

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 (AD) 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	2
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	2
環境関連の許可	2
データ収集マシン	2
PowerShell のリモート処理	2
Active Directory 評価のセットアップ	7
管理されたサービス アカウントで構成する	7
ユーザー アカウントで構成する	8
スケジュールされたタスクの詳細	10
付録 - データ収集のメソッド	11

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 に 100 万人以上のユーザーがいる場合は、100 万のユーザー オブジェクトごとに 4GB の RAM を追加します。

- 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。
- PowerShell 4.0 以降。

インストールされた PowerShell のバージョンが少なくとも 4.0 であり (PowerShell ウィンドウに `$PsVersionTable` と入力)、CLRVersion が 4.0 に等しいか、それ以上であることを確認します。

- 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。既定で PowerShell バージョン 2 がインストールされなかった場合。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、Windows Server 2016 および Windows Server 2019 では、既定で WinRM と PowerShell の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、実装する必要があります。

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）
 - Windows Server 2012 R2（以降）で “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、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

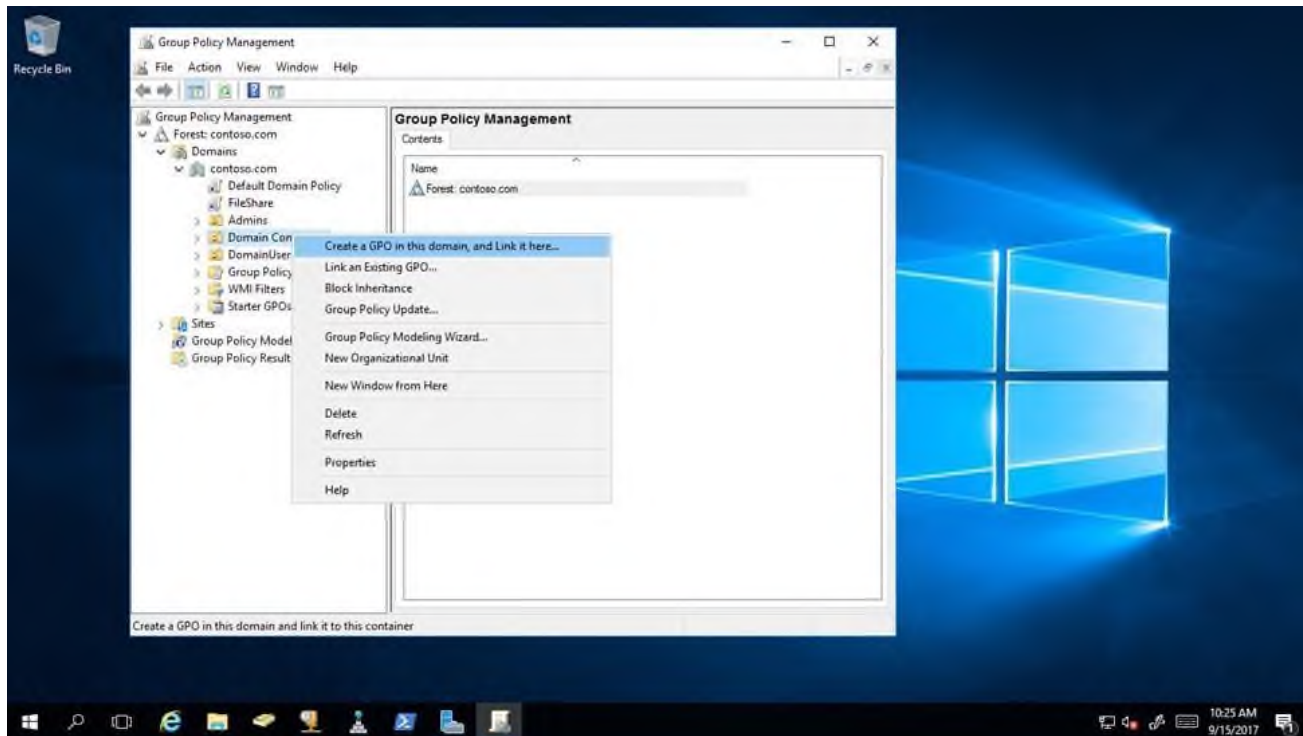
サブネット マスク : X.X.X.X

デフォルト ゲートウェイ : X.X.X.X

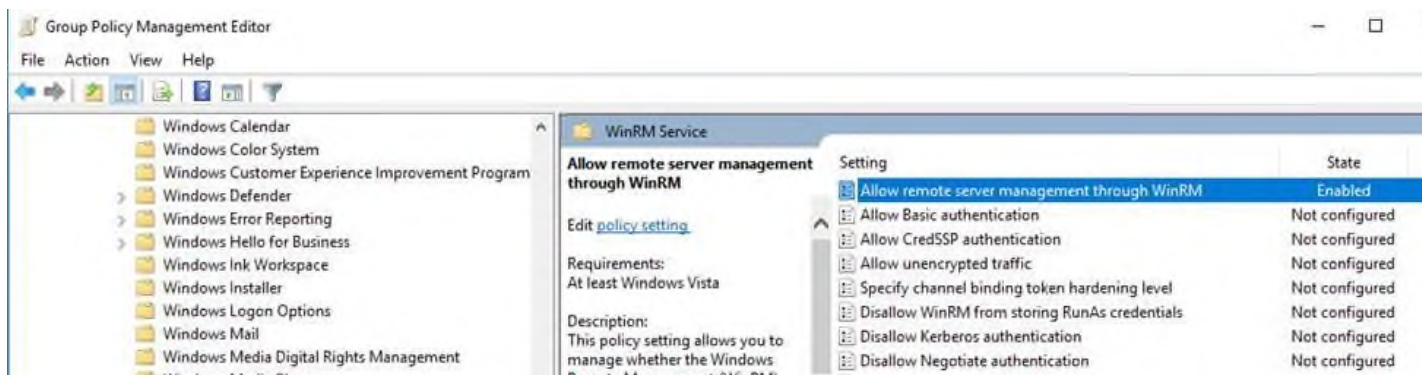
マシンの IPv4 アドレスをメモします。構成の最後の手順では、このアドレスを使用して、データ収集マシンのみがドメイン コントローラーで Windows Update エージェントと通信できることを確認します。

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 コントローラー OU にリンクさせます。

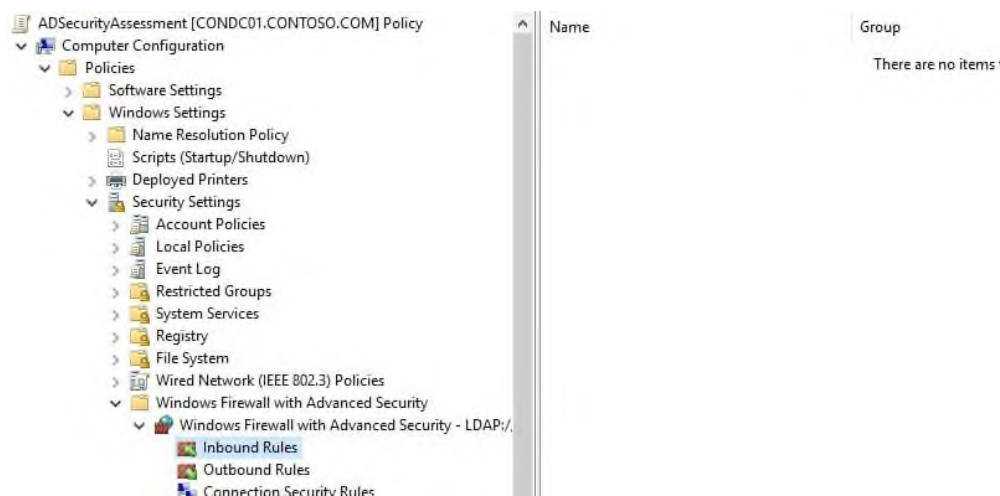
1. 新しい GPO を作成します。GPO がドメイン コントローラーの組織単位に適用されていることを確認します。グループ ポリシーの名前付け規則、または“AD セキュリティ評価”のようにその目的を識別するものに基づいて、新しいグループ ポリシーに名前を付けてください。



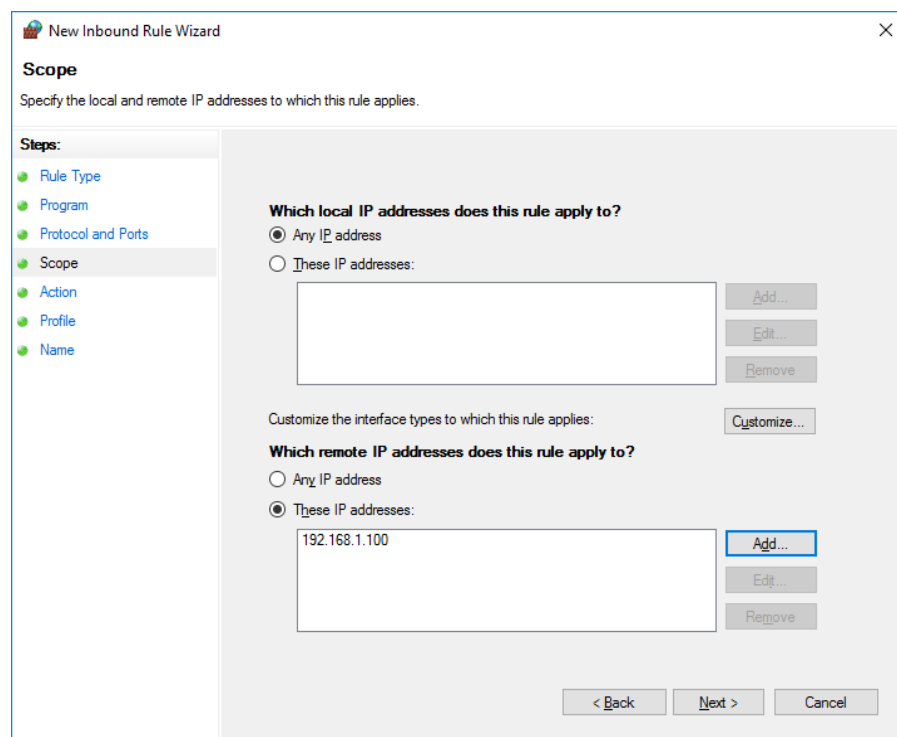
2. GPO 内で次を開きます: (コンピューターの構成¥ポリシー¥管理用テンプレート¥Windows コンポーネント¥Windows リモート管理 (WinRM)¥WinRM サービス)。OS に応じて、“WinRM 経由のリモート サーバー管理を許可する” または “リスナーの自動構成を許可する” を有効にします。



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 評価のセットアップ

Microsoft Management Agent/OMS Gateway のインストールを完了したら、Active Directory 評価をセットアップする準備が整っています。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。

注意: セットアップ タスク中に、“環境” のフレンドリ名を追加することができます。これは、結果を確認する場合に評価された環境が特定される名前です。設定しない場合の環境名は “フォレスト FQDN” になります (例: *contoso.com*)。より親しみやすい名前を使用する場合は、セットアップ コマンドの “-environment” オプションを使用します。

セットアップ中に使用できるオプションは次のとおりです:

- EnvironmentName
 - 結果を確認する場合に環境のフィルター処理で使用する、環境のフレンドリ名 (既定ではフォレスト FQDN) を追加します。
- AssessmentID
 - この評価された環境を識別する GUID。省略しても、ユーザー用に 1 つ生成されます。
- ManagementGroup
 - Microsoft Monitoring Agent をリンクした ManagementGroup の名前が含まれます。

上記のオプションを求めるプロンプトは表示されないの、それらを設定しない場合は、既定の設定が使用されます。Active Directory に必要な最小入力パラメーターは以下のとおりです:

- WorkingDirectory
- Scheduledtaskusername - この後、パスワードの入力が求められます。

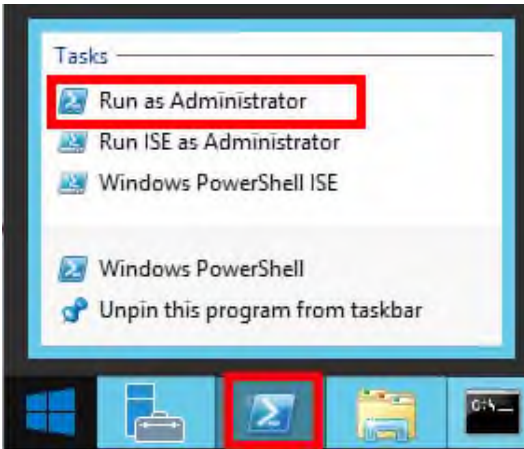
管理されたサービス アカウントで構成する

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-ADAssessmentTask -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-ADAssessmentTask** 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。

Select Administrator: Windows PowerShell

```
PS C:\> Add-ADAssessmentTask -WorkingDirectory c:\oms -ScheduledTaskUsername gmsa-svc$ -RunWithManagedServiceAccount $true
```

3. **Add-ADAssessmentTask** 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。

Administrator: Windows PowerShell

```
PS C:\> Add-ADAssessmentTask -WorkingDirectory c:\oms -ScheduledTaskUsername gmsa-svc$ -RunWithManagedServiceAccount $true

cmdlet Add-ADAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskPassword: 
```

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。

Administrator: Windows PowerShell

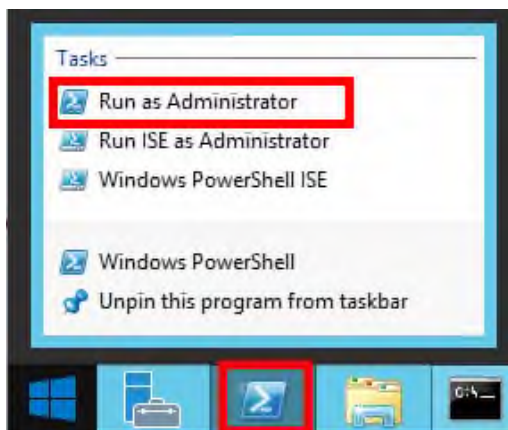
```
PS C:\> Add-ADAssessmentTask -WorkingDirectory c:\oms -ScheduledTaskUsername gmsa-svc$ -RunWithManagedServiceAccount $true

cmdlet Add-ADAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskPassword:
[ADAssessment]Detected agent configuration for Management Group AOI-1fd0f139-...7cda
[ADAssessment][2812]To start an ADAssessment the gmsa-svc$ user must have the 'Log on as a batch job' right. Please verify using Local Security Policy manager.
[ADAssessment]Creating Windows Schedule task to run assessment...
[ADAssessment]Task Creation Successful
[ADAssessment]ADAssessment setup successful.
[ADAssessment]Detailed log is at: C:\Users\administrator.CONTOSO\AppData\Local\Temp\Assessments_Configuration_20190417_072851.log
[ADAssessment][2804]To receive continued assessment updates, please close this Powershell window
PS C:\> 
```

ユーザー アカウントで構成する

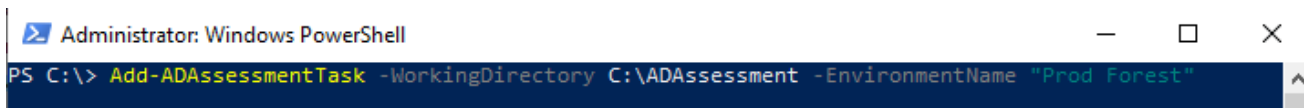
指定されたデータ収集マシンで次の手順を実行します：

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

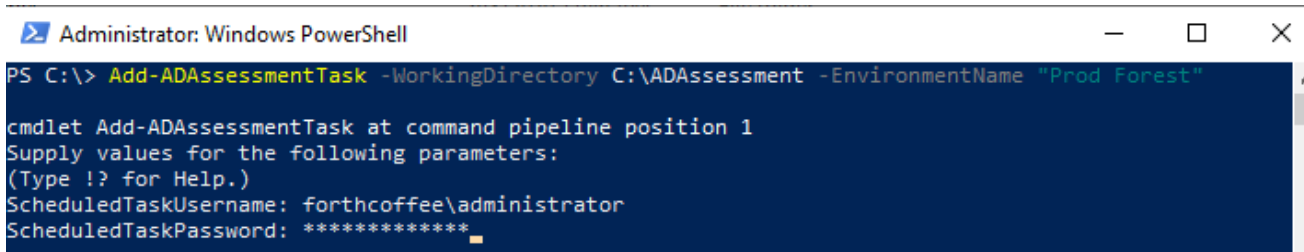


6. **Add-ADAssessmentTask -WorkingDirectory <Directory>** コマンドを実行します。このコマンドでは、<Directory> が環境からのデータを収集および分析している間に作成されたファイルを保存するために使用する既存のディレクトリへのパスになります。

注意: コマンド **Add-ADAssessmentTask** 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。



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 評価を実行するために使用されます。間違ったパスワードを入力すると、スケジュールされたタスクの作成に失敗します。**TaskCredential** を示す赤いテキストが表示されます。



8. エージェントも SCOM に接続されている場合など、複数の管理グループまたはワークスペースが検出された場合は、ADAssessment で使用する管理グループ/ワークスペースを選択するよう求められます。番号を入力します。この例では “1” です

```
Administrator: Windows PowerShell

PS C:\> Add-ADAssessmentTask -WorkingDirectory C:\ADAssessment -EnvironmentName "Prod Forest"

cmdlet Add-ADAssessmentTask at command pipeline position 1
Supply values for the following parameters:
(Type !? for Help.)
ScheduledTaskUsername: forthcoffee\administrator
ScheduledTaskPassword: *****
[ADAssessment]Agent is connected to multiple Management Group(s)/Workspace(s).
[ADAssessment]1.AOI-0291a062-aaa4-47e7-81be-bf205e207996
[ADAssessment]2.AOI-22e4c571-be11-4242-8f0b-5fe40b265433
[ADAssessment]Select the Management Group/Workspace to be used with ADAssessment. (Enter the number
corresponding to list item):
1
```

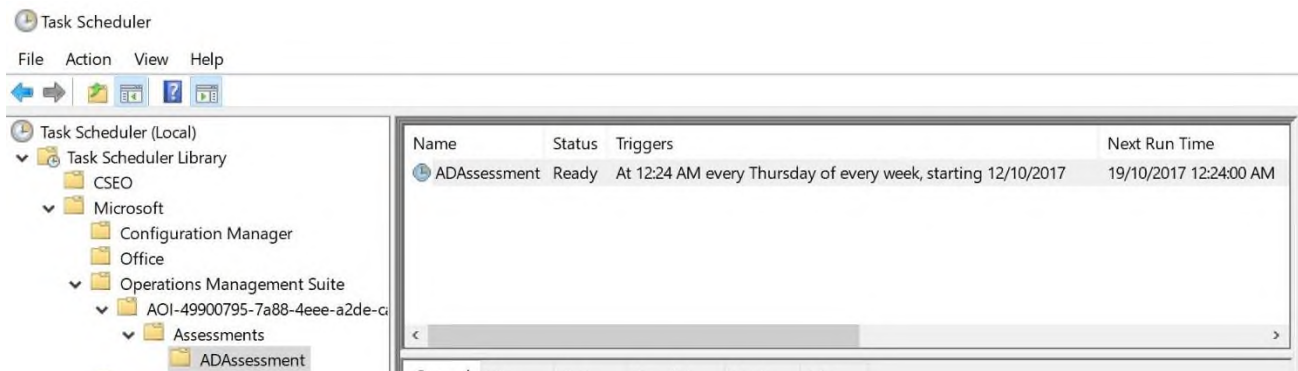
9. 必要な構成に基づいてスクリプトが実行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。

```
[ADAssessment]Generating new random AssessmentId de99d584-360f-4e21-8755-397e3223cef0
[ADAssessment]Created schedule task with AssessmentId de99d584-360f-4e21-8755-397e3223cef0
[ADAssessment]Are you aware that creating ADAssessment task accepts a (g)MSA account as the Task Ru
nner? This is more secure and doesn't require specifying or changing passwords. You may ask your sy
stem administrator to provide you with a (g)MSA account
[ADAssessment][2861]To start an ADAssessment the forthcoffee\administrator user must have the 'Log
on as a batch job' right. Please verify using Local Security Policy manager.
[ADAssessment]Storing AssessmentId de99d584-360f-4e21-8755-397e3223cef0 in registry

[ADAssessment]Creating Windows Schedule task to run assessment...
[ADAssessment]Task Creation Successful
[ADAssessment]ADAssessment setup successful.
```

スケジュールされたタスクの詳細

データ収集は、名前「ADAssessment」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。タスクを別の日時に実行するように変更することができます。



評価結果の使用に関するガイダンスおよび詳細については、Services Hub リソース センターの[評価結果での作業](#)を参照してください。

付録 – データ収集のメソッド

Log Analytics ワークスペースと **Microsoft Unified Support ソリューション パックの AD 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、環境からデータを収集するために使用されるメソッドについて説明します。データ収集に Microsoft Visual Basic (VB) のスクリプトは使用していません。

1. レジストリ コレクター
2. LDAP コレクター
3. .NET Framework
4. イベント ログ コレクター
5. Active Directory サービス インターフェイス (ADSI)
6. Windows PowerShell
7. ファイル データ コレクター
8. Windows Management Instrumentation (WMI)
9. DCDIAGAPI
10. NTFRSAPI
11. 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、ユーザーは、ドメイン コントローラーごとに Active Directory データベースとログ ファイルがある場所を確認したり、Active Directory の適切な機能に関連するサービスごとに詳細な情報を入手したりできるようになります。Microsoft では、すべてのサービスの情報を収集するのではなく、Active Directory に関連するサービスの情報のみ収集します。

- HKLM¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion からのオペレーティング システム情報。これにより、ユーザーは 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、AD 自体から、ドメイン、ドメイン コントローラー、nTDSSiteSettings オブジェクト、パーティション、およびその他のコンポーネントのデータを収集するために使用されます。AD に必要なポートの完全なリストについては、こちら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 名前空間と以下のメソッドを使用します：

- [GetReplicationNeighbors](#) は、レプリケーションの状態の詳細を取得するために呼び出されます。
- [Domain.GetAllTrustRelationships](#)– 各ドメインの信頼関係のコレクションを取得します。
- [Forest.GetAllTrustRelationships](#)– フォレストの信頼関係のコレクション。

4. イベント ログ コレクター

ドメイン コントローラーからイベント ログを収集します。Microsoft では、アプリケーション、分散ファイル システム レプリケーション (DFSR)、DNS、ファイル レプリケーション サービス (FRS)、およびシステム イベント ログから過去 7 日間の警告とエラーを収集します。ディレクトリ サービス イベント ログの場合のみ、空白のログが有効になっている場合は、データベース内の空白の量を検出するために情報イベントも収集されます。

5. ADSI

ドメイン ObjectClass を使用して、フォレストの各ドメインのドメイン パスワード情報を取得するために、[ADSI](#) を使用します。ドメイン パスワード情報は、ドメインの最小パスワード有効期間、最大パスワード有効期間、最小パスワード長、およびデフォルトのドメイン ポリシーに保存されているその他の設定で構成されています。

6. Windows PowerShell

ドメイン コントローラーにインストールされた更新プログラムと修正プログラムの WMI 情報を収集するために使用されます。

7. ファイル データ コレクター

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。

8. 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

フォレスト内のドメイン コントローラーごとにボリューム設定に関する情報を収集します。例えば、その情報はシステム 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、その評価ではシステム 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。その情報により、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。

9. DCDIAGAPI

DC から診断情報を収集します。DCDIAG では、フォレスト内のすべての DC の状態を分析し、検出した問題を報告します。

10. NTFRSAPI

FRS は、SYSVOL および Netlogon フォルダのコンテンツをレプリケーションするために使用できます。NTFRSapi は、DC の NT ファイル レプリケーション サービス (NTFRS) の内部テーブル、スレッド、およびメモリ情報をダンプするために使用されます。FRS の正常性に関する分析情報を提供します。

11. 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。