクリックします。
11. KDC で信頼性情報、複合認証、および Kerberos 防御をサポートするウィンドウで、[有効] を選択し、[オプション] セクションで、[常に信頼性情報を提供する] を選択して、[OK] をクリックします。
12. グループ ポリシー管理エディターとグループ ポリシーの管理コンソールを閉じます。
13. [スタート] をクリックし、[Windows PowerShell] をクリックします。
14. Windows PowerShell ウィンドウで、「gpupdate /force」と入力し、Enter キーを押します。グループ ポリシーが更新されたら、Windows PowerShell ウィンドウを閉じます。
15. Active Directory ユーザーとコンピューターに切り替えます。

16. ナビゲーション ウィンドウで、[Research] OU をクリックし、コンテンツ ウィンドウで [Connie Vaughn] を右クリックし、[プロパティ] をクリックします。
17. Connie Vaughn のプロパティ ウィンドウで、[組織] タブをクリックします。
18. [部署] ボックスに [Research] という値が設定されていることを確認し、[キャンセル] をクリックします。
19. Active Directory ユーザーとコンピューターを閉じます。

要求、リソース プロパティ、および集約型アクセス規則を構成する

1. サーバー マネージャーで、[ツール]、[Active Directory 管理センター] の順にクリックします。
2. Active Directory 管理センターのナビゲーション ウィンドウで、[ダイナミック アクセス制御] をクリックし、[Claim Types] をダブルクリックします。
3. タスク ウィンドウで、[新規] をクリックし、[要求の種類] をクリックします。
4. 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] を見つけて選択します。
5. [表示名] ボックスに「Company Department」と入力します。
6. [ユーザー] と [コンピューター] チェック ボックスの両方をオンにして、[OK] をクリックします。
7. Active Directory 管理センターで、[ダイナミック アクセス制御] をクリックし、[Resource Properties] をダブルクリックします。
8. [Resource Properties] リストで、[Department] を右クリックし、[有効] をクリックします。
9. [Department] をダブルクリックします。
10. [提案された値] セクションまで下にスクロールし、[追加] をクリックします。
11. 提案された値の追加ウィンドウで、[値] ボックスと [表示名] ボックスの両方に「Research」と入力し、[OK] を 2 回クリックします。
12. [ダイナミック アクセス制御] をクリックし、[Resource Property Lists] をダブルクリックします。
13. コンテンツ ウィンドウで、[Global Resource Property List] をダブルクリックし、リソースプロパティのリストに [Department] と [Confidentiality] の両方が表示されていることを確認し、[キャンセル] をクリックします。表示されない場合は、[追加] をクリックし、これら 2 つのプロパティを追加して、[OK] をクリックします。
14. 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、[Central Access Rules]] をダブルクリックします。
15. タスク ウィンドウで、[新規] をクリックし、[集約型アクセス規則] をクリックします。
16. [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。
17. [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。
18. [集約型アクセス規則] ダイアログ ボックスで、[条件の追加] をクリックします。
19. 最後のドロップダウン リストで、[Research] を選択します。条件が [リソース]、[Department]、[次の値と等しい]、[値]、[Research] であることを確認し、[OK] をクリックします。
20. [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] を選択し、[編集] をクリックします。
21. OWNER RIGHTS のアクセス許可エントリを選択し、[削除] をクリックします。[Administrators (ADATUM¥Administrators)] および [SYSTEM] グループに対して、この手順を繰り返します。
22. [アクセス許可のセキュリティの詳細設定] ダイアログ ボックスで、[追加] をクリックします。

23. [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。
24. ユーザー、コンピューター、サービス アカウント、またはグループを選択ウィンドウで、「Authenticated Users」と入力し、[名前の確認]、[OK] の順にクリックします。
25. [基本のアクセス許可] セクションで、[変更]、[読み取りと実行]、[読み取り]、[書き込み] を選択します。
26. [条件の追加] をクリックします。
27. [グループ] ドロップダウン リストから [Company Department] を、[値] ドロップダウン リストから [リソース] を、最後のドロップダウン リストから [Department] を選択して、[OK] をクリックします。

ファイルを手動で分類する

1. LON-SVR1 に切り替えます。
2. [スタート] をクリックし、[サーバー マネージャー] をクリックします。
3. サーバー マネージャーで、[ツール]、[ファイル サーバー リソース マネージャー] の順にクリックします。
4. ファイル サーバー リソース マネージャーで、[分類管理] を展開し、[分類プロパティ] を右クリックし、[最新の情報に更新] をクリックします。
5. [Department] プロパティが一覧表示されることを確認します。
6. 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。
7. エクスプローラーのアドレス バーに「E:¥Labfiles¥Mod11」と入力し、Enter キーを押し、コンテンツ ウィンドウで [Research] フォルダーを右クリックし、[プロパティ] をクリックします。
8. [分類] タブで、[Department] をクリックし、[値] セクションで [Research] をクリックして、[OK] をクリックします。

集約型アクセス ポリシーを構成して展開する

1. LON-DC1 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、[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。
3. タスク ウィンドウで、[新規]、[集約型アクセス ポリシー] の順にクリックします。
4. [名前] ボックスに「Department Match」と入力し、[追加] をクリックします。
5. [Department Match] 規則をクリックし、[>>] をクリックして、[OK] を 2 回クリックします。
6. Active Directory 管理センターを閉じます。
7. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
8. グループ ポリシーの管理コンソールで、[DAC-Protected Computers] を右クリックし、[このドメインに GPO を作成し、このコンテナーにリンクする] をクリックします。
9. [新しい GPO] ダイアログ ボックスで、[名前] ボックスに「DAC Policy」と入力し、[OK] をクリックします。
10. [DAC Policy] を右クリックし、[編集] をクリックします。
11. グループ ポリシー管理エディターの [コンピューターの構成] で、[ポリシー]、[Windows の設定]、[セキュリティの設定]、[ファイル システム] の順に展開し、[集約型アクセス ポリシー] を右クリックして、[集約型アクセス ポリシーの管理] をクリックします。
12. [Department Match]、[追加]、[OK] の順にクリックします。

13. グループ ポリシー管理エディターとグループ ポリシーの管理コンソールを閉じます。
14. LON-SVR1 に切り替えます。
15. LON-SVR1 で [スタート] をクリックし、[Windows PowerShell] をクリックします。
16. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate /force
```

17. Windows PowerShell ウィンドウを閉じます。
18. エクスプローラーに切り替えます。
19. エクスプローラーで、[Research] フォルダーを右クリックし、[プロパティ] をクリックします。
20. [Research のプロパティ] ダイアログ ボックスで、[セキュリティ] タブをクリックし、[詳細設定] をクリックします。
21. Research のセキュリティの詳細設定ウィンドウで、[集約型ポリシー] タブをクリックして、[変更] をクリックします。
22. ドロップダウン リストから [Department Match] を選択し、[OK] を 2 回クリックします。

デモンストレーション : アクセス拒否アシスタンスの構成

デモンストレーションの手順

1. LON-DC1 に切り替えます。
2. LON-DC1 のサーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
3. グループ ポリシーの管理コンソールで、[DAC Policy] を右クリックして、[編集] をクリックします。
4. グループ ポリシー管理エディターの [コンピューターの構成] で、[ポリシー]、[管理用テンプレート]、[システム] の順に展開し、[アクセス拒否アシスタンス] をクリックします。
5. 詳細ウィンドウで、[アクセス拒否エラーのメッセージをカスタマイズする] をダブルクリックします。
6. アクセス拒否エラーのメッセージをカスタマイズするウィンドウで、[有効] をクリックします。
7. [アクセスが拒否されたユーザーに次のメッセージを表示] ボックスに「アクセス許可ポリシーによって、アクセスが拒否されました。アクセス許可を要求してください。」と入力します。
8. [ユーザーがアシスタントを要求できるようにする] をオンにします。その他のオプションを確認しますが、変更はおこなわず、[OK] をクリックします。
9. グループ ポリシー管理エディターの詳細ウィンドウで、[クライアントですべてのファイルの種類についてアクセス拒否アシスタンスを有効にする] をダブルクリックし、[有効]、[OK] の順にクリックします。
10. グループ ポリシー管理エディターとグループ ポリシーの管理コンソールを閉じます。

演習の復習の質問と解答

演習 A : クォータとファイル スクリーン処理

質問と解答

質問 : サーバーのファイル構造の管理に FSRM を使用するためには、どのような条件を満たす必要がありますか。

解答 : FSRM を使用するためには、サーバーが Windows Server 2003 SP1 以降を実行している必要があります。FCI を使用する場合は、Windows Server 2008 R2 以降を実行している必要があります。また、FSRM 操作を実行するボリュームを NTFS でフォーマットする必要があります。

質問 : 複雑なファイルとフォルダーの構造を取り扱う場合、どのようにして、分類管理およびファイル管理タスクにより、管理のオーバーヘッドを減らすことができますか。

解答 : 分類管理とファイル管理タスクにより、管理者は手動の分類とファイル サーバー上のファイルの変更を自動化できます。管理者は、手動でファイルを調べ、手動のファイル操作をおこなうのではなく、FCI をセットアップしてファイルを分類し、ファイル管理タスクを使用して、それらのファイルに対して必要な操作をおこなうことができます。

演習 B : ダイナミック アクセス制御の実装

質問と解答

質問 : ファイル分類により、ダイナミック アクセス制御の用途はどのように拡張されますか。

解答 : ファイル分類を使用すると、ファイルに属性を自動的に設定できます。ダイナミック アクセス制御を実装すると、それらの属性を条件式で使用することができます。

質問 : 集約型アクセス ポリシーなしで、ダイナミック アクセス制御を実装できますか。

解答 : はい、直接、リソースに対して、条件式を設定できます。

復習とまとめ

ベスト プラクティス

- クォータ テンプレートを使用して、グループが格納するデータ量を制御し、監視します。
- ファイル分類を使用して、特定の種類のデータを識別し、それらに対するきめ細かい制御を実現します。

一般的な問題とトラブルシューティングのヒント

一般的な問題	トラブルシューティングのヒント
コマンド プロンプトでファイル管理タスクを実行しようとすると、タスクが見つからないことを示すエラーが表示されます。	ファイル サーバー インターフェイスのタスク名が、コマンド プロンプトが要求するタスク名と一致していないため、このエラーが発生します。例えば、Task1 という名前のタスクを作成し、コマンド プロンプトが要求している名前が FileManagement-Task1 の場合です。

復習問題

質問 : クォータとファイル スクリーン用の FSRM テンプレートは、どのようにして、より効率的な FSRM 管理エクスペリエンスを実現しますか。

解答 : テンプレートにより、管理者は、事前定義されたテンプレートに基づき、クォータとファイル スクリーンを簡単に作成することができます。また、テンプレートを使用して、1 対多の方法で子クォータを管理することもできます。テンプレートで作成された複数のクォータのファイル サイズを変更するためには、テンプレートを変更することのみが必要です。

質問 : アクセス拒否アシスタンスは、どのようにしてユーザー エクスペリエンスを向上しますか。

解答 : アクセス拒否アシスタンス機能が、わかりやすい説明と最新の連絡先情報で構成されていると、ユーザーが特定のリソースにアクセスできない理由を理解するために役立ち、アクセスを提供できる適切な連絡先に彼らをリダイレクトすることができます。

ツール

ツール	用途	アクセス方法
ファイル サーバー リソース マネージャー	クォータ、ファイル スクリーン、分類管理、および記憶域レポートの管理	• 役割と機能の追加ウィザードで、または Windows PowerShell を使用して、FSRM 役割サービスを追加する • [サーバー マネージャー]、[ツール]
Windows PowerShell	FSRM の管理	Windows PowerShell `import-module FileServerResourceManager`

第 12 章

ファイアウォールと暗号化によるネットワーク トラフィックのセキュリティ保護

目次

レッスン 1
ネットワーク関連のセキュリティの脅威の理解

目次

質問と解答

討論 : 一般的なネットワーク関連のセキュリティの脅威

質問 : あなたがよく知っているセキュリティの脅威をいくつか挙げてください。

解答 : 解答はさまざまですが、フィッシング詐欺メール、スパイウェア、およびランサムウェアが含まれる可能性があります。

参考資料

既知のポート

参考資料 : 既知のポートと登録済みポートの完全な一覧については、次のサイトを参照してください。
Service Name and Transport Protocol Port Number Registry
https://aka.ms/ivsdso

レッスン 2
セキュリティが強化された Windows ファイアウォールの理解

目次

質問と解答

質問 : セキュリティが強化された Windows ファイアウォールなど、ホスト ベースのファイアウォールを使用することのメリットは何ですか。

解答 : セキュリティが強化された Windows ファイアウォールのメリットは次のとおりです。

- 内部ネットワークの攻撃からコンピューターを保護する機能が向上しました。未承諾の受信トラフィックをブロックすることで、マルウェアが内部ネットワーク内を移動することを防ぐことができます。
- 受信の規則により、ネットワーク内のホストを識別するためのネットワーク スキャンを防ぎます。最も簡単なネットワーク スキャンは、ネットワーク内のホストに ping を実行して、ホストを識別しようとします。セキュリティが強化された Windows ファイアウォールは、メンバー サーバーが ping 要求に応答することを防止します。ドメイン コントローラーは ping 要求に応答します。
- 送信の規則を有効にすると、マルウェアがネットワーク上で通信することを防ぐことで、マルウェアの拡散を防止できます。ウィルスの発生時には、特別な送信の規則をコンピューターに構成し、ウィルスがネットワークを越えて通信することを防ぐことができます。
- 接続セキュリティの規則により、コンピューターとユーザーの認証情報を使用して高いセキュリティのコンピューターとの通信を制限する、精緻なファイアウォールの規則を作成することができます。

デモンストレーション : Windows ファイアウォールによるネットワーク トラフィックの管理

デモンストレーションの手順

受信のファイアウォール規則を作成する

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1、LON-SVR2、LON-CL1 を起動します。
2. LON-CL1 で、コマンド プロンプトを開き、次のコマンドを入力して、Enter キーを押します。

```
ping LON-SVR2
```

注 : 結果は、要求タイムアウトとなります。

3. LON-SVR2 に切り替え、Windows PowerShell ウィンドウを開き、次のコマンドレットを入力して、Enter キーを押します。

```
Test-Connection LON-DC1
```

注 : LON-DC1 への ping は成功します。

4. [スタート] をクリックし、[コントロール パネル] をクリックします。
5. [システムとセキュリティ]、[Windows ファイアウォール] の順にクリックします。
6. Windows Firewall ウィンドウで、左側の [詳細設定] リンクをクリックし、セキュリティが強化された Windows ファイアウォール管理コンソールを開きます。
7. [セキュリティが強化された Windows ファイアウォール (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、[受信の規則] をクリックします。

8. [受信の規則] を右クリックし、[新しい規則] をクリックします。
9. 新規の受信の規則ウィザードの [規則の種類] ページで、[カスタム]、[次へ] の順にクリックします。
10. [プログラム] ページで、[すべてのプログラム]、[次へ] の順にクリックします。
11. [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。
12. [スコープ] ページで、[次へ] をクリックします。
13. [操作] ページで、[接続を許可する]、[次へ] の順にクリックします。
14. [プロファイル] ページで、[次へ] をクリックします。
15. [名前] ページで、[名前] ボックスに「Allow Ping Rule」と入力し、[完了] をクリックします。
16. ナビゲーション ウィンドウで、[監視] を展開し、[ファイアウォール] をクリックします。
17. [Allow Ping Rule] が作成されたことを確認します。

受信のファイアウォール規則をテストする

1. LON-DC1 に切り替え、Windows PowerShell ウィンドウで、次のように入力し、Enter キーを押します。

```
ping LON-SVR2
```

注 : LON-SVR2 への ping は成功します。

送信のファイアウォール規則を作成する

1. LON-SVR2 に切り替え、[送信の規則] をクリックします。
2. [送信の規則] を右クリックし、[新しい規則] をクリックします。
3. 新規の送信の規則ウィザードの [規則の種類] ページで、[カスタム]、[次へ] の順にクリックします。
4. [プログラム] ページで、[すべてのプログラム]、[次へ] の順にクリックします。
5. [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。
6. [スコープ] ページで、[次へ] をクリックします。
7. [操作] ページで、[接続をブロックする]、[次へ] の順にクリックします。
8. [プロファイル] ページで、[次へ] をクリックします。
9. [名前] ページで、[名前] ボックスに「Prevent Ping Rule」と入力し、[完了] をクリックします。
10. ナビゲーション ウィンドウで、[監視] を展開し、[ファイアウォール] をクリックします。
11. [Prevent Ping Rule] が作成されたことを確認します。

送信のファイアウォール規則をテストする

1. Windows PowerShell ウィンドウで、次のように入力し、Enter キーを押します。

```
Test-Connection LON-DC1
```

注 : 結果は、[Test-Connection : コンピューター 'LON-DC1' への接続テストが失敗しました: Unknown error (0x2b2a).] となります。

ファイアウォール規則をリセットする

1. セキュリティが強化された Windows ファイアウォール管理コンソールに切り替え、ナビゲーション ウィンドウで、[セキュリティが強化された Windows ファイアウォール (ローカル コンピューター)] をクリックします。
2. [操作] ウィンドウで、[既定のポリシーの復元] をクリックします。
3. [セキュリティが強化された Windows ファイアウォール] ダイアログ ボックスで、[はい] をクリックし、[OK] をクリックします。
4. Windows PowerShell ウィンドウに切り替え、次のように入力し、Enter キーを押します。

```
Test-Connection LON-DC1
```

注 : LON-DC1 への ping は成功します。

レッスン 3
IPsec の構成

目次

質問と解答

質問 : あなたの環境で、IPsec を使用していますか。または、将来、使用しますか。

解答 : 解答はさまざまです。討論を開始するために、境界ゾーン システムまたはパブリック インターネットを通過する VPN トンネルに対して IPsec を使用することを提案できます。

参考資料

IPsec とは

参考資料 : 詳細については、次のサイトを参照してください。
What Is IPSec?
http://aka.ms/G0crt8

デモンストレーション : 接続セキュリティの規則の作成と構成

デモンストレーションの手順

ICMP トラフィックに対するファイアウォール規則を構成する

1. LON-SVR1 に切り替えます。
2. サーバー マネージャーを開き、[ツール]、[セキュリティが強化された Windows ファイアウォール] の順にクリックします。
3. セキュリティが強化された Windows ファイアウォール ウィンドウで、[受信の規則]、[新しい規則] の順にクリックします。
4. 新規の受信の規則ウィザードで、[カスタム]、[次へ] の順にクリックします。
5. [プログラム] ページで、[次へ] をクリックします。
6. [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。
7. [スコープ] ページで、[次へ] をクリックします。
8. [操作] ページで、[セキュリティで保護されている場合のみ接続を許可する]、[次へ] の順にクリックします。
9. [ユーザー] ページで、[次へ] をクリックします。
10. [コンピューター] ページで、[次へ] をクリックします。
11. [プロファイル] ページで、[次へ] をクリックします。
12. [名前] ページで、[名前] ボックスに「ICMPv4 allowed」と入力し、[完了] をクリックします。

サーバーの接続に関するサーバー間の規則を作成する

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 ウィンドウで、[接続セキュリティの規則] 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]、[次へ] の順にクリックします。
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、[受信接続と送信接続に対して認証を要求する]、[次へ] の順にクリックします。

5. [認証方法] ページで、[詳細設定]、[カスタマイズ] の順にクリックします。
6. [詳細な認証方法のカスタマイズ] ダイアログ ボックスで、[1 番目の認証方法] の [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、「secret」と入力して、[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] ページで、[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 に関するサーバー間の規則を作成する

1. LON-CL1 に切り替えます。
2. 必要に応じて、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。
3. Cortana に「Windows Firewall」と入力し、[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. [接続セキュリティの規則] を右クリックし、[新しい規則] をクリックします。
5. 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]、[次へ] の順にクリックします。
6. [エンドポイント] ページで、[次へ] をクリックします。
7. [要件] ページで、[受信接続と送信接続に対して認証を要求する]、[次へ] の順にクリックします。
8. [認証方法] ページで、[詳細設定]、[カスタマイズ] の順にクリックします。
9. [詳細な認証方法のカスタマイズ] ダイアログ ボックスで、[1 番目の認証方法] の [追加] をクリックします。
10. [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。
11. [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。
12. [認証方法] ページで、[次へ] をクリックします。
13. [プロファイル] ページで、[次へ] をクリックします。
14. [名前] ページで、[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. LON-CL1 で、コマンド プロンプトを開きます。
2. コマンド プロンプトで、「ping 172.16.0.11」と入力し、Enter キーを押します。
3. [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。
4. [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。
5. メイン モード ウィンドウで、表示された項目をダブルクリックします。
6. [メイン モード] の情報を確認し、[OK] をクリックします。
7. [クイック モード] をクリックします。
8. クイック モード ウィンドウで、表示された項目をダブルクリックします。
9. [クイック モード] の情報を確認し、[OK] をクリックします。

レッスン 4
データセンター ファイアウォール

目次

質問と解答

質問 : あなたの環境で、データセンター ファイアウォールや NSG を使用する計画がありますか。

解答 : 解答はさまざまです。ネットワークの複雑性により異なります。

演習の復習の質問と解答

演習 : セキュリティが強化された Windows ファイアウォールの構成

質問と解答

質問 : 特定のポートを使用する必要がある新しいアプリケーションを導入したいと考えています。セキュリティが強化された Windows ファイアウォールを構成するには、どのような情報が必要ですか。また、その情報をどこから取得できますか。

解答 : アプリケーションが使用するポートと IP アドレスを知る必要があります。それにより、セキュリティの脅威から保護しながら、アプリケーションを実行することができます。この情報はアプリケーションのベンダーから得ることができます。

質問 : 演習で、LON-CL1 は LON-SVR1 と LON-SVR2 に接続できるのに対して、LON-SVR2 は LON-SVR1 に接続できない理由を説明してください。

解答 : LON-SVR1 はサーバー分離用に構成されているため、IPsec を使用してネットワーク トラフィックを保護するコンピューターのみサーバーに接続することができます。LON-CL1 は Secure Clients OU に含まれるので Request Security ポリシーが適用されます。そのため、別のサーバーに接続する際は IPsec を要求します。LON-SVR2 にはセキュリティが構成されていないため、LON-CL1 は IPsec を使用せずに LON-SVR2 に接続することができます。LON-SVR2 はセキュリティを要求するように構成されておらず、LON-SVR1 はセキュリティで保護されていない接続はすべて拒否しているため、LON-SVR2 は LON-SVR1 に接続することはできません。

復習とまとめ

復習問題

質問 : 特定のポートでアプリケーションへのアクセスを許可するファイアウォール規則を構成する際、規則でどのネットワーク プロファイルを適用する必要がありますか。

解答 : トラフィックが発生するネットワーク プロファイルを適用する必要があります。

質問 : プライベート ネットワーク環境でデータセンター ファイアウォールを使用するメリットは何ですか。

解答 : 次のようなメリットがあります。

- Virtual Machine Manager と統合されたソフトウェア ベースのファイアウォール ソリューションを提供します。テナントまたは管理者により管理可能で、小規模および大規模な仮想マシンの展開に合わせてスケーリングできます。
- 仮想マシンに割り当てられたファイアウォール ポリシーは、仮想マシンが新しいホストに移動されると、仮想マシンと共に移動します。これが可能な理由は次のとおりです。
    - データセンター ファイアウォールは、vSwitch ホスト エージェント ファイアウォールとして展開される。
    - サービス プロバイダー テナントによって割り当てられたデータセンター ファイアウォール ポリシーは、テナントの他のファイアウォール設定から独立している。
    - 各 vSwitch ポートは、仮想マシンが稼働しているホストから独立して構成される。
- データセンター ファイアウォールは、テナントのゲスト オペレーティング システムから独立した保護機能をテナント仮想マシンに提供します。

質問 : どのようなシナリオで、IPsec を使用しますか。

解答 : 解答はさまざまです。次のようなシナリオで IPsec を使用することができます。

- 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
- L2TP の使用
- サイト間 (ゲートウェイ間) トンネリング
- 論理ネットワークの強制

質問 : 境界ネットワークのコンピューターと内部ネットワークのコンピューターの間をトラフィックが通過する際、トラフィックが暗号化され、認証されるようにする必要があります。境界ネットワークのコンピューターは、AD DS フォレストのメンバーではありません。これらの 2 台のコンピューター間で IPsec 規則を確立しようとする場合、どのような認証方法を使用できますか。

解答 : 境界コンピューターがフォレストにないため、Kerberos 認証を使用することはできません。そのため、証明書または事前共有キーは使用することができます。

第 13 章

ネットワーク トラフィックのセキュリティ保護

目次

レッスン 1
高度な DNS 設定の構成

目次

質問と解答

質問 : DNS ポリシーと RRL は、Windows Server 2016 の新機能です。あなたの環境では、これらの新機能をどのように使用しますか。

解答 : 解答はさまざまです。受講者のネットワーク セキュリティへの取り組み方法によって異なります。インターネットに接続する Windows DNS サーバーに関わる受講者は、通常、RRL を実装したいと考えます。

参考資料

DNS ポリシー

参考資料 : 詳細については、次のサイトを参照してください。
Set-DnsServerQueryResolutionPolicy
http://aka.ms/D9e1pv

デモンストレーション : DNSSEC の構成

デモンストレーションの手順

DNS コンソールでゾーン署名ウィザードを使用して DNSSEC を構成する

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1、LON-CL1 を起動します。
2. LON-DC1 で、サーバー マネージャーを起動し、[ツール] をクリックして、ドロップダウン リストで [DNS] をクリックします。
3. [DNS] で、[LON-DC1]、[前方参照ゾーン] の順に展開し、[Adatum.com] を右クリックします。
4. メニューで、[DNSSEC]、[ゾーンへの署名] の順にクリックします。
5. ゾーン署名ウィザードで、[次へ] をクリックします。
6. [ゾーン署名パラメーターをカスタマイズする] をクリックし、[次へ] をクリックします。
7. [キー マスター] ページで、[DNS サーバー LON-DC1 をキー マスターにする]、[次へ] の順にクリックします。
8. [キーを署名するキー (KSK)] ページで、[次へ] をクリックします。
9. [キーを署名するキー (KSK)] ページで、[追加] をクリックします。
10. [キーを署名するキー (KSK)] ページで、[OK] をクリックします。
11. [キーを署名するキー (KSK)] ページで、[次へ] をクリックします。
12. [ゾーンを署名するキー (ZSK)] ページで、[次へ] をクリックします。
13. [ゾーンを署名するキー (ZSK)] ページで、[追加] をクリックします。
14. [新しいゾーンを署名するキー (ZSK)] ページで、[OK] をクリックします。
15. [ゾーンを署名するキー (ZSK)] ページで、[次へ] をクリックします。
16. [Next Secure (NSEC)] ページで、[次へ] をクリックします。
17. [トラスト アンカー (TA)] ページで、[このゾーンに対するトラスト アンカーの配布を有効にする] チェック ボックスをオンにして、[次へ] をクリックします。

18. [署名とポーリングのパラメーター] ページで、[次へ] をクリックします。
19. [DNS セキュリティ拡張機能] ページで、[次へ] をクリックし、[完了] をクリックします。
20. DNS マネージャーで、[トラスト ポイント]、[com] の順に展開し、[Adatum] をクリックします。DNSKEY リソース レコードが存在し、その状態が有効であることを確認します。
21. サーバー マネージャーで、[ツール] をクリックし、ドロップダウン リストで [グループ ポリシーの管理] をクリックします。
22. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[Default Domain Policy] を右クリックして、[編集] をクリックします。
23. 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]、[ポリシー]、[Windows の設定] の順に展開し、[名前解決ポリシー] フォルダーをクリックします。
24. [規則の作成] セクションの [サフィックス] ボックスに「Adatum.com」と入力し、規則を名前空間のサフィックスに適用します。
25. [この規則で DNSSEC を有効にする] チェック ボックスと [DNS クライアントに、DNS サーバーで名前とアドレス データが検証されたことを確認するよう要求する] チェック ボックスをオンにし、[作成] をクリックします。
26. 下にスクロールして、[適用] をクリックします。
27. 開いているウィンドウをすべて閉じます。

デモンストレーション : DNS ポリシーと RRL の構成

デモンストレーションの手順

DNS ポリシーを構成する

1. LON-DC1 で、[スタート] をクリックし、[Windows PowerShell] をクリックします。
2. London のクライアント用の新しいクライアント サブネットを作成するために、Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerClientSubnet -Name "LondonSubnet" -IPv4Subnet "172.16.0.0/16" -PassThru
```

3. Paris のクライアント用の新しいクライアント サブネットを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerClientSubnet -Name "ParisSubnet" -IPv4Subnet "172.17.0.0/16" -PassThru
```

4. England 用の新しいゾーン スコープを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerZoneScope -ZoneName "adatum.com" -Name "adatum_england" -PassThru
```

5. France 用の新しいゾーン スコープを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerZoneScope -ZoneName "adatum.com" -Name "adatum_france" -PassThru
```

6. England の Web サーバーを検索するためのリソース レコードを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerResourceRecord -ZoneName "adatum.com" -A -Name "www" -IPv4Address 172.16.0.26 -ZoneScope "adatum_england" -PassThru
```

7. France の Web サーバーを検索するためのリソース レコードを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerResourceRecord -ZoneName "adatum.com" -A -Name "www" -IPv4Address 172.17.0.26 -ZoneScope "adatum_france" -PassThru
```

8. England の DNS ポリシーを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerQueryResolutionPolicy -Name "EnglandPolicy" -Action ALLOW -ClientSubnet 'eq,LondonSubnet' -ZoneScope 'adatum_england,1' -ZoneName "adatum.com" -PassThru
```

9. France の DNS ポリシーを作成するために、次のコマンドレットを入力し、Enter キーを押します。

```
Add-DnsServerQueryResolutionPolicy -Name "FrancePolicy" -Action ALLOW -ClientSubnet 'eq,ParisSubnet' -ZoneScope 'adatum_france,2' -ZoneName "adatum.com" -PassThru
```

10. 定義された DNS ポリシーを表示するために、次のコマンドレットを入力し、Enter キーを押します。

```
Get-DnsServerQueryResolutionPolicy -ZoneName adatum.com
```

11. 名前解決が機能していることを確認するために、次のコマンドレットを入力し、Enter キーを押します。

```
ping www.adatum.com
```

注 : アドレス www.adatum.com は、172.16.0.26 に解決されます。

12. 時間ベースのポリシーを構成するために、次のコマンドレットを入力し、午前 9 時から午後 5 時までの時間の 90 % で Paris が使用されるように時間の範囲を変更します。

```
Add-DnsServerQueryResolutionPolicy -Name AdatumPeakPolicy -Action ALLOW -ZoneScope 'adatum_england,1;adatum_france,9' -TimeOfDay 'EQ,09:00-17:00' -ZoneName adatum.com -ProcessingOrder 1 -PassThru
```

注 : 現在の時刻が -TimeofDay 値に含まれるようにします。

13. 名前解決をテストするに、次のコマンドを入力して、Enter キーを押します。

```
ping www.adatum.com
```

注 : 90 % の期間、アドレス www.adatum.com は、172.17.0.26 に解決されます。
最初にそのように解決されない場合、コマンド プロンプトで「ipconfig /flushdns」と入力して DNS キャッシュをフラッシュした後、再試行します。

RRL を構成する

1. 既定の設定で RRL を有効化するために、Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Set-DNSServerRRL
```

2. 確認のメッセージが表示されたら、「y」と入力し、Enter キーを押します。
3. 表示された警告を読みます。
4. RRL 設定を表示するために、次のコマンドレットを入力し、Enter キーを押します。

```
Get-DNSServerRRL | FL
```

5. 表示された RRL 設定を確認します。

レッスン 2
Message Analyzer によるネットワーク トラフィックの検査

目次

質問と解答

質問 : Message Analyzer は、次のどの種類の問題をトラブルシューティングする際に使用するのが最も有効ですか。

( ) ファイルに対するアクセス拒否

( ) 共有に対するアクセス拒否

( ) Web サイトに対するアクセス拒否

( ) 低速の接続

( ) 上記のすべて

解答 :

( ) ファイルに対するアクセス拒否

( ) 共有に対するアクセス拒否

( ) Web サイトに対するアクセス拒否

( ) 低速の接続

(√) 上記のすべて

フィードバック

Message Analyzer は、ネットワーク トラフィックのみではなく、Windows イベント ログとテキスト ベースのログ ファイルを含めて評価します。

デモンストレーション : Message Analyzer のインストール

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1、LON-CL1 を起動します。
2. LON-SVR1 に切り替えます。
3. [スタート] をクリックし、[エクスプローラー] をクリックします。エクスプローラーで、[PC]、[Allfiles (E:)]、[Labfiles] の順に展開し、[Mod13] フォルダーをクリックします。
4. [Mod13] フォルダーの [MessageAnalyzer64.msi] をダブルクリックします。
5. Microsoft Message Analyzer Setup ウィザードの [Welcome to the Microsoft Message Analyzer Setup Wizard] ページで、[Next] をクリックします。
6. [End-User License Agreement] ページで、[I accept the terms in the License Agreement] チェック ボックスをオンにし、[Next] をクリックします。
7. [Microsoft Message Analyzer Optimization] ページで、[Next] をクリックします。
8. [Ready to install Microsoft Message Analyzer] ページで、[Install] をクリックします。
9. [Completed the Microsoft Message Analyzer Setup Wizard] ページで、[Finish] をクリックします。
10. インストールが完了したら、開いているすべてのウィンドウを閉じて、LON-SVR1 を再起動します。
11. サーバーが再起動したら、ユーザー名「Adatum¥Administrator」、パスワード「Pa55w.rd」を使用してサインインします。

デモンストレーション : Message Analyzer によるトラフィックのキャプチャと分析

デモンストレーションの手順

暗号化されていないネットワーク トラフィックをキャプチャする

1. LON-SVR1 で、[スタート] をクリックし、[Microsoft Message Analyzer] フォルダーを展開し、[Microsoft Message Analyzer] をクリックします。
2. [Welcome to Microsoft Message Analyzer] ダイアログ ボックスで、[Do not update items] と [No, I do not want to participate] の両方を選択して、[OK] をクリックします。
3. スタート ページを確認し、[Start Local Trace] をクリックします。
4. キャプチャが開始されたら、LON-CL1 に切り替えます。
5. LON-CL1 で、[スタート] をクリックして、「¥¥lon-svr1¥e$¥Labfiles¥Mod13」と入力し、Enter キーを押します。
6. MessageAnalyzer64.msi ファイルをローカル デスクトップにコピーします。
7. LON-SVR1 に切り替えます。
8. Microsoft Message Analyzer で、[Session]、[Stop] の順にクリックします。

分析ツールを検証する

1. [Filter] フィールドに次を入力し、[Apply] をクリックします。

```
*address==172.16.0.40
```

2. [Module] ヘッダーをクリックして、モジュールごとに並べ替えます。

注 : モジュール名をポイントすると、ツール ヒントにより正式名称が表示されます。

3. [Module] 列に [SMB2] が表示されるまで、下にスクロールします。
4. [Module] 列の [SMB2] を右クリックし、[Add 'Module' to Filter] をクリックして、フィルターを追加します。
5. フィルターの [OR] を [AND] に変更し、[Apply] をクリックします。
6. SMB2 トラフィックを確認します。

グループ ポリシー オブジェクト (GPO) で IPsec を有効にする

1. LON-DC1 でサーバー マネージャーを開きます。
2. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
3. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[Default Domain Policy] を右クリックして、[編集] をクリックします。
4. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に展開し、[IP セキュリティ ポリシー] をクリックします。
5. [Server (Request Security)] を右クリックし、[割り当て] をクリックします。
6. 開いているウィンドウをすべて閉じます。
7. LON-SVR1 に切り替えます。
8. [スタート] をクリックし、[Windows PowerShell] をクリックします。

9. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate /force
```

10. 更新が完了したら、Windows PowerShell ウィンドウを閉じます。
11. LON-CL1 に切り替えます。
12. [スタート] をクリックし「PowerShell」と入力して、[Windows PowerShell] をクリックします。
13. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate /force
```

14. 更新が完了したら、開いているウィンドウをすべて閉じます。

暗号化されたネットワーク トラフィックをキャプチャする

1. LON-SVR1 の [Global] ツール バーで [New Session] をクリックします。
2. [New Session] ダイアログ ボックスで、[Live trace]、[Select Scenario]、[Local Network Interfaces (Win 8.1 and later)] の順にクリックします。
3. [Start] をクリックします。
4. キャプチャが開始されたら、LON-CL1 に切り替えます。
5. LON-CL1 で、[スタート] をクリックし「¥¥lon-svr1¥e$¥Labfiles¥Mod13」と入力して、Enter キーを押します。
6. MessageAnalyzer64.msi ファイルをローカル デスクトップにコピーします。ダイアログ ボックスが表示されたら、デスクトップのファイルの置換を選択します。
7. LON-SVR1 に切り替えます。
8. Microsoft Message Analyzer で、[Session]、[Stop] の順にクリックします。

分析ツールを検証する

1. [Filter] フィールドに次を入力し、[Apply] をクリックします。

```
*address==172.16.0.40
```

2. [Module] ヘッダーをクリックして、Module ごとに並べ替えます。
3. 開いているウィンドウをすべて閉じます。

GPO で IPsec を無効にする

1. LON-DC1 でサーバー マネージャーを開きます。
2. サーバー マネージャーで、[ツール]、[グループ ポリシーの管理] の順にクリックします。
3. グループ ポリシーの管理コンソールで、[フォレスト : Adatum.com]、[ドメイン]、[Adatum.com] の順に展開し、[Default Domain Policy] を右クリックして、[編集] をクリックします。
4. グループ ポリシー管理エディターで、[コンピューターの構成]、[ポリシー]、[Windows の設定]、[セキュリティの設定] の順に展開し、[IP セキュリティ ポリシー] をダブルクリックします。
5. [Server (Request Security)] を右クリックし、[割り当ての解除] をクリックします。
6. 開いているウィンドウをすべて閉じます。
7. LON-SVR1 に切り替えます。
8. [スタート] をクリックし、[Windows PowerShell] をクリックします。

9. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate /force
```

10. 更新が完了したら、開いているウィンドウをすべて閉じます。
11. LON-CL1 に切り替えます。
12. Cortana に「Windows PowerShell」と入力して、[Windows PowerShell] をクリックします。
13. Windows PowerShell ウィンドウで、次のコマンドを入力し、Enter キーを押します。

```
gpupdate /force
```

14. 更新が完了したら、開いているウィンドウをすべて閉じます。

レッスン 3
SMB トラフィックのセキュリティ保護と分析

目次

質問と解答

質問 : 環境で SMB 1.x を有効にしたままにすると、どのようなリスクを伴いますか。

解答 : SMB 1.x は、安全なプロトコルではありません。SMB 1.x が環境で有効にされていると、SMB 1.x を悪用する攻撃に対して脆弱になる可能性があります。

参考資料

SMB 3.1.1 プロトコル セキュリティの理解

参考資料 : 詳細については、次のサイトを参照してください。
Microsoft Open Specifications Support Team Blog
http://aka.ms/Aldg7y

デモンストレーション : SMB 1.0 の無効化と共有での SMB 暗号化の構成

デモンストレーションの手順

Windows 10 で SMB 1.x を無効にする

1. LON-CL1 に切り替えます。
2. [スタート] をクリックし「Windows PowerShell」と入力して、[Windows PowerShell] をクリックします。
3. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

4. メッセージ ダイアログが表示されたら、「Y」と入力し、Enter キーを押します。
5. 開いているウィンドウをすべて閉じます。

Windows Server 2016 で SMB 1.x を無効にする

1. LON-SVR1 に切り替えます。
2. [スタート] をクリックし、[Windows PowerShell] をクリックします。
3. Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押します。

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

4. メッセージ ダイアログが表示されたら、「Y」と入力し、Enter キーを押します。

暗号化された SMB 共有を構成する

1. LON-SVR1 で、Windows PowerShell ウィンドウで、次のコマンドレットを入力し、Enter キーを押して、暗号化された共有を作成します。

```
New-SmbShare -Name “Mod13” -Path "E:¥Labfiles¥Mod13" -EncryptData $true
```

2. 共有のフル コントロールのアクセス許可を Everyone に付与するために、次のコマンドレットを入力し、Enter キーを押します。

```
Grant-FileShareAccess -Name Mod13 -AccountName "Everyone" -AccessRight Full
```

暗号化された SMB トラフィックをキャプチャする

1. LON-SVR1 で、[スタート] をクリックし、[Microsoft Message Analyzer] フォルダーを展開し、[Microsoft Message Analyzer] をクリックします。
2. スタート ページで、[Start Local Trace] をクリックします。
3. キャプチャが開始されたら、LON-CL1 に切り替えます。
4. LON-CL1 で、[スタート] をクリックし「¥¥lon-svr1¥Mod13」と入力して、Enter キーを押します。
5. MessageAnalyzer64.msi ファイルをローカル デスクトップにコピーします。ダイアログ ボックスが表示されたら、デスクトップのファイルの置換を選択します。
6. LON-SVR1 に切り替えます。
7. Microsoft Message Analyzer で、[Session]、[Stop] の順にクリックします。

分析ツールを検証する

1. [Filter] フィールドに次を入力し、[Apply] をクリックします。

```
(*address==172.16.0.40) and (SMB2)
```

2. [Summary] ヘッダーをクリックして、モジュールごとに並べ替えます。
3. 最も多くキャプチャされたトラフィックは、[TransformMessage, Encrypted] であることを確認します。

演習の復習の質問と解答

演習 A : DNS のセキュリティ保護

質問と解答

質問 : メイン モード監視でのみ、暗号化が使用中であることが表示された理由は何ですか。

解答 : 暗号化が ICMPv4 プロトコルに対してのみ構成され、クイック モードのセッションでは ICMPv4 を使用しないためです。

質問 : DNSSEC で使用するために、個別のゾーンを作成する理由は何ですか。

解答 : 解答はさまざまです。理由の 1 つとして、異なるゾーンに対して異なる設定を可能にし、1 つのゾーンが侵害された場合に、他のゾーンが必ずしも侵害されないようにすることが挙げられます。

演習 B : Microsoft Message Analyzer と SMB 暗号化

質問と解答

質問 : IPsec がすべてのトラフィックに適用された状態で、ネットワーク キャプチャにより、トラフィックの目的に関する手掛かりが得られますか。

解答 : いいえ、IPsec で保護されたすべてのトラフィックは、ESP トラフィックとして表示され、パケット内に含まれるものについての表示はありません。

質問 : あなたの環境では、IPsec と SMB 3.1.1 暗号化のどちらの方法がより良く機能しますか。

解答 : 解答はさまざまです。IPsec を構成して、すべてのネットワーク トラフィックを暗号化することができます。一方、SMB 3.1.1 では、Windows 10 または Windows Server 2016 の共有からの SMB トラフィックのみを暗号化します。

復習とまとめ

復習問題

質問 : どのようなシナリオで、トラブルシューティング ツールとして Message Analyzer の使用を考慮しますか。

解答 : 解答はさまざまです。Message Analyzer を使用して、不正なネットワーク トラフィックを特定し、アプリケーションやネットワークの問題をトラブルシューティングできます。

質問 : SMB 1.0 通信を無効化した場合、どのようなリスクがありますか。この古いプロトコルを無効化しない場合、どのようなリスクがありますか。

解答 : SMB 1.0 は、SMB 3.0 以降のようなセキュリティへの配慮を含まずに開発された古いプロトコルです。SMB 1.0 では暗号化を強制しないため、セキュリティが低くなります。ただし、一部の古いアプリケーションにはこのプロトコルが必要な場合があるため、SMB 1.0 を無効化すると、それらのアプリケーションは機能しません。SMB 1.0 を無効化しない場合、SMB 3.0 以降で利用可能なセキュリティ機能を使用できません。

第 14 章

Windows Server の更新

目次

レッスン 1
WSUS の概要

目次

質問と解答

質問 : WSUS で更新できる製品は、次のうちどれですか。

(　) Microsoft Visual Studio 2010

(　) Microsoft Security Essential

(　) Microsoft Office 2010

(　) Microsoft Silverlight

(　) Windows RT

解答 :

(√) Microsoft Visual Studio 2010

(√) Microsoft Security Essential

(√) Microsoft Office 2010

(√) Microsoft Silverlight

(√) Windows RT

フィードバック

WSUS は、広範な Microsoft 製品をサポートします。

参考資料

WSUS サーバーの展開オプション

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

レッスン 2
WSUS による更新プログラムの展開

目次

質問と解答

質問 : 自社の WSUS 環境で複数のコンピューター グループを使用していますか。

解答 : 解答はさまざまです。更新プログラムを手動でテストし、承認してから自動的に展開する場合もあれば、広範囲への自動展開をおこなう前に、テスト用の自動展開を使用する場合もあります。

参考資料

WSUS のトラブルシューティング

 **参考資料 :** 詳細については、次のサイトを参照してください。
Windows Server Update Services Tools and Utilities
http://aka.ms/Erqdqk

デモンストレーション : WSUS による更新プログラムの承認

デモンストレーションの手順

1. LON-DC1 を起動します。この仮想マシンが起動したら、LON-SVR1 を起動します
2. LON-SVR1 で、[スタート]、[Windows 管理ツール]、[Windows Server Update Services] コンソールの順にクリックします。
3. [Windows Server Update Services] で、[LON-SVR1]、[更新プログラム] の順に展開し、[重要な更新プログラム] をクリックし、[状態] ドロップダウン リストで [すべて] を選択し、[最新の情報に更新] をクリックします。
4. [Windows 10 Version 1607 for x64-based Systems 用更新プログラム (KB3199209)] を右クリックし、[承認] をクリックします。
5. 更新プログラムの承認ウィンドウで、[すべてのコンピューター] ドロップダウン リストから [インストールの承認] を選択します。
6. [OK] をクリックし、[閉じる] をクリックします。
7. [承認] 列に [インストール] と表示されることを確認します。
8. Update Services コンソールを閉じます。

演習の復習の質問と解答

演習 : 更新管理の実装

質問と解答

質問 : Research 部門用に個別のグループを作成しました。組織のコンピューターの一部のために、個別のグループを構成した理由は何ですか。

解答 : Research 部門には、組織の他の部門とは異なる更新プログラムのテストと承認のプロセスが必要な、特別な考慮事項やセキュリティ プラクティスがある場合があります。さらに、他の部門には、更新プログラムの承認プロセスの管理責任を委任済みの管理者がいる可能性があります。

質問 : ダウンストリーム WSUS サーバーを構成するメリットは何ですか。

解答 : メイン WSUS サーバーとダウンストリーム WSUS サーバーが低速のワイド エリア ネットワーク (WAN) 接続でリンクされている場合、メイン WSUS サーバーから WAN 接続を介して、各クライアント コンピューターが個別に更新プログラムをダウンロードするのではなく、ダウンストリーム WSUS サーバーがサービス対象のクライアント コンピューター向けに更新プログラムを 1 度だけダウンロードします。

復習とまとめ

復習問題

質問 : 更新プログラムがリリースされた場合、Windows オペレーティング システムへの更新プログラムをすべて自動で適用する必要があるかどうかを尋ねられました。別の方法を勧めますか。

解答 : 運用環境で適用する前に、すべての更新プログラムをテストする必要があります。つまり、WSUS を使用して、まず、一連のテスト コンピューターに更新プログラムを展開する必要があります。

質問 : 組織は、Microsoft 以外のいくつかのアプリケーションを実装しています。同僚は、WSUS を使用してアプリケーションとオペレーティング システムの更新プログラムを展開することを提案しています。WSUS を使用する場合、潜在的な問題がありますか。

解答 : はい。WSUS は、Microsoft Office System などの Microsoft アプリケーション用の更新プログラムや Windows オペレーティング システムの更新プログラムを展開するための優れたツールです。ただし、WSUS では、すべての Microsoft アプリケーション用の更新プログラムを展開する訳ではありません。また、Microsoft 以外のアプリケーション用の更新プログラムは展開しません。Microsoft 以外のアプリケーション用の更新プログラムを展開する必要がある場合、Microsoft System Center 2012 Configuration Manager が適しています。

質問 : WSUS を Active Directory ドメイン サービス (AD DS) ドメインで管理する方が容易な理由は何ですか。

解答 : WSUS では、グループ ポリシーを介してクライアント設定を展開するために、AD DS の組織単位 (OU) 構造を活用します。また、グループ ポリシー設定を使用して、クライアント側のターゲット設定を構成し、クライアント コンピューターの WSUS グループ メンバーシップを決定することもできます。

ツール

次の表で、この章で必要なツールを示します。

ツール	用途	アクセス方法
WSUS 管理コンソール	WSUS の管理	[サーバー マネージャー] の [ツール]
Windows PowerShell WSUS コマンドレット	コマンド ライン インターフェイスからの WSUS の管理	Windows PowerShell