

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、Microsoft Azure Log Analytics ワークスペースと Microsoft Unified Support ソリューション パックに含まれている Exchange Server 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
Active Directory 評価のセットアップ	7
付録	5
データ収集メソッド	5

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。

サポートされているバージョン

- Exchange Servers では、Exchange Server 2010、Exchange Server 2013、Exchange Server 2016、または Exchange Server 2019 を実行する必要があります。

環境関連の許可

- ユーザー アカウントの権利:
 - 次の権利を持つドメイン アカウント:
 - Exchange 組織に対する Exchange 表示専用管理者の権限
 - 組織の各 Exchange Server への管理者アクセス権。
 - Exchange 組織に対するパブリック フォルダー管理者の権限
- 注意:** ドメイン アカウントがドメイン管理者または Exchange 管理者（完全）の場合は必要ありません
- 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バッチ ジョブ特権としてログオンする

データ収集マシン

- データ収集マシン**は、Windows Server 2012 以降を実行するコンピューターを必要とします（または Windows 8.1 以降 - **重要:** Windows 10 と Windows Management Framework 5 (PowerShell 5) は、現在サポートされていません）。
- 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 8 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。
- データ収集マシン**は、組織のすべての Exchange Servers に接続し、そこから情報を収集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)、PowerShell、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。データ収集マシンは、組織内のすべての Exchange Server への無制限のアクセスを必要とします。
- Microsoft .NET Framework 4.6.2 以降がインストールされています。
- データ収集マシンの CLR バージョンでは、.NET 4.0 以上を使用する必要があります。PowerShell プロンプトで \$PSVersionTable.CLRVersion を実行すると、これを確認できます。
- PowerShell の AD モジュールがインストールされている必要があります (RSAT-AD-PowerShell)。
- データ収集マシン**は、Microsoft Monitoring Agent をインストール済みで、HTTPS を使用してインターネットに接続し、収集したデータを Log Analytics ワークスペースに送信できる必要があります。この接続は、直接の場合、あるいは、プロキシまたは OMS ゲートウェイ経由の場合があります。

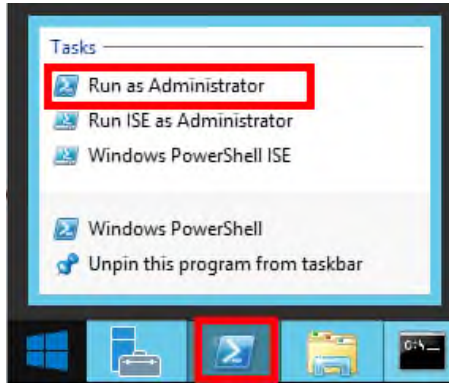
Exchange Server 評価のセットアップ

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

以下の手順に従って、Exchange Server 評価をセットアップします。

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-ExchangeAssessmentTask - 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の使用する既存のディレクトリへのパスになります。

```
Administrator: Windows PowerShell
PS C:\users\romin> Add-ExchangeAssessmentTask -WorkingDirectory "C:\OMS\Exchange_Assessment"
```

3. 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。これらの認証情報は、Exchange Server 評価を実行するために使用されます。

```
PS C:\users\romin> Add-ExchangeAssessmentTask -WorkingDirectory "C:\OMS\Exchange_Assessment"
[ExchangeAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[ExchangeAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[ExchangeAssessment]User(DomainName\UserName):
```

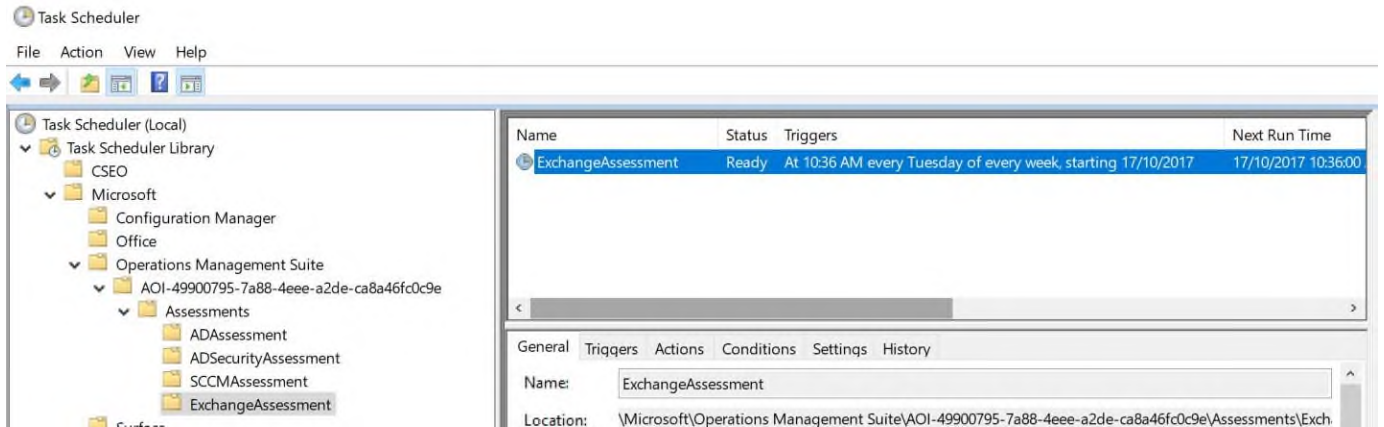
注：このドメイン アカウントは、以下のすべての権限を持っている必要があります。

- 組織内のすべての Exchange Server への管理者アクセス権を持つドメイン アカウント。
- 組織内のすべての Exchange Server への無制限のネットワーク アクセス。

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:\users\romin> Add-ExchangeAssessmentTask -WorkingDirectory "C:\OMS\Exchange_Assessment"
[ExchangeAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[ExchangeAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[ExchangeAssessment]User(DomainName\UserName):
redmond\romin
[ExchangeAssessment]Enter the password for redmond\romin:
*****
[ExchangeAssessment]Creating Windows Schedule task to run assessment...
[ExchangeAssessment]ExchangeAssessment setup successful.
[ExchangeAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171017_043648.log
```

5. データ収集は、名前「ExchangeAssessment」のスケジュールされたタスクによって、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。このタスクは、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 Exchange Server 評価では、複数のデータ収集メソッドを使用し、環境から情報を収集します。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. EventLogCollector
5. Windows PowerShell
6. FileDataCollector
7. WMI
8. カスタム C# コード
9. システム パフォーマンス データ

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 Exchange Server 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、評価では AD データベースとログ ファイルが各サーバーのどこに配置されているかを確認し、AD の適切な機能に関連する各サービスの詳細情報を取得できるようになります。すべてのサービスを収集するのではなく、ADに関連するサービスのみを収集します。

- 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、評価では、Windows Server 2012、Windows Server 2016、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、DC、nTDSiteSettings 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 が必要とするポートの完全なリストについては、次を参照してください：
<http://support.microsoft.com/kb/179442>。

3. .NET Framework

Exchange Server 評価では、[System.DirectoryServices.ActiveDirectory](#).NET Framework の名前空間を利用し、次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](#) では、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](#) は、フォレストの信頼関係のコレクションです。

4. EventLogCollector

Exchange Server からイベント ログを収集します。アプリケーションとシステムのイベント ログから、過去 7 日間の警告とエラーを収集します。

5. Windows PowerShell

構成データを収集するために、PowerShell が Exchange Server 評価で広く使用されます。

- Exchange Server 2010 以降の場合は、リモート PowerShell が Exchange Server 固有の情報を収集するために活用されます。

6. 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。例えば、各ハブ サーバーの EdgeTransport.exe.config ファイルを収集して、設定を検証する場合があります。

Windows Management Instrumentation (WMI)

7. [WMI](#) は、以下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

フォレスト内の各 DC の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、Exchange Server 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。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。

8. 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。

9. システム パフォーマンス データ

パフォーマンス ログと警告のサービスを利用して、各ターゲット サーバーでデータ コレクターを作成します。既定では、パフォーマンス データは各サーバーの c:\perflogs ディレクトリに書き込まれます。収集を開始する前に、必要なディスク領域がコレクターによって確認されます。収集が完了すると、データ収集の構成と収集されたデータが各ターゲット サーバーから削除されます。