

# 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 Microsoft Unified Support ソリューション パックに含まれている SharePoint 評価の構成に必要な手順を説明します。

## チェック リスト

### 1. Azure

- ☒ [Azure サブスクリプション](#)を確認します
- ☒ Azure Log Analytics ワークスペースを確認します

### 2. 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：

- ☒ ファーム管理者グループのメンバー。
- ☒ 少なくとも、ファーム内のすべての Web アプリケーションへの読み取りアクセス権。
- ☒ すべてのサービス アプリケーションへの完全なコントロール。
- ☒ 評価が行われている SharePoint ファームに関連するすべての SharePoint Server および SQL Server に対するローカル管理者の権限。
- ☒ SharePoint データベースを収納する SQL インスタンスすべての “SysAdmin” サーバーロールのメンバー。
  - 注：SQL 認証はサポートされていません。

### 3. ターゲット サーバー

- ☒ データは、ターゲット サーバーと呼ばれるファーム内の SharePoint Server のいずれかに接続することにより、データ収集マシンによって収集されます。
- ☒ ターゲット サーバーは、IP フィルターを使用せずに、WinRM 経由でリモート サーバー管理を実行できる必要があります。
- ☒ ターゲット サーバーでは、リモート PowerShell および CredSSP が有効でなければなりません。

### 4. データ収集マシン

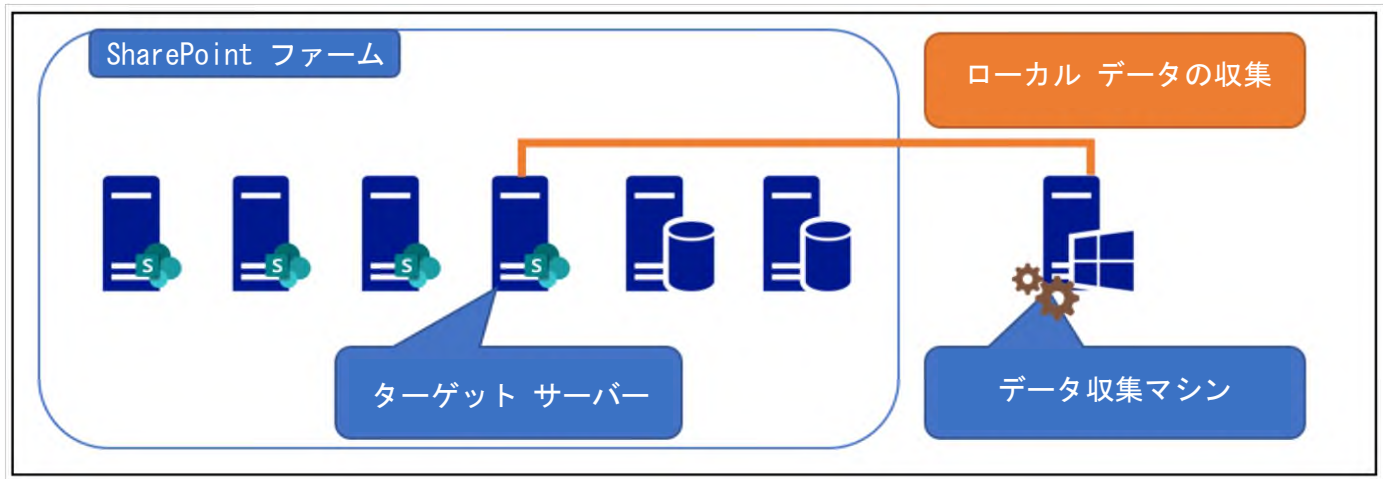
- ☒ データ収集はマシン（別名データ収集用のマシン）から実行されます。これは、SharePoint ファームと同じドメインに参加しているものです。
  - ✧ 以下のデータ収集の構成がサポートされています：
    - Windows マシン（SharePoint サーバー以外） -> リモートデータ収集
    - ターゲット サーバー SharePoint ファーム サーバー -> ローカル データの収集

### 5. ネットワークとリモート アクセス

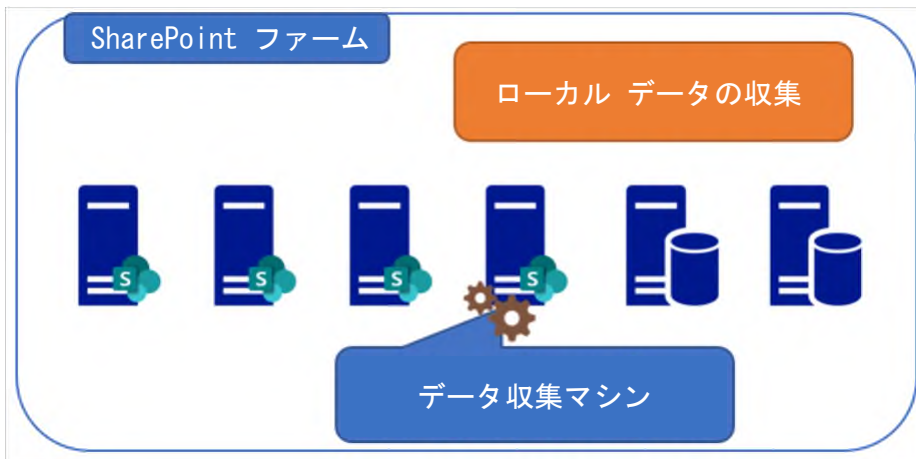
- ☒ SharePoint ファーム内のすべてのサーバー（SQL サーバーを含む）とデータ収集マシン間の無制限のネットワーク アクセス。
- ☒ Windows リモート管理（WinRM）では、HTTP にポート 5985、HTTPS にポート 5986 を使用します。PowerShell コマンドはこのポートを介してリモートで実行されるため、データ収集マシンと、ポート 5985 または ポート 5986 上のデータ収集の対象となる SharePoint サーバー間の通信を有効にする必要があります。

サンプル アーキテクチャはこちらです

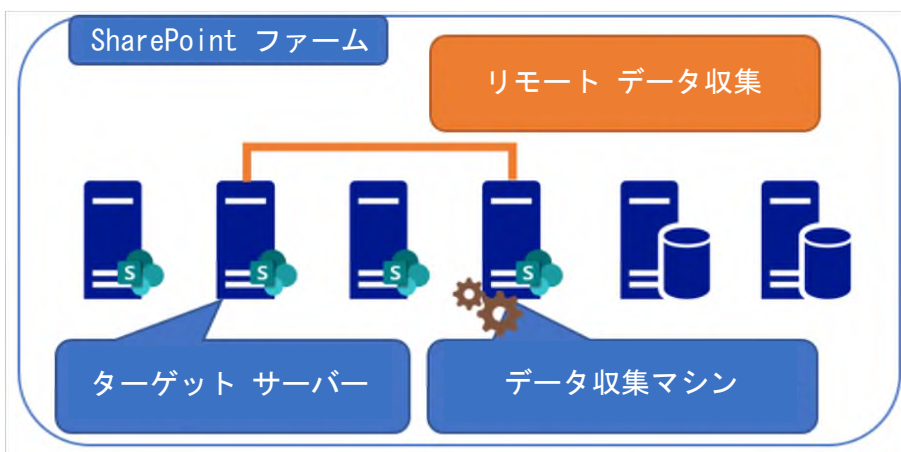
ケース 1.



ケース 2.



ケース 3.



## OMS Gateway

評価を構成するために使用できるシナリオは 2 つあります。組織に最も適したシナリオを選択してください。

1. OMS Gateway とデータ収集マシン
2. データ収集マシンのみ

評価を構成するために使用できるシナリオは 2 つあります。組織に最も適したシナリオを選択してください。

1. OMS Gateway とデータ収集マシン
2. データ収集マシンのみ

### OMS Gateway とデータ収集マシン

このシナリオは最も安全な推奨オプションで、評価の実行に必要なこのデータ収集マシンで構成され、スケジュールされたタスクで使用する特権アカウントの資格情報を保護するのに役立ちます。このシナリオには 2 つのコンピューターが必要です。1 台はデータ収集マシンとして指定され、第 2 コンピューターは OMS Gateway となります。このシナリオでは、データ収集マシンはインターネット接続を使用しないで、OMS Gateway に接続し、Log Analytics にデータをアップロードします。OMS Gateway にはインターネットへのアクセスが必要です。このシナリオは、データ収集マシンのインターネット接続が制限されている環境、またはこのスケジュール タスク要件のためにセキュリティが懸念される環境に推奨されます。OMS Gateway に関する詳細情報については、次にアクセスしてください：

<https://go.microsoft.com/fwlink/?linkid=830157>

データ収集マシンは評価される SharePoint ファームと同じドメインに参加している必要があります。データ収集マシンの場合は、SharePoint ファームの SharePoint サーバーまたは Windows マシン（SharePoint サーバー以外）がサポートされます。SharePoint ファームのすべてのサーバーからデータを収集します。データが収集されると、データ収集マシンがその情報を分析し、セキュリティ向上のために OMS Gateway にデータを転送し、Log Analytics にそのデータをアップロードします。

次のパスは、OMS Gateway とデータ収集マシンのインストールおよび構成後の Windows コンピューターと Log Analytics との関係を示しています。

*データ収集マシン→環境内のすべての SharePoint サーバーからデータを収集 → 収集したデータを OMS Gateway に転送→データを Log Analytics ワークスペースに送信*

#### データ収集マシンのみ

このシナリオは、データ収集マシンが Log Analytics に直接コンタクトできる場合に利用できます。データ収集マシンとして指定するコンピューターが 1 つ必要になります。そのコンピューターは、Log Analytics にデータをアップロードするために、インターネットにアクセスする必要があります。このシナリオは、インターネット接続が制限されない環境に適用できます。

データ収集マシンは評価される SharePoint ファームと同じドメインに参加している必要があります。データ収集マシンの場合は、SharePoint ファームの SharePoint サーバーまたは Windows マシン（SharePoint サーバー以外）がサポートされます。ファーム内のすべての SharePoint サーバーからデータを収集します。データが収集された後に、データ収集マシンで情報が分析されると、Log Analytics にデータが直接アップロードされます。これを行うには、Log Analytics ワークスペースへの HTTPS 接続が必要です。次のパスは、データ収集マシンのインストールおよび構成後の Windows コンピューターと Log Analytics との関係を示しています：

*データ収集マシン→環境内のすべての SharePoint サーバーからデータを収集→データを Log Analytics ワークスペースに送信*

これらの構成と要件に関する詳細情報については、このドキュメントの後半に一覧表示されています。

このドキュメントの最終更新日は、2020 年 2 月 20 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=860119>

## 目次

チェック リスト .....	1
システム要件および構成の概要 .....	5
サポートされているバージョン .....	5
両方のシナリオに共通 .....	5
ターゲット サーバー .....	5
データ収集マシン .....	5
ネットワークとリモート アクセス .....	6
OMS Gateway (OMS Gateway とデータ収集マシンのシナリオで必要です) .....	6
PowerShell のリモート処理 .....	7
リモート PowerShell および CredSSP 構成 (データ収集マシン) .....	12
リモート PowerShell および CredSSP の構成 (ターゲット サーバー) .....	13
リモート PowerShell および CredSSP 構成のテスト .....	15
ユーザー プロファイル サービス .....	15
SharePoint 評価のセットアップ .....	16
付録 .....	20
ターゲット サーバーの要件 .....	20
SharePoint 評価の資格情報の前提条件 .....	22
データ収集メソッド .....	24

## 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

- SharePoint 環境は、SharePoint Server 2019、SharePoint Server 2016、SharePoint Server 2013、または SharePoint Server 2010 で実行する必要があります。
  - SharePoint 評価は、SQL Server 2017、SQL Server 2016、SQL Server 2014、および SQL Server 2012 を実行している SQL サーバーを基盤とする SharePoint ファームをサポートします。以前のバージョンの SQL Server はサポートされていません。
  - データは、ターゲット サーバーと呼ばれるファーム内の SharePoint Server のいずれかに接続することにより、データ収集マシンによって収集されます。ターゲット サーバー要件の詳細については、このドキュメントの後半に記載されています。

## 両方のシナリオに共通

- Azure サブスクリプションが必要です
- 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：
  - ファーム管理者グループのメンバー。
  - 少なくとも、ファーム内のすべての Web アプリケーションへの読み取りアクセス権。
  - すべてのサービス アプリケーションへの完全なコントロール。
  - 評価が行われている SharePoint ファームに関連するすべての SharePoint Server および SQL Server に対するローカル管理者の権限。
  - SharePoint データベースを収納する SQL インスタンスすべての “SysAdmin” サーバーロールのメンバー。
    - ・ 注：SQL 認証はサポートされていません。

## ターゲット サーバー

- データは、ターゲット サーバーと呼ばれるファーム内の SharePoint Server のいずれかに接続することにより、データ収集マシンによって収集されます。
- ターゲット サーバーは、IP フィルターを使用せずに、WinRM 経由でリモート サーバー管理を実行できる必要があります。これに関する詳細は、このドキュメントの「付録：ターゲット サーバーの要件」に記載されています。
- ターゲット サーバーでは、リモート PowerShell および CredSSP が有効でなければなりません。
- Windows リモート管理 (WinRM) では、HTTP にポート 5985、HTTPS にポート 5986 を使用します。PowerShell コマンドはこのポートを介してリモートで実行されるため、データ収集マシンと、ポート 5985 またはポート 5986 上のデータ収集の対象となるターゲット サーバー間の通信を有効にする必要があります。

## データ収集マシン

- **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。
- 上位のワークステーション：Windows 10/Windows 8.1  
サーバー：Windows Server 2019/Windows Server 2016/Windows Server 2012 R2
  - 64 ビット オペレーティング システム可能
- **データ収集マシン**は評価される SharePoint ファームと同じドメインに参加している必要があります。
  - データ収集マシンとして、以下のマシンがサポートされています

- Windows マシン (SharePoint サーバー以外) -> リモートデータ収集
  - SharePoint ファームのターゲット サーバー -> ローカル データ収集
- [Microsoft .NET Framework 4.6.2](#) 以降がインストールされています。
- Windows PowerShell 4.0 以降
  - PowerShell の実行ポリシーは、データ収集マシンとサーバーの両方で **remotesigned** に設定する必要があります
  - 実行ポリシーの設定は、PowerShell コマンド ウィンドウの “get-executionpolicy -list” を使用して検証できます。
- **データ収集マシン**は、ファーム内のすべてのサーバーに接続し、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、SQL クエリ、PowerShell コマンドレットを介して通信しています。
- リモート管理 (RPC) のファイアウォールの例外 - 動的ポート範囲
- データ収集マシンは、HTTPS を使用してインターネットに接続し、収集データを Log Analytics ワークスペースに送信する必要があります。この接続は直接の場合、またはプロキシ経由の場合があります。
- **Microsoft Monitoring Agent** で Log Analytics サービスに接続および登録するには、それがインターネットにアクセスできる必要があります。エージェントと Log Analytics サービス間の通信でプロキシ サーバーを使用している場合は、適切なリソースにアクセスできることを確認する必要があります。インターネットへのアクセスを制限するためにファイアウォールを使用している場合は、Log Analytics へのアクセスを許可するために、ファイアウォールを構成する必要があります。データを送信できることを確認するには、次にアクセスし、*Log Analytics* でのプロキシとファイアウォールの設定の構成の手順に従ってください: <https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/>.

## ネットワークとリモート アクセス

- **SharePoint ファーム内のすべてのサーバー (SQLサーバーを含む) への無制限のネットワーク アクセス。**
  - これは、任意のファイアウォール、およびサーバーへのトラフィックを制限している可能性のあるルーター ACL 経由のアクセスを意味します。これには、DCOM、リモート レジストリ サービス、WMI サービス、および既定の管理共有 (C\$、D\$、IPC\$) へのリモート アクセスが含まれます。
  - データ収集に使用するマシンに、すべてのサーバーへの RPC アクセスを含む、完全な TCP/UDP アクセスが付与されていることを確認してください。
  - ポート 135、139、または 445 を介したアクセスも必要です。
- Windows リモート管理 (WinRM) では、HTTP にポート 5985、HTTPS にポート 5986 を使用します。PowerShell コマンドはこのポートを介してリモートで実行されるため、ツール マシンとポート 5985 またはポート 5986 でのデータ収集の対象となる SharePoint サーバー間の通信を有効にする必要があります。
  - **注:** このドキュメントのセクション 6 にあるリモート PowerShell および CredSSP の構成手順を実行すると、構成の一部として、ポート 5985 および 5986 を開くことを許可するように求められるので、画面の指示に従って、[はい] を選択し、ポートを開くことを許可してください。

## OMS Gateway (OMS Gateway とデータ収集マシンのシナリオで必要です)

- **OMS Gateway** は、スタンドアロンの場合、またはメンバー サーバーの場合があります。Windows Server 2012 R2 以降が必要とされます。
- **OMS Gateway** は、HTTPS を使用してインターネットに接続し、収集されたデータを Log Analytics ワークスペースに送信する必要があります。この接続は直接の場合、またはプロキシ経由の場合があります。
- **OMS Gateway のハードウェア:** 最小 4 GB の RAM と 2 GHz のプロセッサ。
- **OMS Gateway ユーザー アカウントの権利:** 必要なし。

リンクをクリックし、“評価のセットアップ” のドキュメントをダウンロードし、OMS Gateway と Microsoft Monitoring Agent をインストールします。

<https://go.microsoft.com/fwlink/?linkid=860142>



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。

## 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。

### Windows Server 2012 R2（または既定が変更されている場合はそれ以降のバージョン）の追加要件ターゲットマシン:

次の 3 つの項目は、データ収集をサポートするために、SharePoint サーバーで構成される必要があります: 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。

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) SharePoint サーバ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

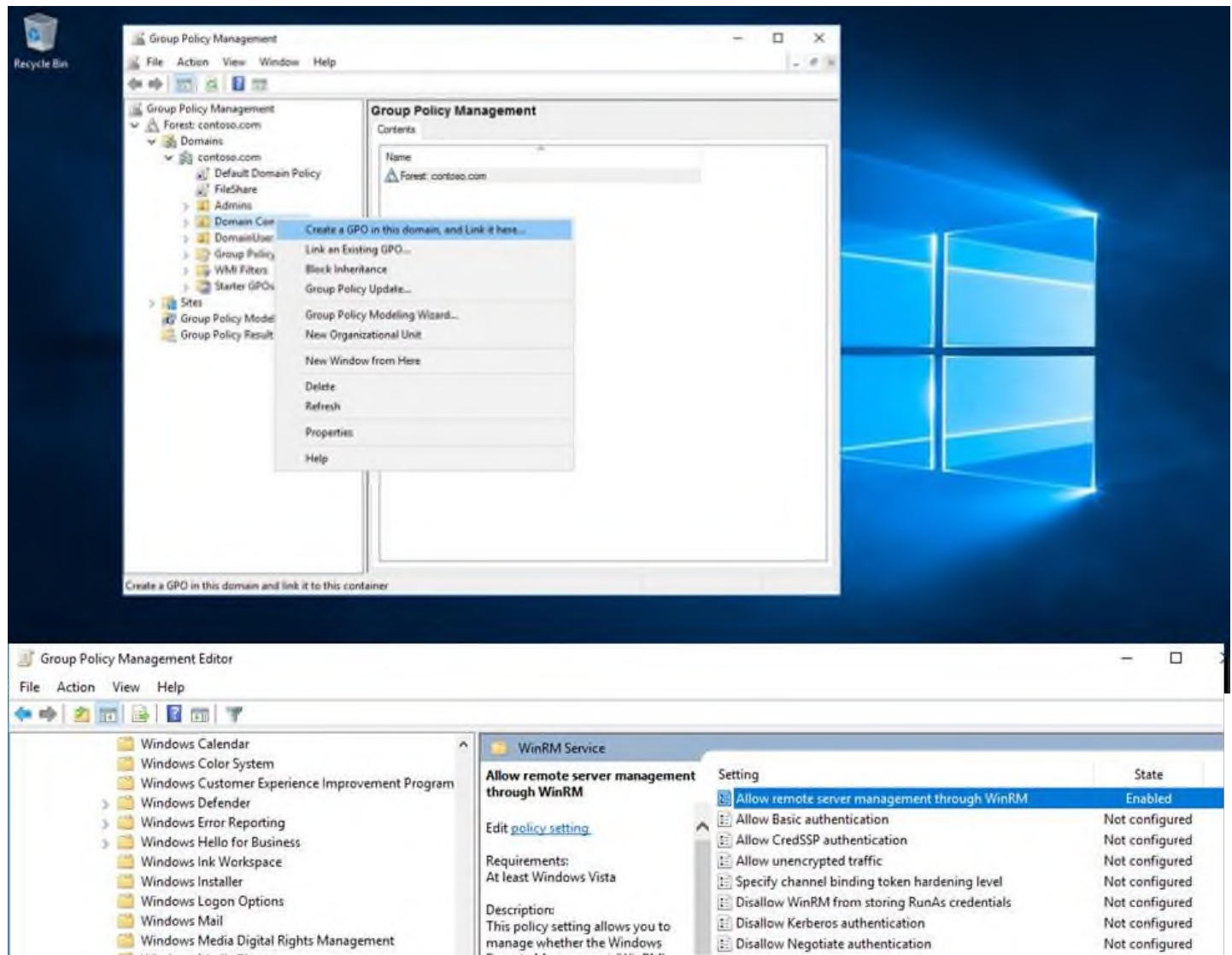
サブネット マスク . . . . . : X.X.X.X

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、データ収集マシンのみが SharePoint サーバーで 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、フォレスト内の各ドメインの SharePoint サーバー OU にリンクさせます。

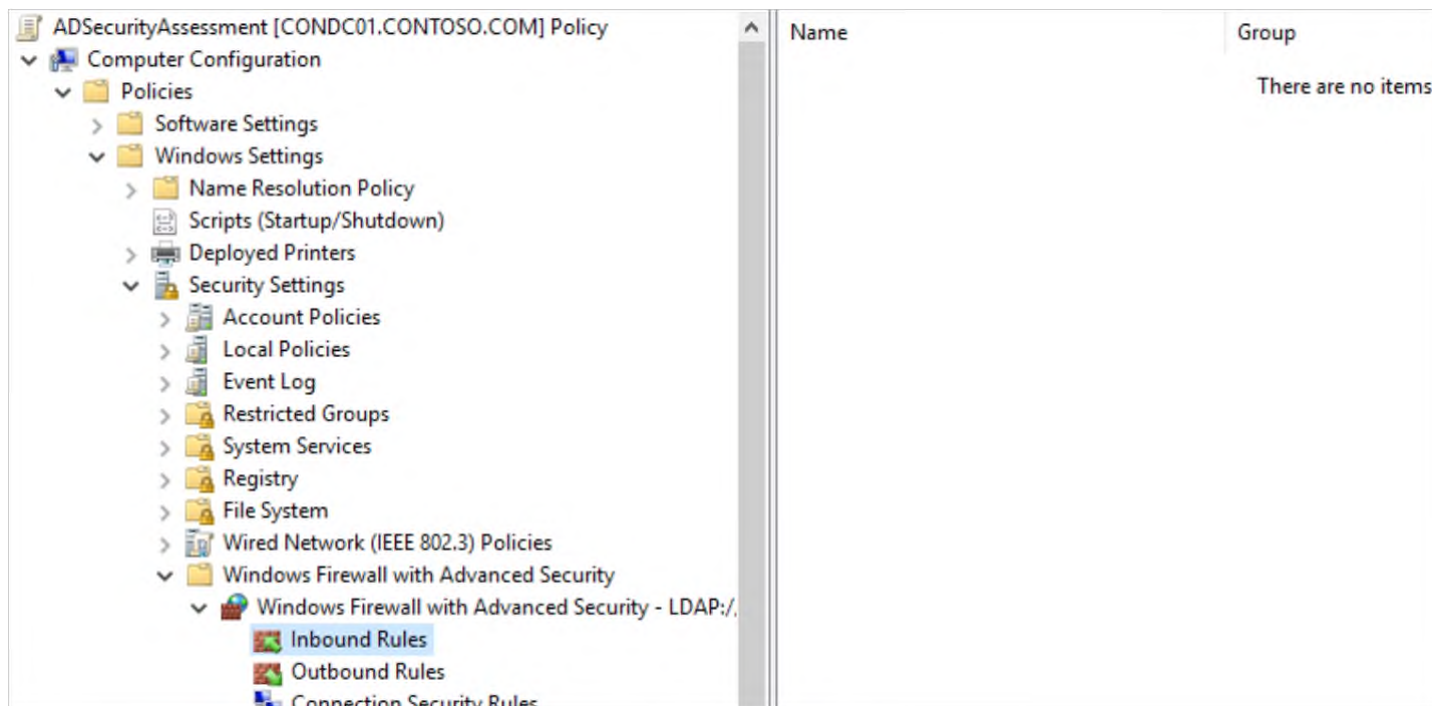
1. 新しい GPO を作成します。GPO が SharePoint サーバーの組織単位に適用されていることを確認します。グループ ポリシーの名前付け規則、または “SP 評価” のようにその目的を識別するものに基づいて、新しいグループ ポリシーに名前を付けてください。



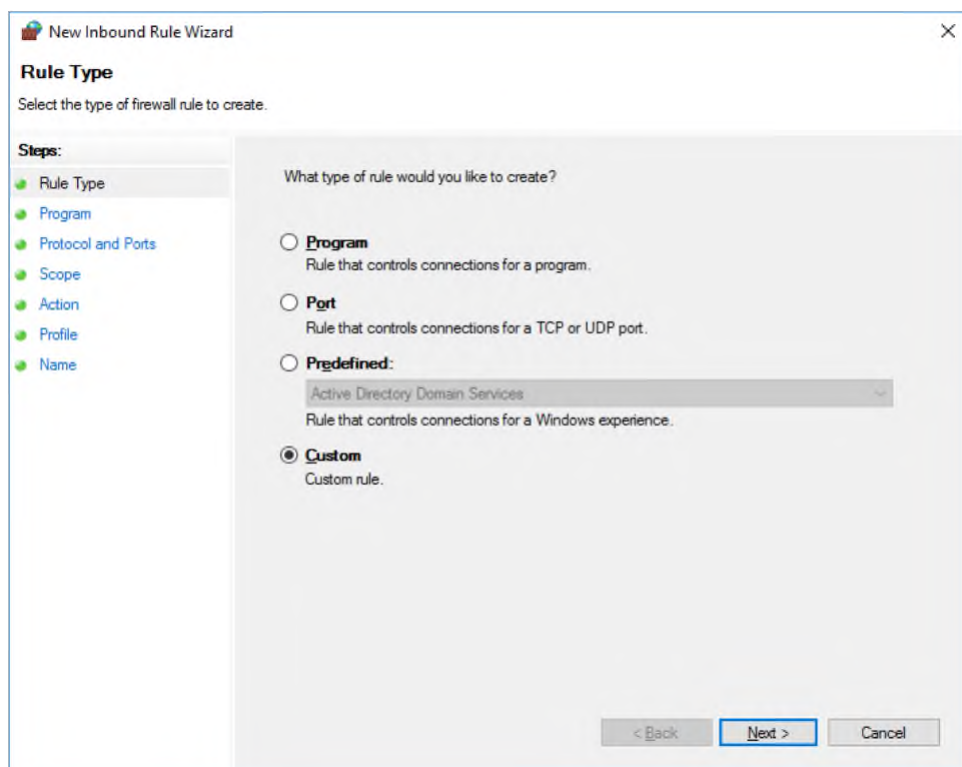
管理 (WinRM)¥WinRM サービス)OS に応じて、“WinRM 経由のリモート サーバー管理を許可する” または “リスナーの自動構成を許可する” を有効にします。

2. 詳細なファイアウォールの受信規則を作成し、ツール マシンから SharePoint サーバーへ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)

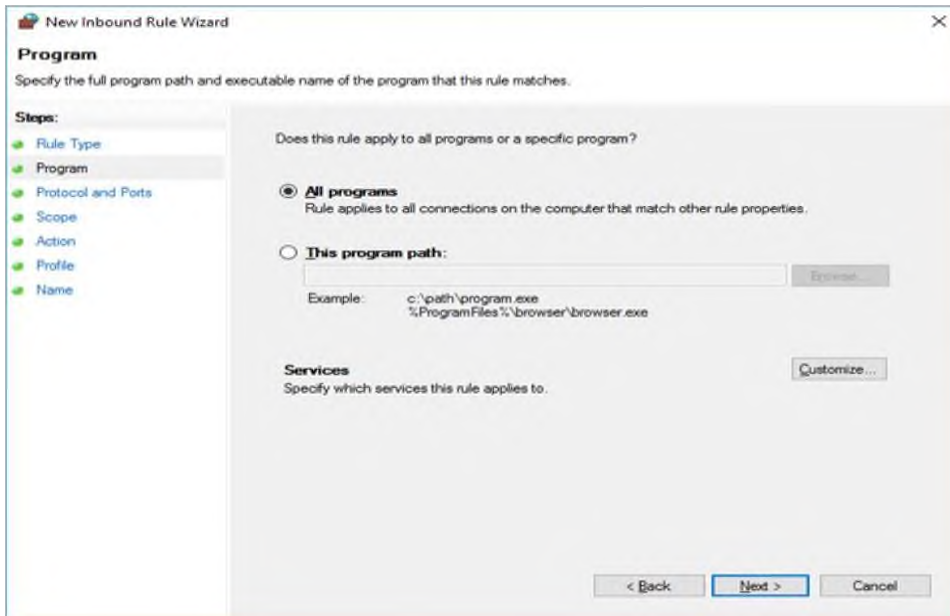




3. 新しい規則を作成するには、[受信規則] をクリックし、[新規] を選択します
4. カスタムの規則を作成し、[次へ] を選択します

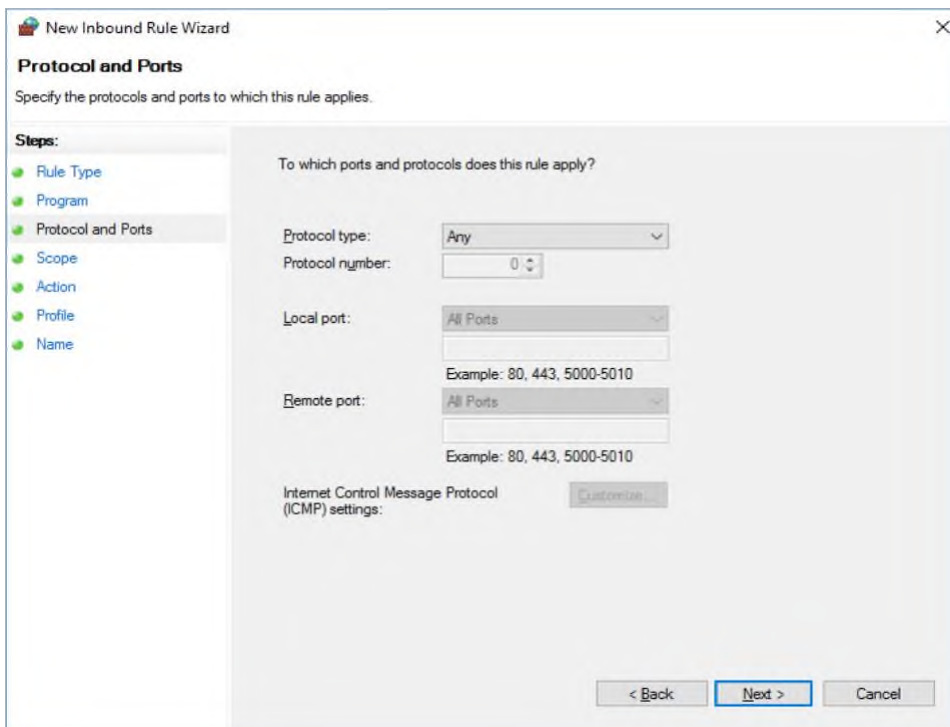


5. ツール マシンの [すべてのプログラム] を許可し、[次へ] をクリックします。



The screenshot shows the 'Program' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name. The main area asks 'Does this rule apply to all programs or a specific program?'. The 'All programs' radio button is selected, with the text 'Rule applies to all connections on the computer that match other rule properties.' Below it, the 'This program path:' option is unselected, with a text box and a 'Browse...' button. An example path is shown: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. The 'Services' section is also unselected, with a 'Customize...' button. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

6. すべてのプロトコルとポートを許可し、[次へ] をクリックします。



The screenshot shows the 'Protocol and Ports' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope, Action, Profile, and Name. The main area asks 'To which ports and protocols does this rule apply?'. The 'Protocol type' dropdown is set to 'Any'. The 'Protocol number' is set to '0'. The 'Local port' dropdown is set to 'All Ports'. The 'Remote port' dropdown is set to 'All Ports'. Examples for both are '80, 443, 5000-5010'. The 'Internet Control Message Protocol (ICMP) settings:' section is unselected, with a 'Customize...' button. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

7. ツール マシンの IP アドレスを指定し、[次へ] をクリックします。

New Inbound Rule Wizard

**Scope**

Specify the local and remote IP addresses to which this rule applies.

**Steps:**

- Rule Type
- Program
- Protocol and Ports
- Scope**
- Action
- Profile
- Name

**Which local IP addresses does this rule apply to?**

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: [Customize...](#)

**Which remote IP addresses does this rule apply to?**

☐ Any IP address

☒ These IP addresses:

192.168.1.100

Add... Edit... Remove

< Back Next > Cancel

8. 「接続を許可する」を選択し、[次へ] をクリックします。
9. 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。
10. 規則の名前を選択します (例: SPAssessmentToolsMachine)

## リモート PowerShell および CredSSP 構成（データ収集マシン）

データ収集マシンで、“管理者として実行” オプションで PowerShell プロンプトを開きます。そして、次のコマンドを実行します（以下のコマンドを実行する前に、以下の重要な注意を参照してください）

```
winrm quickconfig
```

```
Enable-WSManCredSSP -Role client -DelegateComputer <SharePointServer FQDN>
```

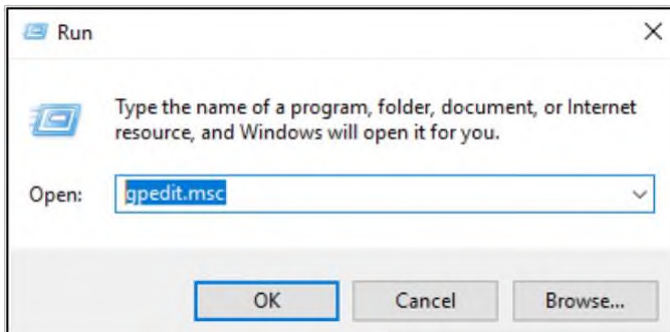
注意：

上記のコマンドの “SharePointServerFQDN” は、データ収集時に “データ収集マシン” が接続する “ターゲット サーバー” です。ホスト名だけでなく、SharePoint Server の FQDN を使用する必要があります。

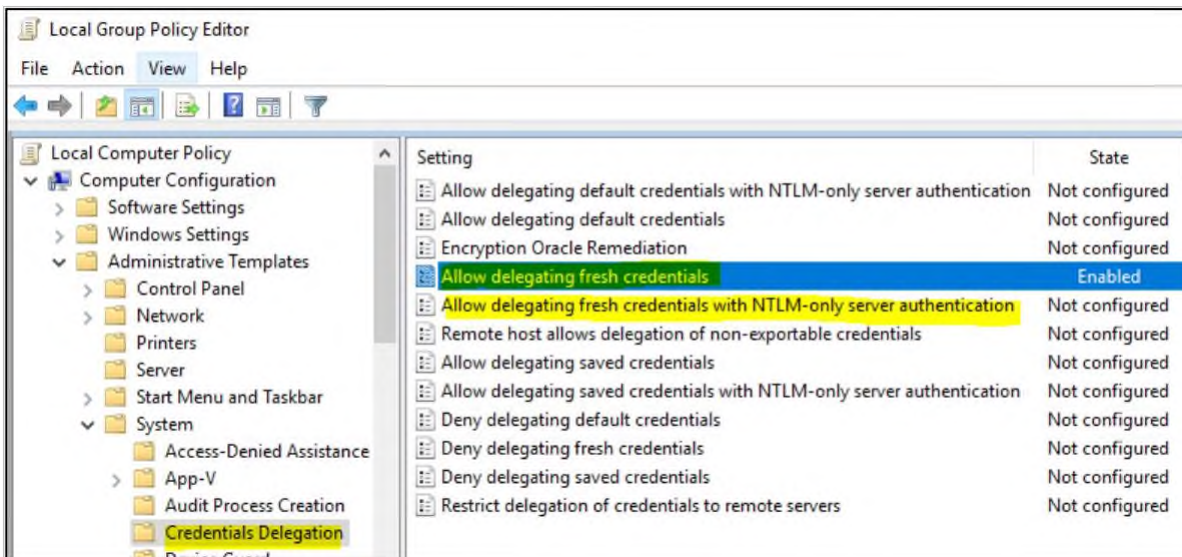
このコマンドを成功させるには、WinRM サービスが実行されている必要があります。

### ローカル グループ ポリシーの編集（データ収集マシン）

1. gpedit.msc を実行します。



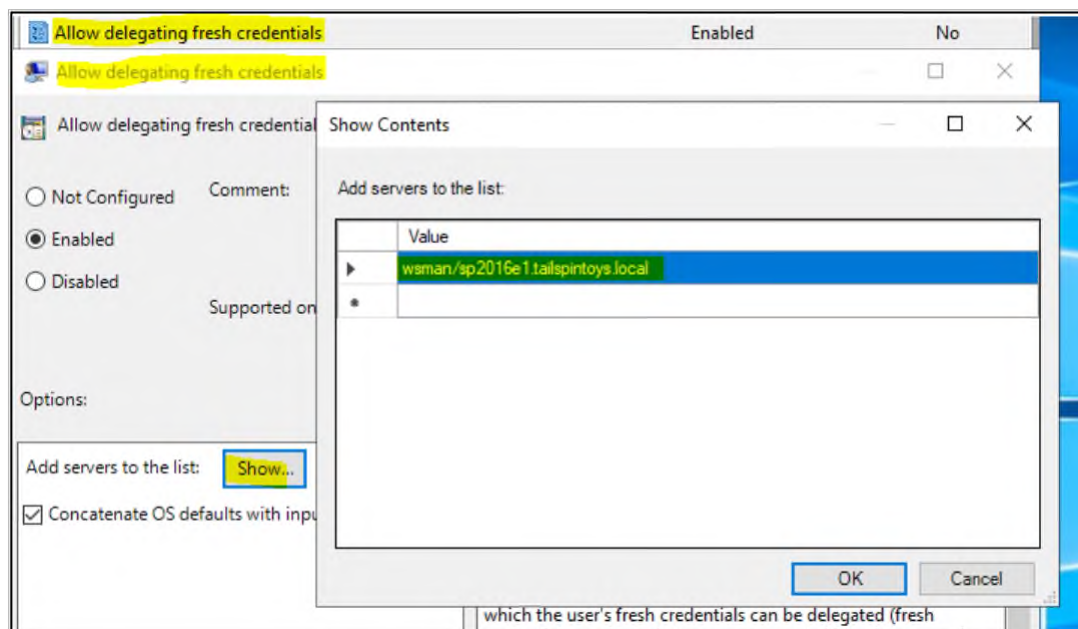
2. ローカル グループ ポリシー エディターで次の順に展開します：[コンピュータの構成]-[管理用テンプレート]-[システム]-[資格情報の委任]



3. 以下の設定を編集し、“wsman/<TargetServer FQDN>” をチェック/追加します。

[新しい資格情報の委任を許可する]

[NTLM のみのサーバー認証で新しい資格情報の委任を許可する]



4. `gpupdate /force` を実行します。

## リモート PowerShell および CredSSP の構成 (ターゲット サーバー)

ターゲット サーバーで、“管理者として実行” オプションで PowerShell プロンプトを開きます。以下のコマンドを実行します。

**winrm quickconfig**

**Enable-WSManCredSSP -Role server**

(Windows Server 2008 R2 の場合のみ、次の 2 つのコマンドを実行します)

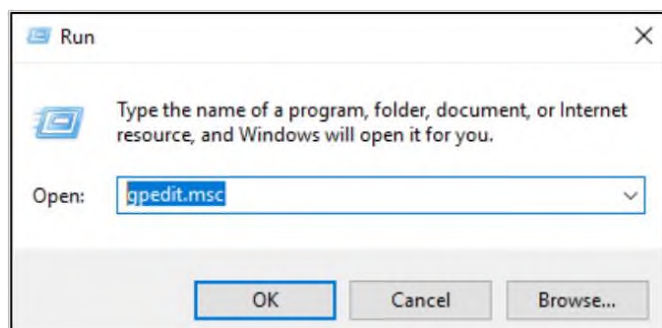
```
winrm set winrm/config/winrs '@{MaxShellsPerUser="25"}'
```

```
winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="600"}'
```

(上記の最後の 2 つのコマンドの引用符に注意)

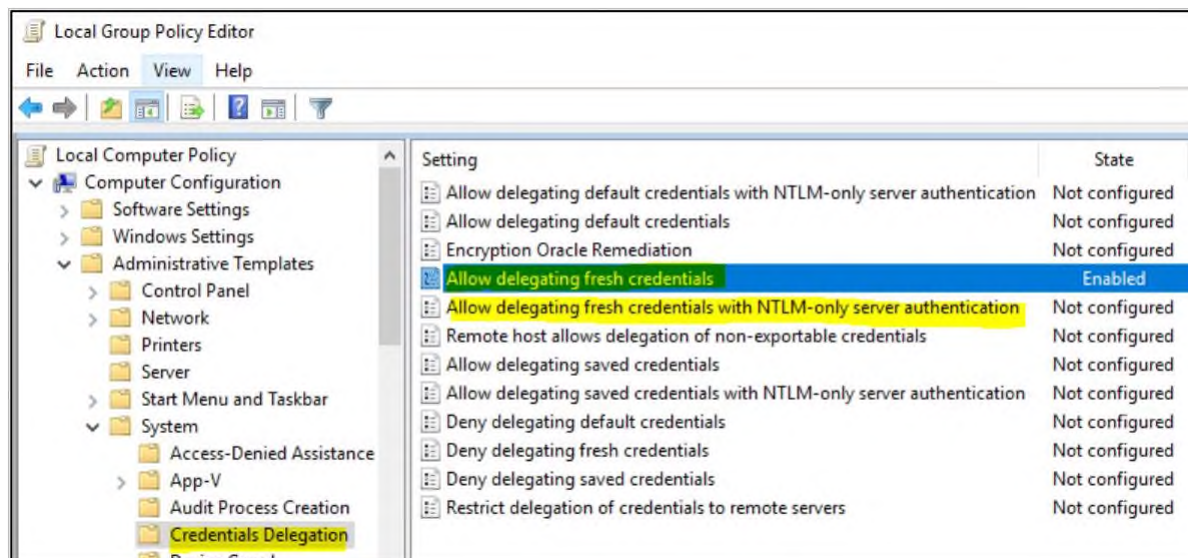
**ローカル グループ ポリシーを編集します (ターゲット サーバー)**

5. `gpedit.msc` を実行します。





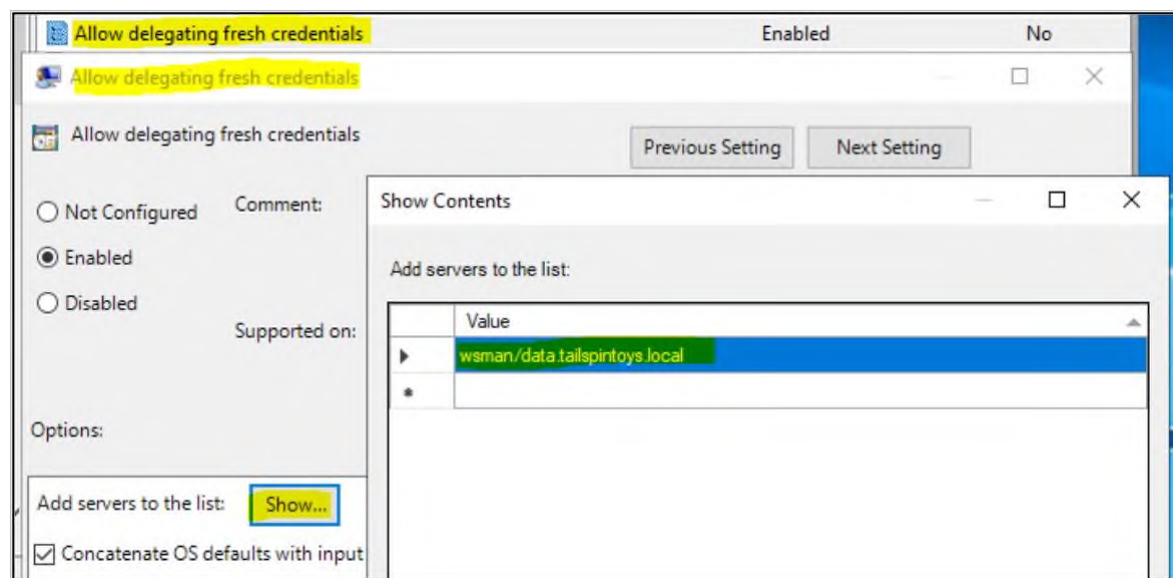
6. ローカル グループ ポリシー エディターで次の順に展開します: [コンピュータの構成]-[管理用テンプレート]-[システム]-[資格情報の委任]



7. 以下の設定を編集し、“wsman/<DataCollectionMachine FQDN>” をチェック/追加します。

[新しい資格情報の委任を許可する]

[NTLM のみのサーバー認証で新しい資格情報の委任を許可する]



8. gpupdate /force を実行します。

Microsoft 監視エージェント/OMS Gateway のインストールを完了し、ターゲット マシンで PowerShell リモート処理を構成したら、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。



## リモート PowerShell および CredSSP 構成のテスト

評価の一環として、SharePoint 情報のほとんどが、データ収集マシンからリモート/ローカルで PowerShell スクリプトを実行することにより収集されます。PowerShell スクリプトをターゲット サーバー上でリモートで実行できるように、CredSSP 委任を正しく構成することは非常に重要です。以下のスクリプトは、ターゲット サーバー上のスクリプトに接続して実行することにより、CredSSP が正しく構成されているかどうかを知るのに役立ちます。**データ収集マシンから以下のスクリプトを実行します。**

# 以下のスニペットを実行すると、SharePoint ファームのすべての SharePoint コンテンツ データベースの一覧が出力されます。

```
$farm = Get-Credential
```

```
$s = New-PSSession -ComputerName [Target Server FQDN] -Authentication CredSSP -Credential $farm Invoke-Command -Session $s  
-ScriptBlock { add-psnapin Microsoft.SharePoint.PowerShell -ea 0 }
```

```
Invoke-Command -Session $s -ScriptBlock { get-spfarm }
```

```
Invoke-Command -Session $s -ScriptBlock { get-spcontentdatabase }
```

```
Get-PSSession | Remove-PSSession
```

## ユーザー プロファイル サービス

ユーザー ログオフに関するユーザー プロファイル サービスの既定動作を変更する必要があります。ユーザー レジストリ ハイブへの開いているハンドルを持つアプリケーションがある場合でも、既定で Windows により、ログオフ時に強制的にユーザー レジストリ ハイブがアンロードされます。この既定動作は、スケジュールされたタスクによるオンデマンドの評価の実行中にリモート PowerShell の初期化ルーチンに干渉するので、評価データの正常な収集、および Log Analytics ポータルへの送信を妨げる場合があります。

データ収集マシンで、グループ ポリシー エディター (gpedit.msc) の以下の設定を、[未構成] から [有効] に変更します。

[コンピューターの構成] -> [管理用テンプレート] -> [システム] -> [ユーザー プロファイル] 'ユーザーのログオフ時にユーザー レジストリを強制的にアンロードしない'



Setting	State	Comment
Do not forcefully unload the users registry at user logoff	Enabled	No
Add the Administrators security group to roaming user profiles	Not configured	No
Delete user profiles older than a specified number of days on...	Not configured	No
Do not check for user ownership of Roaming Profile Folders	Not configured	No
Delete cached copies of roaming profiles	Not configured	No
Turn off the advertising ID	Not configured	No
Disable detection of slow network connections	Not configured	No
Prompt user when a slow network connection is detected	Not configured	No
Leave Windows Installer and Group Policy Software Installatio...	Not configured	No
Only allow local user profiles	Not configured	No
Set roaming profile path for all users logging onto this comp...	Not configured	No
Download roaming profiles on primary computers only	Not configured	No

Microsoft Monitoring Agent/OMS Gateway のインストールを完了し、データ収集マシンとターゲット マシンでセキュリティ更新プログラムの前提条件を構成したら、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。

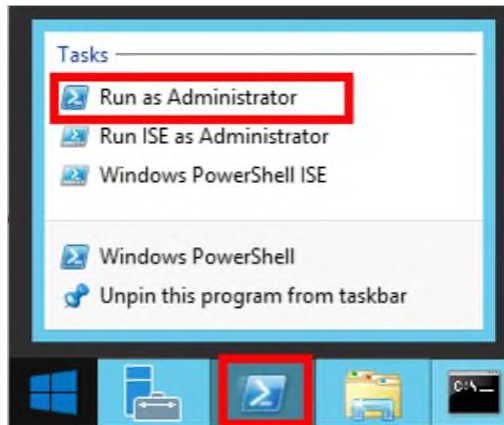
## SharePoint 評価のセットアップ

**注:** 自動パスワード オプションの使用を計画している場合は、このセクションをスキップして、[次のセクション](#)に記載されている手順を使用してください。

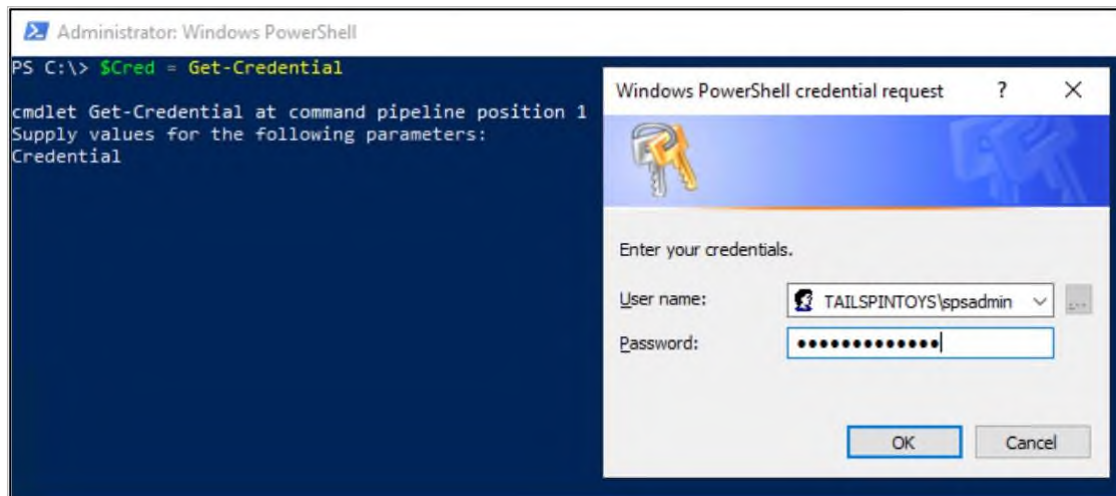
Microsoft Monitoring Agent/OMS Gateway のインストールを完了したら、SharePoint 評価をセットアップする準備は整っています。

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. 管理者として Windows PowerShell コマンド プロンプトを開きます。



2. Run `$Cred = Get-Credential`



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。これらの資格情報が SharePoint 評価を実行するために使用されます。

### 注意

1. このドメイン アカウントには以下のすべて権限が必要です:

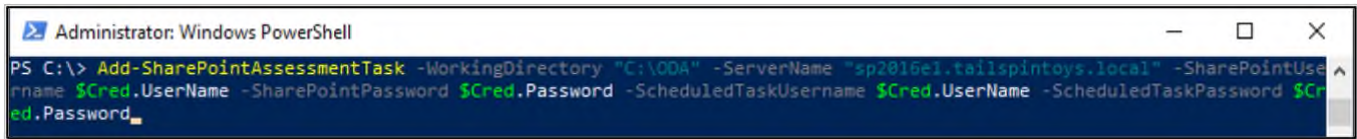
- ファーム管理者グループのメンバー。
- 少なくとも、ファーム内のすべての Web アプリケーションへの読み取りアクセス権。
- すべてのサービス アプリケーションへの完全なコントロール。
- 評価が行われている SharePoint ファームに関連するすべての SharePoint Server および SQL Server に対するローカル管理者の権限。
- SharePoint データベースを収納する SQL インスタンスすべての "SysAdmin" サーバーロールのメンバー。
  - ・ 注: SQL 認証はサポートされていません。

2. ファーム内のすべての SharePoint サーバーへの無制限のネットワーク アクセス。

**重要:**

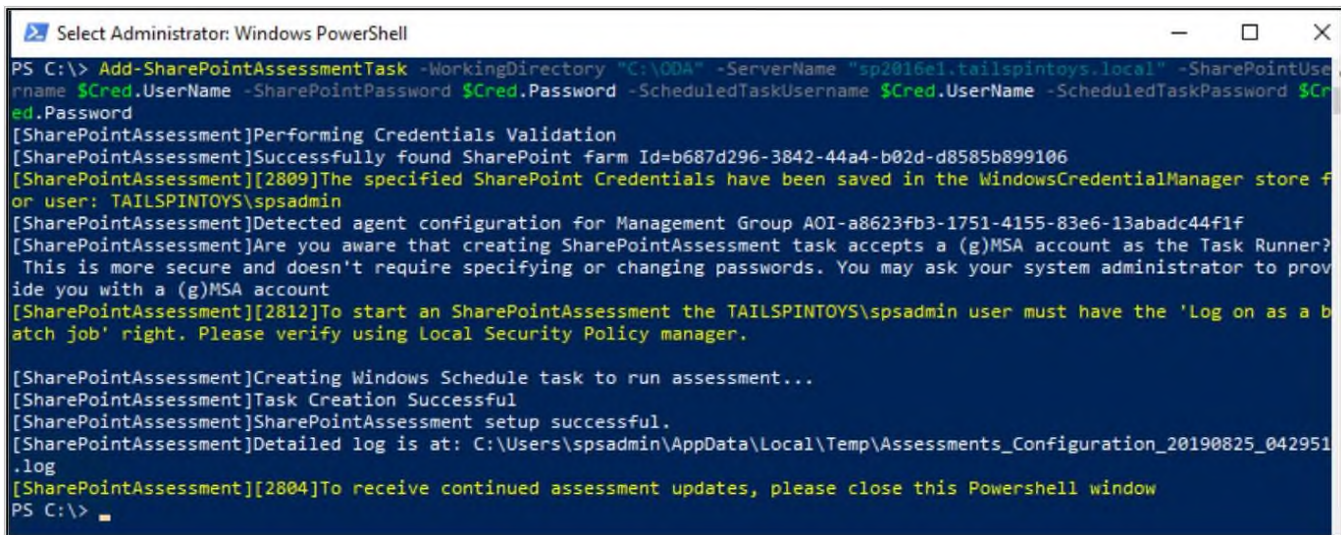
- 評価タスクの設定に使用するアカウントは、マシンのローカル管理者である必要があります。
  - アカウントは、マシンのログイン アカウントと同じである必要があります。
- これにより、アカウントに Windows Credential Manager の資格情報への適切なアクセス権が与えられることを保証します。

4. **Add-SharePointAssessmentTask -WorkingDirectory <Directory> -ServerName <TargetServer> -SharePointUsername \$Cred.UserName -SharePointPassword \$Cred.Password -ScheduledTaskUsername \$Cred.UserName -ScheduledTaskPassword \$Cred.Password** 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。また、<TargetServer> がターゲット サーバーの名前です。



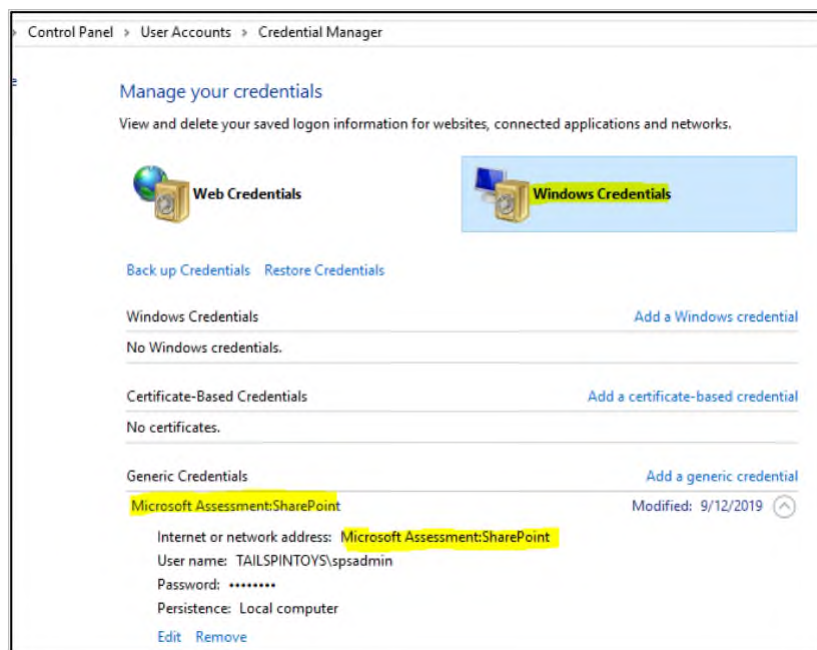
```
Administrator: Windows PowerShell
PS C:\> Add-SharePointAssessmentTask -WorkingDirectory "C:\ODD" -ServerName "sp2016el.tailspintoys.local" -SharePointUsername $Cred.UserName -SharePointPassword $Cred.Password -ScheduledTaskUsername $Cred.UserName -ScheduledTaskPassword $Cred.Password
```

5. 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。

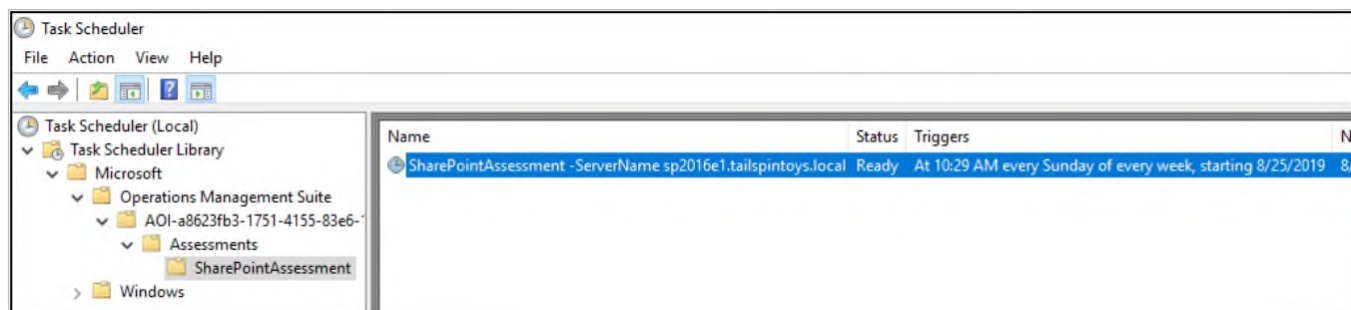


```
Select Administrator: Windows PowerShell
PS C:\> Add-SharePointAssessmentTask -WorkingDirectory "C:\ODD" -ServerName "sp2016el.tailspintoys.local" -SharePointUsername $Cred.UserName -SharePointPassword $Cred.Password -ScheduledTaskUsername $Cred.UserName -ScheduledTaskPassword $Cred.Password
[SharePointAssessment]Performing Credentials Validation
[SharePointAssessment]Successfully found SharePoint farm Id=b687d296-3842-44a4-b02d-d8585b899106
[SharePointAssessment][2809]The specified SharePoint Credentials have been saved in the WindowsCredentialManager store for user: TAILSPINTOYS\spsadmin
[SharePointAssessment]Detected agent configuration for Management Group AOI-a8623fb3-1751-4155-83e6-13abadc44f1f
[SharePointAssessment]Are you aware that creating SharePointAssessment task accepts a (g)MSA account as the Task Runner? This is more secure and doesn't require specifying or changing passwords. You may ask your system administrator to provide you with a (g)MSA account
[SharePointAssessment][2812]To start an SharePointAssessment the TAILSPINTOYS\spsadmin user must have the 'Log on as a batch job' right. Please verify using Local Security Policy manager.
[SharePointAssessment]Creating Windows Schedule task to run assessment...
[SharePointAssessment]Task Creation Successful
[SharePointAssessment]SharePointAssessment setup successful.
[SharePointAssessment]Detailed log is at: C:\Users\spsadmin\AppData\Local\Temp\Assessments_Configuration_20190825_042951.log
[SharePointAssessment][2804]To receive continued assessment updates, please close this Powershell window
PS C:\>
```

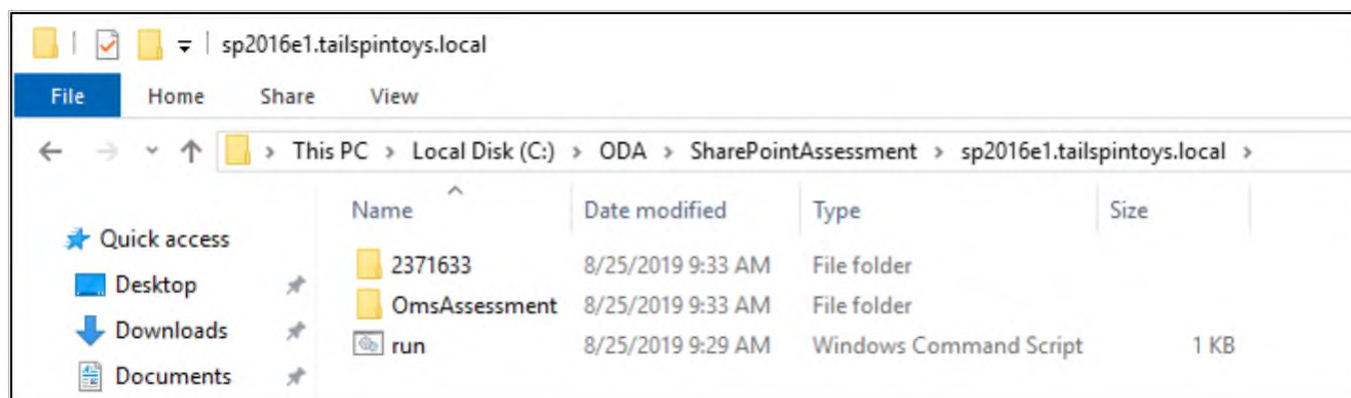
6. Windows Credential Manager で以下の入力を確認します。



7. データ収集は、名前 **SharePointAssessment -ServerName <Server Name>** 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。

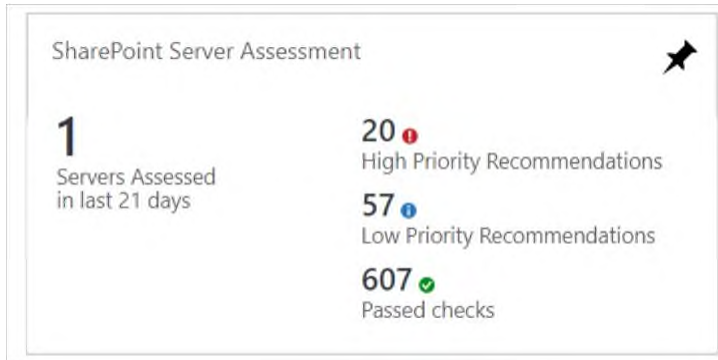


8. 収集および分析している間に、次の構造を使用し、セットアップ時に構成された **WorkingDirectory** フォルダの下にデータが一時的に保存されます：

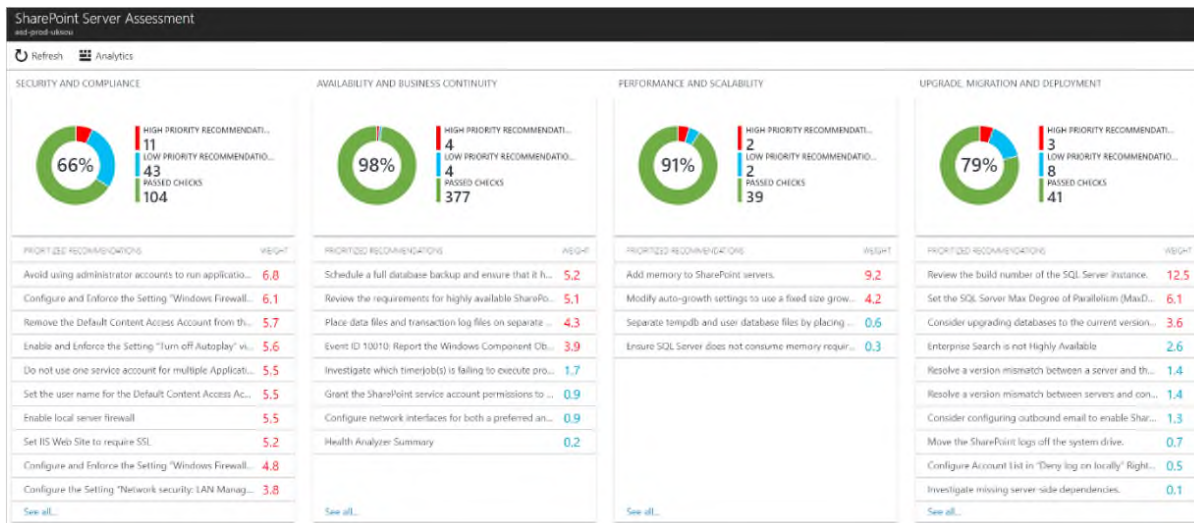




9. ツール マシンでデータ収集と分析を完了したら、次の選択したシナリオにより、log analytics ワークスペースに送信されます：
  - **直接**、データ収集マシンをインターネットに接続して構成している場合は、直接送信されます。**OMS Gateway** サーバー経由、このオプションが構成されている場合は、Log Analytics ワークスペースにそのデータが送信されます。
10. データ収集には約 30～60 分の時間がかかります。
11. データ収集が完了すると、Log Analytics ワークスペースに自動的にアップロードされます。評価結果を Log Analytics ダッシュボードに表示することができます。SharePoint Server 評価タイルをクリックし、次を確認します：



12. 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。

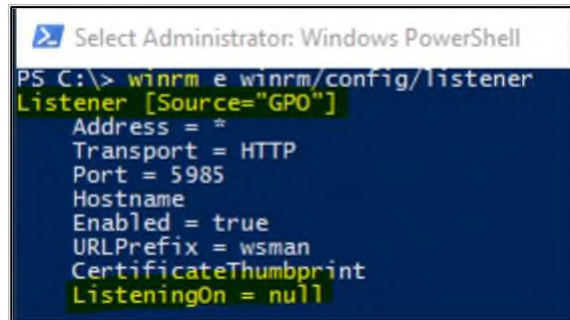


## 付録

### ターゲット サーバーの要件

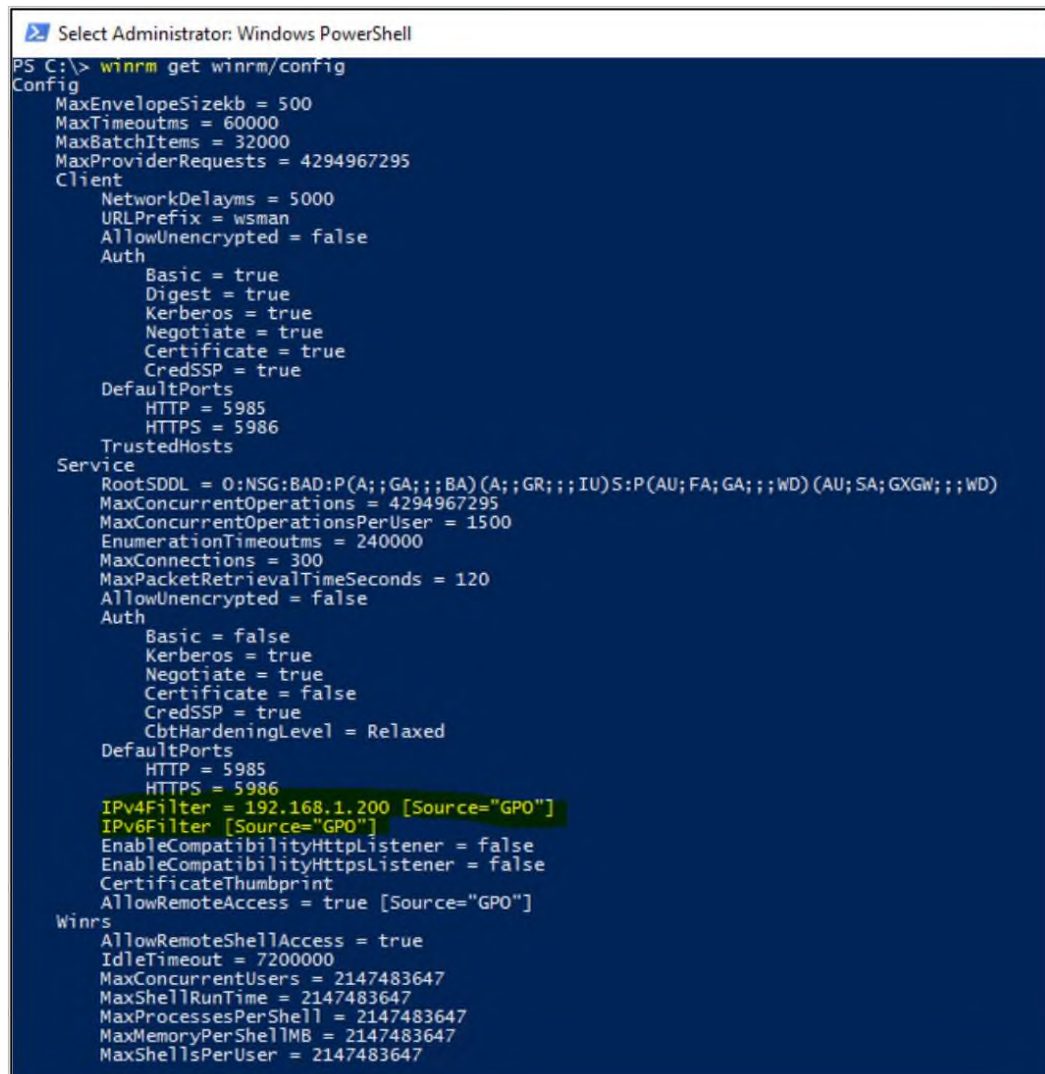
ターゲット サーバーで次のコマンドを実行し、以下の結果を取得したら、SharePoint 評価の設定に失敗したことになります。

> winrm e winrm/config/listener



```
Select Administrator: Windows PowerShell
PS C:\> winrm e winrm/config/listener
Listener [Source="GPO"]
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = null
```

> winrm get winrm/config



```
Select Administrator: Windows PowerShell
PS C:\> winrm get winrm/config
Config
  MaxEnvelopeSizekb = 500
  MaxTimeoutms = 60000
  MaxBatchItems = 32000
  MaxProviderRequests = 4294967295
  Client
    NetworkDelays = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
      Basic = true
      Digest = true
      Kerberos = true
      Negotiate = true
      Certificate = true
      CredSSP = true
    DefaultPorts
      HTTP = 5985
      HTTPS = 5986
    TrustedHosts
  Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
      Basic = false
      Kerberos = true
      Negotiate = true
      Certificate = false
      CredSSP = true
      CbtHardeningLevel = Relaxed
    DefaultPorts
      HTTP = 5985
      HTTPS = 5986
    IPv4Filter = 192.168.1.200 [Source="GPO"]
    IPv6Filter [Source="GPO"]
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true [Source="GPO"]
  Winrs
    AllowRemoteShellAccess = true
    IdleTimeout = 7200000
    MaxConcurrentUsers = 2147483647
    MaxShellRunTime = 2147483647
    MaxProcessesPerShell = 2147483647
    MaxMemoryPerShellMB = 2147483647
    MaxShellsPerUser = 2147483647
```

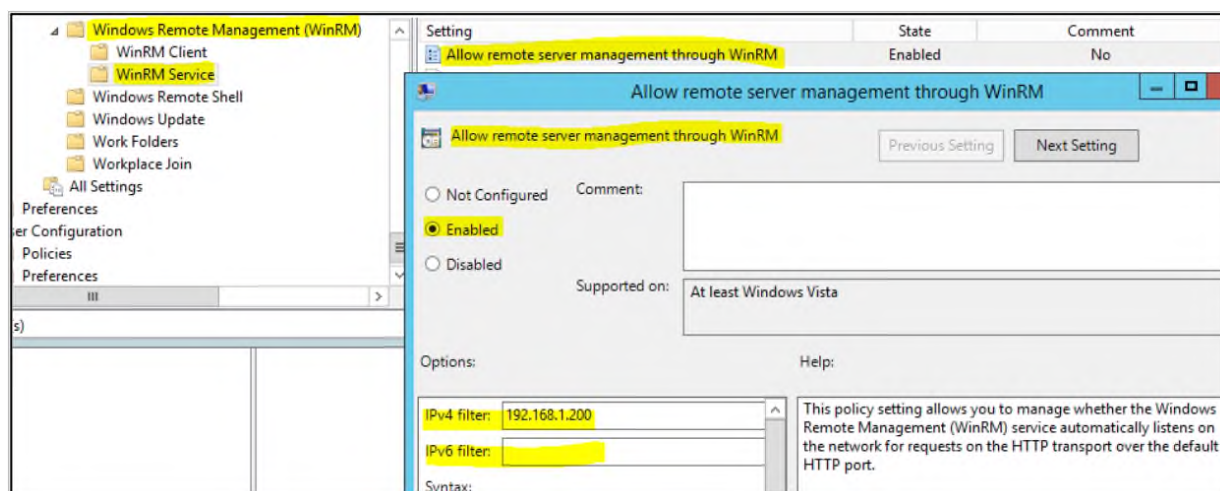
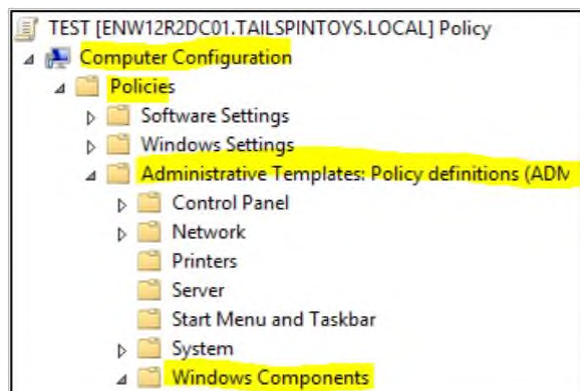


## エラー メッセージ

```
Administrator: Windows PowerShell
PS C:\> $Cred = Get-Credential

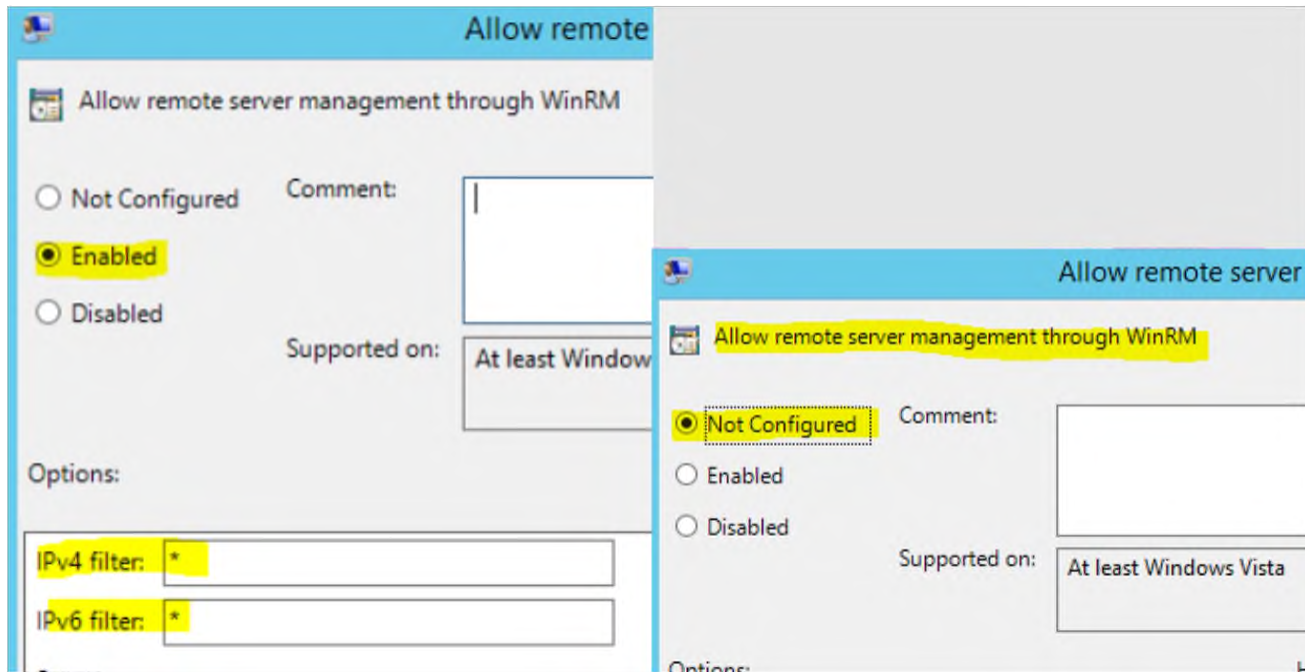
cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\> Add-SharePointAssessmentTask -WorkingDirectory "C:\ODA" -ServerName "ensp2019.tailspintoys.local" -SharePointUser
name $Cred.UserName -SharePointPassword $Cred.Password -ScheduledTaskUsername $Cred.UserName -ScheduledTaskPassword $Cr
ed.Password
[SharePointAssessment]Performing Credentials Validation
[SharePointAssessment][2932]ERROR: Connecting to remote server ensp2019.tailspintoys.local failed with the following err
or message : The WinRM client cannot process the request. A computer policy does not allow the delegation of the user cr
edentials to the target computer. Use gpedit.msc and look at the following policy: Computer Configuration -> Administrat
ive Templates -> System -> Credentials Delegation -> Allow Delegating Fresh Credentials. Verify that it is enabled and
configured with an SPN appropriate for the target computer. For example, for a target computer name "myserver.domain.com
", the SPN can be one of the following: WSMAN/myserver.domain.com or WSMAN/*.*.domain.com. For more information, see the a
bout_Remote_Troubleshooting Help topic.
[SharePointAssessment][2915]Terminating PowerShell errors while performing credentials validation
ExceptionType: Microsoft.PowerShell.Oms.Assessments.Commandlets.CredentialsValidation.CredentialValidationException
ExceptionMessage: Connecting to remote server ensp2019.tailspintoys.local failed with the following error message : The
WinRM client cannot process the request. A computer policy does not allow the delegation of the user credentials to the
target computer. Use gpedit.msc and look at the following policy: Computer Configuration -> Administrative Templates ->
System -> Credentials Delegation -> Allow Delegating Fresh Credentials. Verify that it is enabled and configured with a
n SPN appropriate for the target computer. For example, for a target computer name "myserver.domain.com", the SPN can be
one of the following: WSMAN/myserver.domain.com or WSMAN/*.*.domain.com. For more information, see the about_Remote_Troub
leshooting Help topic.
StackTrace: at Microsoft.PowerShell.Oms.Assessments.Commandlets.CredentialsValidation.SharePointCredentialsValidator.
ValidateCommand(PowerShell ps, Boolean terminate)
at Microsoft.PowerShell.Oms.Assessments.Commandlets.CredentialsValidation.SharePointCredentialsValidator.ValidateCred
entials(String username, SecureString password)
[SharePointAssessment][2916]Credentials validation failed. Ensure you specify correct credentials with Administrative ri
ghts. Terminating processing
PS C:\>
```

この場合、ドメイン レベルの GPO での “WinRM を介したリモート サーバー管理を許可する” により、次のようになります：



従って、AD/GPO 管理者にターゲット サーバーのポリシー設定を変更するよう連絡する必要があります。

設定のサンプル:



## SharePoint 評価の資格情報の前提条件

SharePoint 評価の検出では、資格情報を使用して次の 2 つのことを実行します:

1. WCM から読み取る
2. これらの資格情報が SP ファームへのアクセスに機能していることを検証する。SharePoint が実行してくれるため、Windows レベルでは資格情報を検証しません。

2 つの手順のいずれかに失敗した場合は、新しい資格情報を要求してみてください。

以下の手順では、すべてのコマンドが、**管理者特権**でのコマンド プロンプトまたは**管理者特権**での PowerShell から実行されます。

### 手順 #1 -WCM から資格情報を取得する

データ収集マシンで UserA としてログオン済みで、スケジュールされたタスクが UserB として実行されていることを知っている場合

- UserA = UserB の場合は、CmdKey のみが必要になり、このコマンドを試すことができます

```
cmdkey /list
```

このようなエントリが表示されるはずです (異なる資格情報で!)

```
Target: LegacyGeneric:target=Microsoft Assessment:SharePoint
Type: Generic
User: Genetier\Luc
```

Windows Credentials Manager を使用することもできます。

- **UserA ≠ UserB**の場合は、以下のコマンドのように、RunAs コマンドを使用して UserB として偽装する必要があります

```
runas /profile /user:domainB\UserB "cmdkey.exe /list"
```

(UserA=UserB) の場合でも、同じ結果が表示されるはずですが。

**この場合、Windows Credentials Manager を使用できません** (WCM GUI は現在ログオンしているユーザーにのみ機能します)

これは、資格情報のマネージャー エントリの有無を検証するだけなので、そのコンテンツを検証するものではありません。

資格情報の入力を取得するために、PowerShell を使用できます。

それに特定のモジュールをインストールしてから、コンテンツを取得するためのコマンドを使用する必要があります。

```
Install-Module CredentialsManager -force
```

```
Get-StoredCredential -Target "Microsoft Assessment:SharePoint"
```

パスワードを読み取る場合の方法があります (顧客からパスワードが送信されないことを確認してください!)

```
$cred = Get-StoredCredential -Target "Microsoft Assessment:SharePoint"
```

```
(new-object System.Net.NetworkCredential($cred.UserName, $cred.Password)).Password
```

RunAs と PowerShell を使用する必要がある場合は、Start-Process を試すか、コマンド プロンプトから、runas /profile/user:domainB\UserB powershell.exe を試します

いずれの場合も、対話型ログオンを許可するのに十分な Windows 特権が userB に与えられている必要があります (ODA には不要、これらのテストを実行する場合のみ)。

## 手順 #2

次に、SharePoint ファームにアクセスするための資格情報が有効であることを検証する必要があるので、次のスクリプトを使用します。

```
Add-PSSnapin -Name Microsoft.SharePoint.PowerShell
```

```
Get-SPFarm
```

データ収集マシンが SharePoint サーバーの場合は、これをローカルで実行できます (偽装された PowerShell ウィンドウを使用)

それ以外の場合は、WinRM を使用して、適切に構成する必要があります - CredSSP 構成手順を検証します。

## 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 SharePoint 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。

データ収集ではワークフローとコレクターを使用します。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. イベント ログ コレクター
3. Windows PowerShell
4. ファイル データ コレクター
5. SQL データ コレクター
6. Windows Management Instrumentation (WMI)

### 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サーバ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、Operations Manager サービスの状態を分析できるようになります。

### イベント ログ コレクター

サーバーからイベント ログを収集します。SharePoint サーバーおよび関連する SQL サーバー、アプリケーションおよびシステムのイベント ログから、過去 5 日間の情報、警告およびエラーを収集します。

### Windows PowerShell

次のようなさまざまな情報が収集されます：

SharePoint ファーム情報

SharePoint コンテンツ データベース情報

### 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。

### SQL データ コレクター

SQL クエリは、SQL Server のセットアップなど、SharePoint ファーム構成に関する情報を収集するために使用されます。

### 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  
環境にある各サーバー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、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  
環境にある各サーバー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。