

SQL 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 Microsoft Unified Support ソリューション パックに含まれている SQL Server 評価に必要な構成の手順を説明します。

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、インターネット接続がデータ収集マシンから制限されている環境、または、このスケジュールされたタスクの要件によりセキュリティ上の懸念事項がある環境に対して推奨されます。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 SQL Server 環境が含まれるドメインのメンバーである必要があります。SQL Server を実行する複数のサーバーまたはフェールオーバー クラスターからの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 → SQL Server を実行する複数のサーバーまたはフェールオーバー クラスターからのデータを収集 → OMS Gateway への収集データの転送 → Log Analytics ワークスペースへのデータの送信

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 SQL Server 環境が含まれるドメインのメンバーである必要があります。SQL Server を実行する複数のサーバーまたはフェールオーバー クラスターからの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 → SQL Server を実行する複数のサーバーまたはフェールオーバー クラスターからのデータの収集 → Log Analytics ワークスペースへのデータの送信。

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をご覧ください。

このドキュメントの最終更新日は、2021 年 3 月 7 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://docs.microsoft.com/en-us/services-hub/health/assessment_prereq_docs/prereqssqlassessment.pdf

目次

システム要件および構成の概要	3
サポートされているバージョン	3
両方のシナリオに共通	3
データ収集マシン	3
OMS Gateway (OMS Gateway とデータ収集マシンのシナリオが必要です)	4
PowerShell のリモート処理	4
ユーザー プロファイル サービス	10
SQL 評価のセットアップ	10
付録 - A データ収集マシン	15
付録 - B ポート要件	17
付録 - C Azure の可用性グループ クラスターに関する特別要件	18
付録 - D sysadmin なしで実行するための要件	19

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

- SQL Server 環境は、SQL Server 2008、SQL Server 2008 R2、SQL Server 2012、SQL Server 2014 または SQL Server 2016、SQL Server 2017 で実行される必要があります。Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019 のフェールオーバー クラスタまたはスタンドアロンサーバーのインストールがサポートされています。

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:
 - ドメイン アカウント、スタンドアロンの管理されたサービス カウント (sMSA) またはグループ管理サービス アカウント (gMSA) には、次の権利が含まれます:
 - 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
 - 環境にあるすべての Microsoft SQL Servers に関する SysAdmin ロール
 - スタンドアロンの管理されたサービス カウント (sMSA) またはグループ管理サービス アカウント (gMSA) については、こちらを参照することができます: <https://docs.microsoft.com/en-us/services-hub/health/kb-running-assessments-with-msas>

データ収集マシン

- Microsoft Monitoring Agent** (OnDemand 評価を使用) は、Windows Server 2008 R2 SP1 以降 (または Windows 7 SP1 以降) を必要とします。重要: クライアント オペレーティング システムでの Microsoft Monitoring Agent のインストール オプションについては、特権を持つドメイン アカウントの資格情報が信頼性の低いワークステーションに公開される危険があるため、避けることを強く推奨します。
- Microsoft .NET Framework 4.6.2 以降をインストール済み
- データ収集マシンは、評価される必要がある SQL Server 環境が含まれている 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、および最小 10 GB の空きディスク領域。
- データ収集マシンは、SQL Server 環境を実行しているサーバーに接続し、環境から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 Server、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、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できる必要があります。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://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent#network-firewall-requirements>

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

- **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 10、Windows 7、Windows 8.1、Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 または Windows Server 2016 が必要です。
- **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できる必要があります。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 サービス**: Windows ファイアウォール サービスが無効の場合は、OMS Gateway のインストールが失敗します。
- **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>

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のスキャンを取得するために、すべての SQL Servers で実行されている必要があります
- PowerShell バージョン 2 以降が、ターゲット SQL Servers で必要になり、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>

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 SQL Servers 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: 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。Windows Server 2008 から Windows Server 2012 では、WinRM と PowerShell のリモート処理が既定で無効になっています。次のいずれかの構成オプションは、WinRM と PowerShell のリモート処理が任意のターゲット SQL サーバーで無効になっている場合に、PowerShell のリモート処理をサポートするために実装する必要があります:

オプション 1: 評価の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

オプション 2: 以下の 3 つの手順すべてを実装します。

1. 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)
 - a. 2008 R2 で “リスナーの自動構成を許可します”。
 - b. 2012 R2 (以降) で “WinRM 経由のリモート サーバー管理を許可します”。

2. 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）
 - a. 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
3. **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 SQL Servers 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。

オプション 2: 上記の 3 つの手順を実装するための詳細なステップバイステップの手順。

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) SQL Server 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

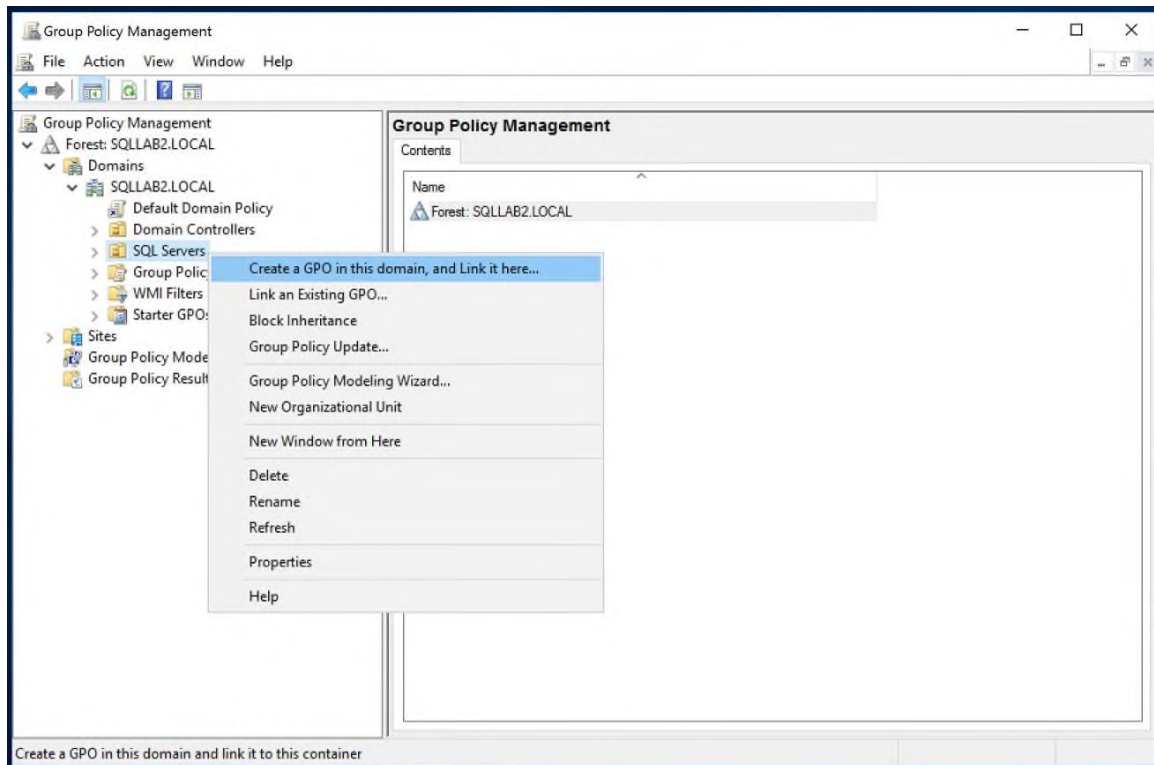
サブネット マスク : X.X.X.X

デフォルト ゲートウェイ : X.X.X.X

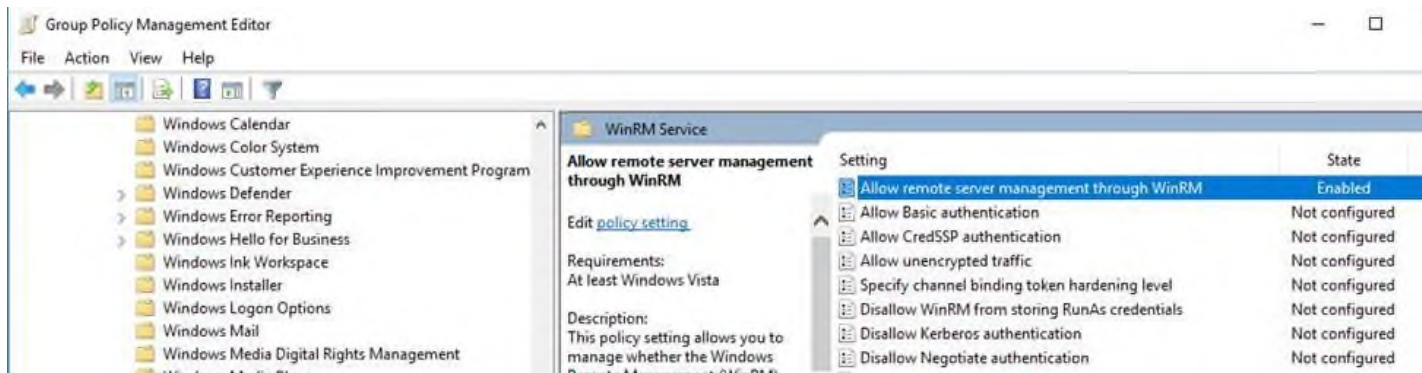
マシンの IPv4 アドレスをメモします。構成の最後の手順では、このアドレスを使用し、データ収集マシンのみが SQL Servers で Windows Update エージェントと通信できることを確認します。

B.) グループ ポリシー オブジェクトを作成および構成し、ターゲット SQL Servers を使用する SQL Servers OU にリンクさせます。

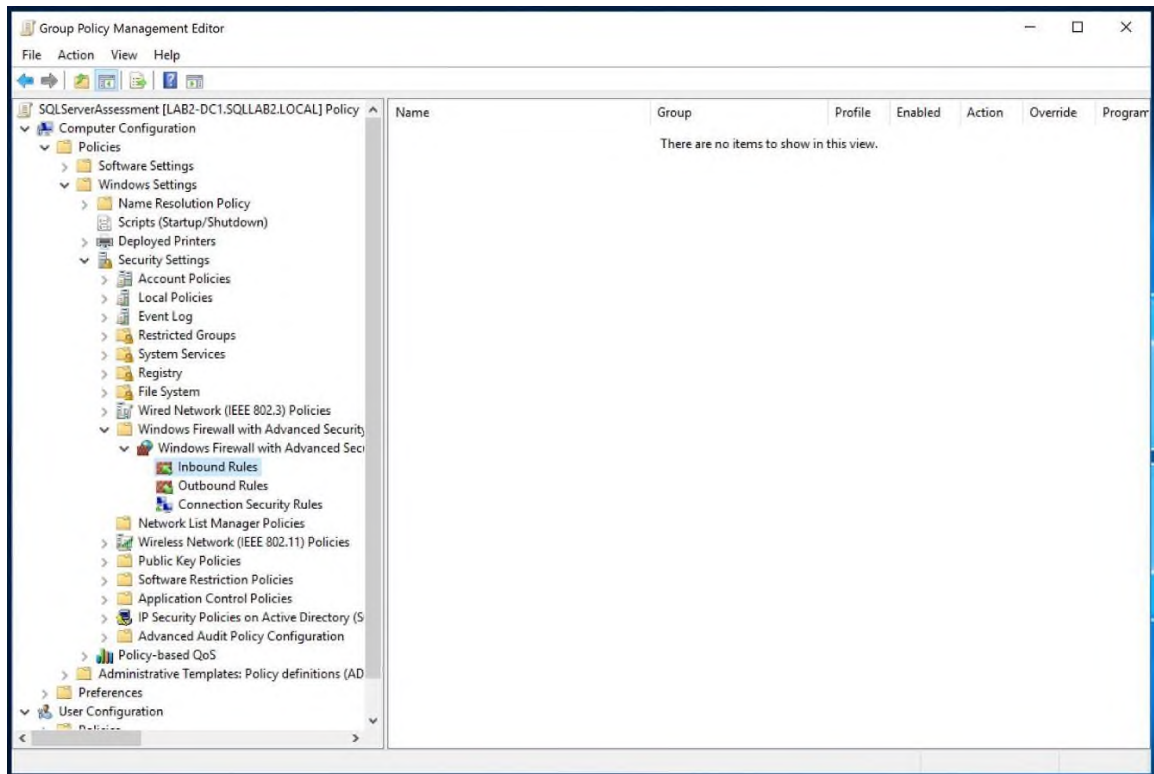
1. 新しい GPO を作成します。GPO が SQL Servers の組織単位に適用されていることを確認します。グループ ポリシーの名前付け規則、または“SQLServerAssessment”のようにその目的を識別するものに基づいて、新しいグループ ポリシーに名前を付けます



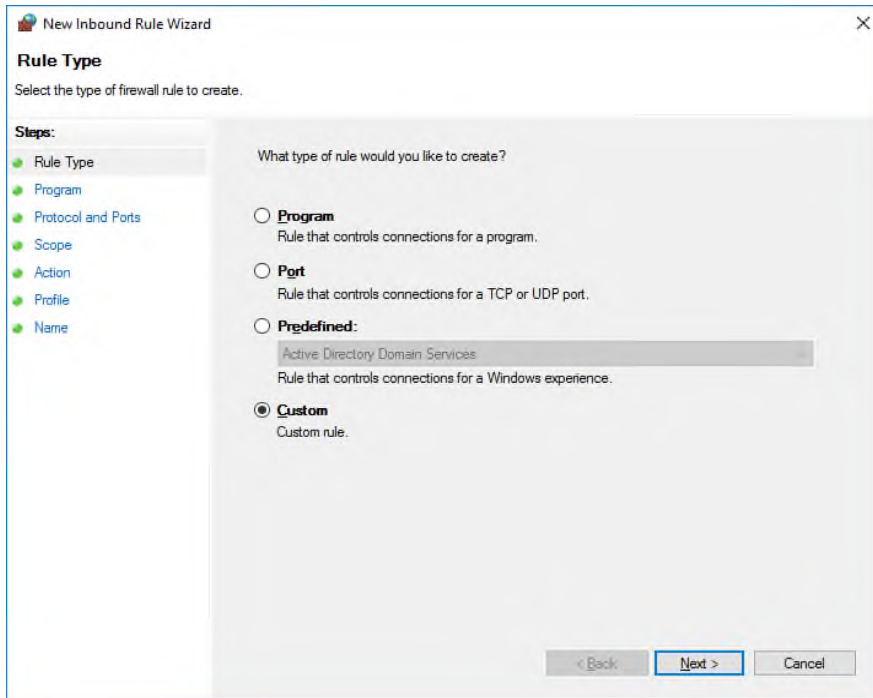
2. GPO 内で開き、新しい GPO を右クリックして [編集] を選択し、“コンピューターの構成¥ポリシー¥管理用テンプレート¥Windows コンポーネント¥Windows リモート管理 (WinRM)¥WinRM サービス” に移動します。OS に応じて、“WinRM 経由のリモート サーバー管理を許可する” または “リスナーの自動構成を許可する” を有効にします。



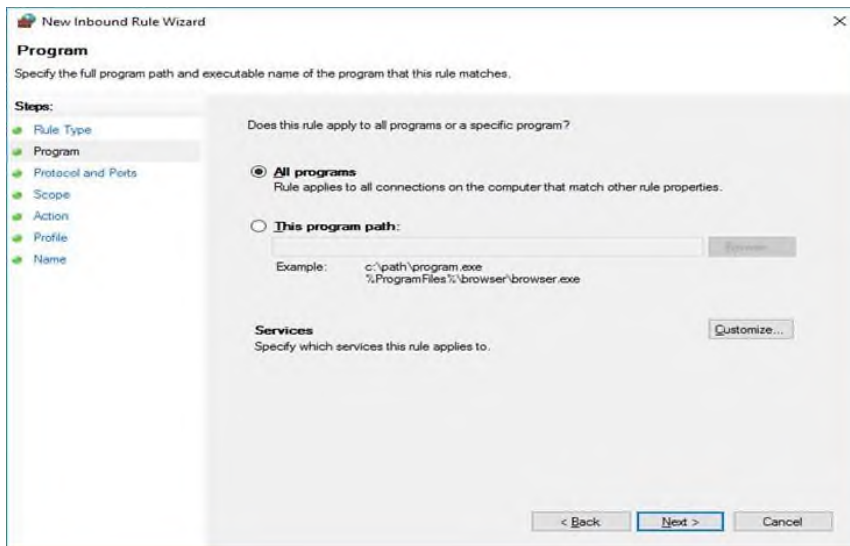
3. 詳細なファイアウォールの受信規則を作成し、ツール マシンから SQL Servers へのすべてのネットワーク トラフィックを許可します。これは、上記の 手順 1 で使用した同じ GPO に適用できます。(コンピューターの構成¥ポリシー¥Windows の設定¥セキュリティの設定¥セキュリティが強化された Windows ファイアウォール¥セキュリティが強化された Windows ファイアウォール -LDAP:/xxx¥受信規則)



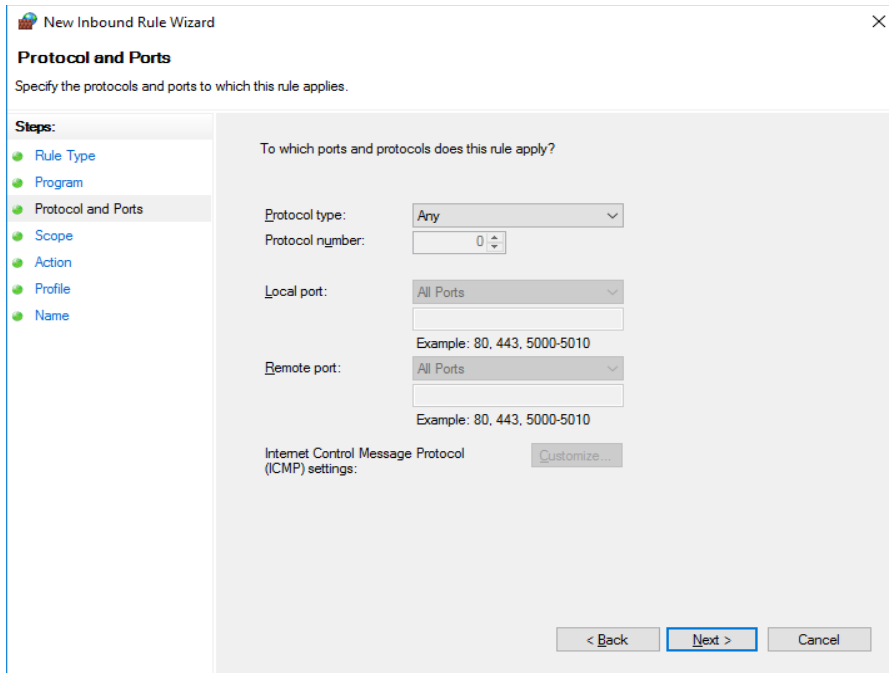
4. 新しい規則を作成するには、[受信規則] をクリックし、[新規] を選択します
5. カスタムの規則を作成し、[次へ] を選択します



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。



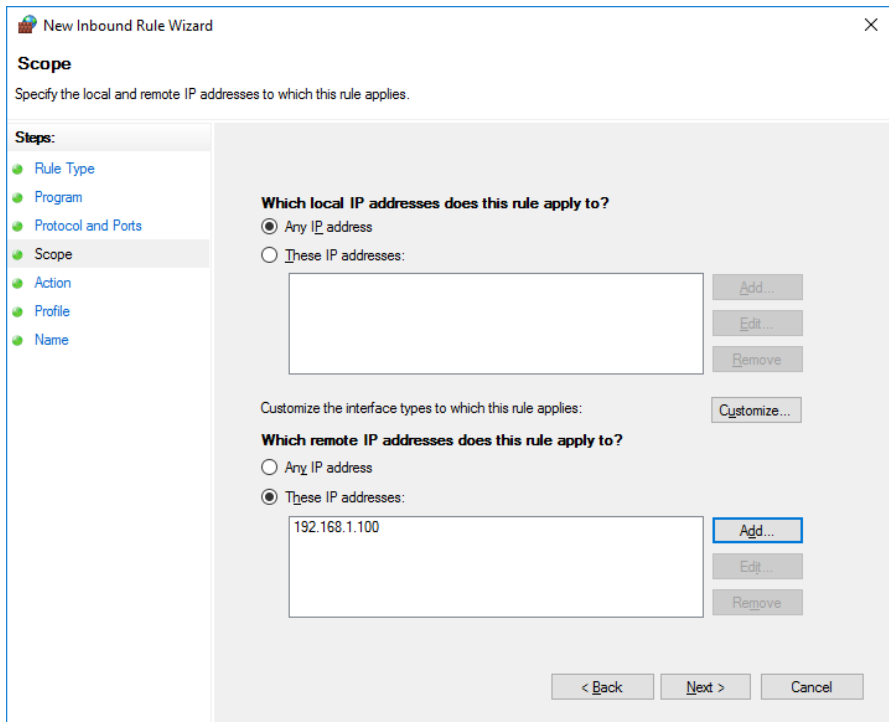
7. すべてのプロトコルとポートを許可し、[次へ] をクリックします。



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 text box containing '0'.
- Local port:** A dropdown menu set to 'All Ports'.
- Remote port:** A dropdown menu set to 'All Ports'.
- Example:** The text '80, 443, 5000-5010' is shown below both the local and remote port dropdowns.
- Internet Control Message Protocol (ICMP) settings:** A button labeled 'Customize...'.
- Navigation buttons:** '< Back', 'Next >', 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 fields and controls:

- Which local IP addresses does this rule apply to?**
 - ☒ Any IP address
 - ☐ These IP addresses: A text box with 'Add...', 'Edit...', and 'Remove' buttons.
- 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.
- Navigation buttons:** '< Back', 'Next >', 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（例: SQLAssessmentToolsMachine）、保存します。
12. 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 サービスに移動します。自動スタートアップの Windows リモート管理（WS 管理）サービスを選択および定義します。
13. GPO を保存し、ターゲット SQL サーバーが適用されていることを確認します。

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 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。

追加の詳細については、[Microsoft オンデマンド評価の構成](#)を参照してください

記憶域のパスワード ポリシーを許可しない

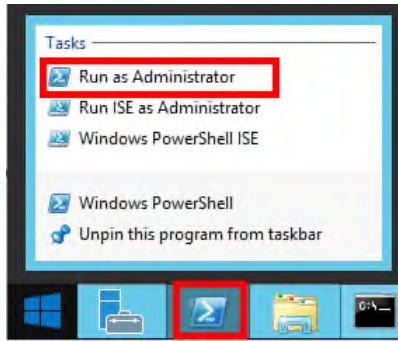
収集マシンに関しては、“ネットワーク アクセス: ネットワーク認証の記憶域のパスワードと資格情報を許可しない” というポリシーを明示的に無効にする必要がある場合があります。追加の詳細については、[Microsoft オンデマンド評価の構成](#)を参照してください

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



2. **Add-SQLAssessmentTask -SQLServerName <YourServerName> - WorkingDirectory <Directory>** コマンドを実行します。このコマンドでは、<YourServerName> が SQL Server を実行する単一サーバーまたはフェールオーバー クラスターの完全修飾ドメイン名 (FQDN) または NetBIOS 名です。複数の環境に評価を実施する場合は、各環境の間に「;」を入れます。フェールオーバー クラスターに関しては、フェールオーバー クラスター仮想ネットワーク名を確認するので、<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。

Administrator: Windows PowerShell

```
PS C:\users\romin> Add-SQLAssessmentTask -SQLServerName "asttest.redmond.corp.microsoft.com" -WorkingDirectory "C:\OMS\SQL"
```

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。これらの資格情報は、SQL 評価を実行するために使用されます。sMSA または gMSA については、parameter RunWithManagedServiceAccount を指定する必要があるので、それを \$True に設定します。このコマンドレットでパスワードの入力をユーザーに求める場合、空白のままにして<Enter>を押します。詳細については、この記事の[“マネージド サービス アカウントによるアセスメントの実行”](#) をご確認ください。

Administrator: Windows PowerShell

```
PS C:\Users\romin> Add-SQLAssessmentTask -SQLServerName "asttest.redmond.corp.microsoft.com" -WorkingDirectory "C:\OMS\SQL"
[SQLAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[SQLAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[SQLAssessment]User(DomainName\UserName):
redmond\romin
[SQLAssessment]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。

- 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
- 環境にあるすべての Microsoft SQL Servers に関する SysAdmin ロール

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-SQLAssessmentTask -SQLServerName "asttest.redmond.corp.microsoft.com" -WorkingDirectory "C:\OMS\SQL"
[SQLAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
[SQLAssessment]Enter the credential to be used to run this assessment. Credentials will be used to connect to remote server(s) for assessment.
[SQLAssessment]User(DomainName\UserName):
redmond\romin
[SQLAssessment]Enter the password for redmond\romin:
*****
[SQLAssessment]Creating Windows Schedule task to run assessment...
[SQLAssessment]SQLAssessment setup successful.
[SQLAssessment]Detailed log is at: C:\Users\romin\AppData\Local\Temp\Assessments_Configuration_20171018_093612.log
PS C:\Users\romin>
```

5. データ収集は、名前「SQLAssessment -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。

Task Scheduler

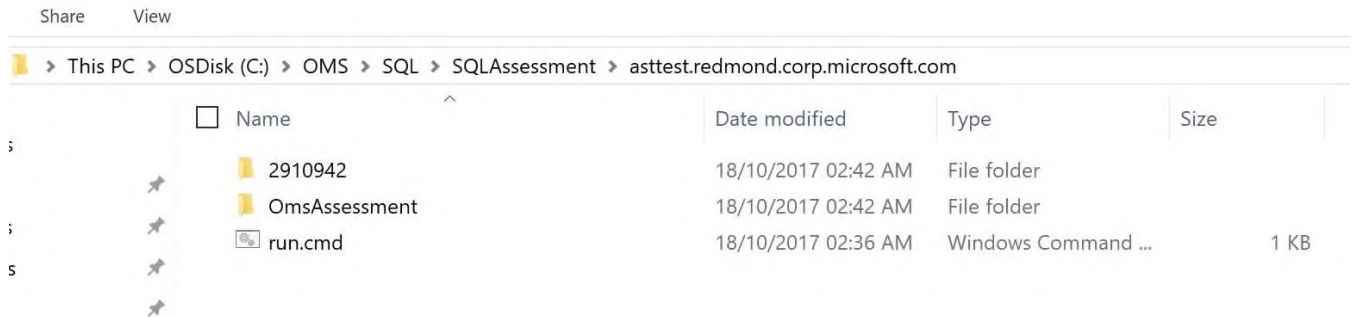
File Action View Help

Task Scheduler (Local)

- Task Scheduler Library
 - CSEO
 - Microsoft
 - Configuration Manager
 - Office
 - Operations Management Suite
 - AOI-49900795-7a88-4eee-a2de-ca8a46fc0c9e
 - Assessments
 - ADAssessment
 - ADSecurityAssessment
 - SCCMAssessment
 - ExchangeAssessment
 - SCOMAssessment
 - SfBAAssessment
 - SharePointAssessment
 - SQLAssessment

Name	Status	Triggers	Next Run Time
SQLAssessm...	Ready	At 03:36 AM every Wednesday of every week, starting 18/10/2017	18/10/2017 3:36:00 AM

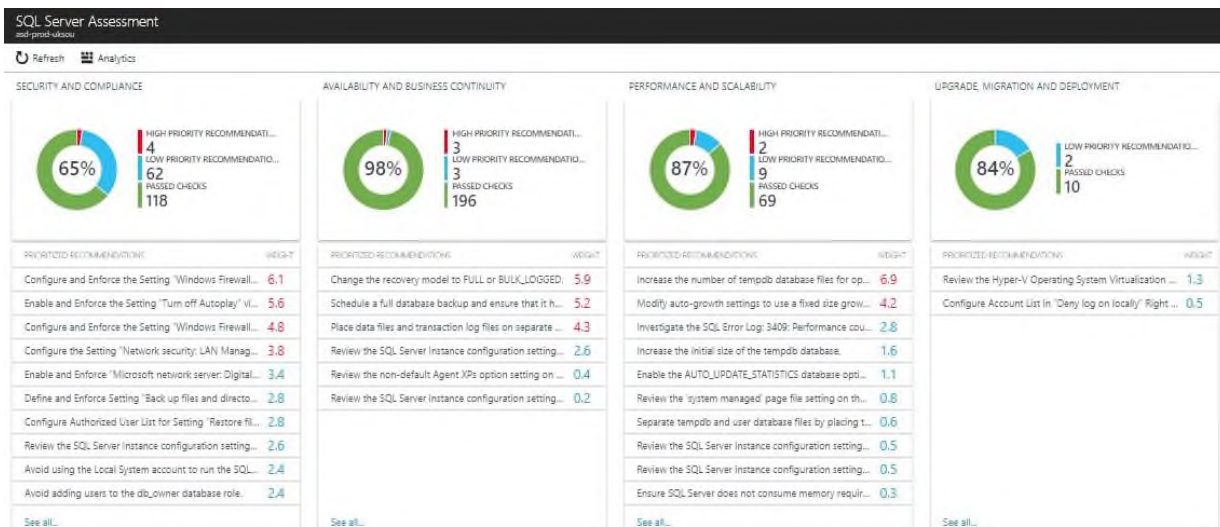
6. 収集および分析している間に、次の構造を使用し、セットアップ時に構成された WorkingDirectory フォルダーの下にデータが一時的に保存されます：



7. 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いる場合。
 - OMS Gateway 経由、データ収集マシンをインターネットに接続していない場合。
8. 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。SQL 評価タイルをクリックし、次を確認します：



9. 重点領域でグループ化された検出事項が表示されます。



付録 - A データ収集マシン

Log Analytics ワークスペースと Microsoft Unified Support ソリューション パックの SQL 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. イベント ログ コレクター
2. ファイル データ コレクター
3. レジストリ データ コレクター
4. ユーザー権利コレクター
5. マウント ポイント データ コレクター
6. SQL データ コレクター
7. SQL エラー ログ コレクター
8. WMI データ コレクター
9. Windows PowerShell データ コレクター

1. イベント ログ コレクター

SQL Servers からの警告とエラーなど、過去 7 日間のアプリケーションとシステムのイベント ログを収集します。

2. 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。

3. レジストリ データ コレクター

レジストリ キーと値は、SQL Server 環境から収集されます。次のような項目が含まれます：

- “HKLM¥SYSTEM¥CurrentControlSet¥Control¥Power¥User¥PowerSchemes” の電源オプション情報
- これにより、ユーザーは SQL Server に関する電源プランの設定方法を理解できるようになります。

4. ユーザー権利コレクター

ローカル セキュリティ ポリシーを収集します。

5. マウント ポイント データ コレクター

それが存在する場合、マウント ポイントを収集します。

6. SQL データ コレクター

SQL クエリは、次のような情報を収集するために使用されます：

- Always On の構成、データベース名、正常性状態
- TempDB ファイル、ファイル サイズ、自動拡張のサイズ
- バックアップ履歴
- 複製、冗長、無効、仮想インデックス

7. SQL エラー ログ コレクター

過去 15 日間の SQL Server のエラー ログを収集します。ログ ファイルのサイズが 6MB 以上の場合には、分析されません。

8. WMI データ 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
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。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、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。Microsoft では、この情報を使用して、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します。

9. Windows PowerShell データ コレクター

PowerShell 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：

- リソースの依存関係の収集
- 監査構成

付録 - B ポート要件

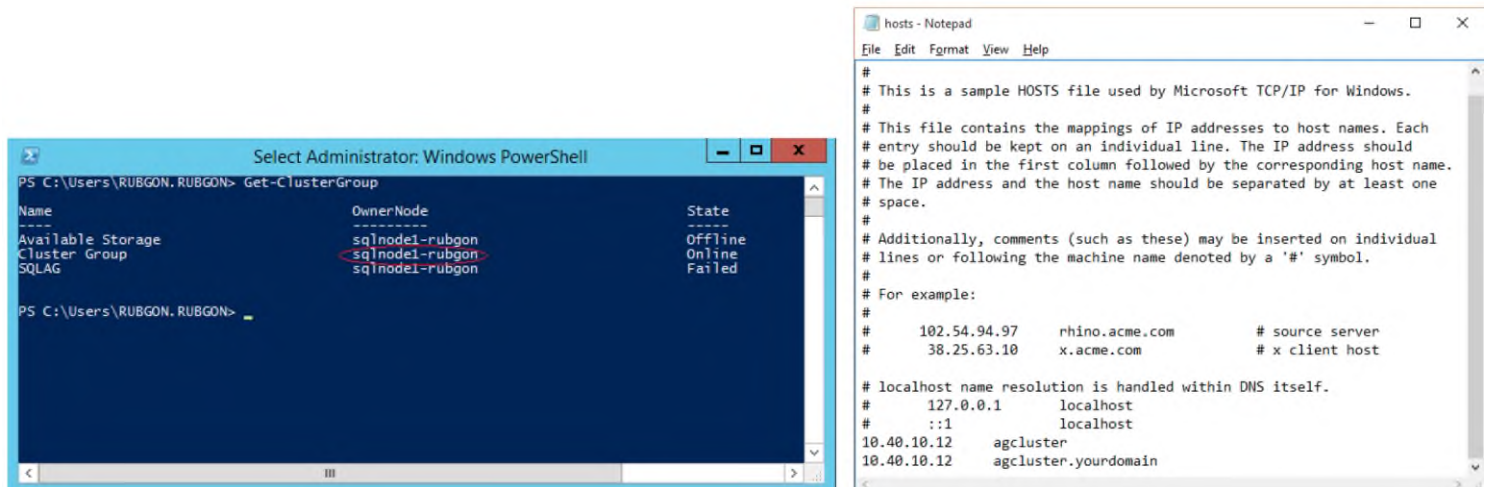
ツール マシンとターゲット サーバー間のポートをすべて開くことが不可能な場合は、こちらがツールセットが正常に機能するために開く必要がある特定のポートの一覧です。これらのポートは、各ターゲット サーバーで開く必要があります。

- 1433 または顧客によって構成された SQL インスタンス ポート。
- SQL Browser ポート - UDP 1434
- RPC 動的ポートの範囲
 - 49152 から 65535 までの既定の TCP ポート
 - この範囲を変更できますが、このポートの範囲が異なるコンポーネントによって使用されるため、評価に必要な何かにその他の影響を与える場合がありますので、ポートが不足しないように注意する必要があります。
<https://support.microsoft.com/en-us/help/929851/the-default-dynamic-port-range-for-tcp-ip-has-changed-in-windows-vista>
- 既定の PS リモート処理のポートは、TCP 5985 と TCP 5986 になり、顧客が変更している場合は、80 および 443 または顧客が指定したその他のポートになる場合があります。
- ポート TCP 135
- ポート UDP 137（必要がない場合があります）
- ポート TCP 139
- ポート TCP 445

付録 - C Azure の可用性グループ クラスターに関する特別要件

Azure の仮想ネットワークでは、ツールセットに影響するクラスターと可用性グループに一部の接続制限を適用します。概要：

1. 外部のロード バランサーを使用する場合は、ディレクトリのリッサー名は使用できません。クラスター名またはノード名を使用できます。
2. クラスター名 IP の HA ポートを含む Standard Load Balancer を使用していない場合は、ホスト ファイルを変更してクラスター コレクターを機能させる必要があります。有効ノードの IP を特定し、以下で示すようにホスト ファイルを変更する必要があります。ホスト ファイルは、“C:¥Windows¥System32¥drivers¥etc” に配置されます。



注意： このホスト構成の変更は、最後にツールセットが実行された後にフェールオーバーが発生した場合、ツールセットの実行時に毎回取得される必要があります。

付録 - D sysadmin なしで実行するための要件

sysadmin 特権を付与することが不可能な場合は、ここで提供されるスクリプトを使用し、評価を実行するアカウントに必要な特権のみを付与します。sysadmin が実行する場合のみ、いくつかの規則で必要なデータを収集することができ、sysadmin 特権で実行していない場合は、これらの規則がスキップされることを考慮してください。

1 つの特例は、読み取り専用データベースを使用している場合です（可用性グループ以外）。その場合、必要なユーザーが作成されないの、複数の規則がこれらの読み取り専用データベースでスキップされます。これらのデータベースに必要な情報を収集するには、読み取り/書き込み専用に変更し、ここで提供されるスクリプトを実行して必要なユーザーおよび権限を作成するか、sysadmin であるアカウントでツールセットを実行してください（このツールセットでは Windows 認証のみがサポートされます）。

以下のスクリプトが長いのは、通常は既定でパブリック ロールに既に付与されている権限を付与するためです。これは、すべての権限がパブリックから取り消されたとしても、このスクリプトが機能するということです。

ログイン ユーザーの作成および権限の付与のためのスクリプトは、ここで提供されます。このスクリプトは、評価される各インスタンスで実行される必要があるのでご注意ください。長いスクリプトを含むドキュメントの制限を指定すると、複数のページにわたってしまうので、スクリプトをコピーする場合にはご注意ください。

```
DECLARE @UserName nvarchar(500) = 'NORTHAMERICANRaaSUser', --replace with your domain and username, the user needs to exist in the domain
@Command nvarchar(max)
SET @Command = 'USE master; IF NOT EXISTS(SELECT name FROM sys.server_principals WHERE name LIKE ''' + @UserName + ''') BEGIN
CREATE LOGIN [' + @UserName + '] FROM WINDOWS WITH DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_english]; END'
EXEC sp_executesql @Command
--Create user on each database
SET @Command = 'USE [?]; IF EXISTS (SELECT 1
FROM sys.databases d LEFT JOIN sys.dm_hadr_database_replica_states r ON d.database_id = r.database_id WHERE d.is_read_only = 0 AND (r.is_primary_replica = 1 OR r.is_primary_replica IS NULL) AND d.name = DB_NAME())
BEGIN
IF NOT EXISTS(SELECT name FROM sys.database_principals WHERE name LIKE ''' + @UserName + ''') BEGIN
CREATE USER [' + @UserName + '] FOR LOGIN [' + @UserName + ']; END
END
'
EXECUTE master.sys.sp_MSforeachdb @Command
--master permissions
SET @Command = '
USE master;
GRANT VIEW SERVER STATE TO [' + @UserName + '];
GRANT VIEW ANY DEFINITION TO [' + @UserName + '];
GRANT SELECT ON sys.master_files TO [' + @UserName + '];
GRANT SELECT ON sys.databases TO [' + @UserName + '];
GRANT SELECT ON sys.configurations TO [' + @UserName + '];
GRANT SELECT ON sys.sql_logins TO [' + @UserName + '];
GRANT SELECT ON sys.server_principals TO [' + @UserName + '];
GRANT SELECT ON sys.server_role_members TO [' + @UserName + '];
GRANT SELECT ON sys.endpoints TO [' + @UserName + '];
GRANT SELECT ON sys.database_mirroring_endpoints TO [' + @UserName + '];
GRANT SELECT ON sys.dm_os_loaded_modules TO [' + @UserName + '];
GRANT SELECT ON sys.servers TO [' + @UserName + '];
GRANT SELECT ON sys.server_audits TO [' + @UserName + '];
GRANT SELECT ON sys.server_event_sessions TO [' + @UserName + '];
GRANT SELECT ON sys.top_endpoints TO [' + @UserName + '];
GRANT SELECT ON sys.database_mirroring TO [' + @UserName + '];
GRANT SELECT ON sys.dm_db_index_usage_stats TO [' + @UserName + '];
GRANT SELECT ON sys.dm_os_performance_counters TO [' + @UserName + '];
GRANT SELECT ON sys.dm_os_sys_info TO [' + @UserName + '];
GRANT SELECT ON sys.dm_os_nodes TO [' + @UserName + '];
GRANT SELECT ON sys.dm_os_schedulers TO [' + @UserName + '];
GRANT SELECT ON sys.dm_db_partition_stats TO [' + @UserName + '];
GRANT SELECT ON sys.dm_db_persisted_sku_features TO [' + @UserName + '];
```

```

GRANT SELECT ON sys.dm_db_missing_index_details TO [' + @UserName + ']
GRANT SELECT ON sys.dm_db_missing_index_groups TO [' + @UserName + ']
GRANT SELECT ON sys.dm_db_missing_index_group_stats TO [' + @UserName + ']
GRANT SELECT ON sys.dm_xe_sessions TO [' + @UserName + ']
GRANT SELECT ON sys.dm_exec_query_stats TO [' + @UserName + ']
GRANT SELECT ON sys.dm_exec_text_query_plan TO [' + @UserName + ']
GRANT SELECT ON sys.dm_exec_sql_text TO [' + @UserName + ']
GRANT SELECT ON sys.dm_os_wait_stats TO [' + @UserName + ']
GRANT SELECT ON sys.dm_exec_connections TO [' + @UserName + ']
,
EXEC sp_executesql @Command
SET @Command = 'GRANT EXEC ON sys.xp_enumerrorlogs TO [' + @UserName + ']
GRANT EXEC ON sys.sp_executesql TO [' + @UserName + ']
GRANT EXEC ON sys.sp_validatelogins TO [' + @UserName + ']
--For SQL Server 2012 or later
IF CONVERT(int, SUBSTRING(CONVERT(varchar, SERVERPROPERTY(''ProductVersion'')), 1, 2)) >= 11
BEGIN
GRANT SELECT ON sys.availability_groups TO [' + @UserName + ']
GRANT SELECT ON sys.availability_replicas TO [' + @UserName + ']
GRANT SELECT ON sys.availability_group_listener_ip_addresses TO [' + @UserName + ']
GRANT SELECT ON sys.availability_group_listeners TO [' + @UserName + ']
GRANT SELECT ON sys.dm_hadr_availability_replica_states TO [' + @UserName + ']
GRANT SELECT ON sys.dm_db_stats_properties TO [' + @UserName + ']
GRANT SELECT ON sys.dm_hadr_availability_group_states TO [' + @UserName + ']
GRANT SELECT ON sys.dm_hadr_database_replica_states TO [' + @UserName + ']
END
--For SQL 2017 or later IF CONVERT(int, SUBSTRING(CONVERT(varchar, SERVERPROPERTY(''ProductVersion'')), 1, 2)) >= 14 BEGIN
GRANT SELECT ON sys.dm_db_log_info TO [' + @UserName + ']
END'

EXEC sp_executesql @Command

--msdb permissions
SET @Command =
USE msdb GRANT SELECT ON dbo.backupmediafamily TO [' + @UserName + ']
GRANT SELECT ON dbo.backupset TO [' + @UserName + ']
GRANT SELECT ON dbo.backupfile TO [' + @UserName + ']
GRANT SELECT ON dbo.backupmediafile TO [' + @UserName + ']
GRANT SELECT ON dbo.restorefile TO [' + @UserName + ']
GRANT SELECT ON dbo.restorefilegroup TO [' + @UserName + ']
GRANT SELECT ON dbo.restorehistory TO [' + @UserName + ']
GRANT SELECT ON dbo.sysdbmaintplans TO [' + @UserName + ']
GRANT SELECT ON dbo.log_shipping_monitor_secondary TO [' + @UserName + ']
GRANT SELECT ON dbo.log_shipping_secondary_databases TO [' + @UserName + ']
GRANT SELECT ON dbo.log_shipping_secondary TO [' + @UserName + ']
GRANT SELECT ON dbo.log_shipping_monitor_primary TO [' + @UserName + ']
GRANT SELECT ON dbo.log_shipping_primary_databases TO [' + @UserName + ']
GRANT SELECT ON dbo.sysjobs TO [' + @UserName + ']
GRANT SELECT ON dbo.sysjobhistory TO [' + @UserName + ']
GRANT SELECT ON dbo.suspect_pages TO [' + @UserName + ']
IF EXISTS(SELECT 1 FROM sys.objects WHERE name = ''MSdistributiondbs'') GRANT SELECT ON dbo.MSdistributiondbs TO [' + @UserName + ']
,

EXEC sp_executesql @Command
--user databases permissions
SET @Command = '
USE [?];
IF EXISTS (SELECT 1
FROM sys.databases d LEFT JOIN sys.dm_hadr_database_replica_states r ON d.database_id = r.database_id WHERE d.is_read_only = 0 AND (r.is_primary_replica = 1 OR r.is_primary_replica IS NULL)
AND d.name = DB_NAME() )
BEGIN
GRANT SELECT ON sys.foreign_keys TO [' + @UserName + ']
GRANT SELECT ON sys.database_files TO [' + @UserName + ']
GRANT SELECT ON sys.allocation_units TO [' + @UserName + ']
GRANT SELECT ON sys.extended_properties TO [' + @UserName + ']
GRANT SELECT ON sys.objects TO [' + @UserName + ']
GRANT SELECT ON sys.partitions TO [' + @UserName + ']
GRANT SELECT ON sys.schemas TO [' + @UserName + ']
GRANT SELECT ON sys.indexes TO [' + @UserName + ']
GRANT SELECT ON sys.internal_tables TO [' + @UserName + ']
GRANT SELECT ON sys.database_principals TO [' + @UserName + ']
GRANT SELECT ON sys.all_objects TO [' + @UserName + ']

```

```

GRANT SELECT ON sys.database_permissions TO [' + @UserName + ']
GRANT SELECT ON sys.database_role_members TO [' + @UserName + ']
END
'

EXECUTE master.sys.sp_MSforeachdb @Command
SET @Command =
USE [?];
IF EXISTS (SELECT 1
FROM sys.databases d LEFT JOIN sys.dm_hadr_database_replica_states r ON d.database_id = r.database_id WHERE d.is_read_only = 0 AND (r.is_primary_replica = 1 OR r.is_primary_replica IS NULL) AND d.name = DB_NAME())
BEGIN
GRANT SELECT ON sys.symmetric_keys TO [' + @UserName + ']
GRANT SELECT ON sys.asymmetric_keys TO [' + @UserName + ']
GRANT SELECT ON sys.assembly_modules TO [' + @UserName + ']
GRANT SELECT ON sys.assemblies TO [' + @UserName + ']
GRANT SELECT ON sys.assembly_types TO [' + @UserName + ']
GRANT SELECT ON sys.xml_indexes TO [' + @UserName + ']
GRANT SELECT ON sys.columns TO [' + @UserName + ']
GRANT SELECT ON sys.index_columns TO [' + @UserName + ']
GRANT SELECT ON sys.foreign_key_columns TO [' + @UserName + ']
GRANT SELECT ON sys.tables TO [' + @UserName + ']
GRANT SELECT ON sys.numbered_procedures TO [' + @UserName + ']
GRANT SELECT ON sys.database_audit_specifications TO [' + @UserName + ']
GRANT SELECT ON sys.filegroups TO [' + @UserName + ']
GRANT SELECT ON sys.stats TO [' + @UserName + ']
GRANT SELECT ON sys.sysindexes TO [' + @UserName + ']
GRANT SELECT ON sys.check_constraints TO [' + @UserName + ']
END
'

EXECUTE master.sys.sp_MSforeachdb @Command

```

評価が実行された後に許可された権限を削除する必要がある場合がありますが、そのような場合、ここで提供されるスクリプトを使用する場合があります：

```

--Clean procedure.最初に RaaSUser を使用して任意のセッションをログオフ
DECLARE @UserName nvarchar (255) = 'Domain\RaaSUser',
@Command nvarchar (max)
SET @Command = 'USE [?];
                IF EXISTS(SELECT 1 FROM sys.database_principals WHERE name = ''' + @UserName + ''')
                    DROP USER [' + @UserName + ']; '
EXECUTE master.sys.sp_MSforeachdb @Command
SET @Command = 'USE master;
                DROP LOGIN [' + @UserName + ']'
EXEC sp_executesql @Command

```