

Windows Server 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 Windows Server (サーバー、セキュリティ、Hyper-V、フェールオーバー クラスターおよび IIS) 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
サポートされていないバージョン	2
両方のシナリオに共通	2
データ収集マシン	2
PowerShell のリモート処理	2
ユーザー プロファイル サービス	9
リモート イベント ログ管理	10
Windows Server 評価のセットアップ	10
付録	14
データ収集メソッド	14

このドキュメントの最終更新日は、2020 年 8 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=865884>

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

このサービスは、Windows Server 2012 以降を実行するサーバーで利用できます。

サポートされていないバージョン

- 共有構成を使用して実行している IIS サーバー (http://www.iis.net/learn/web-hosting/configuring-servers-in-the-windows-web-platform/shared-configuration_211)。
- ワークスペースで実行している IIS サーバー (ドメインに参加していない)。このシナリオは、各ターゲット サーバーで直接個別に収集プロセスを実行することにより、実現できます。

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:
 - 環境にあるすべてのサーバーのローカル管理者グループのメンバー
 - ツール マシンのローカル管理者グループのメンバー
 - ツール マシンからすべてのサーバーへの無制限のネットワーク アクセス

データ収集マシン

- データ収集マシンは、ドメインに参加済みであり、評価されるドメインに参加しているサーバーへの Windows ドメインの信頼パスを使用する必要があります。
- [Windows PowerShell 3.0](#) 以降がインストールされています
- [Log Parser 2.2](#) がインストールされています
- RemoteSigned に設定された PowerShell 実行ポリシー
- 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 5 GB の空きディスク領域、さらに、データ収集中に評価される環境のターゲット サーバーごとに最大 6 GB
- データ収集マシンは、すべてのサーバーに接続し、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。PowerShell プロンプトで `$PSVersionTable.CLRVersion` を実行すると、これを確認できます。
- 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。

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 エージェントは、セキュリティ更新プログラムをスキャンするすべての範囲内のサーバーで実行される必要があります。

Windows Server 2008-2012 R2（またはデフォルトが変更されている場合はそれ以降）ターゲットマシンの追加要件:

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

注意 1: ターゲット マシンでは、PowerShell バージョン 2 以降が必要になり、Windows Server 2008 R2 で始めると、既定でインストールされています。Windows Server 2008 SP2 の場合、既定では、PowerShell version 2 がインストールされていません。こちらからダウンロードできます <https://aka.ms/wmf3download>

注意 2: Windows Server 2012 R2 および Windows Server 2016 は、既定で WinRM および 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 サーバーに対する既定の構成が変更された場合のみ、実行される必要があります。

注意 3: Windows Server 2008 から Windows Server 2012 までは、既定で WinRM が無効になっています。以下で詳しく説明されている次の構成手順は、PowerShell のリモート処理をサポートするために構成される必要があります。

- 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）
 - “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 サーバ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) 範囲内のサーバーの組織単位にリンクされている新しい 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
```

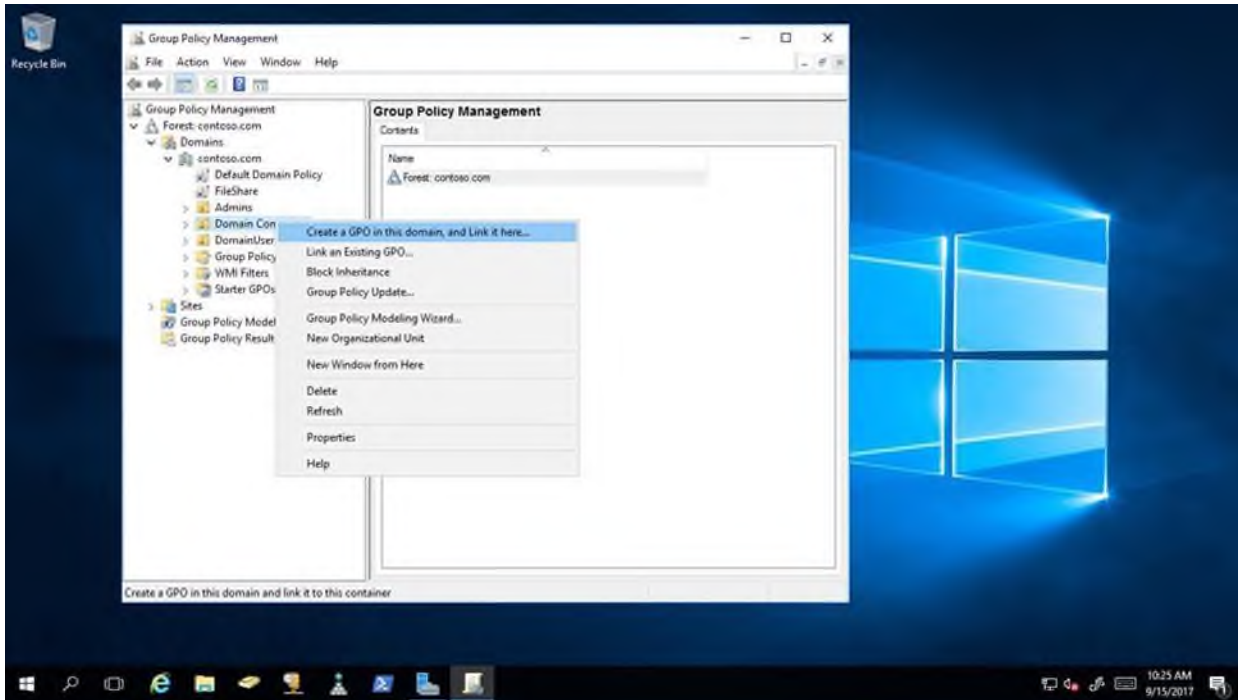
Windows IP の構成

```
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
```

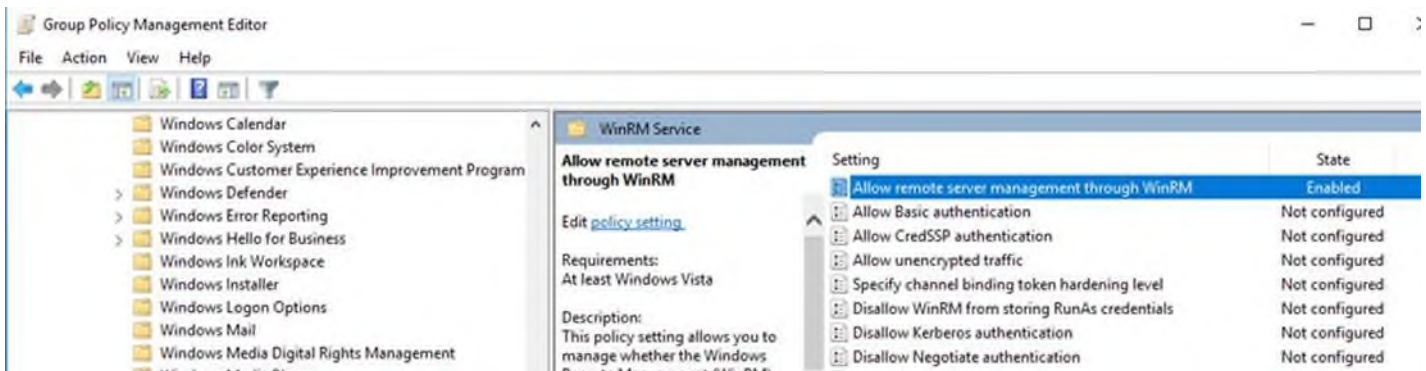
マシンの IPv4 アドレスをメモします。構成の最後の手順では、このアドレスを使用して、データ収集マシンのみがターゲット サーバーで Windows Update エージェントと通信できることを確認します。

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サーバーの OU にリンクさせます。

1. 新しい GPO を作成します。サーバーの組織単位に GPO が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グループ ポリシーの名前付け規則、または“Windows Server 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<グループポリシー>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）。“WinRM 経由のリモート サーバー管理を許可します” を有効にします。IPv4 と IPv6 のフィルターを指定する必要があります。（“*”により、受信サーバー アクセスがすべて許可されますが、ツール マシンの IP アドレスを指定することが推奨されます）



Allow remote server management through WinRM

Allow remote server management through WinRM Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on: At least Windows Vista

Options: Help:

IPv4 filter: *

IPv6 filter: *

Syntax:

Type "*" to allow messages from any IP address, or leave the field empty to listen on no IP address. You can specify one or more ranges of IP addresses.

Example IPv4 filters:

2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22

*

Example IPv6 filters:

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

If you enable this policy setting, the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port.

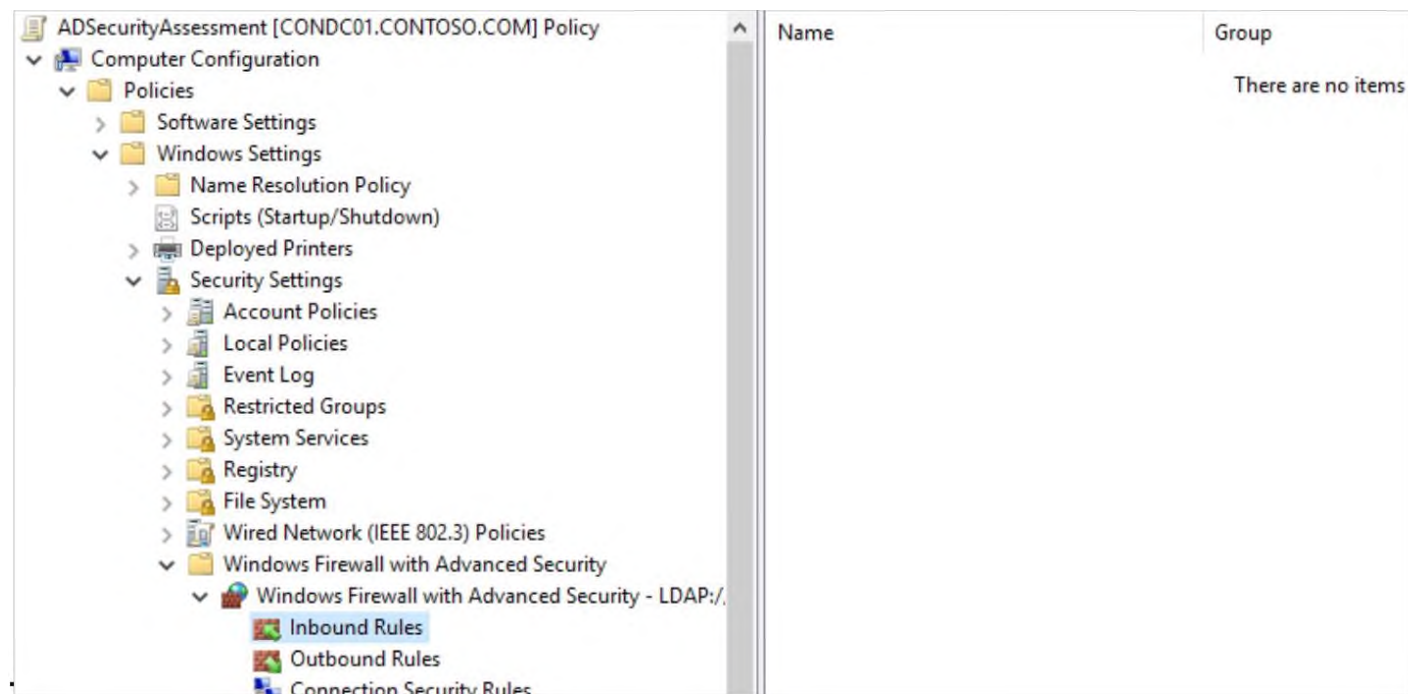
To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting with exceptions for Port 5985 (default port for HTTP).

If you disable or do not configure this policy setting, the WinRM service will not respond to requests from a remote computer, regardless of whether or not any WinRM listeners are configured.

The service listens on the addresses specified by the IPv4 and IPv6 filters. The IPv4 filter specifies one or more ranges of IPv4 addresses, and the IPv6 filter specifies one or more ranges of IPv6 addresses. If specified, the service enumerates the available IP addresses on the computer and uses only addresses that fall within one of the filter ranges.

OK Cancel Apply

3. 詳細なファイアウォールの受信規則を作成し、ツール マシンからターゲット 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 GP0 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. カスタムの規則を作成し、[次へ] を選択します

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

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

What type of rule would you like to create?

☐ **Program**
Rule that controls connections for a program.

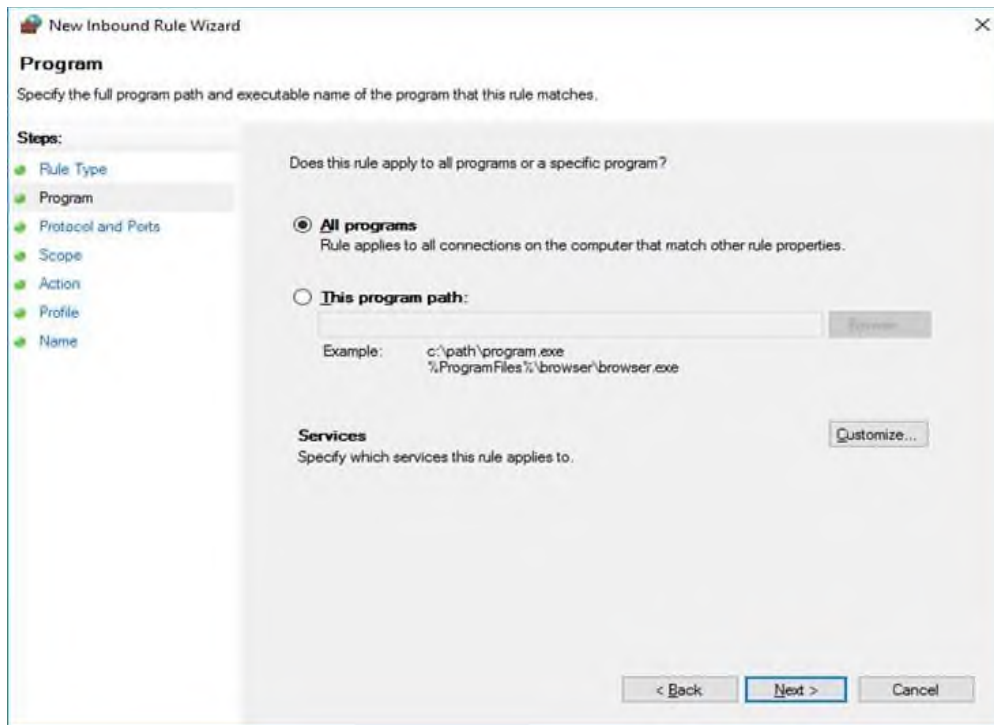
☐ **Port**
Rule that controls connections for a TCP or UDP port.

☐ **Predefined:**
Active Directory Domain Services
Rule that controls connections for a Windows experience.

☒ **Custom**
Custom rule.

< Back **Next >** Cancel

6. 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 contains the following text and controls:

Program
Specify the full program path and executable name of the program that this rule matches.

Steps:

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

Does this rule apply to all programs or a specific program?

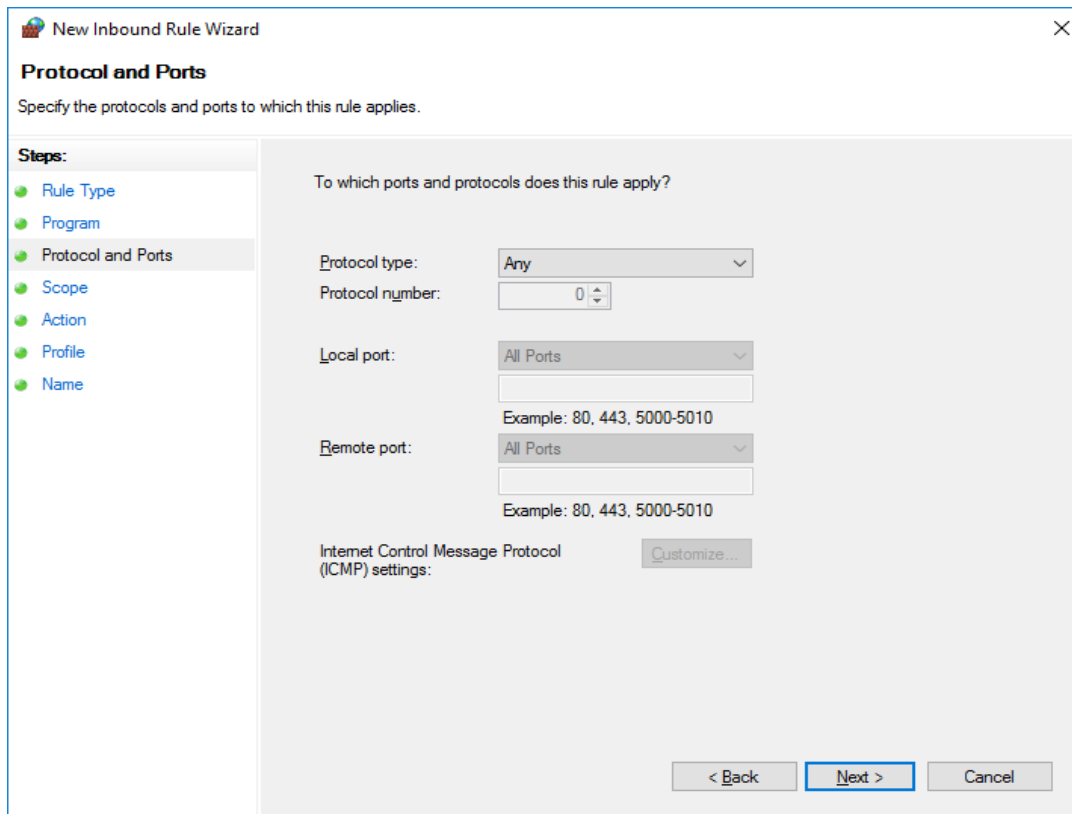
☒ **All programs**
Rule applies to all connections on the computer that match other rule properties.

☐ **This program path:**
Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to. Customize...

< Back **Next >** Cancel

7. 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 contains the following text and controls:

Protocol and Ports
Specify the protocols and ports to which this rule applies.

Steps:

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

To which ports and protocols does this rule apply?

Protocol type: Any
Protocol number: 0

Local port: All Ports
Example: 80, 443, 5000-5010

Remote port: All Ports
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: Customize...

< Back **Next >** Cancel

8. 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

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

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'

Microsoft Management 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。

リモート イベント ログ管理

- ◆ サーバーのファイアウォールを構成し、Windows Server 2008/Windows Server 2008 R2 以降を実行するすべてのサーバーでリモート イベント ログ管理が有効になっていることを確認します。オフライン クライアントは、リモート イベント ログ管理が許可されていない場合に、Windows Server 2008/Windows Server 2008 R2 以降からイベント ログ情報を収集できない場合があります。リモート管理が有効になっている場合は、リモート イベント ログ管理を許可する規則も有効化されます。

Name	Protocol	Local Port	Remote Port	Action	Direction
Remote Administration (RPC-EPMAP)	Remote Administration	All	No	Allow	Ni
Remote Desktop (TCP-In)	Remote Desktop	All	Yes	Allow	Ni
Remote Event Log Management (NP-In)	Remote Event Log Management	All	Yes	Allow	Ni
Remote Event Log Management (RPC)	Remote Event Log Management	All	Yes	Allow	Ni
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Management	All	Yes	Allow	Ni
Remote Scheduled Tasks Management (RPC)	Remote Scheduled Tasks Man...	All	No	Allow	Ni

Windows Server 2008/Windows Server 2008 R2 以降のイベント ログ データをツールで収集できるかどうかをテストするために、eventvwr.msc を使用して、Windows Server 2008/Windows Server 2008 R2 以降への接続を試すことができます。接続できる場合は、イベント ログ データを収集できます。リモート接続が失敗した場合は、Windows 組み込みのファイアウォールを有効にし、リモート イベント ログ管理を許可する必要がある場合があります。

サーバーでリモートからファイアウォール規則を作成する前に、オプションのリモート ファイアウォール管理が、詳細なファイアウォール設定を利用し、Windows Server 2008/Windows Server 2008 R2 以降すべてで有効になっている必要があります。リモート イベント ログ管理を許可するには、新しい GPO を作成します：

GPO を構成する

1. 新しい GPO を作成してサーバーに対応する OU にリンクさせます。

GPO 内で、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 ファイアウォールを開き、[受信規則] を右クリックし、[新しい規則] をクリックします。

2. 新規の受信規則ウィザードの [規則の種類] で、[事前定義] を選択します。規則の一覧で、

[リモート イベント ログ管理] をクリックし、[次へ] をクリックします

3. 事前定義された規則ページで、リモート イベント ログ管理 (RPC) の規則のチェックボックスを選択し、[次へ] をクリックします。注意：評価では他の 2 つのリモート イベント ログ管理の規則は必要ありませんが、リモート イベント ログ管理で必要とされる場合があります。

4. 操作ページで、[接続を許可する] を選択し、[完了] をクリックします。

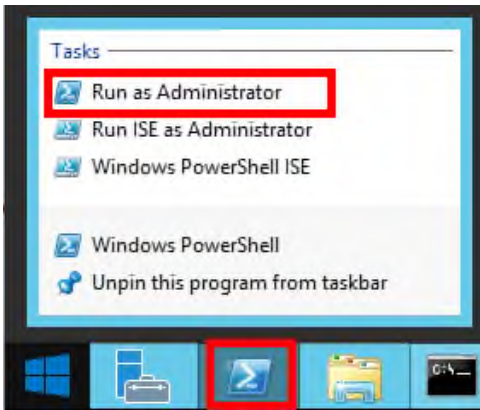
注意： この GPO がレプリケートされ、データ収集を開始する前に、評価が行われるすべてのサーバーに適用されることを許可してください。

Windows 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、Windows Server 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に応じて、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：

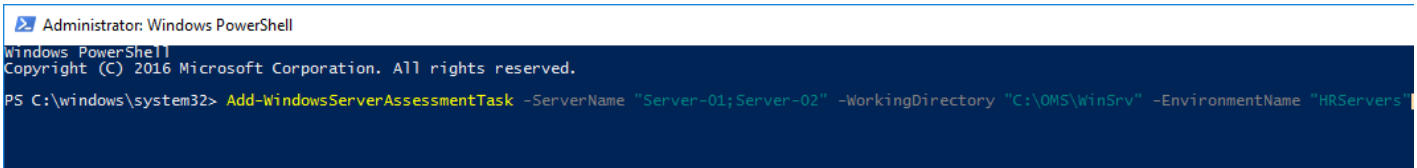
1. Windows PowerShell コマンド プロンプトを管理者として開きます



2. ユーザー アカウントの使用:

Add-WindowsServerAssessmentTask -ServerName <YourServerNames> -WorkingDirectory <DirectoryPath> -EnvironmentName <FriendlyNameforEnvironment> コマンドを実行します。このコマンドでは、<YourServerNames> が環境にある 1 つ以上のサーバーのセミコロン区切りの FQDN 名または NetBIOS 名であり、<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される既存のディレクトリへのパスになり、<EnvironmentName> が評価ポータルフィルターのフレンドリ名です。

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。環境名が提供されていない場合、スケジュールされたタスクが既定の環境名として使用されます。



以下の方法を使用して、テキスト ファイルからサーバーの一覧をインポートすることもできます:

```
PS C:\WINDOWS\system32> $Servers = Get-Content "C:\Docs\ServerList.txt"
```

Add-WindowsServerAssessmentTask -ServerName \$Servers -WorkingDirectory "C:\OMS\WinSrv"、セミコロンで区切られた複数のサーバーの一覧を含むテキスト ファイルの例: "Server01;Server02;Server03"。

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。

- a. 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
- b. 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-WindowsServerAssessmentTask -ServerName <YourServerNames> -WorkingDirectory <DirectoryPath> -ScheduledTaskUsername <MSAname> -RunWithManagedServiceAccount \$True

このコマンドでは、<YourServerNames> が環境にある 1 つ以上のサーバーのセミコロン区切りの FQDN 名または NetBIOS 名であり、<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、Windows Server 評価を実行するために使用されます。

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Add-WindowsServerAssessmentTask -ServerName "cluster-01;cluster-02" -WorkingDirectory "C:\OMS\WinSrv"
[WindowsServerAssessment]Detected agent configuration for Management Group AOI-3c7e8975-4333-4d50-85d8-588f72b7c490
[WindowsServerAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[WindowsServerAssessment]User(DomainName\UserName):
redmond\romin
[WindowsServerAssessment]Enter the password for redmond\romin:
*****
[WindowsServerAssessment]Creating Windows Schedule task to run assessment...
[WindowsServerAssessment]WindowsServerAssessment setup successful.
[WindowsServerAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20180214_113313.log
PS C:\WINDOWS\system32>
```

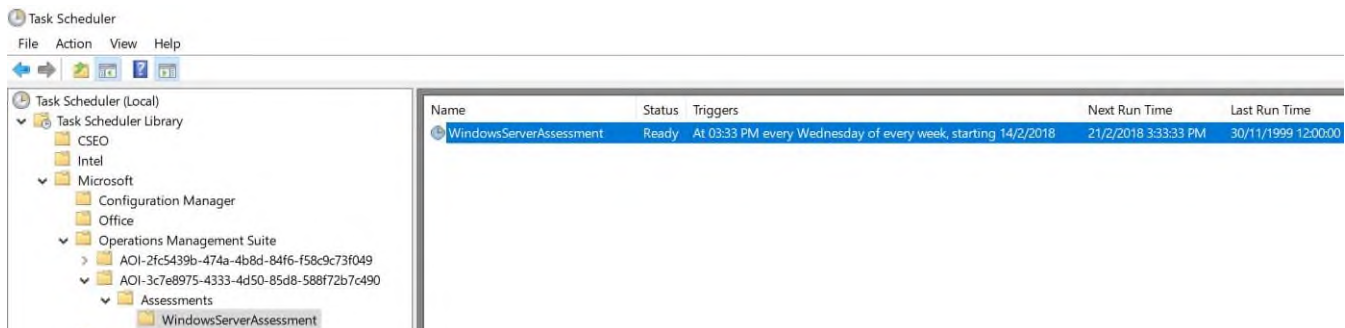
注: このドメイン アカウントは、以下のすべての権限を持っている必要があります。

- データ収集マシンのローカル管理者である必要があります。
- それぞれ評価されるターゲット サーバーのローカル管理者である必要があります
- 評価されるそれぞれのサーバーに対する制限のないネットワーク アクセス

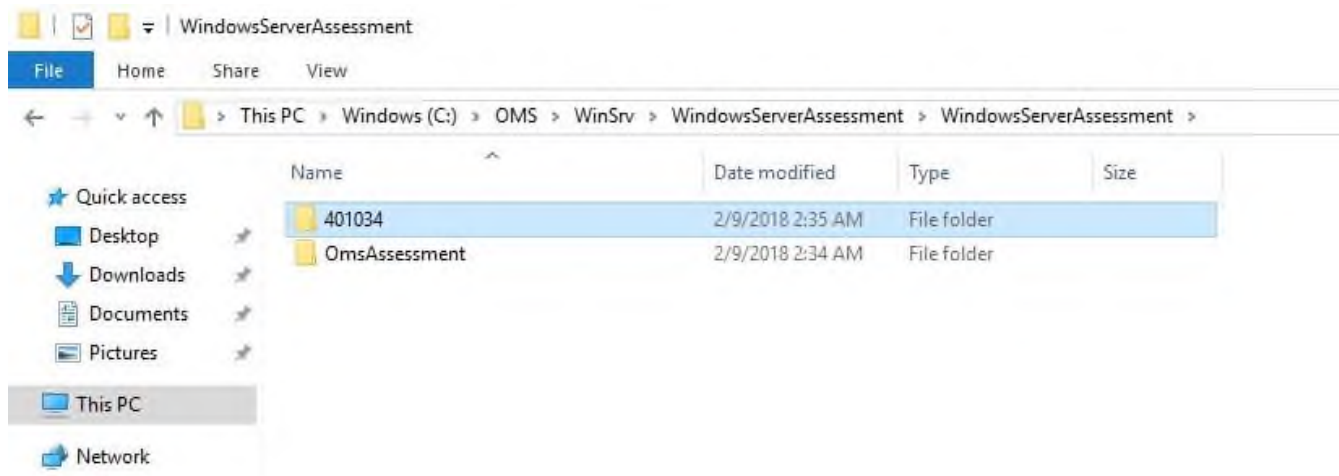
5. 必要な構成に基づいてスクリプトが続行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Add-WindowsServerAssessmentTask -ServerName "cluster-01;cluster-02" -WorkingDirectory "C:\OMS\WinSrv"
[WindowsServerAssessment]Detected agent configuration for Management Group AOI-3c7e8975-4333-4d50-85d8-588f72b7c490
[WindowsServerAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[WindowsServerAssessment]User(DomainName\UserName):
redmond\romin
[WindowsServerAssessment]Enter the password for redmond\romin:
*****
[WindowsServerAssessment]Creating Windows Schedule task to run assessment...
[WindowsServerAssessment]WindowsServerAssessment setup successful.
[WindowsServerAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20180214_113313.log
PS C:\WINDOWS\system32>
```

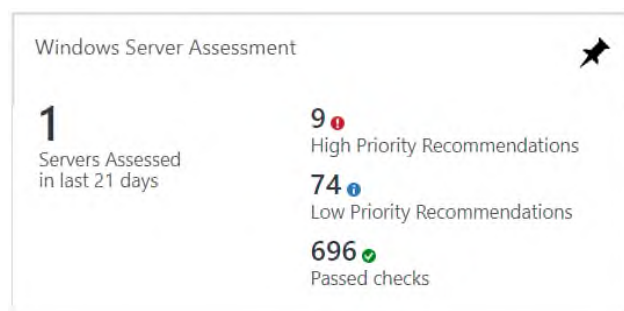
6. データ収集は、名前 “WindowsServerAssessment” のスケジュールされたタスクにより、前のスクリプトの実行後 1 時間以内、それから 7 日ごとにトリガーされます。タスクは、別の日時に実行するように変更できます。また強制的に即実行することもできます。



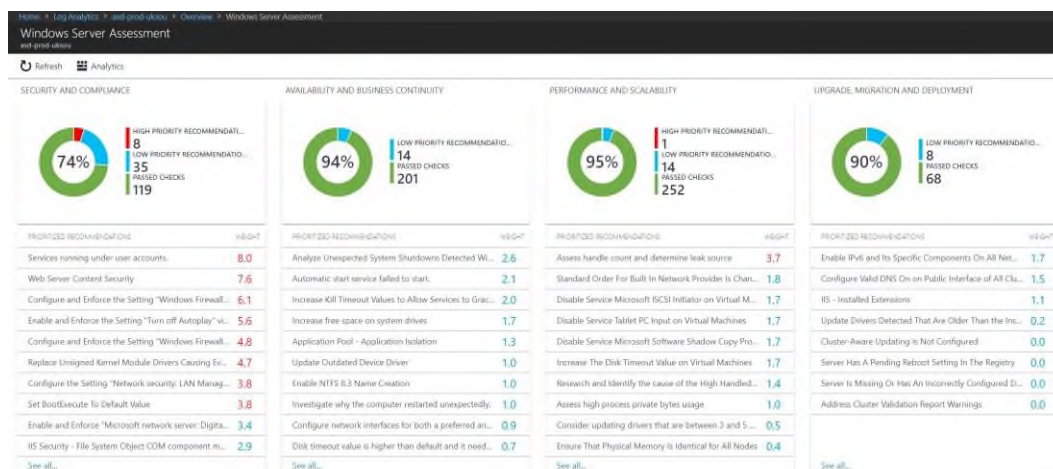
7. 収集および分析している間に、次の構造を使用し、セットアップ時に構成された WorkingDirectory フォルダの下にデータが一時的に保存されます:



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。[Windows Server 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 Windows 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. Xperf
3. EventLogCollector
4. Windows PowerShell
5. FileDataCollector
6. WMI
7. Nltest
8. LDAP コレクター
9. カスタム C# コード
10. 検証

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\SYSTEM\CurrentControlSet\Services のサービス情報
- HKLM_SOFTWARE_Microsoft_Windows_NT_CurrentVersion のオペレーティング システム情報

2. Xperf

[Xperf](#) は、起動時間統計を作成できる [Windows パフォーマンス ツールキット](#)の一部であるツールです。Xperf を使用すると、起動時間が評価され、ディスクや CPU を最も利用する上位 10 のプロセスが特定されます。

3. EventLogCollector

ターゲット マシンからのイベント ログを収集します。多くの場合、過去 7 日間の異なるイベント ログが収集されます。

4. Windows PowerShell

次のようなさまざまな情報が収集されます：

- BCD ストア ブート構成データ
- 最適化レート

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。

6. 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
範囲内のサーバ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。

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、Windows サーバーで有効なユーザーの権利のコレクションです。

8. 検証

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、サーバーで有効なユーザーの権利のコレクションです。

各ターゲット マシンに対してコンピューターのレジストリ FQDN 名と WMI を確認します

```
get-wmiobject Win32_ComputerSystem -computer localhost | fl Name, Domain
```

期待される結果:

名前: <ComputerName> ドメイン : dns.name

管理用共有をすべてのターゲット マシンに対して利用できるかどうかを確認します

```
get-wmiobject WIN32_Share -computer "<ComputerName>" | ?{$_.Name -eq "C$"} | FL Name
```

期待される結果: 名前 : C\$

すべてのターゲット マシンに対してスケジュールされたタスクを確認します

```
$([xml](schtasks /query /XML ONE /S "<ComputerName>")).Tasks.Task.Count
```

期待される結果: > 0

PowerShell のリモート処理が有効化されていることを確認しています:

```
Enter-PSSession -Computer <ComputerName>
```

期待される結果: [ComputerName]: PS C:¥Users¥UserName¥Documents>