

Office 365 Exchange 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 System Center Configuration Manager (SCCM) 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
サポートされているバージョン	2
両方のシナリオに共通	2
データ収集マシン	2
SCCM 評価のセットアップ	3
付録	6
データ収集メソッド	6

このドキュメントの最終更新日は、2020 年 1 月 25 日です。このドキュメントの最新バージョンが与えられていることを確認するには、こちらを確認してください：

<https://go.microsoft.com/fwlink/?linkid=860108>

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

- Windows Server 2012 以降を実行するサイト システムで[サポートされているバージョンの Configuration Manager](#)。
- Configuration Manager 階層は、単一のフォレスト全体にまたがる必要があります。
- Management Point (MP) リストは、MP Checks が失敗しないようにするために、単一のポートで構成される必要があります。これを確認するには、以下の WMI を実行してください：

```
(get-wmiobject -Namespace root\sms\site_<sitecode> -Query "select * from SMS_SCI_Component where ComponentName= 'SMS_MP_CONTROL_MANAGER'").Props | Where-Object {$_.PropertyName -eq "IISPortsList"}
```

両方のシナリオに共通

- Log Analytics ワークスペースが必要です
- 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：
 - Configuration Manager 階層のすべてのサーバー（サイト システム）への管理アクセス権単一のユーザー アカウント（サイト システムが複数ドメイン環境にある場合）
 - Configuration Manager 階層のすべてのサーバー（サイト システム）への無制限のネットワーク アクセス
 - Configuration Manager サイトまたはソフトウェアの更新ポイントが使用するすべての SQL サーバーへの管理者権限
 - すべてのプライマリ サイト内のすべての Configuration Manager サイト オブジェクトへのフル アクセス権
 - Configuration Manager サイトまたはソフトウェアの更新ポイントで使用されているすべての SQL インスタンスへの SysAdmin アクセス権。

データ収集マシン

- データ収集マシンは、評価する SCCM 階層が存在する Active Directory ドメインのメンバー サーバーである必要があります、データ収集マシンには SCCM コンソールがインストールされ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、SCCM 階層に接続し、そこから情報を取得するために使用され、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、SQL データベース、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 を介して通信しています。
- 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。これは、PowerShell プロンプトで \$PSVersionTable.CLRVersion を実行すると、確認できます。
- 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。

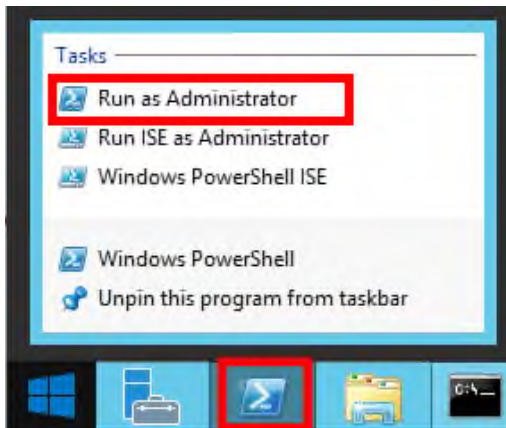
Microsoft Monitoring Agent/OMS Gateway のインストールを完了したら、評価をセットアップするために、次のセクションを続行します。

SCCM 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、SCCM 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 アカウントになるか、ユーザー アカウントになるか応じて、評価のスケジュールされたタスクをセットアップする方法は 2 つあります（以下の手順 2 と 3 に記載されています）。

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. ユーザー アカウントの使用：

`Add-SCCMAssessmentTask -ServerName <YourServerName> -WorkingDirectory <DirectoryPath>` コマンドを実行します。このコマンドでは、<YourServerName>が階層で最上位の管理サーバーのいずれかの FQDN 名または NetBIOS 名（セントラルまたはプライマリ サイト）であり、<DirectoryPath>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る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： ディレクトリが存在しない場合は、実行を続行する前に作成する必要があります。



3. 管理されたサービス アカウントの使用：

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. プロビジョニングの [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ユーザー アカウントの権利の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、管理 PowerShell プロンプトで次を実行してください：

```
Add-SCCMAssessmentTask -ServerName <YourServerName> -WorkingDirectory <DirectoryPath>-  
ScheduledTaskUsername <MSAname> -RunWithManagedServiceAccount $True
```

このコマンドでは、<YourServerName>が階層で最上位の管理サーバーのいずれかの FQDN 名または NetBIOS 名（セントラルまたはプライマリ サイト）であり、<DirectoryPath>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る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（\$ サインで終わる）になります。

4. 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、SCCM 評価を実行するために使用されます。

```
[SCCMAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[SCCMAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for a
ssessment.
[SCCMAssessment]User(DomainName\UserName):
redmond\romin
[SCCMAssessment]Enter the password for redmond\romin:
*****
```

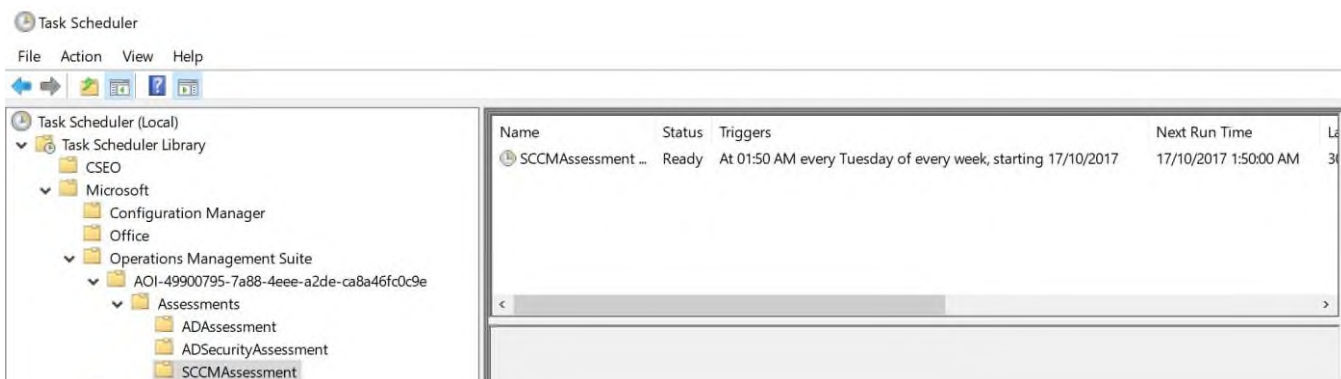
注：このドメイン アカウントは、以下のすべての権限を持っている必要があります。

- Configuration Manager 階層のすべてのサーバー（サイト システム）への管理アクセス権単一のユーザー アカウント（サイト システムが複数ドメイン環境にある場合）
- Configuration Manager 階層のすべてのサーバー（サイト システム）への無制限のネットワーク アクセス
- Configuration Manager サイトまたはソフトウェアの更新ポイントが使用するすべての SQL サーバーへの管理者権限
- すべてのプライマリ サイト内のすべての Configuration Manager サイト オブジェクトへのフル アクセス権
- Configuration Manager サイトまたはソフトウェアの更新ポイントで使用されているすべての SQL インスタンスへの SysAdmin アクセス権。

5. 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。

```
[SCCMAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[SCCMAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for a
ssessment.
[SCCMAssessment]User(DomainName\UserName):
redmond\romin
[SCCMAssessment]Enter the password for redmond\romin:
*****
[SCCMAssessment]Creating Windows Schedule task to run assessment...
[SCCMAssessment]SCCMAssessment setup successful.
[SCCMAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171017_075011.log
PS C:\users\romin>
```

6. データ収集は、名前 “**SCCMAssessment -ServerName <YourServerName>**” 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。



7. 収集および分析している間に、次の構造を使用し、セットアップ時に構成された WorkingDirectory フォルダーの下にデータが一時的に保存されます：

This PC > OSDisk (C:) > OMS > SCCM > SCCMAssessment > asttest.redmond.corp.microsoft.com

<input type="checkbox"/> Name	Date modified	Type	Size
2900753	17/10/2017 12:55 AM	File folder	
OmsAssessment	17/10/2017 12:55 AM	File folder	
run.cmd	17/10/2017 12:50 AM	Windows Command ...	1 KB

8. ツール マシンでデータ収集と分析を完了したら、次の選択したシナリオにより、log analytics ワークスペースに送信されます：
- **直接**、データ収集マシンをインターネットに接続して構成している場合は、直接送信されます。
 - **OMS Gateway サーバー経由**、このオプションが構成されている場合は、Log Analytics ワークスペースにそのデータが送信されます。
9. 数時間後に、Log Analytics ダッシュボードで評価結果を利用できるようになります。System Center Configuration Manager 評価タイルをクリックし、次を確認します：



10. 重点領域によってグループ化された検出結果が表示されます。



付録

データ収集メソッド

Log Analytics ワークスペースでの SCCM 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. Windows PowerShell
4. ファイル データ コレクター
5. Windows Management Instrumentation (WMI)
6. SQL

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 以降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、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 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. 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。

4. 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。

5. Windows Management Instrumentation (WMI) コレクター

[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。

6. SQL データ コレクター

SQL クエリは、サイト サーバーから情報を収集するために使用されます。