## 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 <a href="https://go.microsoft.com/fwlink/?linkid=830157">https://go.microsoft.com/fwlink/?linkid=830157</a>.

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  $\rightarrow$  Collects data from all SharePoint servers in the environment  $\rightarrow$  Forward collected data to the OMS Gateway  $\rightarrow$  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  $\rightarrow$  Collects data from all SharePoint servers in the environment  $\rightarrow$  Submit data to the log analytics workspace.

# Table of Contents

S	ystem Requirements and Configuration at Glance	3
	Supported Versions	3
	Common to Both Scenarios	3
	Data Collection Machine	3
	OMS Gateway (required in the OMS Gateway and data collection machine scenario)	3
	PowerShell Remoting	4
	Remote PowerShell and CredSSP Configuration	9
	User Profile Service	11
S	etting up the SharePoint Assessment	12
	Data Collection Methods	16

# 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: <u>Download .NET Framework 4.8 | Free official downloads (microsoft.com)</u>
- 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 <a href="https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/">https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/</a>.

## 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"

	Group Policy Management			- 🗆 X	
Recycle Bin	File Action View Windo	w Help		- 6 ×	
	💠 🌩 🚾 🙆 🖬 🚥				
	Group Policy Management	Group Policy Ma	anagement		
	✓ M Poresc concost.com	Contents			
	✓ jia contoso.com	Name	^		
	Default Domain	Policy A Forest: contoso.	com		
	> 😭 Admins				
	> 🗾 Domain Con	Create a GPO in this domain, and I	ink it here		
	> 🔟 DomainUser	Link an Existing GPO	JULK IK THEI CHI		
	> Group Policy > How Service Structures	Block Inheritance			
	> 🛅 Starter GPOs	Group Policy Update			
	> 🏥 Sites	Group Policy Modeling Wizard			
	Group Policy Model	New Organizational Unit			
	and strop i only instant				
		New Window from Here			
		Delete			
		Refresh			
		Properties			
		Help			
	Create a GPO in this domain and lii	nk it to this container			
Mi seken M	Management Editor /iew Help				- 0
ting with a star and					
r 🕈 🛛 🔟					
	Windows Calendar	^	📫 WinRM Service	2	
	Windows Color System		Allow remote server management	Setting	State
		ience Improvement Program	through WinRM		
>	Windows Defender			Allow remote server management through Win Allow Basic authentication	Not configured
>	Windows Error Reporting		Edit policy setting	Allow CredSSP authentication	Not configured
>	Windows Hello for Busine Windows Ink Workspace	22	Requirements:	E Allow unencrypted traffic	Not configured
	Windows Ink Workspace		At least Windows Vista	Specify channel binding token hardening level	Not configured
	Windows Logon Options			E Disallow WinRM from storing RunAs credential	
	Windows Mail		Description:	E Disallow Kerberos authentication	Not configured
	Windows Media Digital Ri	ahts Management	This policy setting allows you to manage whether the Windows	Disallow Negotiate authentication	Not configured
	- Minderis Media Digitaria	2	Permete Management (MinPM)	Construction regulate authentication	Not comigured

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)

ADSecurityAssessment [CONDC01.CONTOSO.COM] Policy	^	Name
🗸 👰 Computer Configuration		
🗸 🧮 Policies		
> 🧮 Software Settings		
🗸 🚞 Windows Settings		
> 📔 Name Resolution Policy		
🖹 Scripts (Startup/Shutdown)		
> 👼 Deployed Printers		
🗸 🚋 Security Settings		
> 📑 Account Policies		
> 🝶 Local Policies		
> 🝶 Event Log		
> 📴 Restricted Groups		
> 📴 System Services		
> 📴 Registry		
> 📴 File System		
> 🧾 Wired Network (IEEE 802.3) Policies		
Windows Firewall with Advanced Security		
✓		
🗱 Inbound Rules		
🌠 Outbound Rules		
🏪 Connection Security Rules		1

Group

There are no items

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

Piew Inbound Rule Wizard									
Rule Type									
Select the type of firewall rule to c	reate.								
Steps:									
Rule Type	What type of rule would you like to create?								
Program									
Protocol and Ports	O Program								
Scope	Rule that controls connections for a program.								
Action	⊖ P <u>o</u> rt								
Profile	Rule that controls connections for a TCP or UDP port.								
Name	O Predefined:								
	Active Directory Domain Services $\qquad \qquad \lor$								
	Rule that controls connections for a Windows experience.								
	<u>C</u> ustom								
	Custom rule.								
	< Back Next > Cancel								

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

Prew Inbound Rule Wiza	rd	×
Program		
Specify the full program path an	d executable name of the program that this rule matches.	
Steps:		
Rule Type	Does this rule apply to all programs or a specific program?	
Program		
Protocol and Ports	All programs	
Scope	Rule applies to all connections on the computer that match other rule properties.	
Action	○ This program path:	
Profile	O This program pain.	
Name	Example: c:\path\program.exe %ProgramFiles%\browser\browser.exe	
	Services Customize	
	opcony minuti ad vices una rate applica to.	
	< <u>B</u> ack <u>N</u> ext > Cance	6

7. Allow all protocols and ports, then click "Next".

💣 New Inbound Rule Wiza	Pew Inbound Rule Wizard X						
Protocol and Ports							
Specify the protocols and ports t	to which this rule applies.						
Steps:							
Rule Type	To which ports and pr	rotocols does this rule apply?					
Program							
Protocol and Ports	Protocol type:	Any 🗸					
Scope	Protocol n <u>u</u> mber:	0 🚖					
Action							
Profile	Local port:	All Ports $\lor$					
Name							
		Example: 80, 443, 5000-5010					
	<u>R</u> emote port:	All Ports 🗸					
		Example: 80, 443, 5000-5010					
	Internet Control Mess (ICMP) settings:	sage Protocol <u>C</u> ustomize					
		< Back Next > Ca	ncel				

8. Specify the IP address of the tools machine and click "Next".

	Prew Inbound Rule Wizard						
5	Соре						
S	pecify the local and remote IP ad	ddresses to which this rule applies.					
s	teps:						
۲	Rule Type						
۲	Program	Which local IP addresses does this rule apply to?					
۲	Protocol and Ports	Any IP address					
۲	Scope	○ <u>These IP addresses</u> :					
۲	Action	<u>A</u> dd					
۲	Profile	Edit					
۲	Name						
		<u>R</u> emove					
		Customize the interface types to which this rule applies: Customize					
		Which remote IP addresses does this rule apply to?					
		○ An <u>v</u> IP address					
		Indexe IP addresses:					
		192.168.1.100 A <u>d</u> d					
		Edit					
		Remove					
		< Back Next > Car	cel				
		Car <u>N</u> ext > Car					

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</u> <u>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.

💷 Run	×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	gpedit.msc 🗸
	OK Cancel Browse

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]

Allow delegating fresh	n credentials				Enabled		No	
💭 Allow delegating fresh	h credentials							×
Allow delegating fresh	h credential	Show Conten	ts			_		×
O Not Configured Co	omment:	Add servers t	othe list:					
Enabled		Valu	ie					
O Disabled		► wsm	an/sp2016e1.tailsp	pintoys.local				
Su	pported on	*						
Options:								
Add servers to the list:	Show							
Concatenate OS defaul	lts with inpu							
					-			
					L	OK	Can	celi
			which the	user's fresh cre	dentials can be	delegated (fre	sh	

#### 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'

🧾 User Profiles				
Do not forcefully unload the users		Setting	State	Comment
registry at user logoff		E Add the Administrators security group to roaming user profiles	Not configured	No
Edit policy setting	~	🗈 Delete user profiles older than a specified number of days on	Not configured	No
Eur policy setting		E Do not check for user ownership of Roaming Profile Folders	Not configured	No
Requirements:		E Delete cached copies of roaming profiles	Not configured	No
At least Windows Vista		Turn off the advertising ID	Not configured	No
Description: This policy setting controls whether Windows forcefully		Do not forcefully unload the users registry at user logoff	Enabled	No
		E Disable detection of slow network connections	Not configured	No
		E Prompt user when a slow network connection is detected	Not configured	No
unloads the user's registry at logoff, even if there are open		E Leave Windows Installer and Group Policy Software Installatio	Not configured	No
handles to the per-user registry		E Only allow local user profiles	Not configured	No
keys.		E Set roaming profile path for all users logging onto this comp	Not configured	No
1		Download roaming profiles on primary computers only	Not configured	No

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** 

Administrator: Windows PowerShell				
PS C:\> \$Cred = Get-Credential cmdlet Get-Credential at command pipeline position 1	Windows PowerShell credential request $~~?~~ imes~$			
Supply values for the following parameters: Credential				
	Enter your credentials.			
	User name: 🕵 TAILSPINTOYS\spsadmin 🗸 🔐			
	Password:			
	OK Cancel			

- 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.

Administrator: Windows PowerShell	_	×
PS C:\> Add-SharePointAssessmentTask -WorkingDirectory "C:\ODA" -ServerName "sp2016e1.tailspintoys.local rname \$Cred.UserName -SharePointPassword \$Cred.Password -ScheduledTaskUsername \$Cred.UserName -Scheduled ed.Password_		

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.

Credential Manager		
← → × ↑ 🙆 > Control Pane	→ User Accounts → Credential Manager	
Control Panel Home		
Control Panel Home	Manage your credentials	
	View and delete your saved logon information for we	bsites, connected applications and networks.
	Web Credentials	Windows Credentials
	Back up Credentials Restore Credentials	
	Windows Credentials	Add a Windows credential
	No Windows credentials.	
	Certificate-Based Credentials	Add a certificate-based credential
	No certificates.	
	Generic Credentials	Add a generic credential
	Microsoft Assessment:SharePoint	Modified: 9/6/2019
	Internet or network address: Microsoft Assessn	nent:SharePoint
	User name: TAILSPINTOYS\spsadmin	
	Password: ••••••	
See also	Persistence: Local computer	
User Accounts	Edit Remove	

 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.

Task Scheduler				
File Action View Help				
🗢 🔿 🙍 📰 🛛 🖬				
(D) Task Scheduler (Local)	Name	Status	Triggers	Next Run Time
🗸 🔀 Task Scheduler Library				
CSEO CSEO	SharePointAssessment -ServerName asttest.redm	o Ready	At 03:16 AM every Wednesday of every week, starting 18/10/2017	18/10/2017 3:16:00 A
✓ I Microsoft				
Configuration Manager				
Office				
🗸 🧮 Operations Management Suite				
✓				
✓				
ADAssessment				
ADSecurityAssessment				
SCCMAssessment				
ExchangeAssessment				
SCOMAssessment				
SfBAssessment				
SharePointAssessment				

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

📕 🕨 This PC 🕨 C	OSDisk (C:) > OMS > SharePoint > SharePointA	Assessment > asttest.redmond.co	rp.microsoft.com	
	Name ^	Date modified	Туре	Size
*	2910920	18/10/2017 02:23 AM	File folder	
	OmsAssessment	18/10/2017 02:23 AM	File folder	
*	👼 run.cmd	18/10/2017 02:16 AM	Windows Command	1 KB
*				
*				

- 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.
- 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.

D Refresh ₩ Analytics								
ECURITY AND COMPLIANCE	AVAILABILITY AND BUSINESS CONTINUITY	PERFORMANCE AND SCALABILITY	UPGRADE, MIGRATION AND DEPLOYMENT					
66% HIGH PRIORITY RECOMMENDATI 11 LOW PRIORITY RECOMMENDATIO 43 PASSED CHECKS 104	98% HIGH PRIORITY RECOMMENDATL UW PRIORITY RECOMMENDATIO. PASSED CHECKS 377	91% High PRIORITY RECOMMENDATI 2 ICWN PRORITY RECOMMENDATIO 2 RASEED CHECKS 39	HIGH PRIORITY RECOMMENDATIO 3 100 PRIORITY RECOMMENDATIO 8 PASSED CHECKS 41					
PRIORITIZED RECOMMENDATIONS WEIGHT	PRIORITIZED RECOMMENDATIONS WEIGHT	PRIORITIZED RECOMMENDATIONS WEIGHT	PRIORITIZED RECOMMENDATIONS WEIGHT					
Avoid using administrator accounts to run applicatio 6.8	Schedule a full database backup and ensure that it h 5.2	Add memory to SharePoint servers. 9.2	Review the build number of the SQL Server instance. 12.5					
Configure and Enforce the Setting "Windows Firewall 6.1	Review the requirements for highly available SharePo 5.1	Modify auto-growth settings to use a fixed size grow 4.2	Set the SQL Server Max Degree of Parallelism (MaxD 6.1					
Remove the Default Content Access Account from th 5.7	Place data files and transaction log files on separate 4.3	Separate tempdb and user database files by placing 0.6	Consider upgrading databases to the current version 3.6					
Enable and Enforce the Setting "Turn off Autoplay" vi 5.6	Event ID 10010: Report the Windows Component Ob 3.9	Ensure SQL Server does not consume memory requir 0.3	Enterprise Search is not Highly Available 2.6					
Do not use one service account for multiple Applicati 5.5	Investigate which timerjob(s) is failing to execute pro 1.7		Resolve a version mismatch between a server and th 1.4					
Set the user name for the Default Content Access Ac 5.5	Grant the SharePoint service account permissions to 0.9		Resolve a version mismatch between servers and con 1.4					
Enable local server firewall 5.5	Configure network interfaces for both a preferred an 0.9		Consider configuring outbound email to enable Shar 1.3					
Set IIS Web Site to require SSL 5.2	Health Analyzer Summary 0.2		Move the SharePoint logs off the system drive. 0.7					
Configure and Enforce the Setting "Windows Firewall 4,8			Configure Account List in "Deny log on locally" Right 0.5					
Configure the Setting "Network security: LAN Manag 3.8			Investigate missing server-side dependencies. 0.1					
See all	See all	See all	See all					

## 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.