Active Directory セキュリティ評価 : 前提条件および構成

このドキュメントでは、Azure Log Analytics ワークスペースと資格が与えられている Microsoft オンデマンド評価に含まれている Active Directory セキュリティ (ADS) 評価の構成に必要な手順を説明します。

このドキュメントには、評価のセットアップ　タスクを実行する前に完了させる構成とセットアップのタスクがあります。すべての事前作業については、Services Hub リソース センターの オンデマンド評価の概要 に従ってください。

目次

システム要件および構成の概要

使用するシナリオに従って、次の詳細を確認し、必要な要件を満たしていることを確かめてください。

サポートされるターゲット オペレーティング システムのバージョン

- Active Directory ドメイン コントローラーは、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、または Windows Server 2019 を実行する必要があります。

環境関連の許可

- 評価アカウントの権利:
    - ドメイン アカウント（ユーザーまたは管理されたサービス アカウントの場合もあります）には、次の権利が含まれます:
        - エンタープライズ管理者
        - フォレスト内にある各ドメイン コントローラーへの管理アクセス
        - ドメイン コントローラーが参加するすべての Microsoft ドメイン ネーム システム (DNS) サーバーに対する管理アクセス
        - データ収集マシンの管理者のアクセス
        - データ収集マシンに対するバッチ ジョブ特権としてのログオン

データ収集マシン

- データ収集マシンは、評価されるフォレストのドメインのいずれかに参加している必要があります。
- データ収集マシンのハードウェア: 最小 16 ギガバイト（GB）のRAM、2 ギガヘルツ（GHz デュアル コア プロセッサ）、最小 10 GB の空きディスク領域。Active Directory 内の 100万オブジェクトごとに、追加で 4 GB の RAM が推奨されます。
- データ収集マシンは、フォレスト内にあるすべてのドメイン コントローラーに接続して、そこから情報を取得するために使用されます。マシンは、リモート プロシージャ コール (RPC)、サーバー メッセージ ブロック (SMB)、WMI、リモート レジストリ、ライトウェイト ディレクトリ アクセス プロトコル (LDAP)、および Distributed Component Object Model (DCOM) を介して通信しています。
- Microsoft .NET Framework 4.6.2 以降がインストール済み、および Windows Server 2012 R2 以降を実行しています。
- このドキュメントの最初の展開シナリオのいずれかでは、データ収集マシンで、インストールおよび構成された Microsoft Monitoring Agent を使用する必要があります。

PowerShell のリモート処理

正確な結果で評価を完了させるには、PowerShell のリモート処理の範囲内のターゲット マシンすべてを構成する必要があります。

ツール マシン上の PowerShell は、監視ポリシーの構成、およびインストールされたセキュリティ修正プログラムをスキャンするために使用されます。

- Windows Update Agent は、セキュリティ更新プログラムのスキャンを取得するために、すべてのドメイン コントローラーで実行されている必要があります
- ターゲット ドメイン コントローラーでは PowerShell バージョン 2 以上が必要となり、Windows Server 2008 R2 が起動すると既定でインストールされます。PowerShell バージョン 2 がインストールされていない場合は、こちらからダウンロードできます: https://aka.ms/wmf3download

Windows Server 2012-2012 R2（または、既定を変更している場合はそれ以降）ターゲット マシンの追加要件:

データ収集をサポートするには、ターゲット ドメイン コントローラーで次の 3 つの項目を構成する必要があります: PowerShell のリモート処理、WinRM サービスとリスナー、およびファイアウォールの受信許可規則。

注 1: *Windows Server 2012 R2 および Windows Server 2016 では、既定で WinRM および PowerShell リモート処理が有効になっています。以下で詳しく説明されている次の構成手順は、ターゲット　マシンの既定の構成が変更されている場合のみ、実装される必要があります。*

注 2: *Windows Server 2012 では、既定で WinRM が無効になっています。PowerShell のリモート処理をサポートするには、以下の設定を構成する必要があります:*

- 評価範囲内の各ターゲット マシンで **Enable-PSRemoting** Powershell コマンドレットを実行します。このコマンド 1 つで、Powershell　のリモート処理、WinRM　サービスおよびリスナーが構成され、必要なファイアウォールの受信規則が有効になります。Enable-PSRemoting によって実行されるすべてが文書化されている詳細な説明は、こちらです。

または

- グループ ポリシーを介して **WinRM / PowerShell のリモート処理**を構成します（コンピューターの設定¥ポリシー¥管理用テンプレート¥Windows コンポーネント¥Windows リモート管理 (WinRM)¥WinRM サービス）
    - 2012（および以降）では、“**WinRM 経由のリモート サーバー管理を許可します**“
- グループ ポリシーを介して**自動起動の WinRM サービス**を構成します（コンピューターの構成¥ポリシー¥Windows の設定¥セキュリティの設定¥システム サービス）
    - **自動スタートアップ モードの Windows リモート管理** (WS 管理) サービスを定義**します**
- **ファイアウォールの受信許可規則**の構成: この操作は、各範囲内のターゲット ドメイン コントローラーのローカルのファイアウォール ポリシー、またはツール マシンからの通信を許可するグループ ポリシーを介して個別に実行できます。

グループ ポリシーを構成し、WinRM リスナーと必要なファイアウォールの受信許可規則の両方を有効にするには、次の 2 つの手順を実行します:

A) データ収集の発生元となるソース コンピューターの IP アドレスを特定します。

B) ドメイン コントローラーの組織単位にリンクされた新しい GPO を作成し、ツール マシンの受信規則を定義します

A.）選択したデータ収集マシンにログインし、コマンド プロンプトから IPConfig.exe を実行して、そのマシンの現在の IP アドレスを特定します。

出力の一例は、次の通りです

C:¥>ipconfig

Windows IP の構成

イーサネット アダプター イーサネット:

接続固有 DNS サフィックス:

リンクローカル IPv6 アドレス . . : fe80::X:X:X:X%13

IPv4 アドレス . . . . . : X.X.X.X

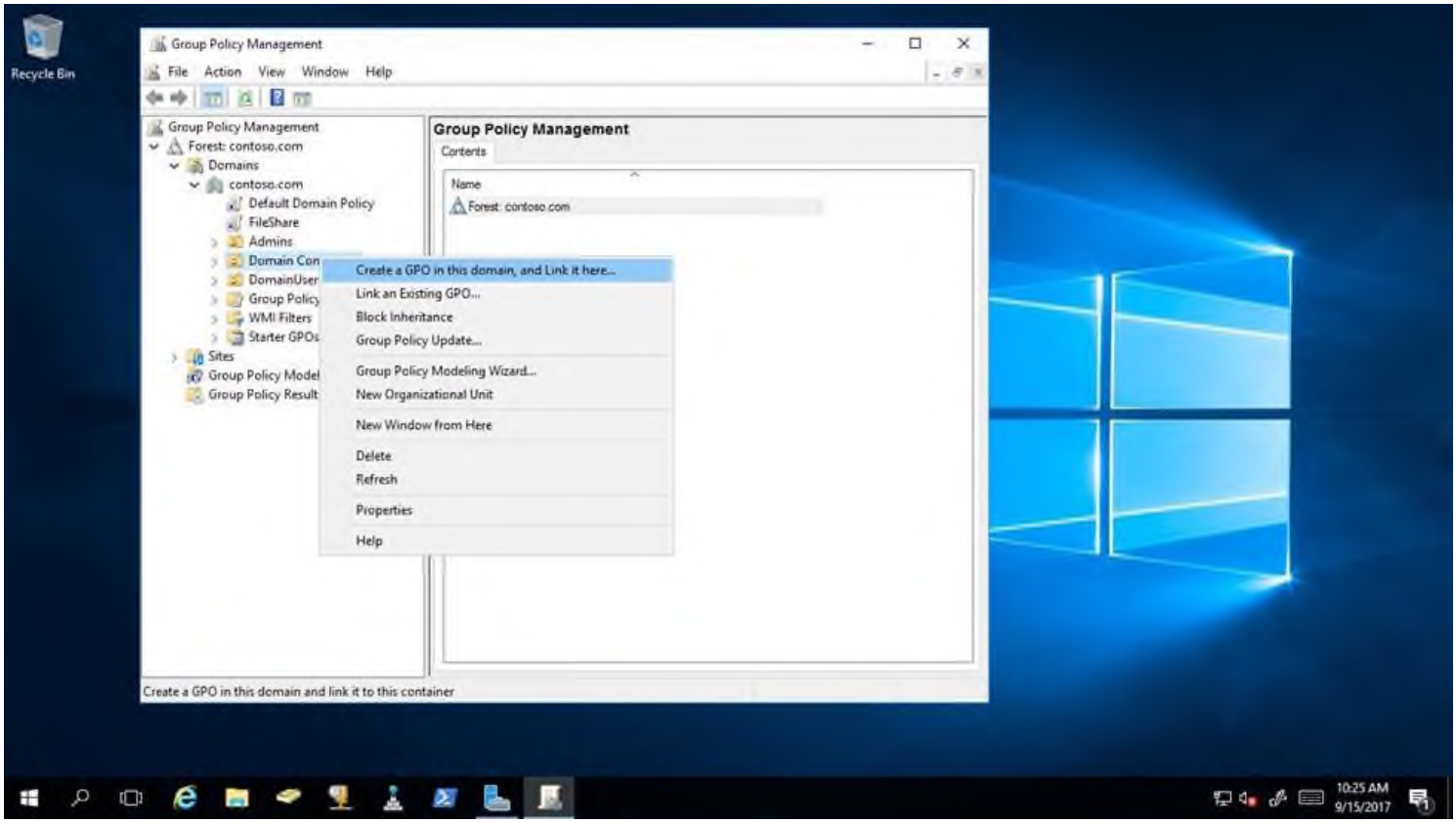
サブネット マスク . . . . . : X.X.X.X

デフォルト ゲートウェイ . . . . . : X.X.X.X

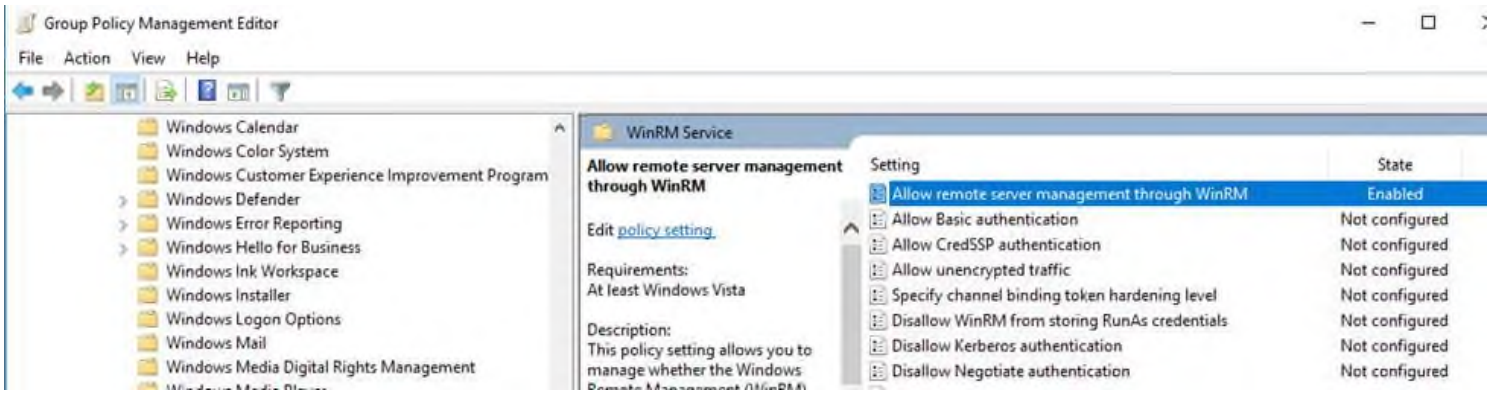
マシンの IPv4 アドレスをメモします。構成の最後の手順では、このアドレスを使用して、データ**収集マシンのみがドメイン コントローラーで Windows Update エージェントと通信できることを確認します。**

B.）グループ ポリシー オブジェクトを作成および構成して、フォレスト内の各ドメインのドメイン コントローラー OU にリンクさせます。

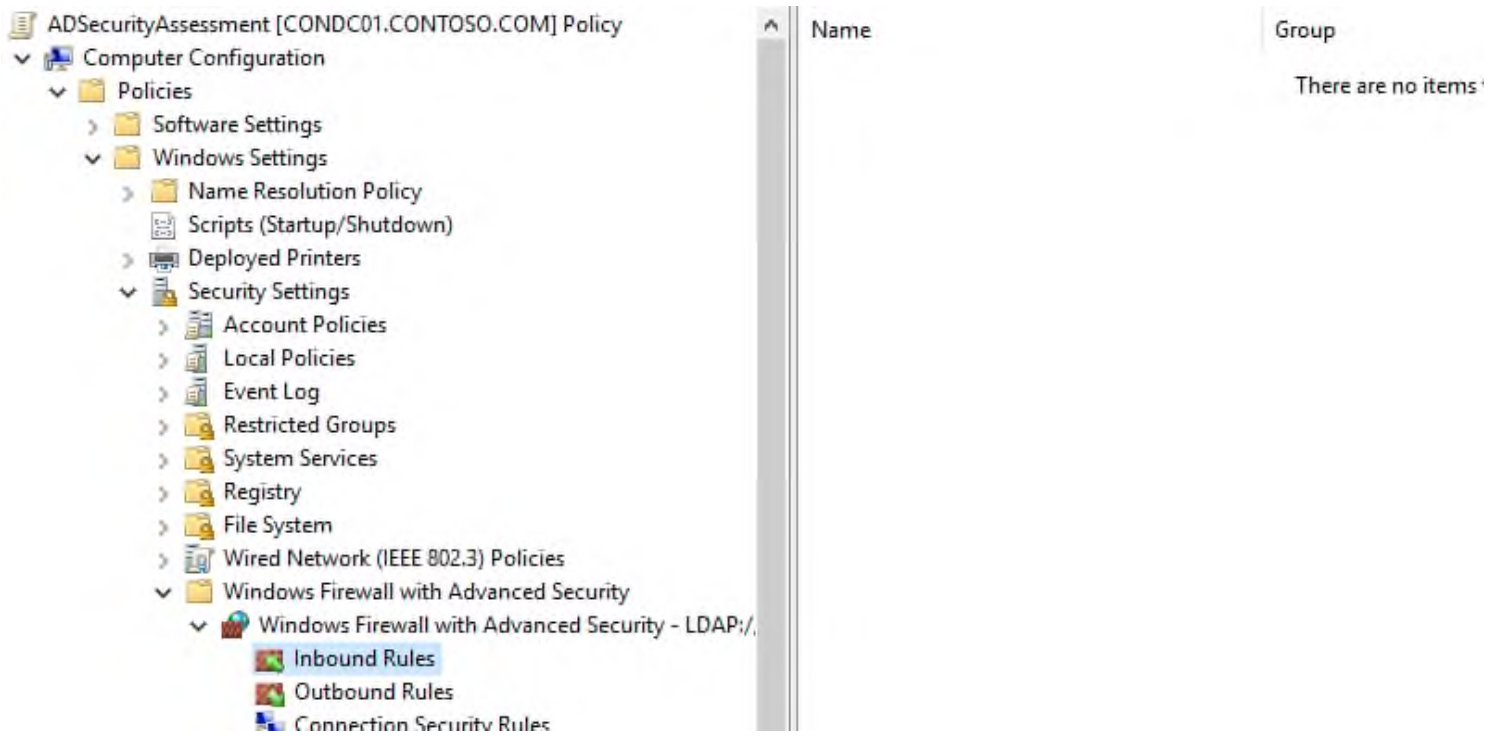
1. **新しい GPO を作成します。GPO がドメイン コントローラーの組織単位に適用されていることを確認します。**グループ ポリシーの名前付け規則、または "AD セキュリティ評価" のようにその目的を識別するものに基づいて、**新しいグループ ポリシーに名前を付けてください。**



2. GPO 内で次を開きます: (コンピューターの構成¥ポリシー¥管理用テンプレート¥Windows コンポーネント¥Windows リモート管理 (WinRM)¥WinRM サービス)。OS に応じて、“WinRM 経由のリモートサーバー管理を許可する“ または “リスナーの自動構成を許可する“ を有効にします。



3. 詳細な受信ファイアウォール規則を作成して、データ収集マシンとドメイン コントローラー間のすべてのネットワーク トラフィックを許可します。これは、上記の手順 1 で使用した同じ GPO に適用できます。(コンピューターの構成¥ポリシー¥Windows の設定¥セキュリティの設定¥セキュリティが強化された Windows ファイアウォール¥セキュリティが強化された Windows ファイアウォール - LDAP:/xxx¥受信規則)



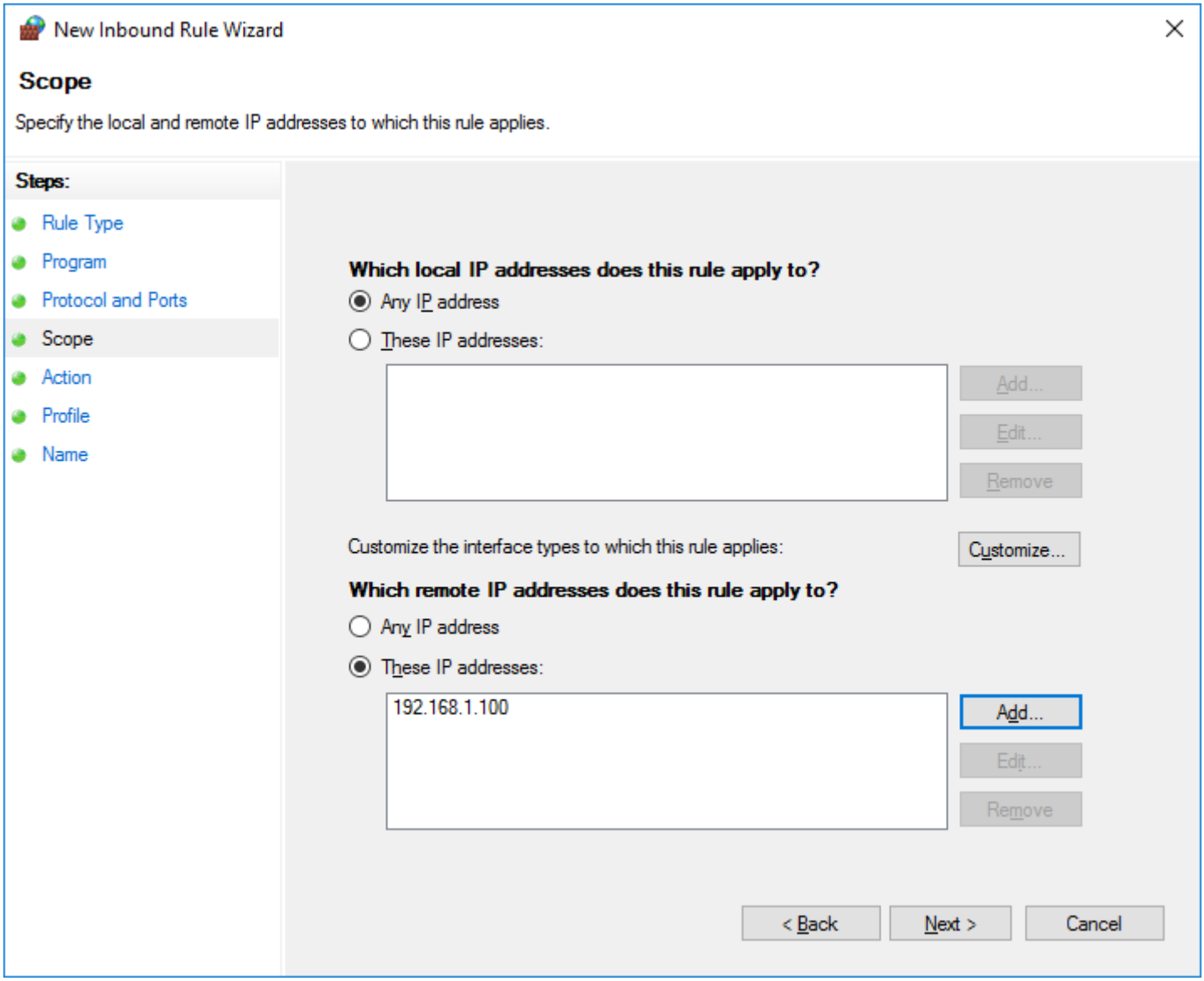
4. 新しい規則を作成するには、[受信規則] をクリックし、[新規] を選択します

5. **規則の種類** ページで、**カスタム**規則を選択し、[次へ] を選択します

6。 **プログラム** ページで、ツール マシンから [**すべてのプログラム**] を選択し、[次へ] をクリックします。

7. **プロトコルとポート** ページで、**任意**のプロトコルと**すべて**のポートが選択されていることを確認し、[次へ] をクリックします。

8. スコープ ページでは、スコープ ページの [**この規則を適用するリモート IP アドレスを選択してください。**] の部分でデータ収集マシンの IP アドレスを指定し、[**次へ**] を選択します。



9. **操作**ページで、[接続を許可] を選択し、[次へ] をクリックします。
10. **プロファイル** ページで、ネットワーク プロファイルの [**ドメイン**] を選択し、[次へ] をクリックします。
11. 規則の名前 (例: ADSecurityAssessmentToolsMachine) を選択し、ウィザードを完了します。

Active Directory セキュリティ評価のセットアップ

Microsoft Monitoring Agent/OMS Gateway のインストールを完了したら、Active Directory セキュリティ評価をセットアップする準備は整っています。スケジュールされたタスクのアカウントが管理されたサービス アカウントかユーザー アカウントかに応じて、スケジュールされたタスクを評価する方法が 2 つあります。

管理されたサービス アカウントで構成する

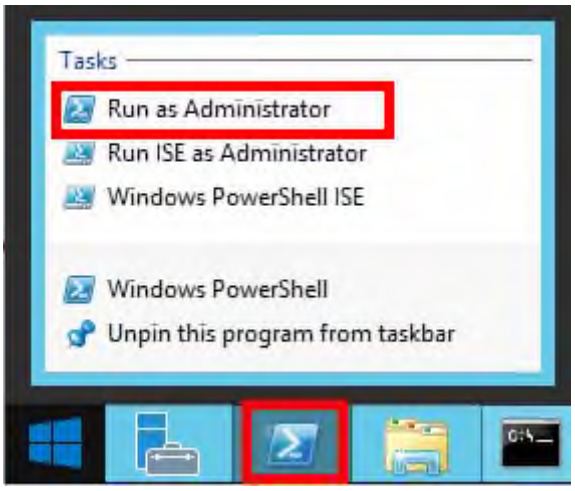
管理されたサービス アカウントは、標準ユーザー アカウントに対しての資格情報の管理とセキュリティに関連する利点により、評価の実行の推奨オプションです。管理されたサービス アカウントは、Active Directory ドメイン サービスでプロビジョニングされ、その環境で承認される必要があります。

1) プロビジョニング KB 記事にある手順に従ってください。

2) このドキュメントの環境関連の許可セクションに基づいて必要な環境アクセスを使用し、アカウントを承認します。

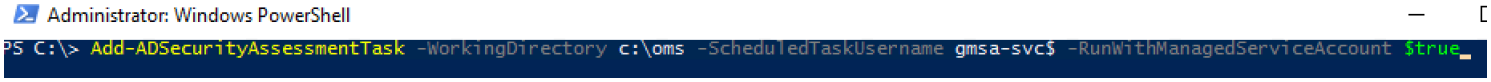
指定されたデータ収集マシンで次の手順を実行します:

1. Windows PowerShell コマンド プロンプトを管理者として開きます

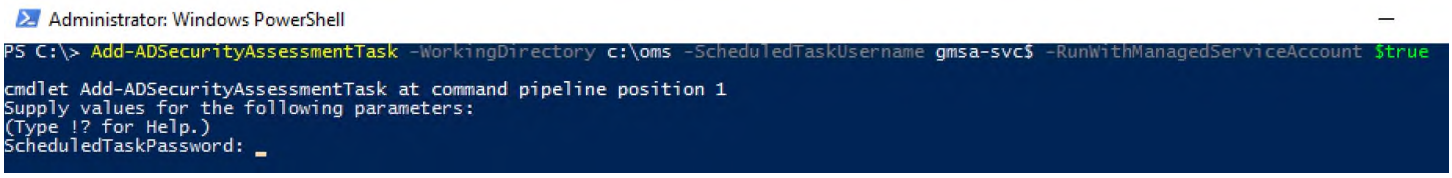


2. **Add-ADSecurityAssessmentTask -WorkingDirectory <Directory> -ScheduledTaskUsername <MSAname> -RunWithManagedServiceAccount $True** コマンドを実行します。このコマンドでは、<Directory> が環境からのデータを収集および分析している間に作成されたファイルを保存するために使用する既存のディレクトリへのパスになり、<MSAname> がプロビジョニングおよび承認済みの管理されたサービス アカウントの SAMアカウント名 ($ 記号で終わる) になります。

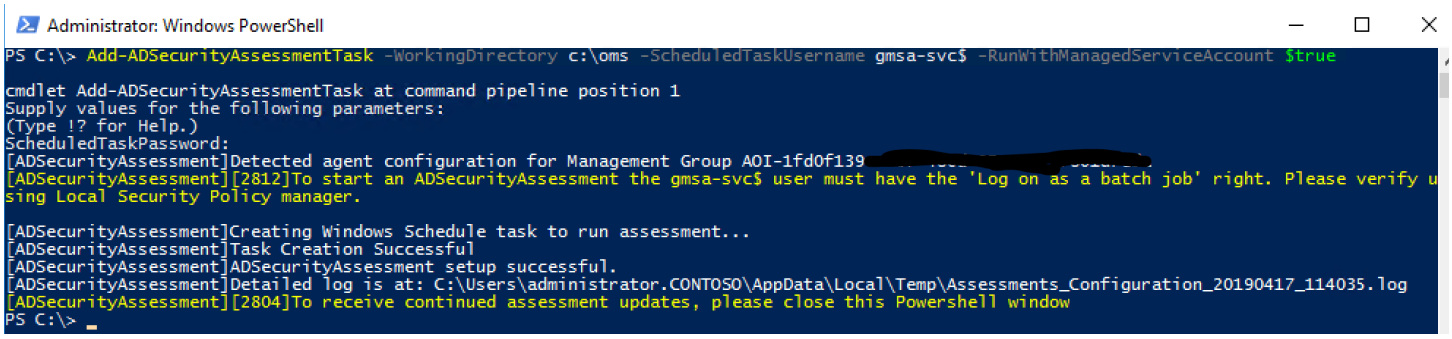
   注意:コマンド **Add-ADSecurityAssessmentTask** が利用できない場合は、モジュールがまだ見つかっていません。エージェントのインストール後、表示されるまでに時間がかかることがあります。



3. Add-ADSecurityAssessmentTask は、MSA パスワードの入力を求めるプロンプトを表示します。管理されたサービス アカウントの資格情報の管理は Active Directory または承認されたコンピューターを介して処理されるため、このプロンプトでの入力は任意のもの、または入力なしでもかまいません。



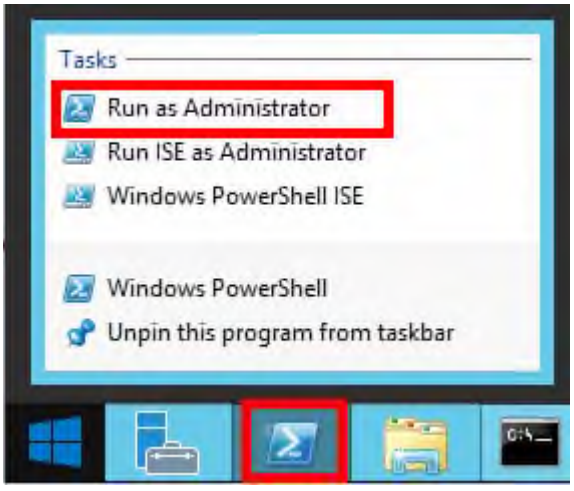
4. 必要な構成に基づいてスクリプトが続行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。



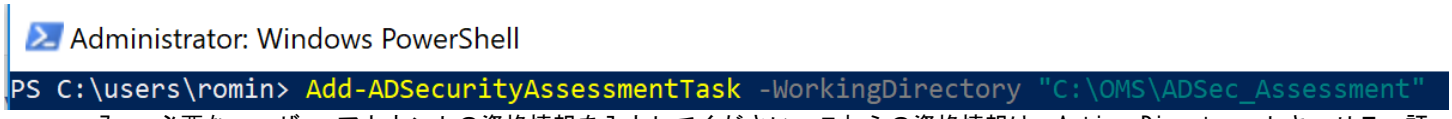
ユーザー アカウントで構成する

指定されたデータ収集マシンで次の手順を実行します:

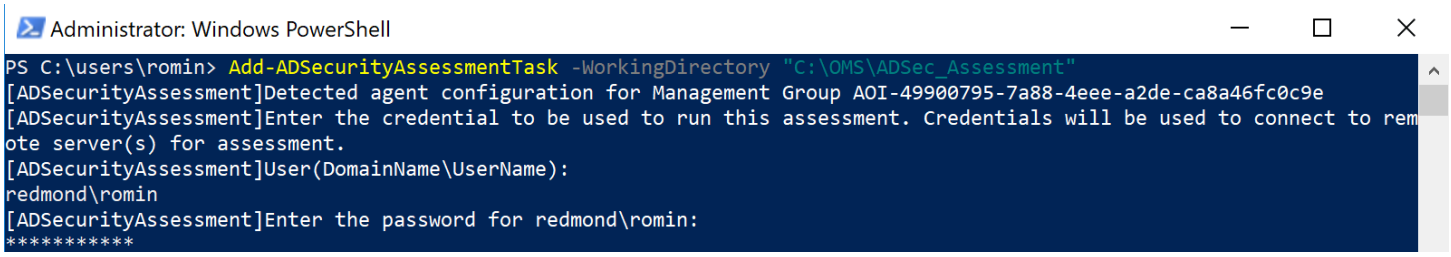
5. Windows PowerShell コマンド プロンプトを管理者として開きます



6。 Add-ADSecurityAssessmentTask コマンドを実行します。この場合、<Directory> が環境からデータを収集および分析している間に作成されたファイルを保存するために使用する既存のディレクトリへのパスになります。



7. 必要なユーザー アカウントの資格情報を入力してください。これらの資格情報は、Active Directory セキュリティ評価を実行するために使用されます。



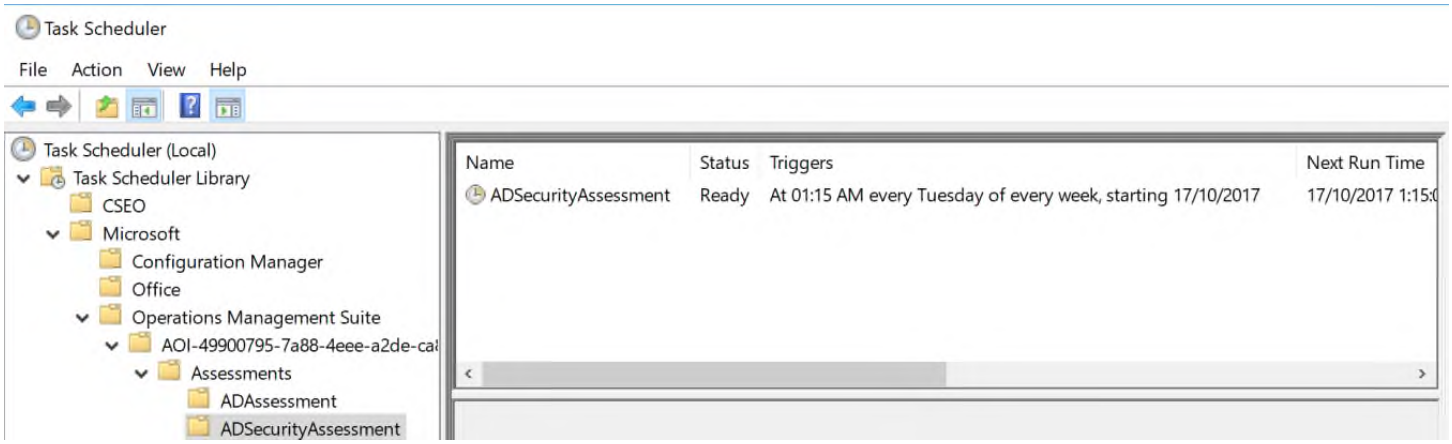
注: このドメイン アカウントは、以下のすべての権限を持っている必要があります。

- フォレスト内の各ドメイン コントローラーへの管理者アクセス権があるエンタープライズ管理者アカウント。
    - 既定では、エンタープライズ管理者グループは、各ドメインの組み込みの Administrators グループのメンバーです。このメンバーシップが変更されていないことを確認してください。エンタープライズ管理者グループがドメインの組み込みの Administrator グループのメンバーではない場合、そのドメインの組み込みの Administrator グループへの Active Directory セキュリティ評価を実行するためのアカウントを追加してください。
- フォレスト内のすべてのドメイン コントローラーへの無制限のネットワーク アクセス。

8. 必要な構成に基づいてスクリプトが続行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。

スケジュールされたタスクの詳細

データ収集は、名前「ADSecurityAssessment」のスケジュールされたタスクにより、前のスクリプトの実行後 1 時間以内、それから 7 日ごとにトリガーされます。タスクは、別の日時に実行するように変更できます。また強制的に即実行することもできます。



付録

データ収集メソッド

Log Analytics ワークスペースと Microsoft Unified Support ソリューション パックの Active Directory セキュリティ評価では、複数のデータ収集メソッドを使用し、環境からの情報を収集します。このセクションでは、Active Directory 環境からのデータ収集に使用されるメソッドについて説明します。コレクターは次のとおりです:

1. レジストリ コレクター
2. LDAP コレクター
3. .NET Framework
4. Windows PowerShell
5. FileDataCollector
6. Windows Management Instrumentation (WMI)
7. カスタム C# コード

1. レジストリ コレクター

レジストリ キーと値は、データ収集マシンとすべてのドメイン コントローラーから読み込まれます。次のような項目が含まれます:

- HKLM¥¥CurrentControlSet¥Services のサービス情報。

  これにより、DC ごとに AD データベースとログ ファイルが配置されている場所を確認したり、AD の適切な機能に関連するサービスごとに詳細情報を取得したりできるようになります。

- HKLM_SOFTWARE_Microsoft_Windows NT_CurrentVersion のオペレーティング システム情報

  これにより、Windows Server 2012 または Windows Server 2019 などのオペレーティング システム情報を確認できるようになります。

2. LDAP コレクター

LDAP クエリは、ドメイン、DC、パーティション、グループ メンバーシップ、アカウント名とそのプロパティ、オブジェクトのアクセス許可、およびその他のコンポーネントのデータを AD 自体から収集するために
使用されます。AD で必要なポートの完全な一覧については、次を参照してください: http://support.microsoft.com/kb/179442 。

3. .NET Framework

評価では、System.DirectoryServices.ActiveDirectory .NET Framework 名前空間を利用して複数のメソッドを使用し、ディレクトリ サービスに関するアーキテクチャ情報を確認および収集します。

4. Windows PowerShell

次のようなさまざまな情報が収集されます:

- Active Directory の組織単位のオブジェクトに関する ACL 情報
- ポリシー構成の監査

- インストール済みのセキュリティ更新プログラム
- スケジュールされたタスク

5. **FileDataCollector**

リモート マシンでフォルダー内のファイルを列挙し、必要に応じてそれらのファイルを取得します。次が例として挙げられます:

- SYSVOL 内のスクリプト
- グループ ポリシーの基本設定の構成ファイル

6。 **Windows Management Instrumentation (WMI)**

WMI は、次のようなさまざまな情報を収集するために使用されます:

- WIN32_Volume

WMI は、フォレスト内の DC ごとにボリューム設定に関する情報を収集します。この情報は、たとえば、システム ボリュームとドライブ レターを確認するために使用され、それにより、クライアントはシステム ドライブにあるファイルの情報を収集できるようになります。

- Win32_Process

フォレスト内の各 DC で実行されているプロセスに関する情報を収集します。この情報により、大量のスレッドやメモリを使用するプロセス、または大きなページ ファイル使用量となるプロセスに関する分析情報が提供されます。

- Win32_LogicalDisk

論理ディスクに関する情報を収集するために使用されます。データベースまたはログ ファイルがある場所のディスクの空き領域の量を確認するために、この情報が使用されます。

7. **カスタム C# コード**

他のコレクターでは得られない情報を収集します。ここでの主な例は、ドメイン コントローラーの有効なユーザー権限のコレクションです。