SharePoint Assessment: Prerequisites and Configuration

This document explains the required steps to configure the SharePoint Assessment included with your Azure Log Analytics Workspace and Microsoft Unified Support Solution Pack.

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

1. OMS Gateway and data collection machine
2. Data collection machine only

OMS Gateway and data collection machine
This scenario is the most secure and recommended option to help protect privileged account credentials which are used on the scheduled task configured on this machine needed to run the assessment. This scenario requires two computers. One will be designated as the data collection machine, and the second machine will be the OMS Gateway. In this scenario, the data collection machine has no Internet connection and connects to the 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. For information about the OMS Gateway, go to https://go.microsoft.com/fwlink/?linkid=830157.

The data collection machine must be a member of the SharePoint farm being assessed. It will collect data from all the servers in the SharePoint farm. 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 all SharePoint servers in the environment → Forward collected data to the OMS Gateway → Submit data to the log analytics *workspace*

Data collection machine only
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 must 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 SharePoint farm being assessed. It will collect data from all the SharePoint Servers in the farm. 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 all SharePoint servers in the environment → Submit data to the log analytics *workspace.*

Table of Contents

System Requirements and Configuration at Glance

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

Supported Versions

- Your SharePoint environment must run on **SharePoint Server 2013, SharePoint Server 2016 or Microsoft SharePoint Server 2019**.
    - They must run on Windows Server 2012 R2 or later.

Common to Both Scenarios

- You will need an **Azure subscription**
- You will need a **log analytics workspace**
- **User account rights:**
    - A domain account with the following rights:
        - Farm Administrator.
        - Local Admin rights on All SharePoint & SQL Servers associated with the SharePoint farm being assessed.
        - Sysadmin rights on all Instances housing SharePoint databases.

Data Collection Machine

- The **Data collection machine** must be joined or be one of the servers in the SharePoint farm. We recommend using the server running Central Administration.
- **Data collection machine hardware:** Minimum 16 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 10 GB of free disk space.
- The **data collection machine** is used to connect to all servers in the farm and retrieve information from them. The machine is communicating over Remote Procedure Call (RPC), Server Message Block (SMB), WMI, remote registry, SQL Queries, PowerShell cmdlets.
- Microsoft .NET Framework 4.8 or newer installed
    - Download from: Download .NET Framework 4.8 | Free official downloads (microsoft.com)
- 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 follow the steps in *Configure Proxy and Firewall Settings in Log Analytics* at https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/.

OMS Gateway (required in the **OMS Gateway and data collection machine** scenario)

- The **OMS Gateway** can be a standalone or a member server. It requires Windows Server 2012 R2 or later.
- 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, via a proxy.
- **OMS Gateway hardware:** Minimum 4 GB of RAM and 2 GHz processor.
- **OMS Gateway user account rights:** None required.

Click the link to download the "Setup Assessment" documentation to install the OMS Gateway and Microsoft Monitoring Agent.
https://go.microsoft.com/fwlink/?linkid=860142

After you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, continue with the next section to set up the assessment.

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 SharePoint servers for the security update scan

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

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

Note1: *Windows Server 2012 R2 and Windows Server 2016 have WinRM and PowerShell remoting enabled by default. The following configuration steps detailed below will only need to be implemented if the default configuration for target machines has been altered.*

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 SharePoint servers 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 IPConfig.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**

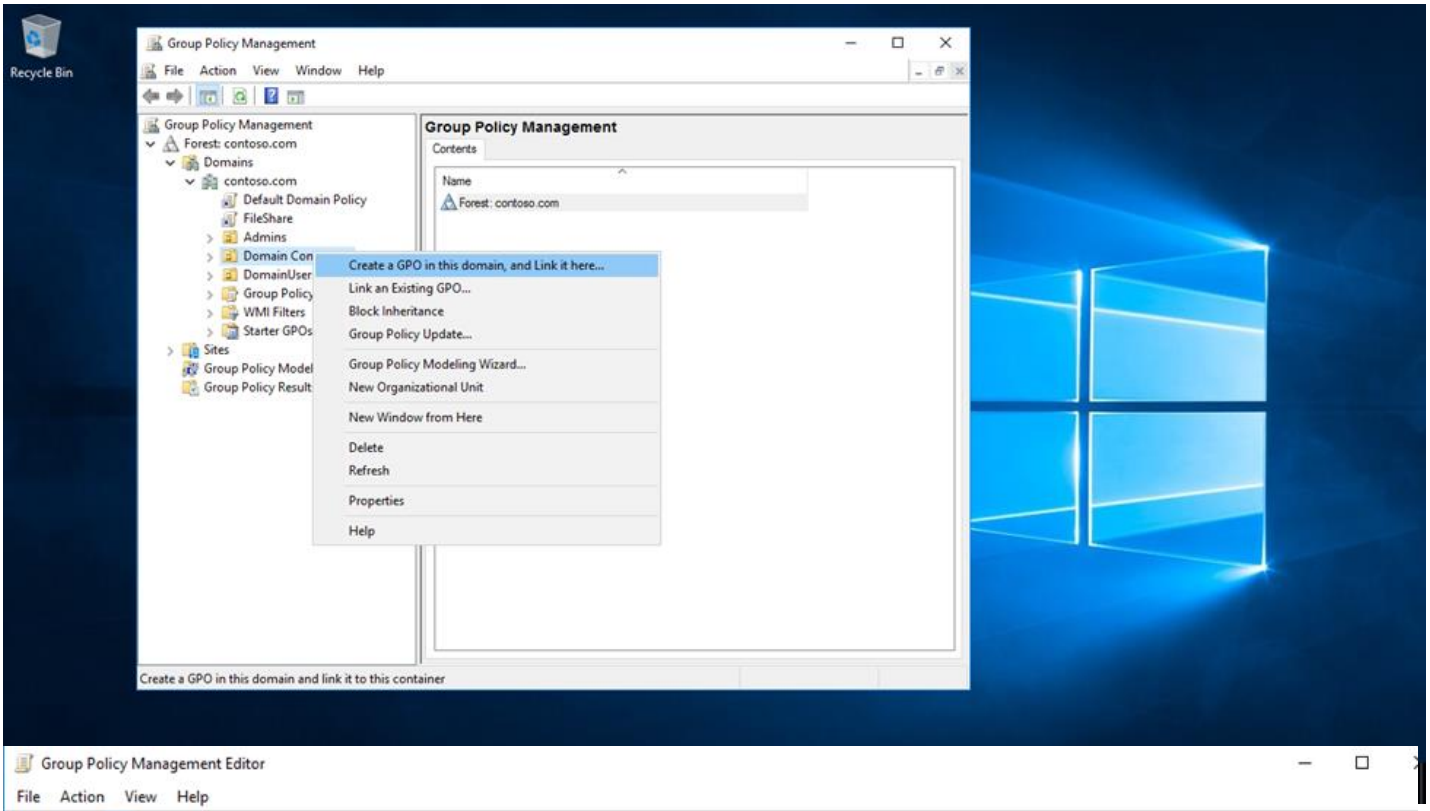
Subnet Mask . . . . . : X.X.X.X

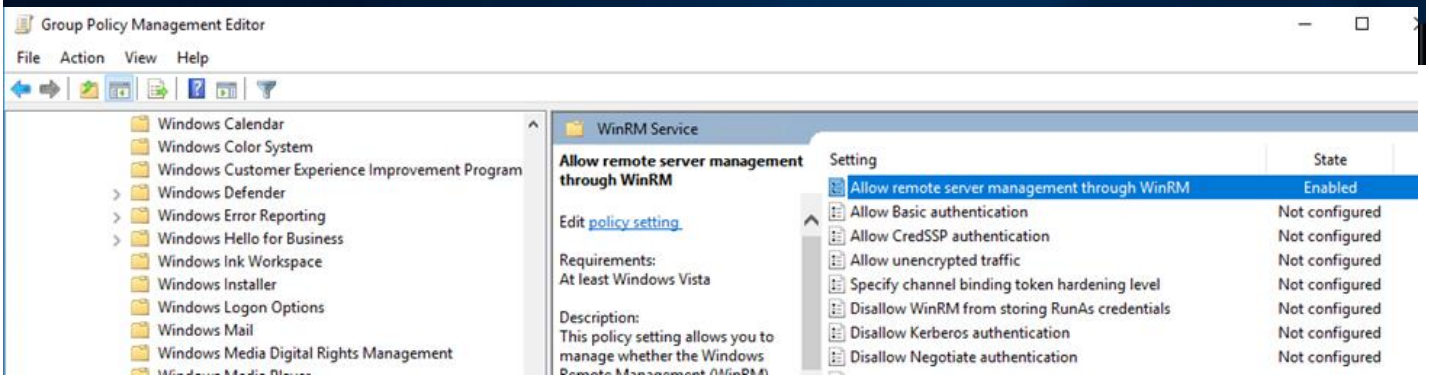
Default Gateway . . . . . : X.X.X.X

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 SharePoint servers.

B.) Create, configure, and link a group policy object to the SharePoint servers OU in each domain in the forest.

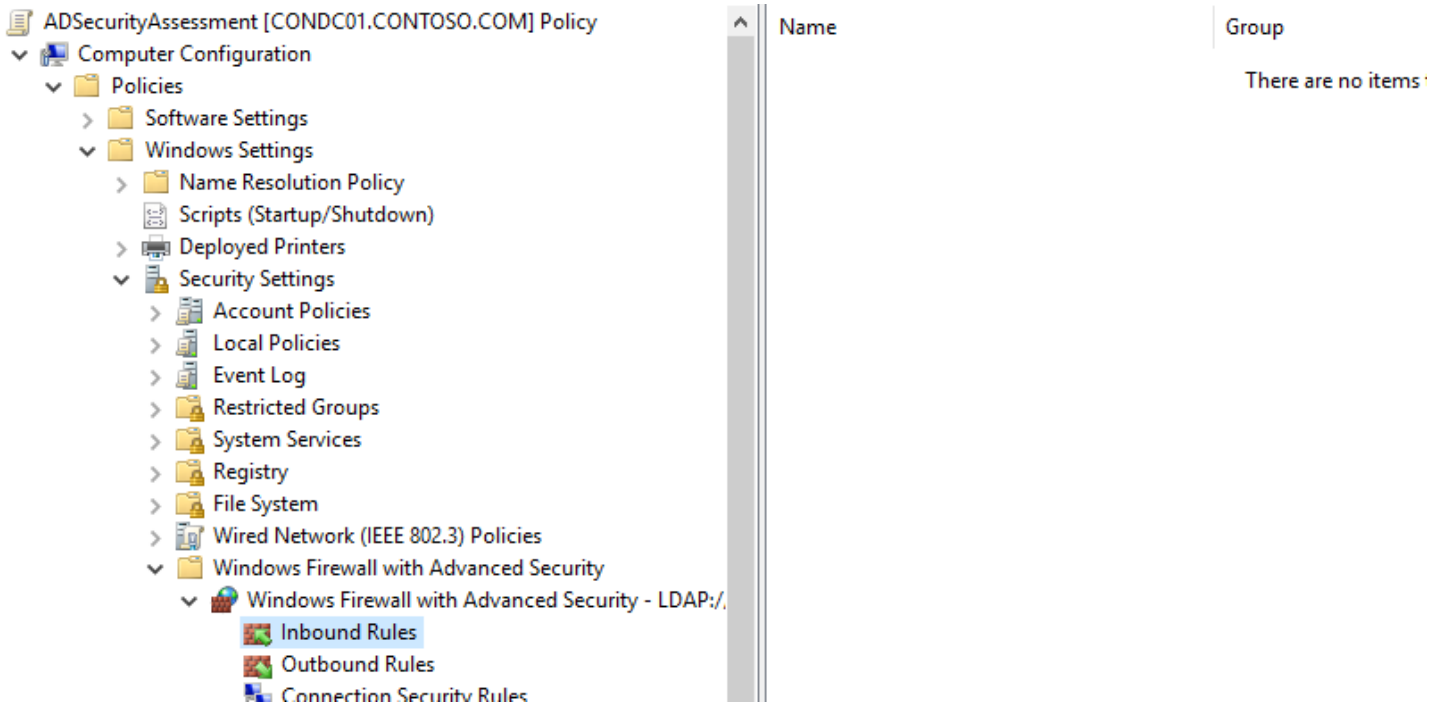
1. Create a new GPO. Make sure the GPO applies to the SharePoint server's organizational unit. Give the new group policy a name based on your group policy naming convention or something that identifies its purpose similar to "SP Assessment"



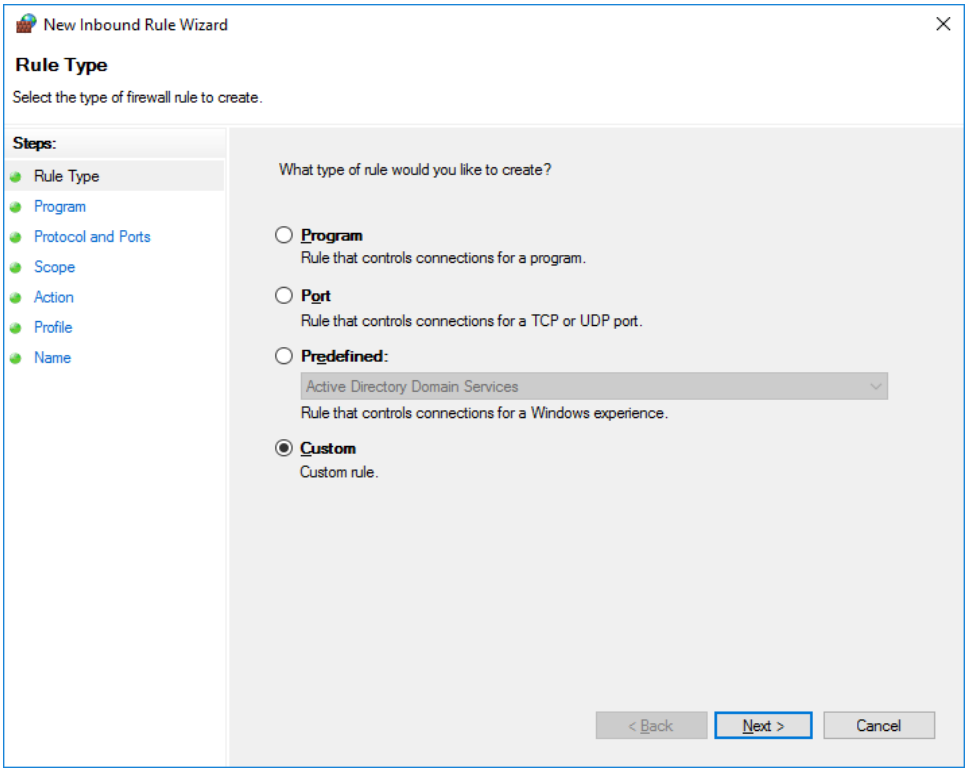


Management (WinRM)\WinRM Service). Enable "**Allow remote server management through WinRM**" or "**Allow automatic configuration of listeners**" depending on your OS.

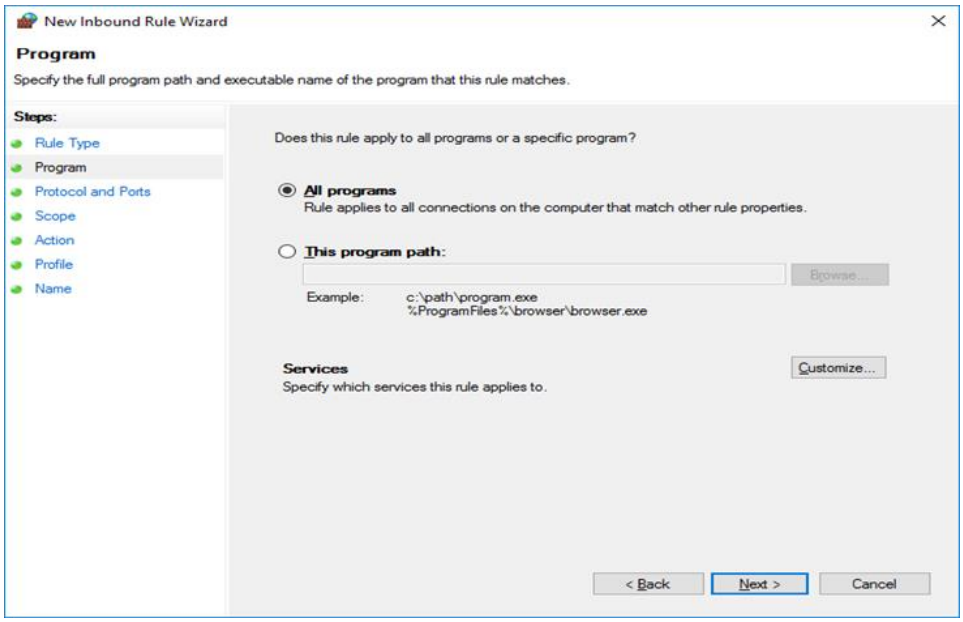
3. Create an advanced Inbound Firewall Rule to allow all network traffic from the tools machine to the SharePoint servers. This can be the applied to the same GPO that was used in step 1 above. (Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security –LDAP:/xxx\Inbound Rules)



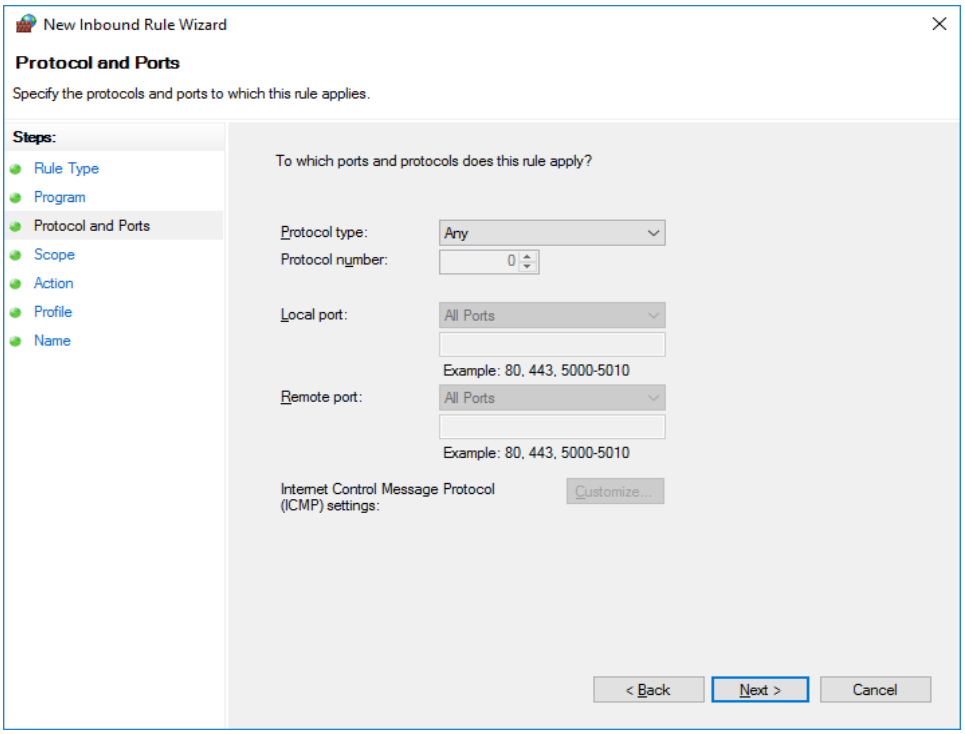
4. To create the new rule, Right Click on “Inbound Rules” and select “New”
5. Create a custom rule and choose “Next”



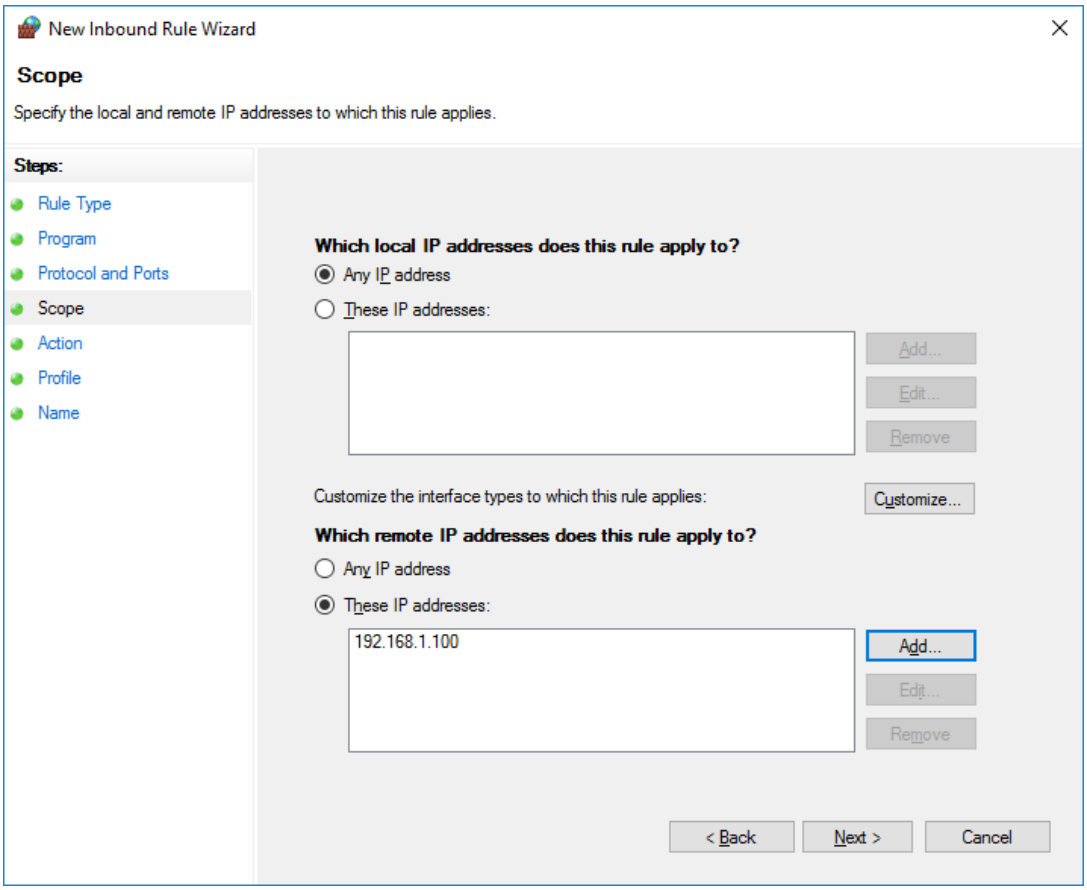
6. Allow “All programs” from the tools machine and click “Next”.



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: SPAssessmentToolsMachine)

Remote PowerShell and CredSSP Configuration

On the Data Collection Machine (SharePoint Server), launch PowerShell Prompt with the option "Run as Administrator". And run the following commands (see important note below before running the below commands)

winrm quickconfig

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

Enable-WSManCredSSP -Role server

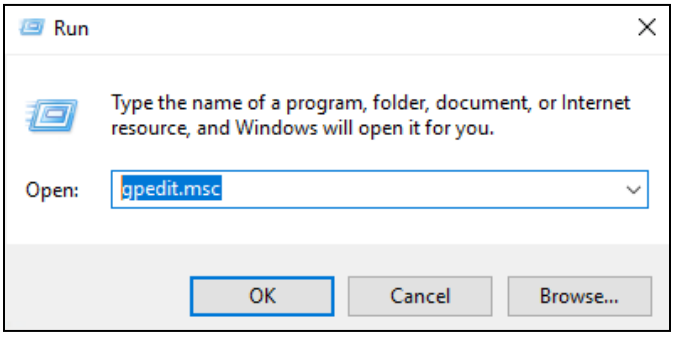
Note :

¨ The **"SharePointServer FQDN"** in the above command is the **"Target Server"**. <u>You must use the FQDN for the SharePoint server and not just the host name.</u>

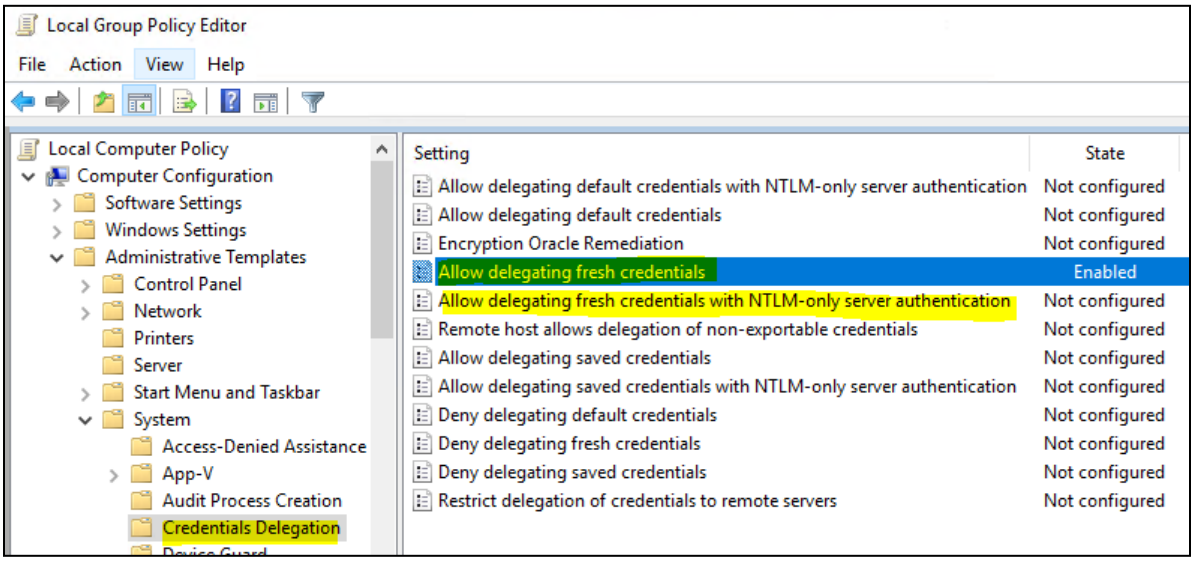
¨ The WinRM service needs to be running for this command to succeed.

Edit local group policies

1. Run **gpedit.msc**.



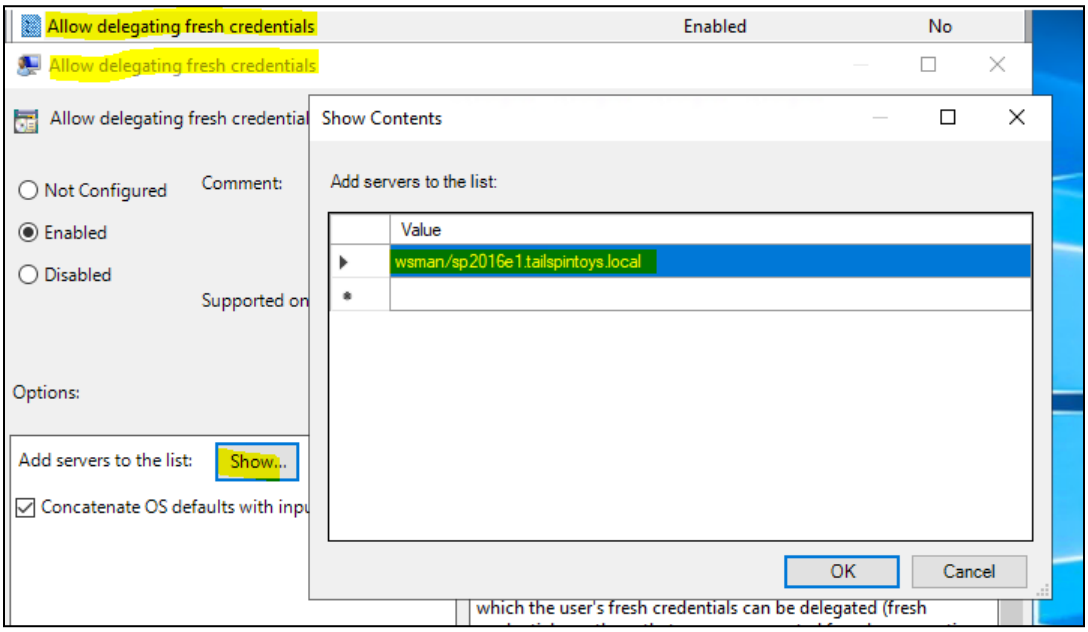
2. Expand [Computer Configuration]-[Administrative Templates]-[System]-[Credential Delegation] on Local Group Policy Editor.



3. Edit the following settings and check/add "**wsman/< *SharePointServer* FQDN>**".

[Allow delegating fresh credentials]

[Allow delegating fresh credentials with NTLM-only server authentication]



4. Run **gpupdate /force.**

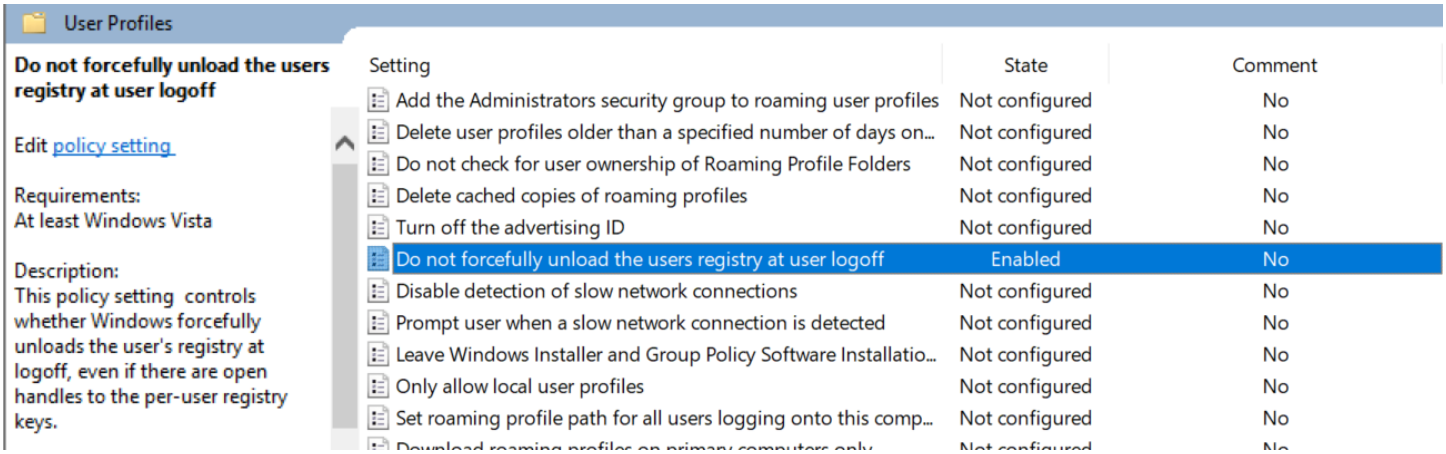
After you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, and configured PowerShell Remoting on the target machines, continue with the next section to set up the assessment.

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'



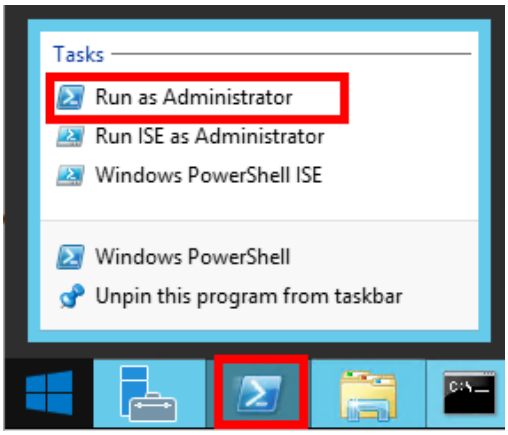
After you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, and configured Security Updates Prerequisites on the Data Collection machine and target machines, continue with the next section to set up the assessment.

Setting up the SharePoint Assessment

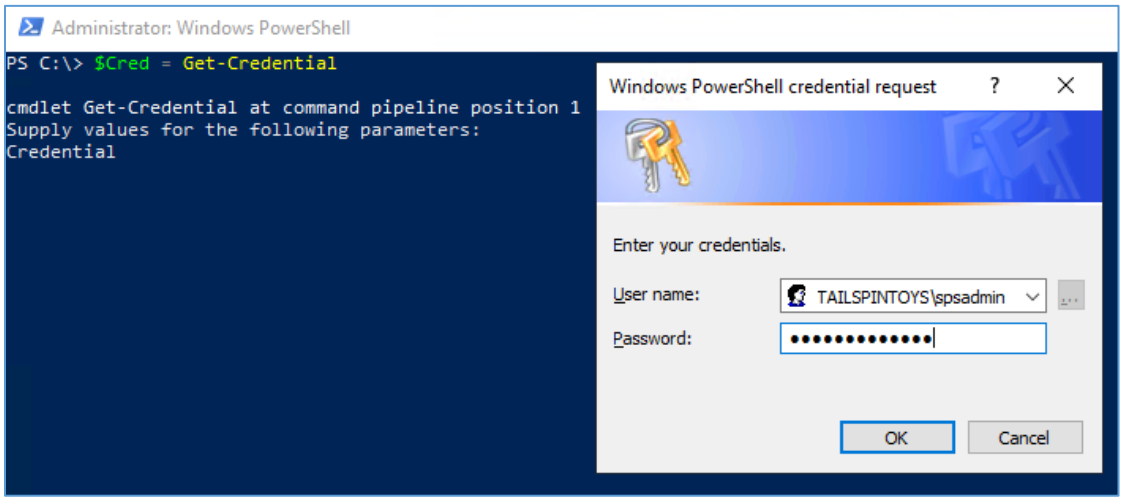
When you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, you are ready to setup the SharePoint Assessment.

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator



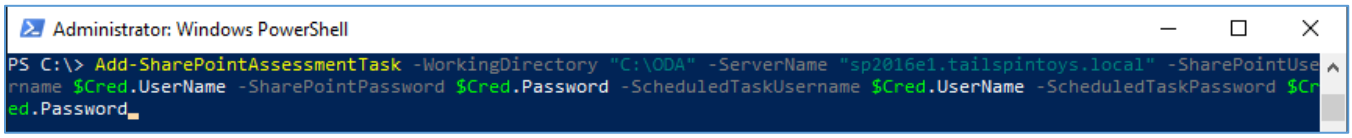
2. Run **$Cred = Get-Credential**



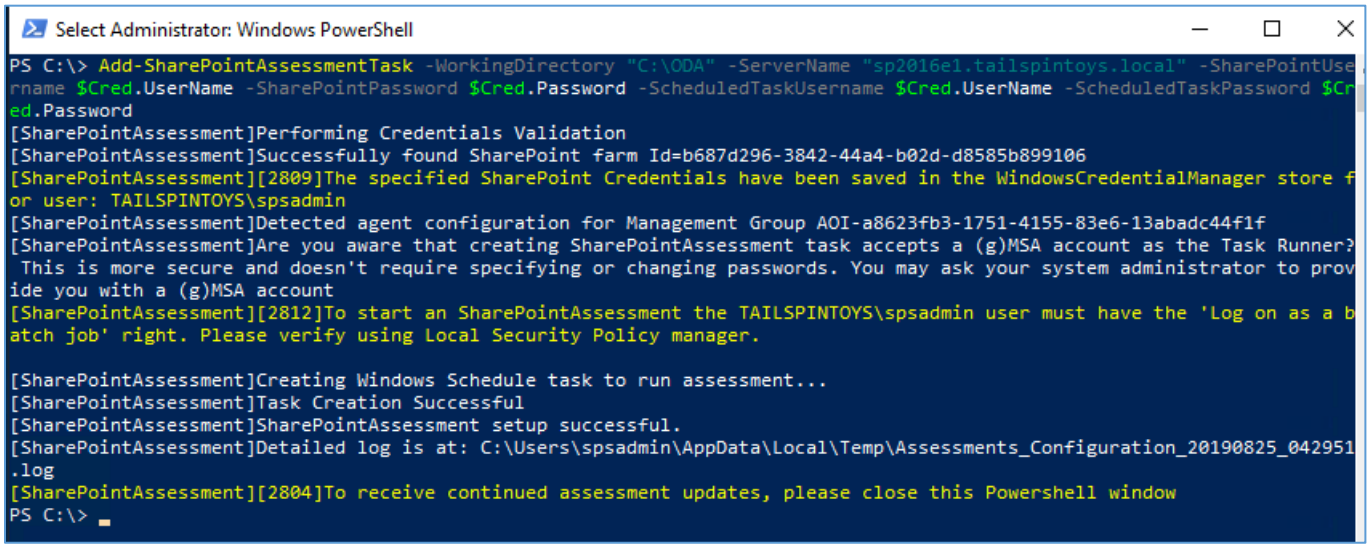
3. Provide the required user account credentials. These credentials are used to run the SharePoint Assessment.
   NOTE: This domain account must have all the following rights:
   - Farm Administrator.
   - Local Admin rights on All SharePoint & SQL Servers associated with the SharePoint farm being assessed.
   - Sysadmin rights on all Instances housing SharePoint databases.
   - Unrestricted network access to every SharePoint server in the farm.

     - **Important:** Ensure that when setting up the assessment, the account that will be used to run the scheduled task is the account that is used to log in and setup the assessment. This ensures the account has correct access to the credentials in Windows Credential Manager

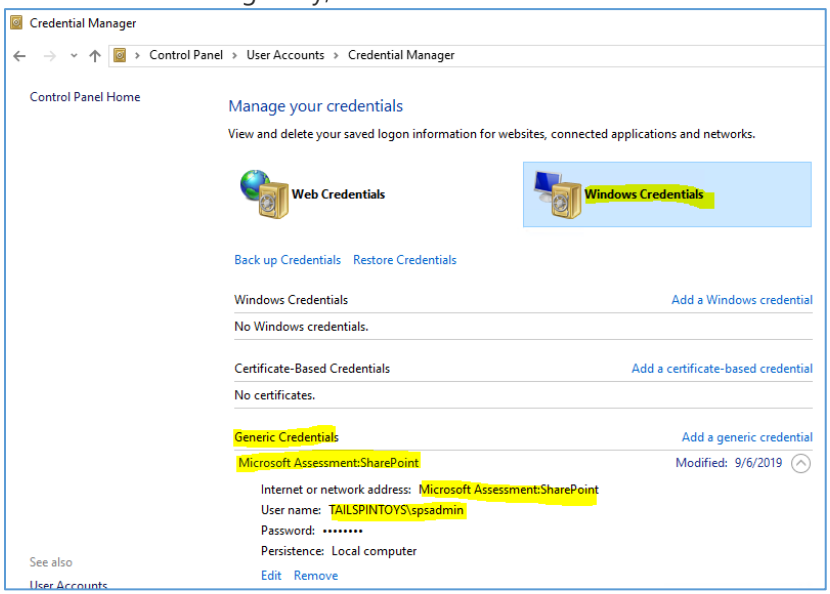
4. Run the **Add-SharePointAssessmentTask -WorkingDirectory <Directory> -ServerName <TargetServer> -SharePointUsername $Cred.UserName -SharePointPassword $Cred.Password -ScheduledTaskUsername $Cred.UserName -ScheduledTaskPassword $Cred.Password** command where <*Directory*> is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment. And the <*TargetServer*> is the name of the target server.



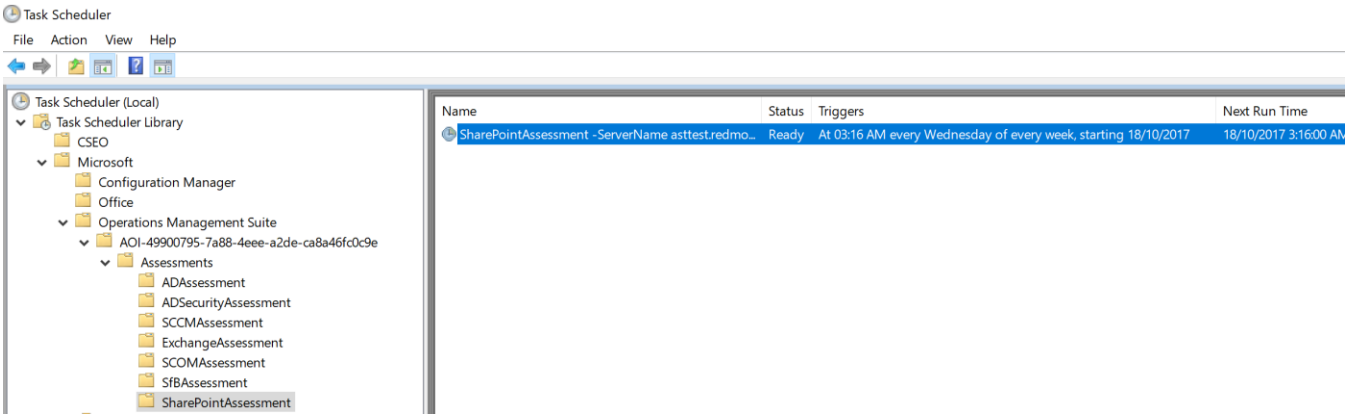
5. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.



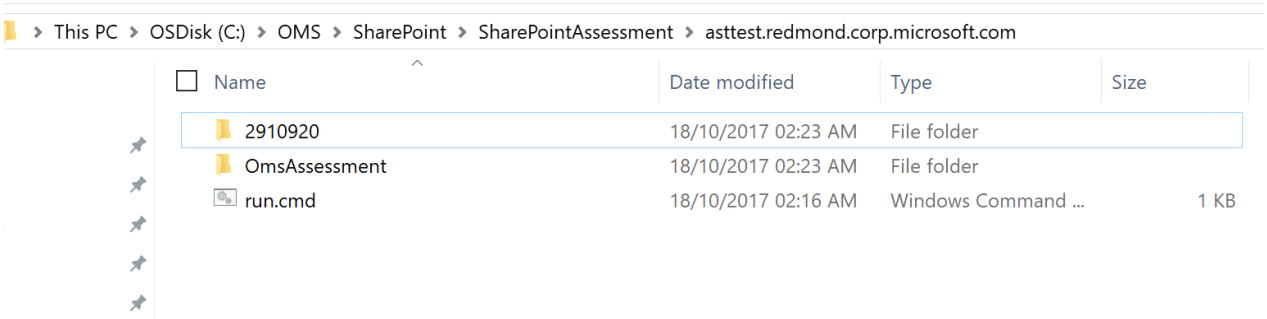
6. Close the Windows PowerShell console.
7. Confirm the following entry, "Microsoft Assessment:SharePoint" on Windows Credential Manager.



8. Data collection is triggered by the **scheduled task** named **SharePointAssessment -ServerName <Server Name>** 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.

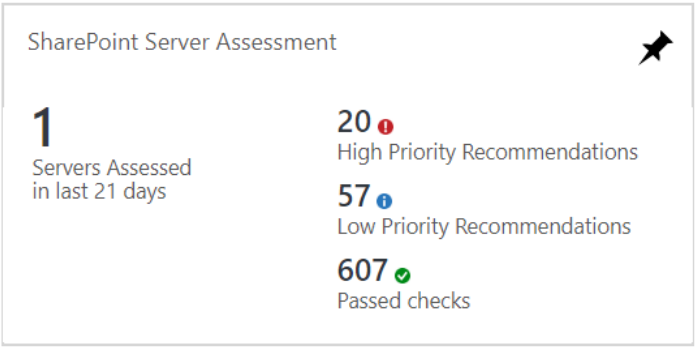


9. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:

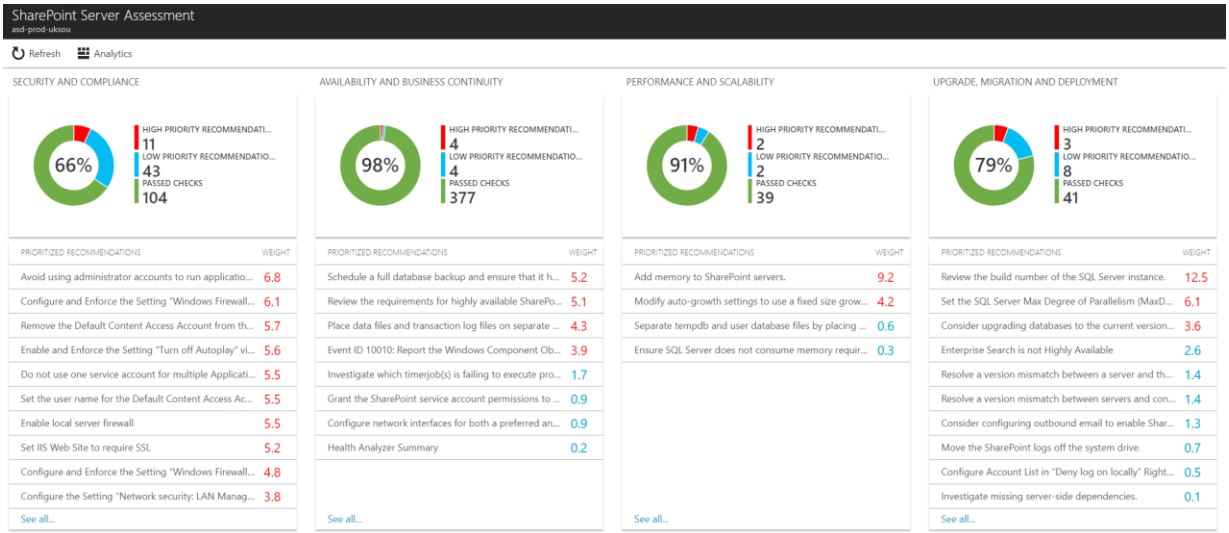


10. After data collection and analysis is completed on the tools machine, it will be submitted to your log analytics workspace depending on the scenario you have chosen:
    - **Directly** if the Data Collection Machine is connected to the Internet and configured to submit directly. **Through the OMS Gateway Server** if this option is configured, then the data will be submitted to your log analytics workspace.
11. Data Collection takes approximately 30 minute to 60 minutes.

12. Once Data Collection has been completed it will then be automatically uploaded to your log analytics workspace. Your assessment results will be available to view on your log analytics dashboard. Click the **SharePoint Server Assessment** tile to review:



13. You will then be presented with findings grouped by the focus area.



Data Collection Methods

The **SharePoint 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.

Data collection uses workflows and collectors. The collectors are:

1. Registry Collectors
2. Event Log Collector
3. Windows PowerShell
4. File Data Collector
5. SQL Data Collector
6. Windows Management Instrumentation (WMI)

Registry Collectors
Registry keys and values are read from the data collection machine and all servers. They include items such as:

- Service information from HKLM\SYSTEM\CurrentControlSet\Services.
- This allow to analyze the status of Operations Manager services

Event Log Collector
Collects event logs from the servers. We collect the last 5 days of Information, Warnings and Errors from the SharePoint Server & Associated SQL Servers, Application and System event logs.

Windows PowerShell
Collects various information, such as:

- SharePoint Farm information
- SharePoint Content Database Information

File Data Collector
Enumerates files in a folder on a remote machine, and optionally retrieves those files.

SQL Data Collector
SQL queries are used to collect information regarding SharePoint Farm Configuration including SQL Server Setup.

Windows Management Instrumentation (WMI)
WMI is used to collect various information such as:

- WIN32_Volume
  Collects information on Volume Settings for each server in the environment. The information is used for instance to determine the system volume and drive letter which allows client to collect information on 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. We use the information to determine the amount of free space on the disk where the database or log files are located.