This document explains the required steps to configure the RAP as a Service for SQL Server.

There are **two scenarios** available to configure the assessment. Determine which scenario fits best for your organization.

1. Data collection machine does not have Internet access
2. Data collection machine has Internet access

**Data collection machine does not have Internet access**
In this scenario, the data collection machine has no Internet connection and connects to either an OMS Gateway or a SCOM server (with or w/o OMS Gateway) to upload the data to log analytics. The OMS Gateway must have Internet access. This scenario is recommended for environments where the Internet connection is restricted from the data collection machine or where security is a concern due to this schedule task requirement.

In the scenario where you use an OMS Gateway, we require two computers. One will be designated as the data collection machine, and the second machine will be the OMS Gateway.

For information about the OMS Gateway, go to [https://go.microsoft.com/fwlink/?linkid=830157](https://go.microsoft.com/fwlink/?linkid=830157).

The data collection machine must be a member of the domain containing the SQL Server environment being assessed. It will collect data from multiple servers or failover clusters running SQL Server. After the data is collected, the data collection machine will analyze the information, and for increased security, will forward the data to an OMS Gateway to upload it to log analytics.

The following path shows the relationship between your Windows computers and log analytics after you have installed and configured the OMS Gateway and data collection machine.

**Data collection machine** → **Collects data from multiple servers or failover clusters running SQL Server** → **Forward collected data to the OMS Gateway** → **Submit data to the log analytics workspace**

**Data collection machine has Internet access**
This scenario can be used when the data collection machine can contact log analytics directly. It requires one computer that will be designated as the data collection machine which has to be able to access the Internet to upload data to log analytics. This scenario can be used in environments where the Internet connection is not restricted.

The data collection machine must be a member of the domain containing the SQL Server environment being assessed. It will collect data from multiple servers or failover clusters running SQL Server. After the data is collected, the data collection machine will analyze the information and then upload the data to log analytics directly, which will require HTTPS connectivity to your log analytics workspace. The following path shows the relationship between your Windows computers and log analytics after you have installed and configured the data collection machine:

**Data collection machine** → **Collects data from multiple servers or failover clusters running SQL Server** → **Submit data to the log analytics workspace.**

**Detailed information on these configurations and requirements are listed later in this document.**
## Table of Contents

**System Requirements and Configuration at Glance**................................. 3  
- Supported Versions................................................................................. 3  
- Common to Both Scenarios................................................................. 3  
- Data Collection Machine..................................................................... 3  
- OMS Gateway (required in the data collection machine does not have Internet access scenario).......................... 4  
- PowerShell Remoting........................................................................... 4  
- User Profile Service............................................................................ 9  

**Appendix A – Setting up the Environment**.................................................. 11  
- Enable the assessment in Services Hub portal ............................................... 11  
  1. Log Analytics OMS Gateway Setup...................................................... 12  
  2. Data Collection Machine Setup............................................................ 13  
  3. Setup and configure log analytics using SCOM........................................ 19  

**Appendix B - Setting up the SQL Server Assessment**.................................. 24  

**Appendix – C Data Collection Methods**....................................................... 28  

© 2019 Microsoft Corporation
System Requirements and Configuration at Glance

According to the scenario you use, review the following details to ensure that you meet the necessary requirements.

Supported Versions


Common to Both Scenarios

- You will need a log analytics workspace
- **User account rights:**
  - A domain account, Standalone Managed Service Account (sMSA) or Group Managed Service Account (gMSA) with the following rights:
    - Member of the local Administrators group on all servers in the environment
    - SysAdmin role on all Microsoft SQL Servers in the environment
  - For Standalone Managed Service Account (sMSA) or Group Managed Service Account (gMSA) you can use this reference [https://docs.microsoft.com/en-us/services-hub/health/kb-running-assessments-with-msas](https://docs.microsoft.com/en-us/services-hub/health/kb-running-assessments-with-msas)

Data Collection Machine

- **Microsoft Monitoring Agent** requires computers running Windows Server 2008 SP1 or later (or Windows 7 SP1 or later – Important: The option of installing the Microsoft Monitoring Agent on client operating systems is strongly discouraged due to the risk of exposing privileged domain account credentials to lower trust workstations.
- The **CLR version** on the data collection machine should be using **.NET 4.0 or greater**. This can be verified by running `$PSVersionTable.CLRVersion` in the PowerShell prompt
- Microsoft **.NET Framework 4.6.2 or newer** installed
- The data collection machine must be a member server of the Active Directory domain which includes the SQL Server environment that needs to be assessed.
- **Data collection machine hardware:** Minimum 8 gigabytes (GB) of RAM, 2 gigahertz (GHz) dual-core processor, and minimum 10 GB of free disk space.
- The **data collection machine** is used to connect to server(s) running SQL Server environment and retrieve information from the environment. The machine is communicating over Remote Procedure Call (RPC), Server Message Block (SMB), WMI, remote registry, SQL Server, Lightweight Directory Access Protocol (LDAP) and Distributed Component Object Model (DCOM).
- Microsoft .NET Framework 4.6.2 or newer installed.
- The **data collection machine** must be able to connect to the Internet using HTTPS to submit the collected data to your log analytics workspace. This connection can be direct, via a proxy.
- For the **Microsoft Monitoring Agent** to connect to and register with the log analytics service, it must have access to the Internet. If you use a proxy server for communication between the agent and the log analytics service, you will need to ensure that the appropriate resources are accessible. If you use a firewall to restrict access to the Internet, you need to configure your firewall to permit access to log analytics. To ensure data can be submitted...

OMS Gateway (required in the data collection machine does not have Internet access scenario)

- The **OMS Gateway** must be able to connect to the Internet using HTTPS to submit the collected data to your log analytics workspace. This connection can be direct or via a proxy.
- **OMS Gateway hardware**: Minimum 4 GB of RAM and 2 GHz processor.
- **OMS Gateway services**: When the Windows Firewall service is disabled the installation of the OMS Gateway fails.
- **OMS Gateway user account rights**: None required.

PowerShell Remoting

To complete the assessment with the accurate results, you will need to configure all in-scope target machines for PowerShell remoting.

PowerShell on the tools machine is used to scan the servers for installed security patches as well as audit policy configuration.

- Windows Update Agent must be running on all SQL Servers for the security update scan
- PowerShell version 2 or greater is required on target SQL Servers and comes installed by default starting with Windows Server 2008 R2. For Windows Server 2008 SP2, PowerShell version 2 is not installed by default. It is available for download here [https://aka.ms/wmf3download](https://aka.ms/wmf3download)

**Additional requirements for Windows Server 2008-2012 R2 (or later if defaults modified) Target Machines:**

The following three items must be configured on target SQL Servers to support data collection: PowerShell Remoting, WinRM service and Listener, and Inbound Allow Firewall Rules.

**Note**: Windows Server 2012 R2 and Windows Server 2016 have WinRM and PowerShell remoting enabled by default. Windows Server 2008—Windows Server 2012 have WinRM and PowerShell remoting disabled by default. One of the following configuration options will need to be implemented support PowerShell Remoting if WinRM and PowerShell remoting are disabled on any target SQL servers:

**Option 1**: Execute **Enable-PSRemoting** PowerShell cmdlet on each target machine within the scope of the assessment. This one command will configure PS-Remoting, WinRM service and listener, and enable required Inbound FW rules. A detailed description of everything Enable-PSRemoting does is documented [here](https://aka.ms/wmf3download).

**OR**

**Option 2**: Implement all three steps below.

1. Configure **WinRM / PowerShell remoting** via Group Policy (Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service)
a. In 2008 R2 it’s “Allow automatic configuration of listeners”.

b. In 2012 R2 (and later) it’s “Allow remote server management through WinRM”.

2. Configure WinRM service for automatic start via Group Policy (Computer Configuration\Policies\Windows Settings\Security Settings\SystemServices)

   a. Define Windows Remote Management (WS-Management) service for Automatic startup mode

3. Configure Inbound allow Firewall Rules: This can be done individually in the local firewall policy of every in-scope target SQL Servers or via a group policy which allow communication from the tools machine.

Option 2: Detailed step by step instructions to implement the above 3 steps.

Two steps are involved to configure a group policy to enable both WinRM listener and the required inbound allow firewall rules:

A) Identify the IP address of the source computer where data collection will occur from.

B) Create a new GPO linked to the SQL Server organizational unit, and define an inbound rule for the tools machine

A.) Log into the chosen data collection machine to identify its current IP address using IPCFG.exe from the command prompt.

An example output is as follows

C:\>ipconfig
Windows IP Configuration
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . : fe80::X:X:X:X%13
   IPv4 Address . . . . . . . . . . : X.X.X.X
   Subnet Mask . . . . . . . . . . : X.X.X.X
   Default Gateway . . . . . . . . : X.X.X.X

Make a note of the IPv4 address of your machine. The final step in the configuration will use this address to ensure only the data collection machine can communicate with the Windows Update Agent on the SQL Servers.

B.) Create, configure, and link a group policy object to the SQL Servers OU which has target SQL Servers.

1. Create a new GPO. Make sure the GPO applies to the SQL Servers organizational unit. Give the new group policy a name based on your group policy naming convention or something that identifies its purpose similar to “SQLServerAssessment”
2. Within the GPO open, right click on the new GPO and select Edit and go to “Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service”. Enable “Allow remote server management through WinRM” or “Allow automatic configuration of listeners” depending on your OS.

3. Create an advanced Inbound Firewall Rule to allow all network traffic from the tools machine to the SQL Servers. This can be the applied to the same GPO that was used in step 1 above. (Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security – LDAP:.xxx\Inbound Rules)
4. To create the new rule, Right Click on “Inbound Rules” and select “New”

5. Create a custom rule and choose “Next”
6. Allow “All programs” from the tools machine and click “Next”.

7. Allow all protocols and ports, then click “Next”.
8. Specify the IP address of the tools machine and click “Next”.

9. Choose to “Allow the connection” and click Next

10. Choose to select network profile “Domain” and click “Next”

11. Choose a name for the rule (Example: SQLAssessmentToolsMachine) and save.


13. Save the GPO and ensure the target SQL servers apply it.

**User Profile Service**

It is necessary to modify the default behavior of the User Profile Service as it relates to user logoff. Windows, by default, forcibly unloads user registry hive on logoff even if there are applications with open handles to the user registry hive. This default behavior interferes with remote PowerShell initialization routines during execution of the on-demand assessment via scheduled task and can prevent successful collection and submission of assessment data to the log analytics portal.

On the data collection machine, change the following setting in the group policy editor (gpedit.msc) from "not configured" to "enabled":

**Computer Configuration->Administrative Templates->System-> User Profiles**

'Do not forcefully unload the user registry at user logoff'
A PFE will assist with the setup, configure both machines and scheduling the SQL assessment during the scoping call. If you do not have an Azure Log Analytics workspace, the PFE assists you creating one and link that workspace with our Services Hub portal where you enable the assessment. Depending on the scenario you have chosen, have one or two machines installed and account ready according to the requirements mentioned above. These machines can be VMs.

The appendix has the information how to setup the OMS Gateway, data collection machine and run the assessment.
Appendix A – Setting up the Environment

Enable the assessment in Services Hub portal

1. To ensure the Microsoft Monitoring Agent knows what assessments can be run, you need to add the assessment you want to run.
   
   If you have not added the assessment you are setting up, do this now. In https://serviceshub.microsoft.com go to Health -> Assessments, select the assessment you want to enable and click Add Assessment.

2. Click **Add** on the Assessment you want to setup

   ![Add Assessment Screenshot](image)

   The option changes from Add to View in Azure Log Analytics. You are now all set for the next steps.

Determine the steps to follow to successfully setup the environment for your scenario:

**Data collection machine has Internet access**

- Follow **Step 2**. Data Collection Machine Setup, then **Appendix B – Setup Assessment**

**Data Collection machine has no Internet access**

- Using OMS Gateway
  - Start with **Step 1**, then **Step 2** and next **Appendix B - Setup Assessment**

- Using SCOM
  - Start with **Step 3**
1. Log Analytics OMS Gateway Setup

If your scenario includes the installation of an OMS Gateway, follow this section. If not, move to the step 2. On the designated OMS Gateway machine, you must install both the OMS Gateway and the Microsoft Monitoring Agent. Follow the instructions in the sections below to set up both components.

Download and install the OMS Gateway

On the designated OMS Gateway server, complete the following:

1. Download the Setup file from https://go.microsoft.com/fwlink/?linkid=837444
2. On the Welcome page, click Next.
3. On the License Agreement page, select I accept the terms in the License Agreement to agree to the EULA, and then click Next.
4. On the Port and Proxy Address page, do the following:
   - Type the TCP port number to be used for the OMS Gateway. Setup opens this port number from Windows firewall. The default value is 8080.
   - [Optional] If the server on which the OMS Gateway resides needs to go through a proxy, input the proxy address where the OMS Gateway needs to connect. For example, myorgname.corp.contoso.com:80. This is an optional value. If it is blank, the OMS Gateway will try to connect to the Internet directly. Otherwise, the OMS Gateway will connect through your internal proxy. If your proxy requires authentication, you can provide a username (domain\user) and password. (NOTE: If you do not provide a domain for the user, it will not work).
   - Click Next.
5. On the Destination Folder page, either retain the default folder location of %ProgramFiles%\OMS Gateway, or type the location where you want to install, and then click Next.
6. On the Ready to install page, select Install. A User Account Control dialog box might appear requesting permission to install. If so, click OK.
7. After Setup completes, click Finish. You can verify that the service is running by opening the Services.msc snap-in and checking the status of the service called OMS Gateway.
8. Download and install the Microsoft Monitoring Agent setup file from log analytics.

Note. It is required to install the Microsoft Monitoring Agent on the OMS Gateway and configure it to with the log analytics workspace that you configure on the data collection machine. Follow the instructions in the next section in this document, Data Collection Machine Setup.
2. Data Collection Machine Setup

Download and install the Microsoft Monitoring Agent setup file from Azure Log Analytics

On the designated data collection machine or OMS Gateway server complete the following:

**Note.** If the collection machine does not have an Internet connection, perform the first 3 steps from an Internet Connected machine.

1. In the Azure portal, go to log analytics, select your workspace and click the **Advanced Settings** Icon.

2. **Click Connected Sources, and then select Windows Servers.**

3. Click the **Download Windows Agent** link that is applicable to your computer processor type to download the setup file. If the agent is downloaded on another machine, copy the Setup file over to the data collection machine or OMS Gateway server.

**Note.** If a monitoring client was installed for System Center Operations Manager (SCOM), the setup only offers to Upgrade the agent, preserving existing settings. The upgrade does not include any of the configuration steps below.

The next steps apply to installations where no monitoring client was installed for SCOM. Refer to the **Microsoft Monitoring Agent Upgrade** section in this document when you are performing an upgrade of the Monitoring Agent for SCOM.
4. Run Setup to install the agent.
5. On the Welcome page, click Next.
6. On the License Terms page, read the license and then click I Agree
7. On the Destination Folder page, change or keep the default installation folder and then click Next.
8. On the Agent Setup Options page, choose the Connect the agent to Azure Log Analytics (OMS) option. Click Next.

9. On the Overview, Settings Dashboard page, click Connected Sources, and then copy and paste the Workspace ID and Workspace Key (Primary Key) from the log analytics portal. (Hint: Click the copy button then paste in the corresponding Agent Setup field). Select Azure Commercial or if you are using an Azure US Government cloud select Azure US Government from the Azure Cloud drop down menu and click OK.
10. If you are currently installing the agent on the data collection machine and using an OMS Gateway as part of the OMS Gateway and Data Collection Machine scenario, or if your company requires access through a proxy server, click the Advanced button to provide HTTP proxy configuration. If you do not use any of the above, click Next and go to step 12.

11. Specify the fully qualified domain name (FQDN) or the IP address and port of the OMS Gateway.
If you use a proxy server instead of an OMS Gateway, add the information for your proxy server and if required, authentication credentials (not required for the OMS Gateway), then click **Next** twice.

12. On the **Microsoft Update** page, optionally select **Use Microsoft Update when I check for updates (recommended)**, then click **Next**.

13. On the **Ready to Install** page, review your choices, and then click **Install**.

14. On the **Microsoft Monitoring Agent configuration completed successfully** page, click **Finish**.

15. When complete, the **Microsoft Monitoring Agent** appears in **Control Panel**. You can review your configuration there and verify that the agent is connected to log analytics. When connected to log analytics, the agent displays a message stating: **The Microsoft Monitoring Agent has successfully connected to the log analytics service.**
**Note.** If you have been installing the Microsoft Monitoring Agent on the OMS Gateway, you need to repeat the installation on the data collection machine.

After setting up the data collection machine, continue with the setup of the Assessment as outlined in the prerequisites and configuration documentation for each technology.
Microsoft Monitoring Agent Upgrade

If a monitoring agent is already installed, the Microsoft Monitoring Agent setup will only display the upgrade option. The upgrade will keep the existing configuration and adds a new option to configure a log analytics workspace.

Follow the steps below to perform an upgrade and configure the agent for the log analytics Workspace.

1. Run Setup to install the agent.
2. On the **Welcome** page, click **Next**.
3. On the **License Terms** page, read the license and then click **I Agree**
4. On the **begin Upgrade** page, click **Upgrade**.
5. On the **Completion** page, click **Finish**.
6. Once the agent installation completed, go to the **Control Panel**.

7. Click **Microsoft Monitoring Agent**
8. If the OMS Gateway scenario is chosen or a Proxy server is in place go to the **Proxy Settings** tab

When this scenario is not used go to step 9.
Select **Use a proxy server** and specify the fully qualified domain name (FQDN) or the IP address and port of the OMS Gateway.
If you use a proxy server instead of an OMS Gateway, add the information for your proxy server and if required, authentication credentials (not required for the OMS Gateway), then Select **Apply**

9. Select the **Azure Log Analytics (OMS)** tab and click **Add...**

![Add a Log Analytics Workspace](image)

10. Copy and paste the **Workspace ID** and **Workspace Key (Primary Key)** from the log analytics portal. (Hint: Click the copy button then paste in the corresponding **Agent Setup** field). Select **Azure Commercial** or, if you are using an Azure US Government cloud select **Azure US Government** from the **Azure Cloud** drop down menu and click **OK**.

11. An exclamation mark will be visible in the Workspaces pane. Click **Apply**. This will stop and start the agent, and the Workspaces pane should look like the following example after a few seconds.

![Microsoft Monitoring Agent Properties](image)

12. Click **OK** to finish the Microsoft Monitoring Agent upgrade for log analytics.
3. Setup and configure log analytics using SCOM

If SCOM is already in use and you want to use SCOM and the already installed agents, follow the steps in this section. In this configuration SCOM will either act as the gateway or it leverages the OMS Gateway itself to send data to log analytics.

Pre-requisites

The SCOM 2012 SP1 UR6 (UR7 for proxy/gateway support) or SCOM 2012 R2 UR2 (UR3 for proxy/gateway support) agent is the minimum version required to fully support log analytics functionality.

If you are using multi homing of log analytics workspaces, we would suggest that you not use the agent that comes with SCOM but use the Microsoft Monitoring Agent from Microsoft Update/log analytics workspace instead. The current Microsoft Monitoring Agent version is backwards compatible and supported with all SCOM 2012 R2/2016 management groups.

1. On the SCOM Administration Console go to **Administration -> Operations Management Suite -> Connection**

   ![Operations Management Suite Overview](image)

2. Click on **Register to Operations Management Suite**

   A login window will appear. Log in with an account that has administrative rights to connect to the log analytics workspace. Select the proper workspace (if there is more than one) and click **Next**. In the **Confirm the settings** window click on **Create**.
3. Go to the log analytics workspace.

4. From the log analytics workspace, to confirm that the Management Group is connected, go to Advanced Settings -> Connected Sources -> System Center:

Back in the SCOM Administration Console you need to opt-in the agents for log analytics/OMS:

1. Go to Administration -> Operations Management Suite -> Connection

2. In the right pane, click on Add a Computer/Group below Actions:
3. Select the **object type** *(Windows Computer or Groups)* and optionally leave the **Filter** field empty to return all objects of the type selected

Verify the solution is downloaded on the data collection machine.

Every agent opted-in will receive Management Packs (MPs) from the log analytics workspace. The MPs will depend on which solutions are added. For the Microsoft Unified Support Assessment, the MPs are named:

Microsoft.IntelligencePacks.<technology>.Assessment

The Microsoft Unified Support assessments MPs will be downloaded as soon as the solution is added to the log analytics workspace. The MPs are downloaded into the Management Pack folder of the agent (this is true regardless of the setup – direct, through GW, or through SCOM):

You can also look at the OperationsManager event log (it’s the same for the SCOM agent or the stand alone MMA agent) for the events indicating the MPs have been downloaded:
Below picture shows how the Management Packs flow from the OMS Workspace

1. Add Microsoft Unified Support Solution Pack & solution assessment

2. MP is distributed to agents

3. Every agent now has the PowerShell modules and can be a collection agent

4. Agent(s) will send back collection data
Collected data from any agent that is running the scheduled task is sent back to the SCOM Management Server which in turn will upload to the log analytics/OMS Workspace

**Note:** the SCOM Management Group might connect directly to the log analytics service or through the OMS Gateway. The OMS Gateway in the picture above is used for certain solutions that cannot leverage SCOM.

Appendix B - Setting up the SQL Server Assessment

When you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, you are ready to setup the SQL Server Assessment.

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator

2. Run the `Add-SQLAssessmentTask -SQLServerName <YourServerName> -WorkingDirectory <Directory>` command where `<YourServerName>` is the fully qualified domain name (FQDN) or the NetBIOS name of single server or failover cluster running SQL Server environment. If more than one environment is assessed, ‘;’ is used between the environments. For failover cluster, check failover cluster virtual network name and `<Directory>` is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment(s).

   **NOTE:** If the directory does not exist, it must be created before you continue with the execution.

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

3. Provide the required user account credentials. These credentials are used to run the SQL Assessment. For sMSA or gMSA review the article [https://docs.microsoft.com/en-us/services-hub/health/kb-running-assessments-with-msas](https://docs.microsoft.com/en-us/services-hub/health/kb-running-assessments-with-msas)

   **NOTE:** This domain account must have all the following rights:

   - Member of the local Administrators group on all servers in the environment
   - SysAdmin role on all Microsoft SQL Servers in the environment
4. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

```
PS C:\users\romin\ ~ Add-SQLAssessmentTask -SQLServerName "attaxt.redmond.conf.microsoft.com" -WorkingDirectory "C:\VMS\SQL"
[SQLAssessment]Detected agent configuration for Management Group AOI-49900795-7a88-4ee8-a2de-ca8a46fc8c9e
[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(Domain\Name\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. Data collection is triggered by the **scheduled task** named `SQLAssessment -ServerName <YourServerName>` within an hour of running the previous script and then every 7 days. The task can be modified to run on a different date/time or even forced to run immediately.
6. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:

```
Share > This PC > OSDisk (C) > OMS > SQL > SQLAssessment > asttest.redmond.corp.microsoft.com
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>2910942</td>
<td>18/10/2017 02:42 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>OmsAssessment</td>
<td>18/10/2017 02:42 AM</td>
<td>File folder</td>
<td></td>
</tr>
<tr>
<td>run.cmd</td>
<td>18/10/2017 02:36 AM</td>
<td>Windows Command</td>
<td>1 KB</td>
</tr>
</tbody>
</table>

7. After data collection and analysis is completed on the tools machine, it will be submitted to your log analytics workspace depending on the scenario you have chosen:
   - **Directly** if the Data Collection Machine is connected to the Internet.
   - **Through the OMS Gateway** if the Data Collection Machine is not connected to the Internet.

8. After a few hours, your assessment results will be available on your log analytics dashboard. Click the **SQL Assessment** tile to review:

![SQL Server Assessment](image)

- 1 Servers Assessed in last 21 days
- 10 High Priority Recommendations
- 77 Low Priority Recommendations
- 444 Passed checks

9. You will be presented with findings grouped by the focus area.
<table>
<thead>
<tr>
<th>SECURITY AND COMPLIANCE</th>
<th>AVAILABILITY AND BUSINESS CONTINUITY</th>
<th>PERFORMANCE AND SCALABILITY</th>
<th>UPGRADE, MIGRATION, AND DEPLOYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>65%</td>
<td>98%</td>
<td>87%</td>
<td>84%</td>
</tr>
<tr>
<td>PROCEDEED RECOMMENDATIONS</td>
<td>WEIGHT</td>
<td>PROCEDEED RECOMMENDATIONS</td>
<td>WEIGHT</td>
</tr>
<tr>
<td>Configure and enforce the setting “Windows Firewall”</td>
<td>6.1</td>
<td>Change the recovery model to FULL or ROLLUP_LOGGED</td>
<td>5.9</td>
</tr>
<tr>
<td>Disable and remove the setting “Turn off Auditing”</td>
<td>5.6</td>
<td>Schedule a full database backup and ensure that it’s...</td>
<td>5.2</td>
</tr>
<tr>
<td>Configure and enforce the setting “Windows Firewall”</td>
<td>4.8</td>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
</tr>
<tr>
<td>Configure the setting “Network security: Allow Management”</td>
<td>3.6</td>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
</tr>
<tr>
<td>Define and enforce “Microsoft networks server Databas...</td>
<td>3.4</td>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
</tr>
<tr>
<td>Configure and enforce the setting “Remote NOS”</td>
<td>2.8</td>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
</tr>
<tr>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
</tr>
<tr>
<td>Avoid adding users to the dellmune database role</td>
<td>2.4</td>
<td>Review the SQL Server instance configuration setting</td>
<td>2.6</td>
</tr>
</tbody>
</table>

See all...
Appendix – C Data Collection Methods

The SQL Assessment in the log analytics workspace and Microsoft Unified Support Solution Pack uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

1. Event Log collectors
   Collects last 7 days of application and system event logs including Warnings and Errors from SQL Servers.

2. File data collectors
   Enumerates files in a folder on a remote machine, and optionally retrieves those files.

3. Registry data collectors
   Registry keys and values are collected from the SQL Server environment. They include items such as:
   - Power options information from "HKLM\SYSTEM\CurrentControlSet\Control\Power\User\PowerSchemes"
   - This allows you to understand how you set power plan on SQL Server.

4. User rights collectors
   Collect local security policies.

5. Mount points data collectors
   Collect mount points if they exist.
6. **SQL data collectors**

   T-SQL queries are used to collect information such as:
   
   - Always On configuration, database names, health status
   - TempDB files, file sizes, auto growth sizes
   - Backup histories
   - Duplicate, redundant, disabled, hypothetical indexes

7. **SQL error log collectors**

   Collects last 15 days SQL Server error logs. If any log file size is more than 6MB, it is not analyzed.

8. **WMI data collectors**

   WMI is used to collect various information such as:
   
   - **WIN32_Volume**
     Collects information on Volume Settings for each server in the environment. For example, the information is used to determine the system volume and drive letter, which allows a client to collect information on the files located on the system drive.
   - **Win32_Process**
     Collect information on the processes running on each server in the environment. The information provides insight in processes that consume a large amount of threads, memory, or have a large page file usage.
   - **Win32_LogicalDisk**
     Used to collect information on the logical disks. Microsoft use the information to determine the amount of free space on the disk where the database or log files are located.

9. **Windows PowerShell data collectors**

   PowerShell is used to collect various information such as:
   
   - Collect resource dependencies
   - Auditing configuration
Appendix – D Ports requirements

If opening all ports between tools machine and target servers is not possible, here is the list of specific ports that need to be open for the toolset to work correctly. These ports need to be open in each target server.

- SQL Instances ports, 1433 or as configured by Customer.
- SQL Browser port – UDP 1434
- RPC Dynamic Ports Range
  o By default TCP ports from 49152 to 65535
  o They can change this range but it could have some other implications that they need to evaluate as this range of ports is used by different components and you need to be careful of not running out of ports. [https://support.microsoft.com/en-us/help/929851/the-default-dynamic-port-range-for-tcp-ip-has-changed-in-windows-vista](https://support.microsoft.com/en-us/help/929851/the-default-dynamic-port-range-for-tcp-ip-has-changed-in-windows-vista)
- Default PS Remoting ports are TCP 5985 and TCP 5986, if customer changed, it could be 80 and 443 or any other ports they specified.
- Port TCP 135
- Port UDP 137 (maybe not necessary)
- Port TCP 139
- Port TCP 445
Appendix – E Special Requirements for Availability Group Cluster in Azure

Virtual networks in Azure put some connectivity restrictions to clusters and availability groups that affect the toolset. In summary:

1. If you are using external load balancer you cannot use the listener name for discovery. You can use the cluster name or a node name.

2. If you are not using an Standard Load Balancer with HA ports for the Cluster Name IP, then you need to modify the hosts file to make the Cluster Collectors work. You need to identify the IP of the active node and modify the hosts files as shown below. The hosts file is located at “C:\Windows\System32\drivers\etc”.

![Hosts File Configuration]

**Note:** The hosts configuration change needs to be reviewed every time you run the toolset in case a failover has happened since the last time the toolset was executed.
Appendix – F Requirements to run without sysadmin

If granting sysadmin privileges is not possible you can use the script provided here to grant only necessary privileges to the account running the assessment. Consider that a few rules can only collect the necessary data when running with sysadmin, these rules will be skipped when not running with sysadmin privileges.

One special case is when you have read only databases (other than availability group databases). In that case the necessary user won’t be created and several rules will be skipped on these read only databases. To collect necessary information for these databases you need to change to read-write only to run the script provided here to create the necessary user and permissions or run the toolset with an account that is sysadmin (the toolset only supports Windows Authentication).

The script below is long because it grants permissions that usually are already granted to public role by default. This means the script will work even when all permissions have been revoked from public.

The script to create the login users and grant permissions is provide here. Remember that the script needs to be run in each instance that will be assessed. Given the limitations of a document to include long scripts, be careful when copying the script as it spans several pages.

```sql
DECLARE @UserName nvarchar(255) = 'DomainName\RaaSUser', --replace with your domain and username, the user needs to exist on the domain specified

@Command nvarchar(max)

SET @Command = 'USE master;
    CREATE LOGIN [' + @UserName + '] FROM WINDOWS WITH DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_english];'
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()
)
    CREATE USER [' + @UserName + '] FOR LOGIN [' + @UserName + '];
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 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 + ']
```
EXECUTE master.sys.sp_MSforeachdb @Command

SET @Command = 'GRANT EXEC ON sys.sp_validatelogins TO [' + @UserName + ']
GRANT EXEC ON sys.sp_executesql TO [' + @UserName + ']
GRANT SELECT ON sys.dm_exec_connections TO [' + @UserName + ']
GRANT SELECT ON sys.dm_os_wait_stats TO [' + @UserName + ']
GRANT SELECT ON sys.dm_xe_sessions TO [' + @UserName + ']
GRANT SELECT ON sys.dm_db_missing_index_groups TO [' + @UserName + ']
GRANT SELECT ON sys.dm_db_missing_index_details TO [' + @UserName + ']
GRANT SELECT ON sys.dm_db_partition_stats TO [' + @UserName + ']

--For SQL Server 2017 or later
IF CONVERT(int,SUBSTRING(CONVERT(varchar,SERVERPROPERTY(''ProductVersion'')), 1, 2)) >= 1
BEGIN
  GRANT SELECT ON dbo.suspect_pages TO [' + @UserName + ']
  GRANT SELECT ON dbo.sysjobhistory TO [' + @UserName + ']
  GRANT SELECT ON dbo.sysjobs TO [' + @UserName + ']
  GRANT SELECT ON dbo.log_shipping_primary_databases TO [' + @UserName + ']
  GRANT SELECT ON dbo.log_shipping_secondary_databases TO [' + @UserName + ']
  GRANT SELECT ON dbo.log_shipping_monitor_primary TO [' + @UserName + ']
  GRANT SELECT ON dbo.log_shipping_monitor_secondary TO [' + @UserName + ']
  GRANT SELECT ON dbo.log_shipping_monitor_secondary_databases TO [' + @UserName + ']
END

--For SQL Server 2012 or later
IF CONVERT(int,SUBSTRING(CONVERT(varchar,SERVERPROPERTY(''ProductVersion'')), 1, 2)) >= 1
BEGIN
  GRANT EXEC ON sys.sp_validatelogins TO [' + @UserName + ']
  GRANT EXEC ON sys.sp_executesql TO [' + @UserName + ']
  GRANT SELECT ON sys.dm_exec_connections TO [' + @UserName + ']
  GRANT SELECT ON sys.dm_os_wait_stats TO [' + @UserName + ']
  GRANT SELECT ON sys.dm_xe_sessions TO [' + @UserName + ']
  GRANT SELECT ON sys.dm_db_missing_index_groups TO [' + @UserName + ']
  GRANT SELECT ON sys.dm_db_missing_index_details TO [' + @UserName + ']
  GRANT SELECT ON sys.dm_db_partition_stats TO [' + @UserName + ']
END

EXECUTE master.sys.sp_MSforeachdb @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.backupmediaset 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.sysbdmaintplans 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 + ']

EXECUTE master.sys.sp_MSforeachdb @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
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.tables 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 + ']

EXEC master.sys.sp_MSforeachdb @Command

You may need to remove the permissions granted after the assessment is run, in that case you may use the script provided here:

--Clean procedure. First log off any session using the RaaSUser
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 + '];

EXEC master.sys.sp_MSforeachdb @Command

SET @Command = 'USE master;
   DROP LOGIN [' + @UserName + ']
EXEC sp_executesql @Command