

# Windows クライアント評価：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 クライアント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
PowerShell のリモート処理 .....	2
ユーザー プロファイル サービス .....	8
Windows クライアント評価のセットアップ .....	8
付録 .....	12
データ収集メソッド .....	12

このドキュメントの最終更新日は、2020 年 8 月 21 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=860120>

## 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 8.1 以降を実行する Active Directory ドメインに参加しているクライアントで利用できます。
- Azure Active Directory またはワークグループに完全に参加しているクライアントは、エージェントおよび評価をターゲットの Windows クライアント マシンで個別に実行している場合にのみサポートされます。

## 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:
    - 環境に含まれるすべてのクライアントにおける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クライアントまで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、評価するドメインに参加しているクライアントへの Windows ドメインの信頼パスを使用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 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 クライアントごとに最大 6 GB。
- **データ収集マシン**は、すべてのクライアントに接続し、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、コンピューターの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のスキャンの範囲内すべてのワークスペースで実行されている必要があります。

### Windows 7 以降のターゲット 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、ターゲットのワークステーション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:** Windows 7 と Windows 10 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。

- 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 ワークステーションのローカルファイアウォール 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) ワークステーション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

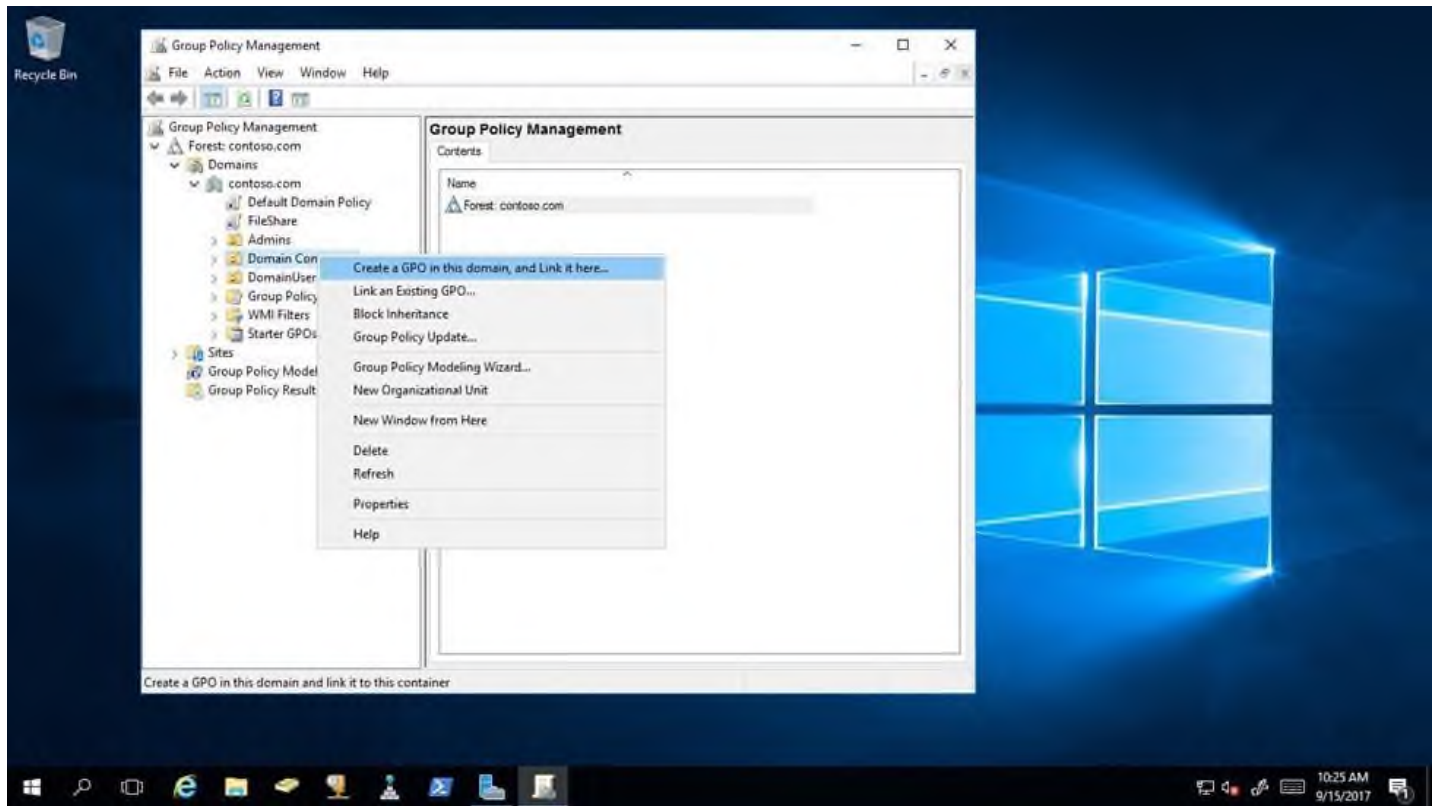
サブネット マスク . . . . . : X.X.X.X

デフォルト ゲートウェイ . . . . . : X.X.X.X

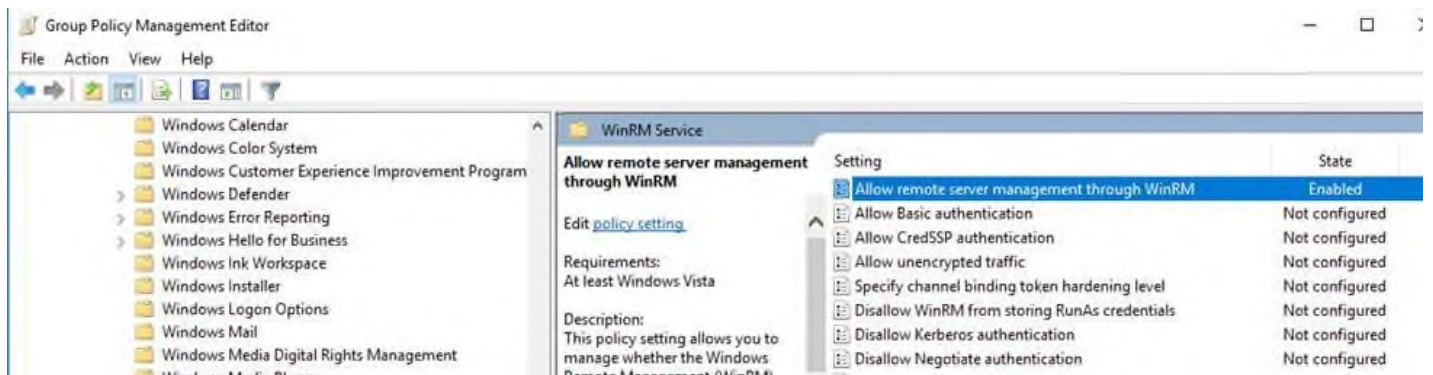
マシンの IPv4 アドレスをメモします。構成の最後の手順では、このアドレスを使用し、データ収集マシンのみがターゲットのワークステーションで Windows Update エージェントと通信できることを確認します。

**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のワークステーション OU にリンクさせます。**

1. 新しい GPO を作成します。ワークステーションの組織単位に 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、または “Windows クライアント評価” 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）。“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:

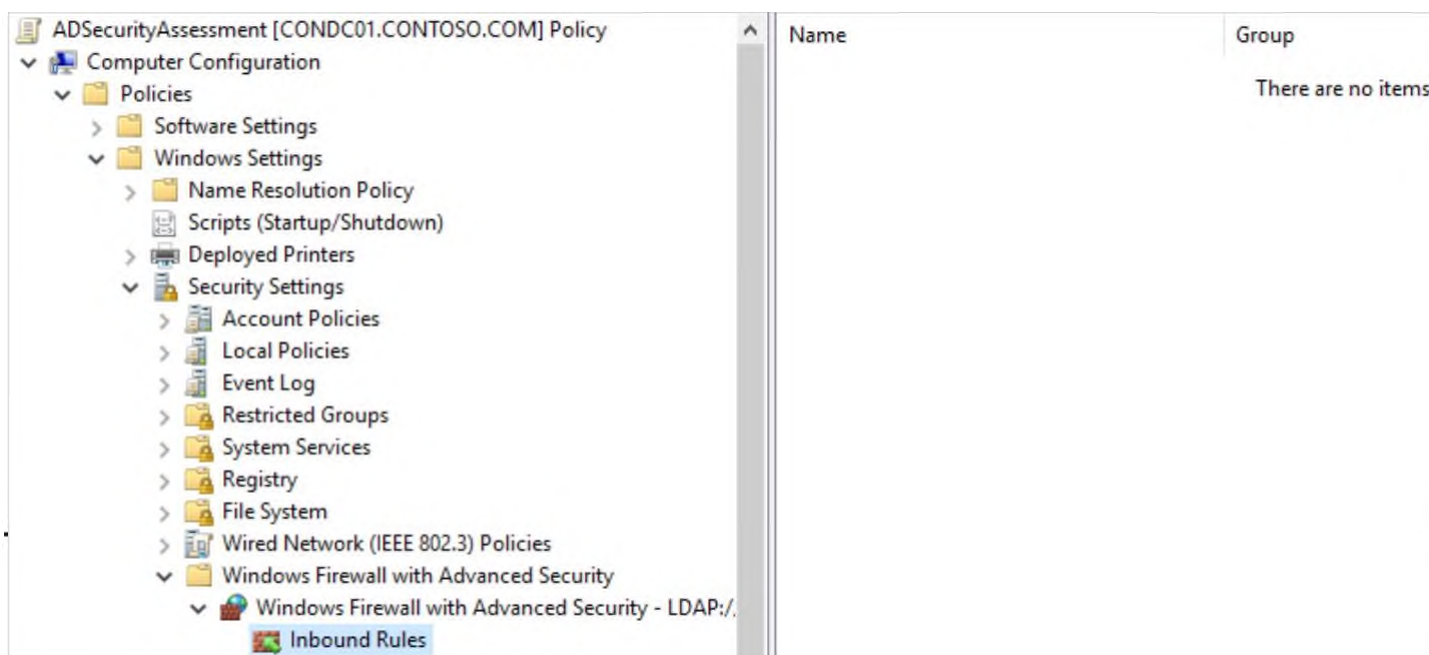
IPv4 filter: \*   
 IPv6 filter: \*

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.

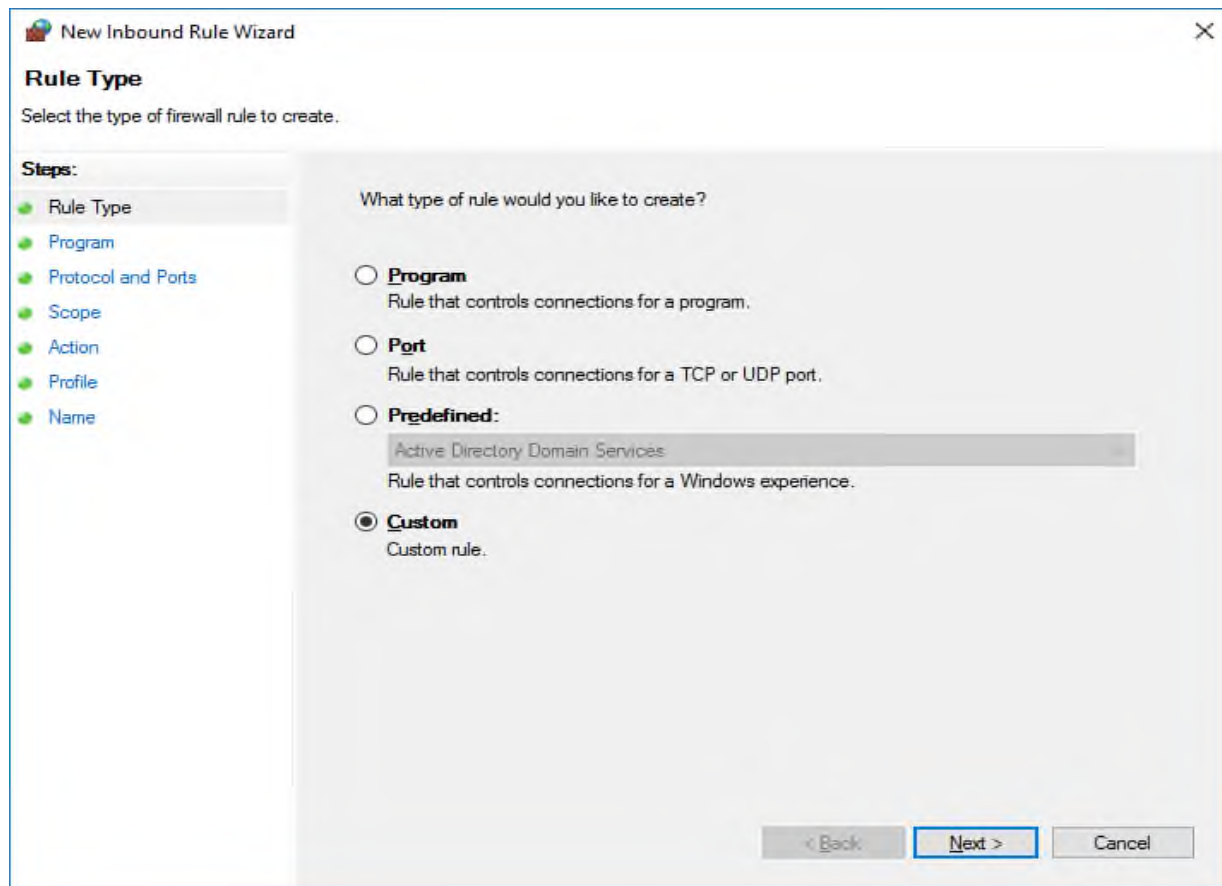
OK Cancel Apply

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 ワークステーション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



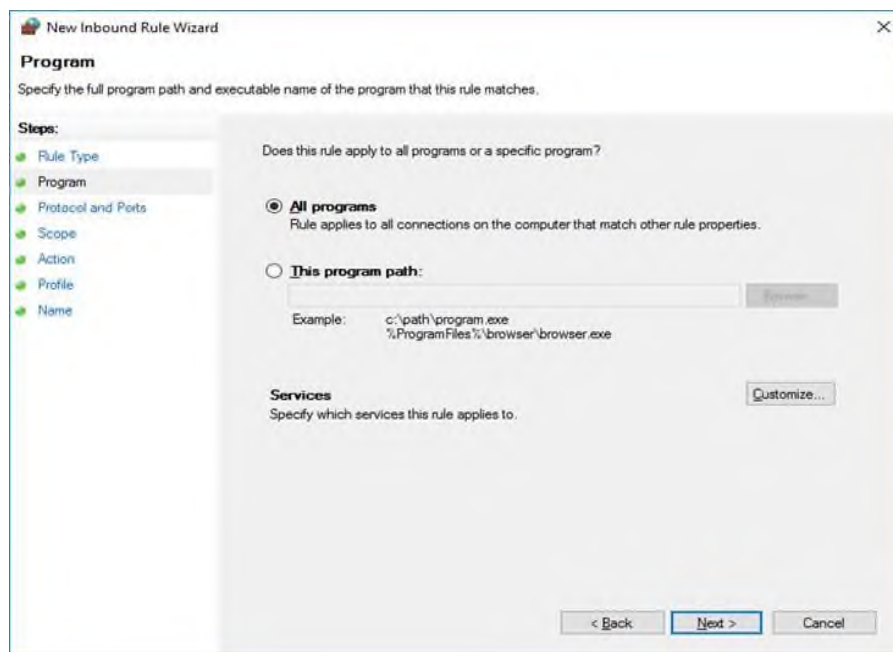


5. カスタムの規則を作成し、[次へ] を選択します



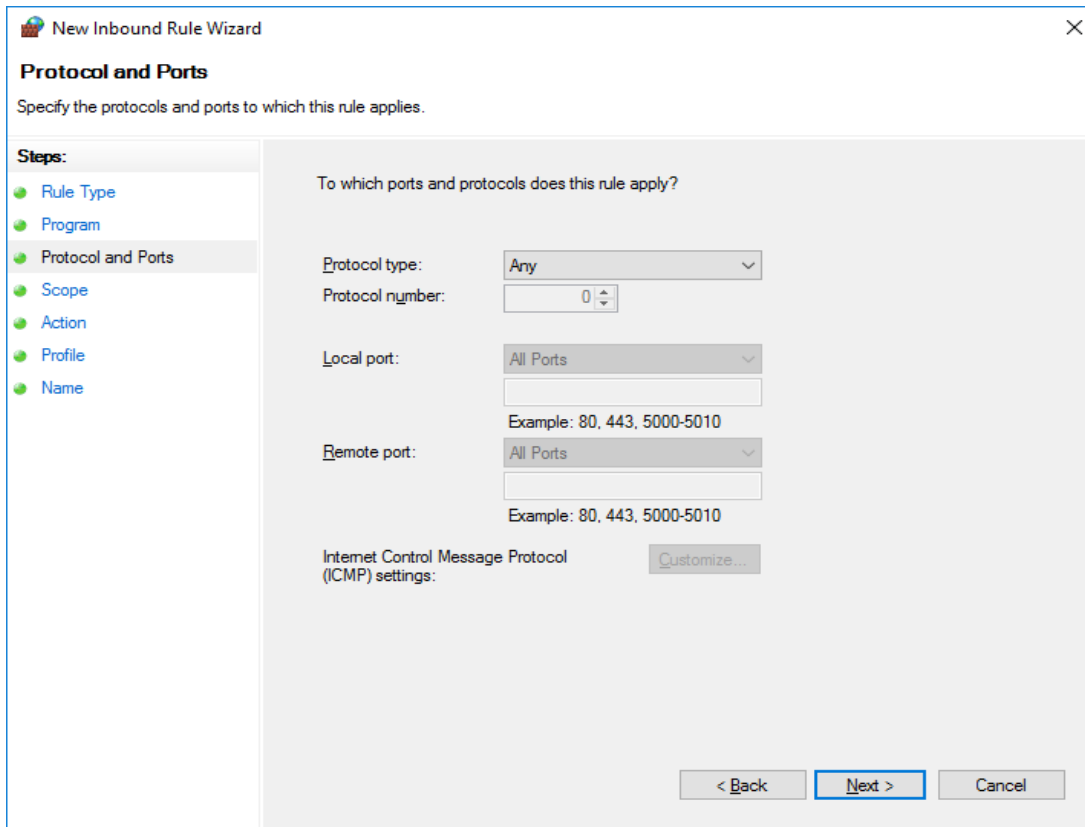
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Rule Type' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Rule Type' with the instruction 'Select the type of firewall rule to create.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile', and 'Name'. The main area asks 'What type of rule would you like to create?' and offers three options: 'Program' (Rule that controls connections for a program.), 'Port' (Rule that controls connections for a TCP or UDP port.), and 'Predefined:' (with a dropdown menu showing 'Active Directory Domain Services' and the description 'Rule that controls connections for a Windows experience.'). The 'Custom' option is selected with a radio button, described as 'Custom rule.'. At the bottom right are buttons for '< Back', 'Next >', and '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 'New Inbound Rule Wizard' window at the 'Program' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Program' with the instruction 'Specify the full program path and executable name of the program that this rule matches.' On the left, the 'Steps:' list has 'Program' highlighted. The main area asks 'Does this rule apply to all programs or a specific program?' and offers two options: 'All programs' (Rule applies to all connections on the computer that match other rule properties.) and 'This program path:' (with a text input field and a 'Browse...' button). Below the input field, an 'Example:' shows two paths: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. At the bottom left, the 'Services' section asks 'Specify which services this rule applies to.' with a 'Customize...' button. At the bottom right are buttons for '< Back', 'Next >', and '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。

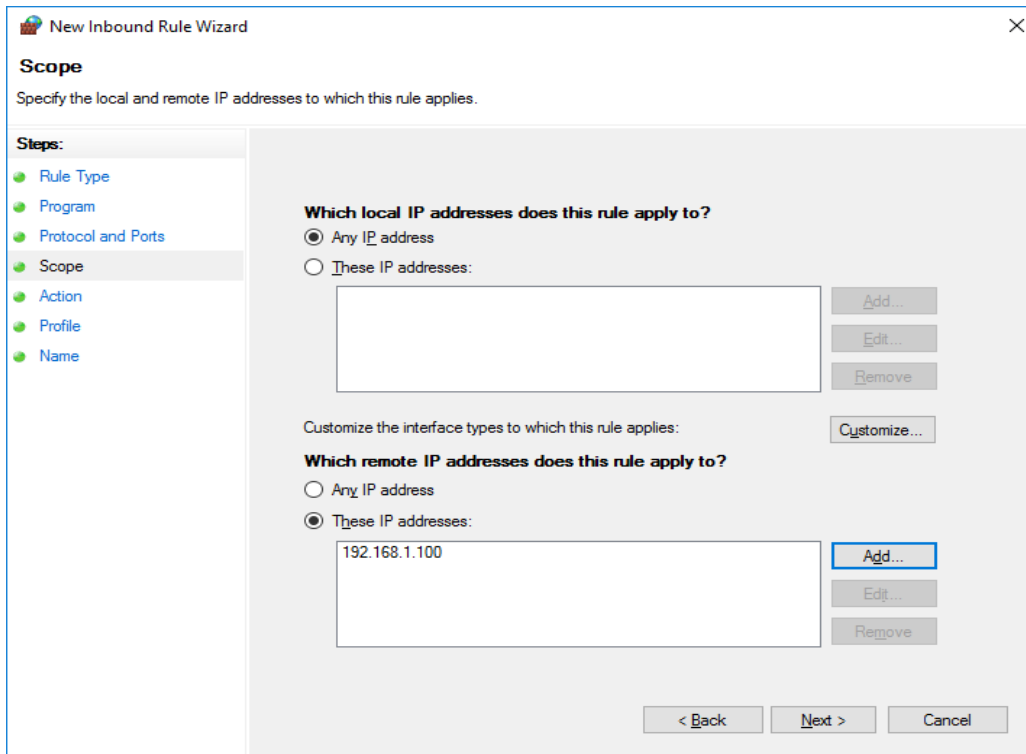


The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Protocol and Ports' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports (selected), Scope, Action, Profile, and Name. The main area is titled 'To which ports and protocols does this rule apply?'. It contains the following fields and controls:

- Protocol type:** A dropdown menu set to 'Any'.
- Protocol number:** A numeric input field set to '0'.
- Local port:** A dropdown menu set to 'All Ports', with an example text 'Example: 80, 443, 5000-5010' below it.
- Remote port:** A dropdown menu set to 'All Ports', with the same example text below it.
- Internet Control Message Protocol (ICMP) settings:** A button labeled 'Customize...'.

At the bottom right, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and '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。



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Scope' step. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports, Scope (selected), Action, Profile, and Name. The main area is titled 'Specify the local and remote IP addresses to which this rule applies.' and contains the following sections:

- Which local IP addresses does this rule apply to?**
  - ☒ Any IP address
  - ☐ These IP addresses: A text box with 'Add...', 'Edit...', and 'Remove' buttons to its right.
- Customize the interface types to which this rule applies:** A button labeled 'Customize...'.
- Which remote IP addresses does this rule apply to?**
  - ☐ Any IP address
  - ☒ These IP addresses: A text box containing '192.168.1.100' with 'Add...', 'Edit...', and 'Remove' buttons to its right.

At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and '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: Windows ClientToolsMachine)

## 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'

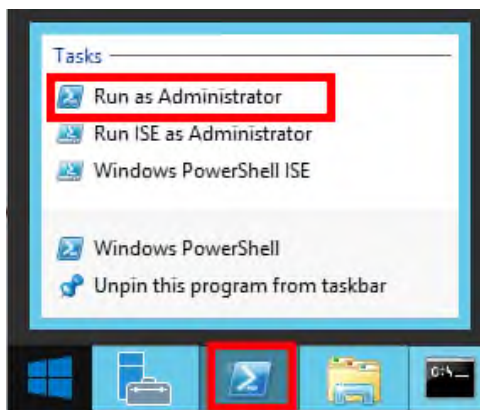
Microsoft Monitoring Agent/OMS Gateway のインストールを完了し、データ収集マシンとターゲット マシンでセキュリティ更新プログラムの前提条件を構成したら、評価をセットアップするために、次のセクションを続行します。

## Windows クライアント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 クライアント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-WindowsClientAssessmentTask -TargetNames <YourClientNames> -TargetDomain <TargetDomain> -WorkingDirectory <Directory> -EnvironmentName <FriendlyNameforEnvironment>** コマンドを実行します。このコマンドでは、<YourClientNames> が環境のクライアントのいずれかの FQDN 名または NetBIOS 名となり、<TargetDomain> はオプション入力で、ターゲット クライアントが選択される元となるドメインの指定になり、<Directory> は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、<EnvironmentName> は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。

```
Scroll Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\windows\system32> Add-WindowsClientAssessmentTask -TargetNames "Client-01;Client-02" -TargetDomain "fourthcoffee.com" -WorkingDirectory "C:\OMS\WinCli" -EnvironmentName "HWorkstations"
```

以下の方法を使用して、テキスト ファイルからコンピューターの一覧をインポートすることもできます:

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

**Add-WindowsClientAssessmentTask -TargetNames \$Clients -TargetDomain <TargetDomain> - WorkingDirectory "C:\OMS\WinCli"**

セミコロンで区切られた複数のクライアントの一覧を含むテキスト ファイルの例: "Client01;Client02;Client03"。

## 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-WindowsClientAssessmentTask -TargetNames <YourClientNames> -TargetDomain <TargetDomain> -WorkingDirectory <Directory> -ScheduledTaskUsername <MSAName> -RunWithManagedServiceAccount \$True -EnvironmentName <FriendlyNameforEnvironment>**

このコマンドでは、<YourClientNames> が環境のクライアントのいずれかの FQDN 名または NetBIOS 名であり、<TargetDomain> がオプション入力で、ターゲット クライアントが選択される元となるドメインの指定になり、<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 クライアント評価を実行するために使用されます。

```
[WindowsClientAssessment]Detected agent configuration for Management Group AOI-2fc5439b-474a-4b8d-84f6-f58c9c73f049
[WindowsClientAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[WindowsClientAssessment]User(DomainName\UserName):
redmond\romin
[WindowsClientAssessment]Enter the password for redmond\romin:
*****
[WindowsClientAssessment]Creating Windows Schedule task to run assessment...
[WindowsClientAssessment]WindowsClientAssessment setup successful.
[WindowsClientAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171102_072712.log
```

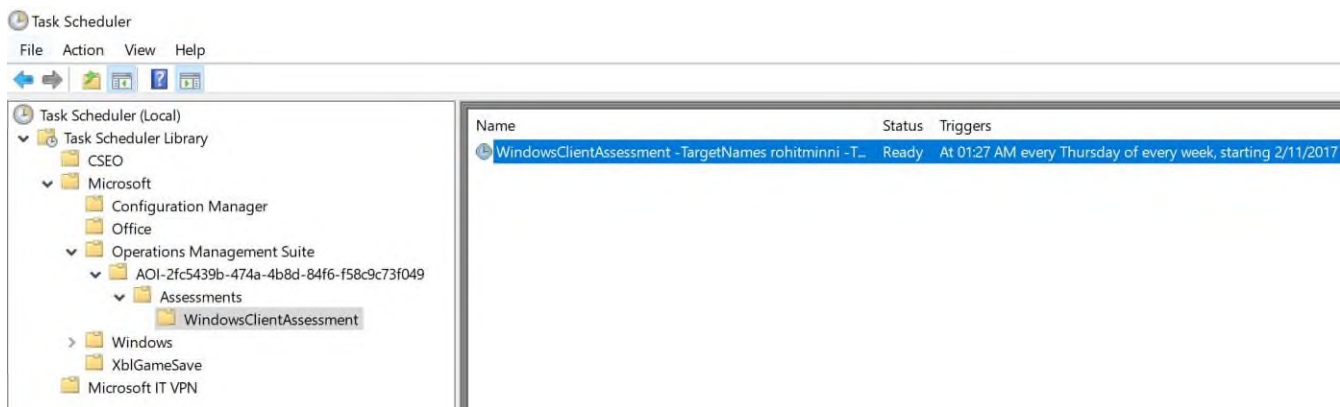
注: このドメイン アカウントは、以下のすべての権限を持っている必要があります。

- 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 クライアント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クライアントに対する制限のないネットワーク アクセス

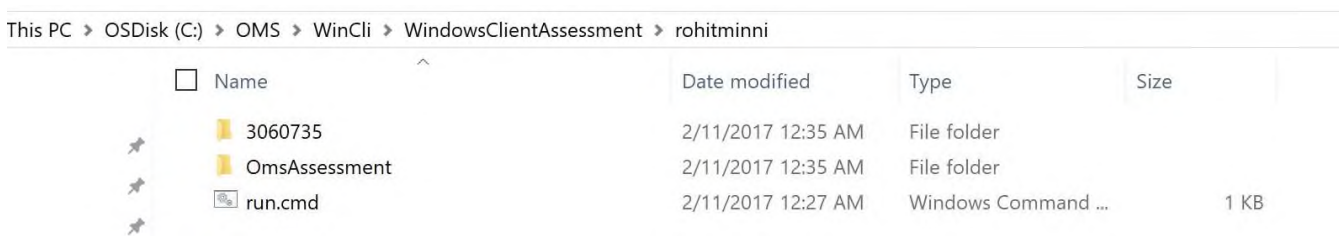
5. 必要な構成に基づいてスクリプトが実行されます。データ収集をトリガーするスケジュールされたタスクが作成されます。

```
Administrator: Windows PowerShell
PS C:\Users\romin> Add-WindowsClientAssessmentTask -TargetNames "rohitminni" -TargetDomain "redmond.comp.microsoft.com" -WorkingDirectory "C:\OMS\WinCli"
[WindowsClientAssessment]Detected agent configuration for Management Group AOI-2fc5439b-474a-4b8d-84f6-f58c9c73f049
[WindowsClientAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[WindowsClientAssessment]User(DomainName\UserName):
redmond\romin
[WindowsClientAssessment]Enter the password for redmond\romin:
*****
[WindowsClientAssessment]Creating Windows Schedule task to run assessment...
[WindowsClientAssessment]WindowsClientAssessment setup successful.
[WindowsClientAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171102_072712.log
```

6. データ収集は、名前 “WindowsClientAssessment” 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：



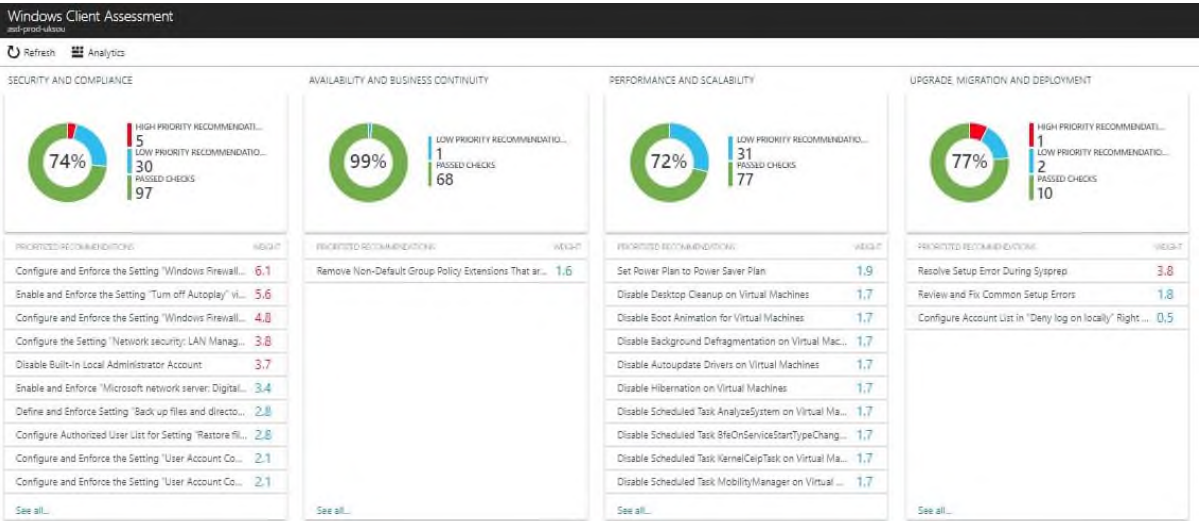
8. ツール マシンでデータ収集と分析を完了したら、次の選択したシナリオにより、log analytics ワークスペースに送信されます：

- 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 コンピューター 経由**、このオプションが構成されると、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 Client Assessment** 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 スペースでの Windows クライアント評価では、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

#### 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ワークステーション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  
範囲内のワークステーション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。