ScienceLogic

Microsoft Automation PowerPacks

Microsoft Hyper-V Automation PowerPack version 101

Windows PowerShell Automations PowerPack version 104

Windows PowerShell User-Initiated Automation PowerPack version 100

Table of Contents

Introduction	5
Microsoft Automation PowerPacks	6
Windows PowerShell Automations	7
What is the Windows PowerShell AutomationsPowerPack?	8
Installing the Windows PowerShell AutomationsPowerPack	8
Standard Automation Policies	9
Authentication for Windows Devices with the Windows PowerShell Automations PowerPack	12
Creating a Credential for Windows PowerShell	13
Creating Custom Windows PowerShell Automation Policies	13
Creating a Custom Action Policy	13
Customizing Automation Actions	15
Creating a New Windows PowerShell Automation Action	17
Microsoft Hyper-V Automation	19
What is the Microsoft Hyper-V Automation PowerPack?	20
Prerequisites	20
Installing the Microsoft Hyper-V Automation PowerPack	20
Standard Automation Policies	21
Credential for Hyper-V Automation	24
Creating and Customizing Hyper-V Automation Policies	24
Creating a Custom Action Policy for Hyper-V	25
Customizing Automation Actions	25
Creating a New Microsoft Hyper-V Automation Action	26
Configuring Device Credentials	27
Creating a Credential	28
Creating and Customizing Automation Policies	30
Prerequisites	31
Creating an Automation Policy	31
Customizing an Automation Policy	32
Removing an Automation Policy from a PowerPack	34
Windows PowerShell User-Initiated Automations	35
What is the Windows PowerShell User-Initiated Automation PowerPack?	36

Installing the Windows PowerShell User-Initiated Automation PowerPack	36
Standard Automation Policies	37
Running a User Initiated Automation Policy	38
Viewing Automation Actions for an Event	39
Run Book Variables	41
Run Book Variables	42
Configuring Windows Servers for Monitoring with PowerShell	. 46
Prerequisites	47
Configuring PowerShell	47
Step 1: Configuring the User Account for the ScienceLogic Platform	48
Option 1: Creating an Active Directory Account with Administrator Access	48
Option 2: Creating a Local User Account with Administrator Access	. 48
Option 3: Creating a Non-Administrator User Account	49
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	[.] 51
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	. 51
Creating a User Group and Adding a User in Active Directory	51
Setting the Session Configuration Parameters and Group Permissions	52
Creating a PowerShell Credential	52
Optional: Configuring the User Account for Access to Windows Failover Cluster	52
Step 2: Configuring a Server Authentication Certificate	52
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	53
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	56
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	56
Step 3: Configuring Windows Remote Management	56
Option 1: Using a Script to Configure Windows Remote Management	56
Option 2: Manually Configuring Windows Remote Management	62
Option 3: Using a Group Policy to Configure Windows Remote Management	66
Configuring an HTTPS Listener with GPO Configuration	. 84
Using Forward and Reverse DNS for Windows Remote Management	84
Step 4: (Optional) Configuring a Windows Management Proxy	85
Step 5: (Optional) Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	87

Chapter

Introduction

Overview

This manual describes how to use the automation policies, automation actions, and custom action types found in Microsoft Automation Power Packs.

NOTE: This PowerPack is available with a ScienceLogic SL1 Standard solution. Contact your ScienceLogic Customer Success Manager or Customer Support to learn more.

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

Microsoft Automation PowerPack	;	6
--------------------------------	---	---

Microsoft Automation PowerPacks

This manual describes content from the following PowerPack versions:

- Microsoft Hyper-V Automation, version 100
- Windows PowerShell Automations, version 104

Chapter

2

Windows PowerShell Automations

Overview

This chapter describes how to use the automation policies, automation actions, and custom action types found in the Windows PowerShell Automations PowerPack.

See the Microsoft Hyper-V Automation section for information about that PowerPack.

This chapter covers the following topics:

What is the Windows PowerShell AutomationsPowerPack?	8
Installing the Windows PowerShell AutomationsPowerPack	8
Standard Automation Policies	9
Authentication for Windows Devices with the Windows PowerShell Automations PowerPack	12
Creating a Credential for Windows PowerShell	13
Creating Custom Windows PowerShell Automation Policies	13
Creating a Custom Action Policy	13

What is the Windows PowerShell AutomationsPowerPack?

The Windows PowerShell Automations PowerPack includes:

- A custom action type for running PowerShell commands on remote devices
- A dynamic device group with rules that include only Windows devices
- A set of automation actions that run diagnostic commands on Windows systems via PowerShell
- A set of automation policies that tie events from monitoring PowerPacks to the automation actions

The Windows PowerShell Automations actions are executed on the SL1 All-In-One Appliance or Data Collector.

In addition to using the standard content, you can use the content in the Windows PowerShell Automations PowerPack to:

- Create your own automation policies that include the pre-defined actions that run different sets of diagnostic commands.
- Use the supplied "Execute PowerShell Request" custom action type to configure your own automation action by supplying a set of commands to be executed via PowerShell.

Installing the Windows PowerShell AutomationsPowerPack

Before completing the steps in this manual, you must import and install the latest version of the Windows PowerShell AutomationsPowerPack.

IMPORTANT: You must install the Datacenter Automation Utilities PowerPack before using the Windows PowerShell Automations PowerPack.

NOTE: The Windows PowerShell AutomationsPowerPack requires SL1 version 8.10.0 or later. For details on upgrading SL1, see the appropriate SL1<u>Release Notes</u>.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the *System Administration* manual.)

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

- Search for and download the PowerPack from the PowerPacks page (Product Downloads > PowerPacks & SyncPacks) at the <u>ScienceLogic Support Site</u>.
- 2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
- 3. Click the [Actions] button and choose Import PowerPack. The Import PowerPack dialog box appears.
- 4. Click [Browse] and navigate to the PowerPack file from step 1.
- 5. Select the PowerPack file and click [Import]. The PowerPack Installer modal displays a list of the PowerPack contents.
- 6. Click [Install]. The PowerPack is added to the PowerPacks page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Standard Automation Policies

The Windows PowerShell Automations PowerPack includes five standard automation policies, shown in the following figure. Each policy triggers a single automation action that collects diagnostic data within a PowerShell session, and an action that formats the output as HTML. All of the automation actions use the same custom action type, "Execute PowerShell Request", which is supplied in the PowerPack.

Manage PowerPack™	Emb	edded Run Boo	k Policies [5]											
Properties		Automat	on Policy Name *		ID	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited	
Build / Export					-	All 🔻	All		,				All	•
Features / Benefits	1.	A Windows Po	verShell: Run CP	U & Me 1	17	Enabled	System		All	1	1	em7admin	2019-11-19 10:28:41	6
Technical Notes	2.	A Windows Po	verShell: Run CP	U Diagr 1	15	Enabled	System		All	2	1	em7admin	2019-11-19 10:28:40	ā
Documentation	3.	A Windows Po	verShell: Run Dis	k I/O Di 1	18	Enabled	System		All	3	1	em7admin	2019-11-19 10:28:41	6
Contents	4.	A Windows Po	verShell: Run Me	mory D 1	16	Enabled	System		All	3	1	em7admin	2019-11-19 10:28:41	6
Dynamic Applications	5.	A Windows Po	verShell: Run Pri	nt Job E 1	19	Enabled	System		All	1	1	em7admin	2019-11-19 10:28:41	9
Event Policies														
Device Categories														
Device Classes														
Device Templates														
Device Groups														
Reports														
Reports Dashboard Widgets														
Reports Dashboard Widgets Dashboards	Aust	ilabla Dup Baak	Delision (0)											
Reports Dashboard Widgets Dashboards Dashboards SL1	Avai	ilable Run Book	Policies [0]											
Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies	Ava	ilable Run Book	Policies [0]		ID	Policy State		Organization	Devices	<u>Events</u>	Actions	Edited By	Last Edited	_
Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies Run Book Actions	Avai	ilable Run Book Automat	Policies [0]		D	Policy State	All	Organization	Devices	Events	Actions	Edited By	Last Edited	Ŧ
Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies Run Book Actions Run Book Action Types	Ava	ilable Run Book	Policies [0]		D	Policy State	All	Organization	<u>Devices</u>	Events	Actions	Edited By	Last Edited All	·
Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies Run Book Actions Run Book Action Types Ticket Templates	Ava	ilable Run Book Automat	Policies [0] on Policy Name •		D	Policy State All V	All	Organization	<u>Devices</u>	<u>Events</u>	Actions	Edited By	Last Edited All	·
Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies Run Book Actions Run Book Action Ticket Templates Credentials	Ava	ilable Run Book	Policies [0] on Policy Name •		D	Policy State All ▼	All	Organization No results to display	Devices	<u>Events</u>	Actions	Edited By	Last Edited All	·
Reports Dashboard Widgets Dashboards Dashboards SL1 Run Book Policies Run Book Actions Run Book Action Types Ticket Templates Credential Credential Tests	Ava	ilable Run Book	Policies [0]		D	<u>Policy State</u> All ▼	All	Organization No results to display	Devices	Events	Actions	Edited By	Last Edited All	·
Reports Dashboard Widgets Dashboards Dashboards St.1 Run Book Actions Run Book Action Types Ticket Templates Credentials Credentials Credentials Transformations	Ava	ilable Run Book	Policies [0] an Policy Name *		D	Policy State All V	All	<u>Organization</u> No results to display	Devices	<u>Events</u>	Actions	Edited By	Last Edited All	·
Reports Dashboard Widgets Dashboard SL1 Run Book Actions Run Book Actions Run Book Action Types Ticket Templates Credentials Credential Tests Prroxy XSL Transformations UI Themes	Ava	ilable Run Book	Policies [0] an Policy Name *		D	<u>Policy State</u> All ▼	All	Organization No results to display	Devices	Events	Actions	Edited By	Last Edited All	•
Reports Dashboard Widgets Dashboards Dashboards Status Run Book Actions Run Book Actions Run Book Action Ticket Templates Credentials Credentials Credentials Credentials Transformations UI Themes II Services	Ava	ilable Run Book	Policies [0] on Policy Name *		<u>ID</u>	Policy State All ▼	All	Organization No results to display	<u>Devices</u>	Events	Actions	Edited By	Last Edited	•
Reports Dashboard Vidgets Dashboard SL1 Run Book Actions Run Book Actions Run Book Action Ticket Templates Credential Credential Tests Credential Tests Proxy XSL Transformations UI Themes IT Services Log File Monitoring Policies	Ava	ilable Run Book	Policies [0]		ID	Policy State	All	<u>Orpanization</u> No results to display	Devices	Events	Actions	Edded By	LastEdited All	·
Reports Dashboard Widgets Dashboards Dashboards Status Run Book Action Status Run Book Action Types Ticket Templates Credentials Credentia	Ava	ilable Run Book	Policies [0] an Policy Name *		ID	Policy State All ¥	All	Organization No results to display	Devices /	Events	Actions	Edited By	Last Edited	•

All of the standard automation policies are tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the Windows Server PowerPack.

Several of the automation actions use the substitution character feature of the "Execute PowerShell Request" custom action type. If an event variable is included in a command (such as "%Y" for the sub-entity name), the custom action type automatically replaces that variable with the value from the triggering event.

The following table shows the standard automation policies, their aligned events, and the automation action that runs in response to the events.

NOTE: The aligned events are included as part of the *Microsoft Windows Server* PowerPack and are not installed with the SL1 platform. You must install the *Microsoft Windows Server* PowerPack to obtain these events.

Automation Policy Name	Aligned Events	Automation Action
Windows PowerShell: Run CPU & Memory Diagnostic Commands	 Minor: Microsoft: Windows Disk Transfer Time (Physical Disk) exceeded threshold 	Windows CPU and Memory Diagnostic Commands
Windows PowerShell: Run CPU Diagnostic Commands	 Minor: Microsoft: Windows CPU Utilization has exceeded the threshold Minor: Microsoft: Windows Processor Queue Length exceeded the threshold 	Windows CPU Diagnostic Commands
Windows PowerShell: Run Disk I/O Diagnostic Commands	 Minor: Microsoft: Windows % Disk Time (Logical Disk) exceeded threshold Minor: Microsoft: Windows % Disk Time (Physical Disk) exceeded threshold Minor: Microsoft: Windows Current Disk QueueLength (Physical Disk)exceeded threshold 	Windows Disk I/O Diagnostic Commands
Windows PowerShell: Run Disk Usage Diagnostic Commands	 Poller: File system usage exceeded (major) threshold Poller: File system usage exceeded (critical) threshold 	 Automation Utilities: Calculate Memory Size for Each Action Windows Get Largest Event Log Files Windows Get Largest
	NOTE: This automation policy is aligned with the Windows Automation device group.	 Files on Disk Windows Disk I/O Diagnostic Commands Datacenter Automation: Format Output as HTML
Windows PowerShell: Run Memory Diagnostic Commands	 Major: Microsoft: Windows Available Memory below threshold Major: Microsoft: Windows Pages per Second has exceeded threshold 	Run Memory Diagnositc Commands

Automation Policy Name	Aligned Events	Automation Action
	 Minor: Microsoft: Windows Paging File Usage has exceeded threshold 	
Windows PowerShell: Run Print Job Error Diagnostic Commands	 Minor: Microsoft: Windows: PowerShell: Print Job Errors exceeded threshold 	Windows Print Job Error Diagnostic Commands

The following figure shows a memory event with a classification of "Major" appears on the **Events** page. Click the **[Actions]** button (--) for an event, and select *View Automation Actions* to see the automation actions triggered by the events.

≡	Events												Jude.Eva	ins-Mccarthy 🗸	STD Sci	incelogio	
88	1 Critic	al I	19 Major	6 Minor	: No	1 tice He	0 althy	27 Events View All								~ Vi	ew
▲	Q Typ	e to sear	ch events													≡	•
	۵	ORG	ANIZATION	SEV	/ERIT	NAME	MESSA	AGE	AGE	TICKET I	co	EVENT NOT	MASKED EVENTS	ACKNOWLEDGE	CLEAR		C
ė		Win	dows Devic	es 🔴	Major	10.2.24.56	Examp	ple Windows CPU Event	8 days		1	Ð		 ✓ Acknowledge 	X Clear]	
		Win	dows Devic	es 🔴	Major	10.2.24.56	Examp	ple Windows Memory Event	8 days		1	F		 Acknowledge 	🗙 Clear		
		Win	dows Devic	es 🔴	Major	10.2.24.56	Examp	ple Windows Disk IO Event	8 days		1	+		✓ Acknowledge	× Clear		
		Win	dows Devic	es 🔴	Major	10.2.24.56	Examp	ple Windows Disk Performa	8 days		1	+		✓ Acknowledge	× Clear		
		Exar	mple Device	s 🔴	Major	netscaler	Devio	e Failed Availability Check: U	7 days 15 ł		2195	 1	Q Masked	✓ Acknowledge	X Clear		
		Exar	nple Device	s 🔴	Minor	ec2-34-200	Netwo	ork latency exceeded thresh	3 days 15 ł		1044	+		✓ Acknowledge	X Clear		
		Linu	x Devices	•	Major	10.2.24.30	/: File	system usage exceeded maj	2 days 19 H	5	268	+		✓ Acknowledge	× Clear		
		Syst	em	•	Major	ec2-18-217	Linux	File System /dev/loop0 : /sn	2 days 1 hc		491	+		✓ Acknowledge	× Clear		
		Syst	em	•	Major	System	EM7 r	major event: Dynamic applic	19 hours 3		20	+		✓ Acknowledge	× Clear		
		Syst	em	•	Major	cscol26	Swap	memory utilization has exce	14 hours 5	9	157	+		✓ Acknowledge	X Clear		
		Syst	em	•	Major	System	Proces	ss time exceeded: Process D	1 hour 23 r		2	+		✓ Acknowledge	X Clear		
		Syst	em	•	Minor	cscol26	App: 9	91, Snippet: 112 reported a c	30 minutes		1	+		✓ Acknowledge	× Clear		
•••		Syst	em		Minor	System	Proces	ss time exceeded: Process E	29 minutes		1	F		 Acknowledge 	× Clear]	•

The results shown for this event, in the Event Actions Log, include the automation policy that ran (shown at the top of the following figure), along with the automation actions (commands) that ran. Results for each command are also displayed. The following figure shows an example of this HTML output.

Event Actions Log For Event [18263]	Refresh	Guide
2019-12-05 16:29:57		
Automation Policy Windows PowerShell: Run CPU & Memory Diagnostic Commands action Windows CPU and Memory Diagnostic Commands with HTML Output ran Successfully Message CustomAction Type (444) executed without incident Result: <u>Enrichment Command Output</u>		
Command: Get-Process Sort CPU -descending Select -first 20 Format-Table -AutoSize Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName		
967480 91 2405648 204260 217,886.92 876 0 svchost		
614 67 272260 183468 182,272.64 1728 0 MshpEng		
554 62 238672 72732 60,299.03 2216 0 sqlservr		
323 21 10072 22432 29,722.22 1840 0 vmtoolsd		
93 8 4988 9280 22,232.44 4980 0 Connost 683 39 159516 63144 21,815.34 464 0 svchost		
1394 71 26240 41664 20,752.52 1040 0 svchost		
93 8 4988 9284 11,400.88 33/2 0 conhost 93 8 5912 9672 11,078.36 3916 0 conhost		
441 17 16092 19708 10,572.31 928 0 svchost		
286 10 5804 9896 10,396.91 596 0 services		
1385 23 8980 17176 9,967.13 604 0 Isass		
381 23 30040 41552 7,418.63 4360 0 Wm/PrvSE		
451 21 14400 20520 /,004.05 2270 0 Wm3PFV5E 590 18 29704 35092 5,240.50 736 0 sychost		
431 17 1980 4336 3,117.50 384 0 csrss		
514 18 5728 14688 2,909.52 692 0 svchost 93 8 4984 9644 2 736 65 7164 c conbost		
Command: Get-Process Select-Object Name, ID, @{Name='ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descendi Name Id ThreadCount 	ng Select	-first 20
svchost 1116 22		
powershell 5060 18		
powershell 5484 17 sychost 928 16		
svchost 940 16		
Wm2PrvSE 2276 16		
svehost 1632 14		
svchost 692 13		
SpoolsV 15/2 13 Svchost 736 13		
tssdis 3052 13		
Command: Get-Process Sort NS -descending Select -first 20 Format-Table -AutoSize Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName		
967475 90 2405432 204096 217.886.97 876 0 svchost		
627 67 275096 183568 182,273.25 1728 0 MsHpEng		-
1 67 67 7777 7777 60 700 77 716 6 Folgenin		•

To learn more about which commands are executed by default for a given automation action, see Customizing Actions.

TIP: Although you can edit the automation actions described in this section, it is a best practice to use "Save As" to create a new automation action, rather than to customize the standard automation policies.

Authentication for Windows Devices with the Windows PowerShell Automations PowerPack

The "Execute PowerShell Request" custom action type supports hard-coded credentials (wherein you specify the ID of a credential in the automation action), or the custom action type can dynamically determine the credential to use. By default, the automation actions use the dynamic method (by specifying credential ID 0 in the input parameters). The dynamic method uses the first credential that matches the following rules:

- If the "Microsoft: Windows Server Configuration Cache" Dynamic Application (from the Microsoft: Windows ServerPowerPack) is aligned to the device associated with the triggering event, the credential aligned to that Dynamic Application is used.
- If the "Microsoft: Windows Server Performance Cache" Dynamic Application (from the Microsoft: Windows ServerPowerPack) is aligned to the device associated with the triggering event, the credential aligned to that Dynamic Application is used.

- If the "Microsoft: Windows Server OS Configuration" Dynamic Application (from the Microsoft: Windows ServerPowerPack) is aligned to the device associated with the triggering event, the credential aligned to that Dynamic Application is used.
- If none of the listed Dynamic Applications are aligned to the device associated with the triggering event, the first available credential aligned to the device as a secondary credential is used.

Creating a Credential for Windows PowerShell

If you do not have the *Microsoft: Windows Server* PowerPack installed, you must create a credential that includes the username and password to communicate with your Windows devices. To create a credential, refer to the **Creating a Credential** section for more information.

To prepare your Windows systems for monitoring, follow the instructions in **Configuring Windows Servers for** *Monitoring with PowerShell*.

NOTE: If you have the *Microsoft: Windows Server* PowerPack installed and configured, you may skip this section.

For more information about configuring credentials in SL1, see the **Discovery and Credentials** manual.

Creating Custom Windows PowerShell Automation Policies

To create and customize Automation Policies for the Windows PowerShell Automations PowerPack, see the **Creating and Customizing Automation Policies** section.

Creating a Custom Action Policy

You can use the "Execute PowerShell Request" action type included with the Windows PowerShell Automations PowerPack to create custom automation actions that you can then use to build custom automation policies.

To create a custom action policy using the "Execute PowerShell Request" action type:

- 1. Navigate to the Action Policy Manager page (Registry > Run Book > Actions).
- 2. In the Action Policy Manager page, click the [Create] button.
- 3. The Action Policy Editor modal appears.

tion Editor	
Policy Editor Creating New Action	Reset
Action Name	Action State
Custom PowerShell Action) [Enabled]
Des	cription
An example of a custom Windows PowerShell action	
Organization	Action Type
[System]	Execute Remote PowerShell Request (1.0)
Execution Environment	Action Run Context
Windows PowerShell Automations	Database T
<pre>"commands": "Get-Printer Get-PrintJo "request_key": " ", "credential_id": 0, }</pre>	b Where-Object JobStatus -like '*error*'",
Save	1

- 4. In the Action Policy Editor page, supply a value in each field.
 - Action Name. Specify the name for the action policy.
 - Action State. Specifies whether the policy can be executed by an automation policy (enabled) or cannot be executed (disabled).
 - **Description**. Allows you to enter a detailed description of the action.
 - Organization. Organization to associate with the action policy.
 - Action Type. Type of action that will be executed. Select the "Execute PowerShell Request (1.0)" action type (highlighted in the figure above).
 - **Execution Environment**. Select from the list of available Execution Environments. The default execution environment is System.
 - Action Run Context. Select Database or Collector as the context in which the action policy will run.
 - Input Parameters. A JSON structure that specifies each input parameter. Each parameter definition includes its name, data type, and whether the input is optional or required for this Custom Action Type. For more information about the available input parameters, see the table in Creating a New Windows PowerShell Automation Action.

NOTE: Input parameters must be defined as a JSON structure.

6. Click **[Save]**. If you are modifying an existing action policy, click **[Save As]**. Supply a new value in the **Action Name** field, and save the current action policy, including any edits, as a new policy.

Customizing Automation Actions

The Windows PowerShell Automations PowerPack includes 5 automation actions that execute the "Execute PowerShell Request" action type to request diagnostic information or remediate an issue. You can specify the host and the options in a JSON structure that you enter in the *Input Parameters* field in the Action Policy Editor modal.

Action Name	Action State
/indows Memory Diagnostic Commands	[Enabled]
· · ·	Description
uns diagnostic commands for Memory-related events on	Windows devices.
Organization	Action Type
System 1	Execute Remote PowerShell Reguest (1.0)
Execution Environment	Action Run Context
Default: Windows PowerShell Automations]	[Collector]
{ "commands": "{\"commands\": [\"Ge "request_key": "", "credential_id": 0	Input Parameters
<pre>{ "commands": "{\"commands\": [\"Ge "request_key": "", "credential_id": 0 }</pre>	Input Parameters
<pre>{ "commands": "{\"commands\": [\"Ge "request_key": "", "credential_id": 0 }</pre>	Input Parameters

The following automation actions that use the "Execute PowerShell Request" action type are included in the Windows PowerShell Automations PowerPack. Compare the commands run with the example in the image above. For more information about input parameter fields, see the table in Creating a New Windows PowerShell Automation Action.

Action Name	Description	Commands Run
Windows CPU and Memory Diagnostic Commands	Runs diagnostic commands for CPU and Memory events on Windows devices	• Get-Process Sort CPU -descending Select -first 20

Action Name	Description	Commands Run
		 Get-Process Select-Object Name, ID, @ {Name='ThreadCount';Expression = {\$Threads.Count}} Sort-Object -Property ThreadCount - Descending Select -first 20
		• Get-Process Sort WS -descending Select - first 20
		 Get-CimInstance -Class Win32_PageFileUsage Format-Table -Property Caption,Name,Status,Description,InstallDate, AllocatedBaseSize,PeakUsage,TempPageFile
		• A command that collects the memory usage of running processes, where the memory usage is aggregated across all instances of each named process. The command is not listed here for clarity.
Windows CPU Diagnostic Commands	Runs diagnostic commands for CPU-related events on Windows devices	 Get-Process Sort CPU -descending Select -first 20 Get-Process Select-Object Name, ID, @ {Name='ThreadCount';Expression = {\$Threads.Count}} Sort-Object -Property ThreadCount - Descending Select -first 20
Windows Disk I/O Diagnostic Commands	Runs diagnostic commands for Disk I/O events on Windows devices	• A command that collects the "IO Data Bytes per second" counter for each running process. The command takes 10 samples at 1- second intervals and returns the average of all samples for each process. The command is not listed here for clarity.
		 A command that collects the "IO Data Operations per second" counter for each running process. The command takes 10 samples at 1-second intervals and returns the average of all samples for each process. The command is not listed here for clarity.
Windows Get Largest Event Log Files	Gets the 20 largest Windows Event Log files.	 Get-ChildItem C:\Windows\System32\winevt\Logs Sort - Descending -Property length Select -first 20
Windows Get Largest Files on Disk	Gets the 20 largest files on the disk specified in the event.	 Get-ChildItem %Y -r -erroraction 'silentlyContinue' Sort -Descending - Property length Select -first 20 Select- Object FullName,@{Name='SizeMB';Expression= [math]::Round(\$Length / 1MB,2)}
Windows Memory Diagnostic Commands	Runs diagnostic commands for Memory-related events on Windows	 Get-Process Sort WS -descending Select -first 20

Action Name	Description	Commands Run
	devices.	 Get-CimInstance -Class Win32_PageFileUsage Format-Table -Property Caption,Name,Status,Description,InstallDate, AllocatedBaseSize,PeakUsage,TempPageFile
		• A command that collects the memory usage of running processes, where the memory usage is aggregated across all instances of each named process. The command is not listed here for clarity.
Windows Print Job Error Diagnostic Commands	Runs diagnostic commands for Print Job Error events on Windows devices.	• Get-Printer Get-PrintJob Where-Object JobStatus -like '*error*'

TIP: For more information about substitution variables, see Appendix A.

Creating a New Windows PowerShell Automation Action

You can create a new automation action that runs remote PowerShell requests using the supplied "Execute PowerShell Request" custom action type. To do this, select "Execute PowerShell Request" in the Action Type dropdown list when you create a new automation action. You can also use the existing automation actions in the PowerPack as a template by using the **[Save As]** option.

Parameter	Input type	Description
commands	string	Specifies a single command or a list of commands, in JSON format, to execute. You can use substitution variables in the commands.
request_key	string	(Optional field)
		Default value: empty
		The unique key for each instance (row) returned by the request. This unique key must be a property name, and the request must include that property (column) and return values from that property name (column).
		Example : Suppose you want to get the ID, number of cores, name, and maximum clock speed of every CPU installed on a Windows system, run the following command, where "DeviceID" is the request key.
		Get-WmiObject -Class Win32_Processor - Property DeviceID, NumberOfCores, Name,

The Windows PowerShell automation actions accept the following parameters in JSON:

Parameter	Input type	Description
		MaxClockSpeed Format-List DeviceID,
		NumberOfCores, Name, MaxClockSpeed
credential_id	integer	Default value: 0
		Specifies the credential_id to use for the connection.
		 If set to 0 (false), the custom action type will dynamically determine the credential. For more information, see Authentication for Windows Devices.
		 If set to an ID number, it maps to the credential ID specified. You can find credential IDs by going to System > Manage > Credentials.

Using Substitution Values. The commands input can contain substitution values that match the keys in EM7_VALUES.

TIP: For more information about substitution variables, see Appendix A.

For a description of all options that are available in Automation Policies, see the **Run Book Automation** manual.

Chapter



Microsoft Hyper-V Automation

Overview

This manual describes how to use the automation policies, automation actions, and custom action types found in the Microsoft Hyper-V Automation PowerPack. Installation of the Windows PowerShell Automations PowerPack is required before using the Microsoft Hyper-V Automation PowerPack.

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

What is the Microsoft Hyper-V Automation PowerPack?	20
Prerequisites	20
Installing the Microsoft Hyper-V Automation PowerPack	. 20
Standard Automation Policies	21
Credential for Hyper-V Automation	24
Creating and Customizing Hyper-V Automation Policies	24
Creating a Custom Action Policy for Hyper-V	25

What is the Microsoft Hyper-V Automation PowerPack?

The Microsoft Hyper-V Automation PowerPack includes:

- A set of automation actions that run diagnostic commands on Hyper-V systems via PowerShell
- A set of automation policies that tie events from monitoring PowerPacks to the automation actions
- A dynamic device group for Hyper-V devices that is used to scope the automation policies

The Microsoft Hyper-V Automation actions are executed on the SL1 All-In-One Appliance or Data Collector.

In addition to using the standard content, you can use the content in the Microsoft Hyper-V Automation PowerPack to create your own automation policies that include the pre-defined actions that run different sets of diagnostic commands.

The Microsoft Hyper-V Automation PowerPack uses the supplied "Execute PowerShell Request" custom action type included with the Windows PowerShell Automations PowerPack.

Prerequisites

Before installing the Microsoft Hyper-V Automation PowerPack, you must perform the following actions:

- Install the Microsoft: Hyper-V Server PowerPack and configure it to monitor your Hyper-V device(s)
- Install version 103 or later of the Windows PowerShell Automations PowerPack
- Install version 102 or later of the Datacenter Automation Utilities PowerPack
- Install the Diag-V plug-in on your Hyper-V server. The plug-in is available here: https://gallery.technet.microsoft.com/scriptcenter/Diag-V-A-Hyper-V-0fe983e4

Installing the Microsoft Hyper-V Automation PowerPack

Before completing the steps in this manual, you must import and install the latest version of the Microsoft Hyper-V Automation PowerPack.

NOTE: The Microsoft Hyper-V Automation PowerPack requires SL1 version 8.10.0 or later. For details on upgrading SL1, see the appropriate SL1<u>Release Notes</u>.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the *System Administration* manual.)

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

- Search for and download the PowerPack from the PowerPacks page (Product Downloads > PowerPacks & SyncPacks) at the <u>ScienceLogic Support Site</u>.
- 2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
- 3. Click the [Actions] button and choose Import PowerPack. The Import PowerPack dialog box appears.
- 4. Click [Browse] and navigate to the PowerPack file from step 1.
- 5. Select the PowerPack file and click [Import]. The PowerPack Installer modal displays a list of the PowerPack contents.
- 6. Click [Install]. The PowerPack is added to the PowerPacks page.
- **NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Standard Automation Policies

The Microsoft Hyper-V Automation PowerPack includes four standard automation policies, shown in the following figure. Each policy triggers three automation actions that collect diagnostic data within a PowerShell session, and an action that formats the output in HTML. All of the automation actions use the same custom action type, "Execute PowerShell Request", which is supplied in the Windows PowerShell AutomationsPowerPack.

	Embedded Run Book Policies [4]									
Properties	Automation Policy Name *	ID	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited
Build / Export			All 🔻	All	•					All
Features / Benefits	1. 🤌 Hyper-V: CPU & Memory Diagnostic C 62	2	Enabled	System		1 group	5	4	em7admin	2020-05-21 16:46:42
Technical Notes	2. A Hyper-V: Disk & Storage Diagnostic Cc 63		Enabled	System		1 group	6	5	em7admin	2020-05-21 16:46:42
Documentation	3. 🥜 Hyper-V: Guests Below Threshold Diag 6*		Enabled	System		All	1	6	em7admin	2020-05-21 16:46:42
ntents	4. 🤌 Hyper-V: Run Time Capacity Diagnosti 60		Enabled	System		All	2	5	em7admin	2020-05-21 16:46:41
Dynamic Applications										
Event Policies										
Device Categories										
Device Classes										
Device Templates										
Device Groups										
Reports										
ashboard Widgets										
Jashboards	Available Due Darch Dallaber (0)									
ashboards SL1	Available Rull Book Policies [0]									
Run Book Policies	Automation Policy Name *	ID	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited
Run Book Actions			Ali 🔻	All	•					All
Run Book Action Types										
licket Templates										
redentials					No results to display.					
Credential Tests										
Proxy XSL Transformations										
JI Themes										
IT Services										
Log File Monitoring Policies										
	1									

All of the standard automation policies are tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the *Microsoft: Hyper-V Server* PowerPack.

Several of the automation actions use the substitution character feature of the "Execute PowerShell Request" custom action type. If an event variable is included in a command (such as "%Y" for the sub-entity name), the custom action type automatically replaces that variable with the value from the triggering event.

The following table shows the standard automation policies, their aligned events, and the automation actions that run in response to the events.

NOTE: The aligned events are included as part of the *Microsoft: Hyper-V Server* PowerPack and are not installed with the SL1 platform. You must install the *Microsoft: Hyper-V Server* PowerPack to obtain these events.

Automation Policy Name	Aligned Events	Automation Actions
Hyper-V: CPU & Memory Diagnostic Commands	 Microsoft: Windows CPU Utilization has exceeded the threshold 	Automation Utilities: Calculate Memory Size for Each action
	Microsoft: Windows Processor Queue Length exceeded the threshold	 Hyper-V Guest Status
	Microsoft: Windows Available	Diagnostic Commands
	Memory below threshold	Hyper-V Log Collection
	 Microsoft: Windows Pages per Second has exceeded threshold 	Datacenter Automation: Format
	 Microsoft: Windows Paging File has exceeded threshold 	Output as HTML
Hyper-V: Disk & Storage Diagnostic Commands	 Microsoft: Windows Disk Transfer Time (Physical Disk) exceeded threshold 	 Automation Utilities: Calculate Memory Size for Each action
	 Microsoft: Windows % Disk Time (Logical Disk) exceeded threshold 	 Hyper-V Guest Replication Diagnostic Command
	 Microsoft: Windows % Disk Time (Physical Disk) exceeded threshold 	 Hyper-V Guest Status Diagnostic Commands
	 Microsoft: Windows Current Disk Queue Length (Physical Disk) 	 Hyper-V Guest Storage Diagnostic Commands
	exceeded threshold	Datacenter
	 Poller: File system usage exceeded (major) threshold 	Automation: Format Output as HTML
	 Poller: File system usage exceeded (critical) threshold 	
Hyper-V: Guests Below Threshold Diagnostic Commands	 Microsoft: Hyper-V Percent VMs Running below threshold 	Automation Utilities: Calculate Memory Size for Each Action
		Hyper-V Guest Replication Diagnostic Command

Automation Policy Name	Aligned Events	Automation Actions
		 Hyper-V Guest Status Diagnostic Commands
		 Hyper-V Guest Storage and Replication Diagnostic Commands
		Hyper-V Log Collection
		 Datacenter Automation: Format Output as HTML
Hyper-V: Run Time Capacity Diagnostic Commands	 Microsoft: Hyper-V Percent Total Run Time has exceeded major threshold Microsoft: Hyper-V Percent Total Run 	 Automation Utilities: Calculate Memory Size for Each Action
	Time has exceeded minor threshold	 Hyper-V Guest Status Diagnostic Commands
		 Hyper-V Allocation Diagnostic Commands
		Hyper-V Log Collection
		Datacenter Automation: Format Output as HTML

The following figure shows a memory event with a classification of "Major" appears on the **Events** page. Click the **[Actions]** button (--) for an event, and select *View Automation Actions* to see the automation actions triggered by the events.

≡	Even	ts												Mantone 🗸	Ð.	ncelogic
88	Cri	1 tical	32 Major	5 Minor	1 Notice	3 Healthy	42 Events View All									~ View
▲	QT	ype to	search events													≡ o
G	¢		ORGANIZATION	51	VERITY	NAME		MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR	c
	Ť		аумен			ragerous		гарстому он стог, гусокс схоронгинен накад гера	+ oays 2 moors		÷.	۳		· removed	• ••••	
ė	~		System	•	Major	PagerDut	(PagerDuty DA Error: PyCURL Exception when making requ	4 days 1 hour		1	Ð		 Acknowledge 	× Clear] -
	~		System	•	Major	Dell EMC	Device	Example EMC Event	3 days 21 hours		1	Ð		 Acknowledge 	× Clear] - [
	~		Windows Device	5	Notice	10.2.24.5	2	Microsoft: Hyper-V Percent Virtual Machines Running is be	3 days 20 hours		5443	Ð		✓ Acknowledge	× Clear	-
	~		Example Devices	s (Major	ec2-34-2	00-97-29	Device Failed Availability Check: UDP - SNMP	21 hours 42 minutes		261	Ð	Q Masked	 Acknowledge 	× Clear	-
	~		Linux Devices	•	Major	10.2.24.3	0	Device Failed Availability Check: UDP - SNMP	21 hours 42 minutes		261	Ð	Q Masked	✓ Acknowledge	× Clear] - [
	~		Example Devices	•	Major	Test CRS-	1 165	Device Failed Availability Check: ICMP Ping	21 hours 42 minutes		261	Ð	Q Masked	✓ Acknowledge	× Clear] - [
	~		Linux Devices	•	Major	10.2.24.3	1	Device Failed Availability Check: UDP - SNMP	21 hours 42 minutes		261	Ð	Q Masked	✓ Acknowledge	× Clear] - [
	~		Windows Device	es 📢	Minor	10.2.24.5	5	CPU utilization has exceeded the threshold 75%. Current v	2 hours 47 minutes		34	Ð		✓ Acknowledge	× Clear] -
	~		Windows Device	в 🌔	Minor	10.2.24.5	5	Processor Queue Length has exceeded the threshold 6 Thr	1 hour 12 minutes		15	Ð		 Acknowledge 	× Clear] - [
	~		Windows Device	в (Healthy	10.2.24.5	5	Network Latency below threshold	17 minutes 6 seconds		1	Ð		✓ Acknowledge	× Clear] -
	~		Windows Device	в	Healthy	10.2.24.5	5	Pages per Second is now below the threshold 200 Pages/S	13 minutes 1 second		1	Ð		✓ Acknowledge	× Clear] - [
	~		Windows Device	в (Major	10.2.24.5	5	C:\: File system usage exceeded major threshold: Limit: 1.0	7 minutes 56 seconds	212	1	Ð		✓ Acknowledge	× Clear] - [
	~		Windows Device	в (Healthy	10.2.24.5	5	C(\; File system usage returned below critcal threshold; Li.,	7 minutes 56 seconds		1	Ð		✓ Acknowledge	× Clear] - [
	~		System	•	Major	Test Com	ponent 2	Content Policy: "Test 6" request timed out against URL htt	6 minutes 32 seconds		5	Ð	Q Masked	Acknowledge	× Clear] - [
	~		VMware Device:	•	Minor	rstlsvcsaó	u2a01	Network latency exceeded threshold: 316.63 ms.	2 minutes 13 seconds		1	Ð		✓ Acknowledge	× Clear] -
	~		System	•	Minor	10.2.24.2	3	Network latency exceeded threshold: 467.48 ms.	2 minutes 13 seconds		1	Ð		✓ Acknowledge	× Clear]

The results shown for this event, in the Event Actions Log, include the automation policy that ran (shown at the top of the following figure), along with the automation actions (commands) that ran. Results for each command are also displayed. The following figure shows an example of this HTML output.

Event Actions Log For Event [96198]	Refresh	Guide	
2020-03-13 19:08:26			
Automation Policy Hyper-V: Guests Below Threshold Diagnostic Commands action Datacenter Automation: Format Output as HTML ran Successfully Message:Snippet (365) executed without incident Result_{Tomated_output: <u>Enrichment Command Output</u>			
Command: Get_WMStatus			
ComputerName Name State CPUUsage MemoryMB Uptime Status			
UTIN_HVPERV_CVR TectVN2 Off 0 0 00:00:00 Operating pormally			
UTN-HYPER-CVB TestVM1 Off 0 0000000 Operating normally			
WIN-HYPERV-CYB Test3 Off 0 0000000 Operating normally			
Command: Get-VMInfo			
Name : Test3			
CPU : 1			
DynamicMemoryEnabled : False			
NemocyNillinum(NB) : 512			
Profile ynds Allidau (dd) - 1024 Tsc Iistened - Salse			
Version : 9.0			
ReplicationHealth : NotApplicable			
OSName : Unknown			
FQDN : Unknown			
VHDType-0 : Dynamic			
VHD51ze(GB)-0 : 0			
MaxSize(GB)-0 : 127			
Name : Testumi			
DroamicMemoryEpabled · Ealse			
Venorvhinimum(NB) : 512			
MemoryMaximum(GB) : 1024			
Isclustered : False			
Version : 9.0			
ReplicationHealth : NotApplicable			
OSName : Unknown			
PON : Unknown			
Amin Aber 20 10 10 10 10 10 10 10 10 10 10 10 10 10			
MaxSiz(GD).0 · 177			
Name : TestVM2			
CPU : 1			
DynamicMemoryEnabled : False			
MemoryMinimum(MB) : 512			
MemoryMaximum(GB) : 1024			.
IsClustered : False			-
4		+	

To learn more about which commands are executed by default for a given automation action, see **Customizing Actions**.

TIP: Although you can edit the automation policies described in this section, it is a best practice to use "Save As" to create a new automation action, rather than to customize the standard automation policies.

Credential for Hyper-V Automation

The Microsoft Hyper-V Automation PowerPack uses the same credential that you created for the Windows PowerShell Automations PowerPack. Refer to the **Creating a Credential** section for more information.

NOTE: If you have the *Microsoft: Windows Server* PowerPack installed and configured, you may skip this section.

For more information about configuring credentials in SL1, see the **Discovery and Credentials** manual.

Creating and Customizing Hyper-V Automation Policies

To create and customize Automation Policies for the Microsoft Hyper-V Automation PowerPack, see the Creating and Customizing Automation Policies section.

Creating a Custom Action Policy for Hyper-V

You can use the "Execute PowerShell Request" action type included with the Windows PowerShell Automations PowerPack to create custom automation actions that you can then use to build custom automation policies. To create a custom action policy, see the Creating a Custom Action Policy section.

Customizing Automation Actions

The Microsoft Hyper-V Automation PowerPack includes 2 automation actions that execute the "Execute PowerShell Request" action type to request diagnostic information or remediate an issue. You can specify the commands and the options in a JSON structure that you enter in the *Input Parameters* field in the Action Policy Editor modal.

Dicy Editor Editing Action [316]	
A sting blows	A sting Otata
Action Name	Action State
Typer-V Allocation Diagnostic Command	
Des Determines the surrent resource allegation health of the Livner V	cription
betermines the current resource allocation health of the Hyper-V	server of cluster.
Organization	Action Type
[System]	Execute Remote PowerShell Request (1.0)
Execution Environment	Action Run Context
[Default: Microsoft Hyper-V Automation]	[Collector]
lanut B	
<pre>{</pre>	arameters erVAllocation\"]}",
<pre>{ "commands": "{\"commands\": [\"Test-Hype "request_key": "", "credential_id": 0 }</pre>	arameters

The following automation actions that use the "Execute PowerShell Request" action type are included in the *Microsoft Hyper-V Automation* PowerPack. Compare the commands run with the example in the image above. For more information about input parameter fields,

see the table in Creating a New Microsoft Hyper-V Automation Action.

Action Name	Description	Commands Run
Hyper-V Allocation Diagnostic Command	Determines the current resource allocation health of the Hyper-V server or cluster.	• Test-HyperVAllocation
Hyper-V Guest Replication Diagnostic Command	Runs a diagnostic command related to Hyper-V guest replication	• Get-VMReplicationStatus
Hyper-V Guest Status Diagnostic Commands	Runs diagnostic commands to collect Hyper-V guest status and configuration information.	 Get-VMStatus Get-VMInfo Format-Table
Hyper-V Guest Storage Diagnostic Commands	Runs diagnostic commands related to Hyper-V Guest storage and replication.	 Get-VMLocationPathInfo Format-Table Get-VMSharedVHDs Format- Table
Hyper-V Log Collection	Collects the most recent 25 log entries from the Hyper-V logs.	 Get-HyperVLogInfo -StartDate ((Get-Date).addminutes(-10))

TIP: For more information about substitution variables, see Appendix A.

Creating a New Microsoft Hyper-V Automation Action

You can create a new automation action that runs remote PowerShell requests using the supplied "Execute PowerShell Request" custom action type. To do this, refer to the **Creating a New Windows PowerShell Automation Action** section

For a description of all options that are available in Automation Policies, see the **Run Book Automation** manual.

Chapter

4

Configuring Device Credentials

This chapter describes how to configure the credentials required by the automation actions in the Microsoft Automations PowerPacks.

This chapter covers the following topics:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

Creating a Credential

If you are creating a credential for the Windows PowerShell Automations PowerPack and do not have the Microsoft: Windows Server PowerPack installed, you must create a credential that includes the username and password to communicate with your Windows devices.

To prepare your Windows systems for monitoring, follow the instructions in **Configuring Windows Servers for** *Monitoring with PowerShell*.

NOTE: If you have the *Microsoft: Windows Server* PowerPack installed and configured, you may skip this section.

To define a PowerShell credential in SL1:

- 1. Collect the information you need to create the credential:
 - The username and password for a user on the Windows device.
 - If the user is an Active Directory account, the hostname or IP address of the Active Directory server and the domain.
 - Determine if an encrypted connection should be used.
 - If you are using a Windows Management Proxy, the hostname or IP address of the proxy server.
- 2. Go to the **Credential Management** page (System > Manage > Credentials).
- 3. In the Credential Management page, click the [Actions] menu. Select Create PowerShell Credential.
- 4. The **Credential Editor** page appears, where you can define the following fields:
 - **Profile Name**. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
 - Hostname/IP. Hostname or IP address of the device from which you want to retrieve data. This field is required.
 - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
 - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the device that is currently using the credential. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
 - You can include the prefix HOST or WSMAN before the variable %D in this field if the device you want to monitor uses a service principal name (for example, "HOST://%D" or "WSMAN://%D").
 SL1 will use the WinRM service HOST or WSMan instead of HTTP and replace the variable with the IP address of the device that is currently using the credential.
 - **Username**. Type the username for an account on the Windows device to be monitored or on the proxy server. This field is required.

NOTE: The user should not include the domain name prefix in the username for Active Directory accounts. For example, use "em7admin" instead of "MSDOMAIN\em7admin".

- **Encrypted**. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
 - yes. When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate.
 - no. When communicating with the Windows server, SL1 will not encrypt the connection.
- **Port**. Type the port number used by the WinRM service on the Windows device. This field is automatically populated with the default port based on the value you selected in the **Encrypted** field. This field is required.
- Account Type. Type of authentication for the username and password in this credential. Choices are:
 - Active Directory. On the Windows device, Active Directory will authenticate the username and password in this credential.
 - Local. Local security on the Windows device will authenticate the username and password in this credential.
- *Timeout (ms)*. Type the time, in milliseconds, after which SL1 will stop trying to collect data from the authenticating server. For collection to be successful, SL1 must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.
- **Password**. Type the password for the account on the Windows device to be monitored or on the proxy server. This field is required.
- **PowerShell Proxy Hostname/IP**. If you use a proxy server in front of the Windows devices you want to communicate with, type the fully-qualified domain name or the IP address of the proxy server in this field.
- Active Directory Hostname/IP. If you selected Active Directory in the Account Type field, type the hostname or IP address of the Active Directory server that will authenticate the credential.
- **Domain**. If you selected Active Directory in the **Account Type** field, type the domain where the monitored Windows device resides.
- 5. To save the credential, click the [Save] button. To clear the values you set, click the [Reset] button.

For more information about configuring credentials in SL1, see the **Discovery and Credentials** manual.

Chapter

5

Creating and Customizing Automation Policies

Overview

This chapter describes how to create automation policies using the automation actions in Microsoft Automation PowerPacks.

This chapter covers the following topics:

Prerequisites	31
Creating an Automation Policy	31
Customizing an Automation Policy	32

Prerequisites

Before you create an automation policy using the automation actions in *Microsoft Automation* PowerPacks, you must determine:

- Which set of commands you want to run on a monitored device when an event occurs. There are ten automation actions in the PowerPack that run the "Execute PowerShell Request" action type with different commands. You can also create your own automation actions using the custom action type supplied in the PowerPack.
- What event criteria you want to use to determine when the automation actions will trigger, or the set of rules that an event must match before the automation is executed. This can include matching only specific event policies, event severity, associated devices, and so on. For a description of all the options that are available in Automation Policies, see the **Run Book Automation** manual.

Creating an Automation Policy

To create an automation policy that uses the automation actions in *Microsoft Automation* PowerPacks, perform the following steps:

- 1. Go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 2. Click [Create]. The Automation Policy Editor page appears.
- 3. Complete the following required fields:
 - Policy Name. Enter a name for the automation policy.
 - **Policy Type**. Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
 - **Policy State**. Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.
 - **Policy Priority**. Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.
 - **Organization**. Select one or more organizations to associate with the automation policy. The automation policy will execute only for devices in the selected organizations (that also match the other criteria in the policy). To configure a policy to execute for all organizations, select *System* without specifying individual devices to align to.

Aligned Actions. This field includes the actions from the PowerPack. To add an action to the Aligned Actions field, select the action in the Available Actions field and click the right arrow (>>). To re-order the actions in the Aligned Actions field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

NOTE: You must have at least two Aligned Actions: one that runs the automation action and one that provides the output format. The actions providing the output formats are contained in the *Datacenter Automation Utilities* PowerPack, which is a prerequisite for running automations in this PowerPack.

NOTE: If you are selecting multiple collection actions that use the "Execute PowerShell Request" action type, you may want to include the "Calculate Memory Size for Each Action" automation action, found in the *Datacenter Automation Utilities* PowerPack, in your automation policy.

- 4. To align the policy with the Windows Automation device group, which is supplied in the PowerPack, do the following:
 - a. In the Align With drop-down menu, select "Device Groups".
 - b. In the **Available Device Groups** field, select, the "Windows Automation" device group, and click the right arrow (>>).
- 5. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
- 6. Click [Save].

NOTE: You can also modify one of the automation policies included with this PowerPack. Best practice is to use the **[Save As]** option to create a new, renamed automation policy, instead of customizing the standard automation policies.

NOTE: If you modify one of the included automation policies and save it with the original name, the customizations in that policy will be overwritten when you upgrade the PowerPack unless you remove the association between the automation policy and the PowerPack before upgrading.

Customizing an Automation Policy

To customize an automation policy:

- 1. Go to the Automation Policy Manager page (Registry > Run Book > Automation).
- 2. Search for the automation policy you want to edit and click the wrench icon (*P*) for that policy . The **Automation Policy Editor** page appears.
- 3. Complete the following fields as needed:

- Policy Name. Type a new name for the automation policy to avoid overwriting the default policy.
- **Policy Type**. Select whether the automation policy will match events that are active, match when events are cleared, or run on a scheduled basis. Typically, you would select *Active Events* in this field.
- **Policy State**. Specifies whether the policy will be evaluated against the events in the system. If you want this policy to begin matching events immediately, select *Enabled*.
- **Policy Priority**. Specifies whether the policy is high-priority or default priority. These options determine how the policy is queued.
- Aligned Actions. This field includes the actions from the PowerPack. You should see "Execute Remote PowerShell Request" action in this field. To add an action to the Aligned Actions field, select the action in the Available Actions field and click the right arrow (>>). To re-order the actions in the Aligned Actions field, select an action and use the up arrow or down arrow buttons to change that action's position in the sequence.

NOTE: You must have at least two Aligned Actions: one that runs the automation action and one that provides the output format. The actions providing the output formats are contained in the *Datacenter Automation Utilities* PowerPack, which is a prerequisite for running automations in this PowerPack.

- Organization. Select the organization that will use this policy.
- 4. To align the policy with the *Windows Automation* device group, which is supplied in the PowerPack, do the following:
 - a. In the Align With drop-down menu, select "Device Groups".
 - b. In the **Available Device Groups** field, select, the "Windows Automation" device group, and click the right arrow (>>).
- 5. Optionally, supply values in the other fields on this page to refine when the automation will trigger.
- 6. Click [Save].

NOTE: You can also modify one of the automation policies included with this PowerPack. Best practice is to use the **[Save As]** option to create a new, renamed automation policy, instead of customizing the standard automation policies.

- **NOTE**: If you modify one of the included automation policies and save it with the original name, the customizations in that policy will be overwritten when you upgrade the PowerPack unless you remove the association between the automation policy and the PowerPack before upgrading.
- 6. Optionally, supply values in the other fields on the **Automation Policy Editor** page to refine when the automation will trigger.
- 7. Click [Save As].

Removing an Automation Policy from a PowerPack

After you have customized a policy from a *PowerPack*, you might want to remove that policy from that PowerPack to prevent your changes from being overwritten if you update the PowerPack later. If you have the license key with author's privileges for a PowerPack or if you have owner/administrator privileges with your license key, you can remove content from a PowerPack.

To remove content from a PowerPack:

- 1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 2. Find the PowerPack. Click its wrench icon (*P*).
- 3. In the PowerPack Properties page, in the navigation bar on the left side, click Run Book Policies.
- 4. In the **Embedded Run Book Polices** pane, locate the policy you updated, and click the bomb icon (*) for that policy. The policy will be removed from the PowerPack and will now appear in the bottom pane.

Chapter



Windows PowerShell User-Initiated Automations

Overview

This manual describes how to use the automation policies found in the Windows PowerShell User-Initiated Automation PowerPack

NOTE: This PowerPack is available with a ScienceLogic SL1 Standard solution. Contact your ScienceLogic Customer Success Manager or Customer Support to learn more.

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

This chapter covers the following topics:

What is the Windows PowerShell User-Initiated Automation PowerPack?	.36
Installing the Windows PowerShell User-Initiated Automation PowerPack	.36
Standard Automation Policies	.37

What is the Windows PowerShell User-Initiated Automation PowerPack?

The Windows PowerShell User-Initiated Automation PowerPack includes automation policies that you can use to run Windows diagnostic commands from the SL1 event console, using Event Tools. This PowerPack is supplemental to the Windows PowerShell Automations PowerPack and is not meant for standalone use.

In addition to using the standard content, you can customize the automation policies, or you can create your own automation policies using any available automation actions.

Installing the Windows PowerShell User-Initiated Automation PowerPack

Before completing the steps in this manual, you must import and install the latest version of the Windows PowerShell Automations PowerPack and the Microsoft: Windows Server PowerPack.

NOTE: The Windows PowerShell User-Initiated Automation PowerPack requires SL1 version 10.1.0 or later. For details on upgrading SL1, see the appropriate SL1<u>Release Notes</u>.

WARNING: You must also install the Datacenter Automation Utilities PowerPack, which provides the output formats for the automation actions included in this PowerPack.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the *Enable Selective PowerPack Field Protection* setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. (For more information, see the *System Administration* manual.)

IMPORTANT: The minimum required MySQL version is 5.6.0.

To download and install the PowerPack:

- Search for and download the PowerPack from the PowerPacks page (Product Downloads > PowerPacks & SyncPacks) at the <u>ScienceLogic Support Site</u>.
- 2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
- 3. Click the [Actions] button and choose Import PowerPack. The Import PowerPack dialog box appears.
- 4. Click [Browse] and navigate to the PowerPack file from step 1.
- 5. Select the PowerPack file and click [Import]. The PowerPack Installer modal displays a list of the
PowerPack contents.

- 6. Click [Install]. The PowerPack is added to the PowerPacks page.
- **NOTE:** If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Standard Automation Policies

The Windows PowerShell User-Initiated Automation PowerPack includes standard automation policies that trigger automation actions that will run Windows diagnostic commands from the SL1 event console.

The automation policies available in this release of the PowerPack are tied to included ScienceLogic SL1 events generated by the Dynamic Applications from the *Microsoft: Windows Server* PowerPack.

The automation policies are of Policy Type, "User Initiated". This means that for an event that matches the criteria, you can run these automation policies from the **Event Console**.

For these automation policies to be visible from the Event Tools in the Event's drawer, the following three things must be true between the event and the automation policy configuration:

- **Organization**. The organization associated with the event must match the organization configured in the automation policy. Policies in the "System" organization match all organizations.
- Aligned Devices. The device for which the event is triggered must be configured as a Aligned Device in the automation policy.
- Aligned Event. The event must match one of the Aligned Events configured in the automation policy.

The following table shows the automation policies, their aligned events, and the automation actions that run in response to the events.

NOTE: The aligned events are included as part of the *Microsoft: Windows Server* PowerPack and are not installed with the SL1 platform. You must install the PowerPack to obtain these events.

Automation Policy Name	Aligned Events	Automation Action
Run CPU & Memory Diagnostics (PowerShell)	 Microsoft: Windows Disk Transfer Time (Physical Disk) exceeded threshold 	 Execute Remote PowerShell Request [101]: Windows CPU and Memory Diagnostic Commands
		 Datacenter Automation: Format Output as HTML
Run CPU Diagnostics (PowerShell)	 Microsoft: Windows CPU Utilization has exceeded the threshold 	 Execute Remote PowerShell Request [101]: Windows CPU Diagnostic Commands

Automation Policy Name	Aligned Events	Automation Action
	 Microsoft: Windows Processor Queue Length exceeded the threshold 	Datacenter Automation: Format Output as HTML
Run Disk I/O Diagnostics (PowerShell)	 Microsoft: Windows % Disk Time (Logical Disk) exceeded threshold Microsoft: Windows % Disk Time (Physical Disk) exceeded threshold Microsoft: Windows Current Disk Queue Length (Physical 	 Execute Remote PowerShell Request [101]: Windows Disk I/O Diagnostic Commands Datacenter Automation: Format Output as HTML
Run Memory Diagnostics (PowerShell)	 Microsoft: Windows Available Memory below threshold Microsoft: Windows Pages per Second has exceeded threshold Microsoft: Windows Paging File Usage has exceeded threshold 	 Execute Remote PowerShell Request [101]: Windows Memory Diagnostic Commands Datacenter Automation: Format Output as HTML
Run Print Job Error Diagnostics (PowerShell)	 Microsoft: Windows Print Job Errors exceeded threshold 	 Execute Remote PowerShell Request [101]: Windows Print Job Error Diagnostic Commands Datacenter Automation: Format Output as HTML

Running a User Initiated Automation Policy

To run a user initiated automation policy, open the drawer for the event and click in the Tools section. Any available user initiated automation policy will be available to run on demand.

≡	Events										Activity Mantone	- 🔊 Scie	enceLogic
88	0 Critical	26 7 Major Minor	3 4 Notice Heal	4 40 Events View All									~ View
	Q. Type to s	search events										=	۵
G	¢ 🗆 11	ST ORGANIZATION	SEVERITY	NAME	MESSAG	36	AGE TICKET ID	COUNT	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR	c
æ	~ D	Network	 Minor 	ec2-34-200-97-29	Netwo	rk latency exceeded threshold: No Response	2 days 20 hours	821	Ð		 Acknowled 	ge 🗶 Clea	ar
	~ 🗆	VMware	 Major 	10.2.5.72	Exampl	le VMware Event	2 days 20 hours	1	Ð		 Acknowled 	ge 🗶 Clea	ar
	<u>^</u>	Windows	 Minor 	Windows 2016 Test	CPU ut	dization has exceeded the threshold 0%. Current v	2 days 20 hours	803	Ð		 Acknowled 	ge 🛛 🗙 Clea	ar
	Vitals					Tools			Logs				
	400					Type to run an action on this	device		🌣 AGE -	SEVERITY	MESSAGE		
	300 -			1		= DEFAULT TOOLS	ARP Lookup		1 minute 46 se	cond: 😑 Mintor	CPU utilization has exceeded the value is 96.6%.	threshold 0%. Cur	rent
	₩ 200 -					Acailability	A8P Ping		7 minutes 43 s	conc 😑 Minor	CPU utilization has exceeded the value is 5.07%.	threshold 0%. Cur	ment
	100	Hund In	L		+	Ping	Trace Route		13 minutes 14	secor 😑 Minor	CPU utilization has exceeded the value is 5.27%.	threshold 0%. Cur	ment
	0	MAMMAN MANAM	MANNAW MAN	TIA WWWII TWWWWWW	ML	Who is	= RUNBOOK ACTIONS		13 minutes 14	secor 🔵 Healthy	Processor Queue Length is now b Threads. Current value is 0 Thread	slow the threshold is.	d 6
		1600 2000	22.301 0	400 0800 I.	2:00	Port Scan	Run CPU Diagnostics (PowerShell)				CPU utilization has exceeded the	threshold 0%. Cur	rrent
	~ 🗆	Windows	😑 Major	Test3	Device	wailabil Deep Port Scan			Ð		 Acknowled 	ge 🛛 🗙 Cles	ar
	~ 🗆	Windows	 Major 	TestVM2	Device	wailability Flapping, Device Now Available	2 days 19 hours	466	Ð		 Acknowled 	ge 🗶 Cles	ar
	~ 🗆	Windows	 Major 	TestVM1	Device	Availability Flapping, Device Now Available	2 days 20 hours	466	Ð		 Acknowled 	ge 🗶 Cles	ar
	~ 🗆	Windows	 Major 	Hyper-V Test	The 'Di	agnostic Policy Service' service is NOT running	2 days 19 hours	703	Ð		 Acknowled 	ge 🗶 Cles	ar
	~ 🗆	Windows	 Notice 	Hyper-V Test	Micros	oft: Hyper-V Percent Virtual Machines Running is b.	2 days 19 hours	641	Ð		 Acknowled 	ge 🗶 Cles	ar
	~ 🗆	Network	😑 Major	ec2-3-93-103-93	Device	Failed Availability Check: UDP - SNMP	2 days 16 hours	771	Ð	Q Masked	 Acknowled 	ge 🛛 🗙 Cles	ar
	×П	Windows	 Major 	Hyper-V Test	The %	Disk Used for logical disk (C) has exceeded the thre	1 day 13 hours	125	F		Acknowled	ge 🗙 Cle	ar

Viewing Automation Actions for an Event

The following figure shows a VMware event with major criticality on the **Events** page. Click the **[Actions]** button (--) for an event, and select View Automation Actions to see the automation actions triggered by the events.

≡	Eve	nts										🔦 Activity Mantone 🗸		eLogic
88	c	0 Iritical 1	26 7 Major Minor	3 4 Notice Hea	40 Events Ithy View All								v	View
	Q	Type to sear	ch events		_								=	٥
G	۵	TEST	ORGANIZATION	SEVERITY	NAME	MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR	c
æ	~		Network	 Minor 	ec2-34-200-97-29	Network latency exceeded threshold: No Response	2 days 20 hours		821	Ð		 Acknowledge 	× Clear	
	~		VMware	 Major 	10.2.5.72	Example VMware Event	2 days 20 hours		1	Ð		 Acknowledge 	X Clear	
÷	~		Windows	 Minor 	Windows 2016 Test	CPU utilization has exceeded the threshold 0%. Current v	2 days 20 hours		803	Ð		 Acknowledge 	× Clear	
	~		Windows	 Major 	Test3	Device Availability Flapping, Device Now Available	2 days 20 hours		466	Ð		View Event		
	~		Windows	😑 Major	TestVM2	Device Availability Flapping, Device Now Available	2 days 20 hours		466	Ð		Edit Event No	te	
	~		Windows	😑 Major	TestVM1	Device Availability Flapping, Device Now Available	2 days 20 hours		466	Ð		Create Ticket		
	~		Windows	😑 Major	Hyper-V Test	The 'Diagnostic Policy Service' service is NOT running	2 days 20 hours		703	Ð		View Automa	tion Actions	
	~		Windows	 Notice 	Hyper-V Test	Microsoft: Hyper-V Percent Virtual Machines Running is b	2 days 20 hours		641	Ð		View Event P	olicy	- 1
	~		Network	😑 Major	ec2-3-93-103-93	Device Failed Availability Check: UDP - SNMP	2 days 16 hours		771	Ð	Q Masked	Suppress Eve	nt for this Dev	vice
	~		Windows	😑 Major	Hyper-V Test	The % Disk Used for logical disk (C) has exceeded the thre	1 day 13 hours		125	Ð		· remaininge	- crear	
	~		Windows	😑 Major	Hyper-V Test	The % Disk Used for logical disk (TOTAL) has exceeded th	1 day 13 hours		125	Ð		✓ Acknowledge	X Clear	
	~		Windows	😑 Major	Hyper-V Test	PowerShell Communication Error: App [1288] Windows d.,	1 day 9 hours		90	Ð		 Acknowledge 	X Clear	
	~		System	 Minor 	cscol26	Net-SNMP: CPU has exceeded threshold: (80%) currently	1 day 9 hours		381	Ð		 Acknowledge 	X Clear	
	~		Windows	 Minor 	Hyper-V Test	Processor Queue Length has exceeded the threshold 6 Thr.	. 16 hours 23 minutes		130	Ð		 Acknowledge 	X Clear	
			System	😑 Major	System	Process time exceeded: Process Data Collection: Dynamic	9 hours 58 minutes		213	Ð		 Acknowledge 	X Clear	
	~		Windows	 Major 	Hyper-V Test	PowerShell Communication Error: App [1392] Windows d.,	8 hours 39 minutes		22	Ð		 Acknowledge 	X Clear	
			Mindows	 Major 	Munner V Test	DeverShell Communication Errors Ann 112973 Mindows d	7 hours 9 minutes		2.4	CA.		- Acknowledge	V Clear	

The results shown for this event, in the **Event Actions Log**, include the automation policy that ran (shown at the top of the following figure), along with the collected data. The following figure shows an example of this output.

Event Actions Log I For Event [3162]	Refresh Guide
2020-06-19 20:40:25	
Automation Policy Windows PowerSRell: Run CPU Diagnostic Commands action Datacenter Automation: Format Output as HTML ran Successfully Message:Snippet (50) executed without incident Result;[ormated_output: <u>Enrichment Command Output</u>]	y
Command: Get-Process Sort CPU -descending Select -first 20 Format-Table -AutoSize	
Handles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName	
592 86 234868 242436 150,890.66 2016 0 MSMpEng	
181628 110 36048/2 11189/6 123,800.61 656 0 SV(NOSL 005 0 124 125 006 12 4 8 SV(tem	
555 69 248324 84744 59 117.42 2464 0 solsenum	
608 26 373664 364152 11.650.31 2668 0 mysald	
378 23 30860 42524 10,569.52 3612 0 WmiPrvSE	
1064 62 20692 27928 7,909.75 1096 0 svchost	
456 20 18780 23076 6,648.56 3568 0 WmiPrvSE	
329 21 10688 10208 4,228.13 1904 0 vmtoolsd	
1134 22 7988 16804 4,001.55 588 0 Isass	
444 1/ 16000 162/2 4,010.13 300 0 SVCNOST	
361 38 230228 131448 3,000.55 644 0 SULIDSL 363 10 EE90 10140 3 140.00 E72 0 services	
97 8 4956 1812 2 169 42 2676 0 scivics	
525 19 51760 52796 1.696.86 736 0 sychost	
93 8 4984 1564 1,237.72 2724 0 conhost	
440 15 2032 2280 906.08 360 0 CSrSs	
501 18 5876 15068 695.72 672 0 svchost	
142 12 2040 3968 519.63 1440 0 svchost	
146 14 1145132 3324 469.41 1824 0 mysqld	
Command: Get-Process Select-Object Name, ID, @{Name='ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Pro	perty ThreadCount -Descending Select -first 20
Name Id Threadcount	
Suctem 4 107	
sychost 656 64	
sdlservr 2464 50	
mysqld 2668 42	
svchost 1096 32	
mysqld 1824 30	
svchost 644 27	
svchost 892 24	
Nspeng 2016 24	
Svchost 3/4 2/	
Independent 18	
sychost 300 16	
sychost 672 14	· ·

NOTE: To learn more about which logs are collected by default for a given automation action, see the *Customizing Windows PowerShell Actions* section.

TIP: Although you can edit the automation policy described in this section, it is a best practice to use "Save As" to create a new automation policy, rather than to customize the standard automation policies.

Appendix



Run Book Variables

Overview

This appendix defines the different variables you can use when creating an action policy.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (三).
- To view a page containing all of the menu options, click the Advanced menu icon (---).

This appendix covers the following topics:

This chapter covers the following topics:

Run Book Variables	. 4	2
--------------------	-----	---

Run Book Variables

You can include variables when creating an action policy. These variables are listed in the table below.

- In an action policy of type **Send an Email Notification**, you can include one or more of these variables in the fields **Email Subject** and **Email Body**.
- In an action policy of type **Send an SNMP Trap**, you can include one or more of these variables in the **Trap OID** field, **Varbind OID** field, and the **Varbind Value** field.
- In an action policy of type **Create a New Ticket**, you can include one or more of these variables in the **Description** field or the **Note** field of the related Ticket Template.
- In an action policy of type **Send an SNMP Set**, you can include one or more of these variables in the **SNMP OID** field and the **SNMP Value** field.
- In an action policy of type Run A Snippet, you can access variables from the global dictionary EM7_ VALUES.
- In a policy of type **Execute an SQL Query**, you can include one or more of these variables in the **SQL Query** field.

Variable	Source	Description
%A	Account	Username
%N	Action	Automation action name
%g	Asset	Asset serial
%h	Asset	Device ID associated with the asset
%i (lowercase "eye")	Asset	Asset Location
%k	Asset	Asset Room
%K	Asset	Asset Floor
%P	Asset	Asset plate
%р	Asset	Asset panel
%q	Asset	Asset zone
%Q	Asset	Asset punch
%U	Asset	Asset rack
%υ	Asset	Asset shelf
%v	Asset	Asset tag
%w	Asset	Asset model
%₩	Asset	Asset make
%m	Automation	Automation policy note
%n	Automation	Automation policy name
%F	Dynamic Alert	Alert ID for a Dynamic Application Alert
%l (uppercase "eye")	Dynamic Alert	For events with a source of "dynamic", this variable contains the index value from SNMP. For events with a source of "syslog" or "trap", this variable contains

Variable	Source	Description
		the value that matches the <i>Identifier Pattern</i> field in the event definition.
%T	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.
%V	Dynamic Alert	Value returned by the Result function in a Dynamic Application Alert.
%L	Dynamic Alert	Value returned by the label variable in a Dynamic Application Alert.
%a	Entity	IP address
%_category_id	Entity	Device category ID associated with the entity in the event.
%_category_ name	Entity	Device category name associated with the entity in the event.
%_class_id	Entity	Device class ID associated with the entity in the event.
%_class_name	Entity	Device class description associated with the entity in the event.
%_parent_id	Entity	For component devices, the device ID of the parent device.
%_parent_ name	Entity	For component devices, the name of the parent device.
%_root_id	Entity	For component devices, the device ID of the root device.
%_root_name	Entity	For component devices, the name of the root device.
%1 (one)	Event	Entity type. Possible values are:
		0. Organization
		• 1. Device
		• 2. Asset
		• 4. IP Network
		• 5. Interface
		• 6. Vendor
		7. Account
		8. Virtual Interface
		9. Device Group
		• 10. IT Service
		• 11. Ticket
%2	Event	Sub-entity type.
		Possible values for organizations are:
		• 9. News feed
		Possible values for devices are:
		• 1. CPU
		• 2. Disk
		• 3. File System
		• 4. Memory

Variable	Source	Description
		• 5. Swap
		6. Component
		• 7. Interface
		• 9. Process
		• 10. Port
		• 11. Service
		12. Content
		• 13. Email
%4	Event	Text string of the user name that cleared the event.
%5	Event	Date/time when event was deleted.
%6	Event	Date/time when event became active.
%7	Event	Event severity (1-5), for compatibility with previous versions of SL1. 1=critical, 2=major, 3=minor, 4=notify, 5=healthy.
		NOTE: When referring to an event, %7 represents severity (for previous versions of SL1). When referring to a ticket, %7 represents the subject line of an email used to create a ticket.
%с	Event	Event counter
%d	Event	Date/time when last event occurred.
%D	Event	Date/time of first event occurrence.
%е	Event	Event ID
%Н	Event	URL link to event
%M	Event	Event message
%s	Event	severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.
%S	Event	Severity (HEALTHY - CRITICAL)
%_user_note	Event	Current note about the event that is displayed on the Events page.
%x	Event	Entity ID
%X	Event	Entity name
%у	Event	Sub-entity ID
%Y	Event	Sub-entity name
%Z	Event	Event source (Syslog - Group)
%z	Event	Event source (1 - 8)
%_ext_ticket_ref	Event	For events associated with an external Ticket ID, this variable contains the external Ticket ID.
%3	Event Policy	Event policy ID
%E	Event Policy	External ID from event policy

Variable	Source	Description
%f	Event Policy	Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one)=stateful; 0 (zero)=not stateful.
%G	Event Policy	External Category
%R	Event Policy	Event policy cause/action text
%_event_policy_ name	Event Policy	Name of the event policy that triggered the event.
%В	Organization	Organization billing ID
%b	Organization	Impacted organization
%С	Organization	Organization CRM ID
%o (lowercase "oh")	Organization	Organization ID
%O (uppercase "oh")	Organization	Organization name
%r	System	Unique ID / name for the current SL1 system
%7	Ticket	Subject of email used to create a ticket. If you specify this variable in a ticket template, SL1 will use the subject line of the email in the ticket description or note text when SL1 creates the ticket.
		NOTE: When referring to a ticket, %7 represents the subject line of an Email used to create a ticket. When referring to an event, %7 represents severity (for previous versions of SL1).
%t	Ticket	Ticket ID
%J	Ticket	Description field from the SL1 ticket.

Appendix

B

Configuring Windows Servers for Monitoring with PowerShell

Overview

The following sections describe how to configure Windows Server 2022, 2019, 2016, 2012, or 2012 R2 for monitoring by SL1 using PowerShell:

This chapter covers the following topics:

Prerequisites	47
Configuring PowerShell	47
Step 1: Configuring the User Account for the ScienceLogic Platform	48
Step 2: Configuring a Server Authentication Certificate	52
Step 3: Configuring Windows Remote Management	56
Step 4: (Optional) Configuring a Windows Management Proxy	85
Step 5: (Optional) Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	87
Optional PowerShell CLI Parameters	87

Prerequisites

Before configuring PowerShell, ensure the following:

- Forward and Reverse DNS should be available for the target Windows server from the SL1 Data Collector. Port 53 to the domain's DNS server should thus be available.
- When using an Active Directory user account as the SL1 credential, port 88 on the Windows Domain Controller, for the Active Directory domain, should be open for Kerberos authentication.
- If encrypted communication between the SL1 Data Collector and monitored Windows servers is desired, port 5986 on the Windows server should be open for HTTPS traffic. If unencrypted communications is being used, then port 5985 on the Windows server should be opened for HTTP traffic
- If multiple domains are in use, ensure that they are mapped in the [domain_realm] section of the Kerberos krb5.conf file on the Linux operating system of the SL1 collector appliance.

Configuring PowerShell

To monitor a Windows Server using PowerShell Dynamic Applications, you must configure the Windows Server to allow remote access from SL1. To do so, you must perform the following general steps:

1. Configure a user account that SL1 will use to connect to the Windows Server. The user account can either be a local account or an Active Directory account.

TIP: For ease of configuration, ScienceLogic recommends using an Active Directory account that is a member of the local Administrators group on the Windows Server.

- Configure a Server Authentication Certificate to encrypt communication between SL1 and the Windows Server.
- 3. Configure Windows Remote Management.
- 4. Optionally, configure a Windows server as a Windows Management Proxy.

NOTE: If you are configuring multiple Windows servers for monitoring by SL1, you can apply these settings using a Group Policy.

5. Optionally, you can *increase the number of PowerShell Dynamic Applications that can run simultaneously* against a single Windows server.

Step 1: Configuring the User Account for the ScienceLogic Platform

To enable SL1 to monitor Windows servers, you must first configure a user account on a Windows Server that SL1 can use to make PowerShell requests. You will include this user account information when creating the PowerShell credential that SL1 uses to collect data from the Windows Server.

To configure the Windows Server user account that SL1 can use to make PowerShell requests, complete one of the following options:

- Option 1: Create an Active Directory Account with Administrator access
- Option 2: Create a local user account with Administrator access
- Option 3: Create a non-administrator user account

TIP: For ease-of-configuration, ScienceLogic recommends creating an Active Directory user account.

After creating your Windows Server user account, depending on your setup and the servers you want to monitor, you might also need to configure the user account for remote PowerShell access to the following server types:

- Microsoft Exchange Server
- Hyper-V Servers

Option 1: Creating an Active Directory Account with Administrator Access

For each Windows server that you want to monitor with PowerShell or WinRM, you can create an Active Directory account that is a member of the local Administrators group on each server. For instructions, consult Microsoft's documentation. On Windows Domain Controller servers, you can use a domain account that is not in the Domain Administrators group by following the configuration instructions for Option 3: Creating a Non-Administrator User Account.

After creating your Active Directory account:

- If you use SL1 to monitor Microsoft Exchange Servers, you must configure the user account for remote PowerShell access to Microsoft Exchange Server.
- If you use SL1 to monitor Hyper-V Servers, you must configure the user account for remote PowerShell
 access to the Hyper-V Servers.
- Otherwise, you can skip the remainder of this section and proceed to Step 3.

Option 2: Creating a Local User Account with Administrator Access

If you have local Administrator access to the servers you want to monitor and are monitoring Windows Server 2016 or Windows Server 2012, you can alternatively create a local user account with membership in the Administrators group instead of an Active Directory account. For instructions, consult Microsoft's documentation.

WARNING: This method does not work for Windows Server 2008.

After creating your local user account with Local Administrator access:

- If you use SL1 to monitor Microsoft Exchange Servers, you must configure the user account for remote PowerShell access to Microsoft Exchange Server.
- If you use SL1 to monitor Hyper-V Servers, you must configure the user account for remote PowerShell access to the Hyper-V Servers.
- Otherwise, you can skip the remainder of this section and proceed to Step 2.

Option 3: Creating a Non-Administrator User Account

If you do not have Local Administrator access to the servers that you want to monitor with PowerShell or WinRM, or if the monitored Windows server is a Domain Controller that will not be in the local Administrators group, then you must first create a domain user account or create a local user account on the Windows Server. For instructions, consult Microsoft's documentation.

After creating your domain user account or local user account:

- You must configure the Windows servers to allow that non-administrator user access. To do so, follow the steps in this section.
- If you use SL1 to monitor Microsoft Exchange Servers, you must also configure the user account for remote PowerShell access to Microsoft Exchange Server.
- If you use SL1 to monitor Hyper-V Servers, you must also configure the user account for remote PowerShell access to the Hyper-V Servers.

To configure Windows Servers to allow access by your non-administrator user account:

1. Start a Windows PowerShell shell with Run As Administrator and execute the following command:

winrm configsddl default

- 2. On the **Permissions for Default** window, click the **[Add]** button, and then add the non-administrator user account.
- 3. Select the Allow checkbox for the **Read (Get, Enumerate, Subscribe)** and **Execute (Invoke)** permissions for the user, and then click **[OK]**.
- 4. Access the Management console. To do this:
 - In Windows Server 2016 and 2012, right-click the Windows icon, click [Computer Management], and then expand [Services and Applications].
- 5. Right-click on [WMI Control] and then select Properties.
- 6. On the WMI Control Properties window, click the [Security] tab, and then click the [Security] button.
- 7. Click the [Add] button, and then add the non-administrator user or group in the Select Users, Service Accounts, or Groups dialog, then click [OK].

- 8. On the **Security for Root** window, select the user o group just added, then in the **Permissions** section at the bottom of the window, select the **Allow** checkbox for the Execute Methods, Enable Account, and Remote Enable permissions.
- 9. Under the **Permissions** section of the **Security for Root** window, click the **[Advanced]** button.
- 10. In the Advanced Security Settings window, double-click on the user account or group you are modifying.
- 11. On the **Permission Entry** window, in the **Type** field, select Allow.
- 12. In the Applies to field, select This namespace and subnamespaces.
- Select the Execute Methods, Enable Account, and Remote Enable permission checkboxes, and then click [OK] several times to exit the windows opened for setting WMI permissions.
- 14. Restart the WMI Service from services.msc.

NOTE: To open services.msc, press the Windows + R keys, type "services.msc", and then press Enter.

- 15. If this is a member server, go to the Management console, go to System Tools > Local Users and Groups > Groups. Right-click on *Performance Monitor Users*, then select *Properties*.
- 16. If this is on a domain controller, go to the Server Manager, go to the Tools menu, and click Active Directory Users and Computers. Locate the Builtin folder. Inside the Builtin folder right-click Performance Monitor Users, and then select Properties.
- 17. On the Performance Monitor Users Properties window, click the [Add] button.
- 18. In the **Enter the object names to select** field, type the non-administrator domain user or group name, and then click **[Check Names]**.
- 19. Select the user or group name from the list and then click **[OK]**.
- 20. In the Performance Monitor Users Properties window, click [OK].
- 21. Perform steps 15-20 for the **Event Log Readers** user group and again for the **Distributed COM Users** user group, the **Remote Management Users** user group, and if it exists on the server, the **WinRMRemoteWMIUsers**_____user group.
- 22. If you intend to use encrypted communications between the SL1 collector host and your monitored Windows servers, each Windows server must have a digital certificate installed that has "Server Authentication" as an Extended Key Usage property. You can create a self-signed certificate for WinRM by executing the following command:

\$Cert = New-SelfSignedCertificate -CertstoreLocation
Cert:\LocalMachine\My -DnsName "myHost"

24. Add an HTTPS listener by executing the following command:

```
New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address * -
CertificateThumbPrint $Cert.Thumbprint -Force
```

NOTE: This command should be entered on a single line.

25. Ensure that your local firewall allows inbound TCP connections on port 5986 if you are going to use encrypted communications between the SL1 collector(s) and the Windows server, or port 5985 if you will be using unencrypted communications between the two. You may have to create a new rule on Windows Firewall if one does not already exist.

Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server

If you use SL1 to monitor Microsoft Exchange Servers:

- 1. Follow the steps in the section Configuring the User Account for SL1.
- 2. Add the new user account to the "Server Management" Exchange security group in Active Directory.
- 3. The user account will then be able to connect to the relevant WinRM endpoint to use cmdlets installed with the Exchange Management Shell. For example, this will give the user account access to the cmdlet "Get-ExchangeServer".

Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers

To use PowerShell Dynamic Applications to monitor a Hyper-V server, you must:

- Create a user group in Active Directory
- Add the user account you will use to monitor the Hyper-V server to the group
- Set the session configuration parameters on the Hyper-V Server
- Set the group permissions on the Hyper-V Server
- Create a PowerShell credential using the new user account

Creating a User Group and Adding a User in Active Directory

To create a group in Active Directory and add a user:

- 1. In Active Directory, in the same DC as the Hyper-V host you want to monitor, in the OU called **Users**, create a group. For example, we called our group **PSSession Creators**.
- 2. Add a user that meets the requirements for monitoring a Windows server via PowerShell to the group. This is the user that you will specify in the PowerShell credential.

NOTE: For details on using Active Directory to perform these tasks, consult Microsoft's documentation.

Setting the Session Configuration Parameters and Group Permissions

To set the Session Configuration and the Group Permissions on the Hyper-V Server:

- 1. Login to the Hyper-V server.
- 2. Open a PowerShell session. Enter the following command:

Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell

- 3. When prompted, select **A**.
- 4. The **Permissions** dialog appears.
- 5. In the **Permissions** dialog, supply values in the following fields:
 - Group or user names. Select the name of the group you created in Active Directory.
 - Permissions for group. For Full Control (All Operations), select the Allow checkbox.
- 6. Click the **[OK]** button.

Creating a PowerShell Credential

To create a PowerShell credential using the new user account, follow the instructions in the Creating a *PowerShell Credential* section.

Optional: Configuring the User Account for Access to Windows Failover Cluster

To configure Windows Servers to allow access to your Windows Failover Cluster:

1. Start a Windows PowerShell shell with Run As Administrator and execute the following command:

'Grant-ClusterAccess -User <domain>\<user> -ReadOnly'

Step 2: Configuring a Server Authentication Certificate

ScienceLogic highly recommends that you encrypt communications between SL1 and the Windows Servers you want it to monitor.

If you have created a **local account on the Windows Server that uses Basic Auth** and that account will allow communication between SL1 and the Windows server, the best practice for security is to enable HTTPS to support encrypted data transfer and authentication. To do this, you must configure WinRM to listen for HTTPS requests. This is called configuring an HTTPS listener.

NOTE: For details on configuring WinRM on your Windows servers to use HTTPS, see <u>https://support.microsoft.com/en-us/help/2019527/how-to-configure-winrm-for-https.</u>

The sections below describe how to configure a Server Authentication Certificate on the Windows Server. This is only one task included in configuring an HTTPS listener. However, not all users need to configure a Server Authentication Certificate. You can find out if your Windows computer has a digital certificate installed for Server Authentication by running 'Get-ChildItem -Path Cert:\LocalMachine\My -EKU "*Server Authentication*"' from a PowerShell command shell.

To support encrypted data transfer and authentication between SL1 and the servers, one of the following must be true:

- Your network *includes a Microsoft Certificate server*. In this scenario, you should work with your Microsoft administrator to get a certificate for your Windows Server instead of configuring a self-signed Server Authentication Certificate. You can skip this section and proceed to Step 3.
- Your network **does not include a Microsoft Certificate server**. In this scenario, you must configure a selfsigned Server Authentication Certificate on the Windows Server that you want to monitor with SL1 using one of the following methods:
 - Option 1: Use the Microsoft Management Console.
 - **Option 2**: If your Windows Server includes Windows Software Development Kit (SDK), you can use the makecert tool.
 - **Option 3:** If you are running PowerShell 4.0 or later, you can use the New-SelfSignedCertificate and Export-PfxCertificate commands.

NOTE: If you have created an Active Directory user account on the Windows Server to allow communication between SL1 and the server, Active Directory will use Kerberos and AES-256 encryption to ensure secure authentication.

Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate

To use the Microsoft Management Console to create a self-signed certificate:

- 1. Log in to the Windows Server that you want to monitor with SL1.
- 2. In the Start menu search bar, enter "mmc" to open a Microsoft Management Console window.

3. Select [File], then Add/Remove Snap-Ins. The Add or Remove Snap-ins window is displayed:

Certificates Microsoft Cor Component Services Microsoft Cor Computer Managem Microsoft Cor Device Manager Microsoft Cor Disk Management Microsoft Cor Event Viewer Microsoft Cor Folder Microsoft Cor Group Policy Object Microsoft Cor IP Security Monitor Microsoft Cor Link to Web Address Microsoft Cor		Move Up Move Down
---	--	----------------------

4. In the **Available snap-ins** list, select Certificates.

5. Click the [Add >] button. The Certificates snap-in window is displayed:

Certificates snap-in	×
Certificates snap-in This snap-in will always manage certificates for: My user account Service account Computer account	
	< Back Finish Cancel

- 6. Select Computer account.
- 7. Click the [Next >] button.
- 8. Click the [Finish] button.
- 9. In the Add or Remove Snap-ins window, click the [OK] button.
- 10. In the left pane of the **Microsoft Management Console** window, navigate to Console Root > Certificates (Local Computer) > Personal.
- 11. Right-click in the middle pane and select *All Tasks* > *Request New Certificate...*. The **Certificate Enrollment** window is displayed.
- 12. Click the [Next] button. The Select Certificate Enrollment Policy page is displayed.
- 13. Select Active Directory Enrollment Policy.
- 14. Click the **[Next]** button. The **Request Certificates** page is displayed.
- 15. Select the **Computer** checkbox.
- 16. Click the **[Enroll]** button.
- 17. After the certificate is installed, click the [Finish] button.

Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate

If your Windows system includes Windows Software Development Kit (SDK), you can use the MakeCert tool that is included in the kit to create a self-signed certificate. For information on the MakeCert tool, or for details about creating a self-signed certificate with MakeCert and installing the certificate in the Trusted Root Certificate Authorities store, see the Microsoft documentation.

Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate

If your Windows system includes PowerShell 4.0 or later, you can use the following PowerShell commands to create a self-signed certificate:

- You can use the **New-SelfSignCertificate** command to create a self-signed certificate. For information on **New-SelfSignCertificate**, see the Microsoft documentation.
- You can use the **Export-PfxCertificate** command to export the private certificate. For information on the **Export-PfxCertificate**, see the Microsoft documentation.

Step 3: Configuring Windows Remote Management

To provide SL1 remote access to the Windows Servers you want to monitor, you must configure Windows Remote Management.

NOTE: This step is required regardless of the user account type that SL1 will use to connect to the Windows Server.

There are three ways to configure Windows Remote Management:

- Option 1: Use the script provided by ScienceLogic.
- Option 2: Manually perform the configuration.
- Option 3: Use a group policy.

Option 1: Using a Script to Configure Windows Remote Management

ScienceLogic provides a PowerShell script in a .zip file in the PowerPack download folder that automates configuration of Windows Remote Management and permissions required for the user account that will be used in the SL1 credential. The script configures all of the base Windows permissions required, except for opening up Windows Firewall ports for HTTP and/or HTTPS traffic. The configuration performed by the script is useful primarily for running collection with the Microsoft: Windows Server, Microsoft: Windows Server Event Logs, and Microsoft: SQL Server Enhanced PowerPacks. (Microsoft: SQL Server Enhanced requires further instance-specific permissions. See the Monitoring SQL Servers manual for more information.

To use the PowerShell script, perform the following steps:

- When you download the Microsoft: Windows Server PowerPack from the <u>ScienceLogic Support</u> site, a .zip file for the WinRM Configuration Wizard Script (winrm_configuration_wizard.ps1) will be in the folder with the PowerPack's EM7PP file.
- 2. Unzip the downloaded file.
- 3. Using the credentials for an account that is a member of the Administrator's group, log in to the Windows server you want to monitor. You can log in directly or use Remote Desktop to log in.
- 4. Copy the PowerShell script named **winrm_configuration_wizard** to the Windows server that you want to monitor with SL1.
- 5. Right-click on the PowerShell icon and select Run As Administrator.
- 6. At the PowerShell prompt, navigate to the directory where you copied the PowerShell script named **winrm_ configuration** wizard.
- 7. At the PowerShell prompt, enter the following to enable execution of the script:

```
Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process -Force
```

NOTE: The execution policy setting persists only during the current PowerShell session.

8. After the warning text, select Y.

NOTE: If your Windows configuration requires further steps to allow execution of the script, PowerShell will display prompts. Follow the prompts.

9. To run the script with interactive dialogs, enter the following at the PowerShell prompt:

.\winrm_configuration_wizard.ps1 -user <domain>\<username>

NOTE: If you have run the script previously and set HTTPS listeners, make sure you have deleted any previous HTTPS listeners with the following command: winrm delete winrm/config/Listener?Address=*+Transport=HTTPS

The user account you wish to use for SL1 collection must be specified with the <u>-user</u> commandline argument regardless of other arguments used. You can obtain the full help for the PowerShell configuration script by entering the following:

help .\winrm configuration wizard.ps1 -full

The most common way to run the script is silently:

```
.\winrm_configuration_wizard.ps1 -user <domain>\<username> -
silent
```

NOTE: If you have multiple certificates installed on your server, running the script with the -silent flag will by default use the first certificate it encounters for your HTTP/HTTPS listeners. To set a specific certificate, run the script without the -silent flag and use the WinRM Installation Wizard.

10. If you start the script without using the -silent command-line argument, the WinRM Installation Wizard modal appears. Click [OK].

WinRM Installation Wizard				
This program will configure Windows Remote Management on your Windows Server, permissions to use WMI, query performance counters and event logs. It will ask a series of questions to determine the preferred security settings and will display your choices at the end. Configuration changes will not be made until the end of the wizard. Before beginning, here are your current settings: Basic Authentication = True Kerberos Authentication = True Allow Unencrypted WinRM Traffic = True Maximum WinRM Requests = 300 HTTP Port = 5985 HTTPS Port = 5986				
NOTE: This wizard cannot override settings applied by Group Policy (GPO). To overwrite those settings, please contact a system administrator.				
Click OK to Continue.				
OK Cancel				

11. The Windows Account Type modal appears. Select the appropriate choice for your environment.



12. The Set Encryption Policy modal appears. Select the appropriate choice for your environment.



- Click YES to us only encrypted data. Click Yes to configure an HTTPS listener for using encrypted communications between the SL1 collectors and the Windows server. Setting up an HTTPS listener requires a digital certificate with Server Authentication EKU to be available on the server. For information on creating a self-signed certificate, see Configuring a Server Authentication Certificate.
- Click NO to allow unencrypted data. For communication between SL1 collectors and the Windows server, if unencrypted traffic is allowed, an HTTP listener will be configured for communication.
- 13. The Change Max Requests modal appears. Click [Yes].

Change Max Requests ×
This host allows 300 WinRM requests at one time. Do you want to change this value of maximum requests? Click YES to edit the maximum number of requests. Click NO to leave the maximum number of requests unchanged.
Yes No

14. The **Change IdleTimeout** modal appears. If you would like to change the value of **IdleTimeout**, click **[Yes]**. If you click **[Yes]**, the **Set WinRM IdleTimeout** modal appears. Enter the new value in the field and click **[OK]**.



15. The **Set Ports for WinRM Traffic** modal appears, and it shows the current settings for the HTTP and HTTPS ports. If you want to make a change to these, click **[YES]**; otherwise, click **[NO]** to continue.

Set Ports for WinRM Traffic X
Your current HTTP port for Windows Remote Management is set to 5985, and the HTTPS port for Windows Remote Management is set to 5986. Do you want to modify these ports for WinRM traffic use? Click YES to edit your HTTP/HTTPS ports. Click NO to continue to the next page.
Yes No

16. Choose which port values you would like SL1 to use when communicating with the Windows server.

Set H	_ D X	
New HTTP port:	5985	[
New HTTPS port:	5986	
		ОК

17. The **Set HTTPS Thumbprint** modal appears. Enter the information for your certificate thumbprint, which is used to create an HTTPS listener, then click **[OK]**.

Set HTTPS Thumbprint
To setup the WinRM HTTPS listener, you will need to use a certificate thumbprint Run the PowerShell cmdlet below on this Windows computer to get your existing certificate thumbprints:
Get-ChildItem -Path Cert:\LocalMachine\My
Then press OK to continue.
Enter your certificate thumbprint here
ОК

- **NOTE:** If the certificate structure for your certificate thumbprint is incomplete or incorrect, an error message appears indicating that the WinRM client cannot process the request. If you think you made an error, click **[OK]** and try to correct it. Otherwise, contact a system administrator for help.
- 18. The Confirm Settings modal appears. If the settings are as you specified, click [OK].

Confirm Settings	x
Please confirm your settings: Authentication Type: Kerberos (for Active Directory) Encryption Policy: Restrict Unencrypted Data Maximum Connections: 300 HTTP Port: 5985 HTTPS Port: 5986 Certificate Thumbprint: 2B496C35B42415356AC63B34D02C909076B16F20	
Click OK to update WinRM settings. Click CANCEL to quit wizard (settings will not be updated).	
OK Cancel	

19. The Complete modal appears. If the settings are correct, click [OK].

Complete	x				
Your Windows Remote Management settings have been updated. To view them when necessary, you can run the following commands in a PowerShell console: winrm get winrm/config/service winrm e winrm/config/listener					
Your updated WinRM settings are detailed below:					
Basic Authentication = true Kerberos Authentication = true Allow Unencrypted WinRM Traffic = true Maximum WinRM Requests = 500 HTTP Port = 5985 HTTPS Port = 5986 Certificate Thumbprint = 4705BE1B838CDCA76BB1993BE3307C85DF61C93F The WinRM service will be restarted after this dialog is closed.					
ОК Са	ncel				

20. Exit the PowerShell session.

Option 2: Manually Configuring Windows Remote Management

To configure a Windows server for monitoring via PowerShell directly, perform the following steps:

- 1. Log in to the server with an account that is a member of the local Administrators group, or a Domain Administrator's account if on a Windows server with the Domain Controller role installed.
- Ensure that your local firewall allows inbound TCP connections on port 5986 if you are going to use encrypted communications between the SL1 Data Collectors and the Windows server, or port 5985 if you will be using unencrypted communications between the two. You may have to create a new rule on Windows Firewall if one does not already exist.
- 3. Right-click on the PowerShell icon in the taskbar or the Start menu, and select Run as Administrator.
- 4. Execute the following command:

Get-ExecutionPolicy

5. If the output is "Restricted", execute the following command:

```
Set-ExecutionPolicy RemoteSigned
```

- 6. Enter "Y" to accept.
- 7. Execute the following command:

winrm quickconfig

- 8. Enter "Y" to accept.
- 9. If you are configuring this Windows server for encrypted communication, execute the following command:

winrm quickconfig -transport:https

- 10. Enter "Y" to accept.
- 11. Execute the following command:

winrm get winrm/config

The output should look like this (additional lines indicated by ellipsis):



12. In the Service section, if the parameter Allow Remote Access is set to false, execute the following command:

NOTE: This setting does not appear for all versions of Windows. If this setting does not appear, no action is required.

Set-Item WSMan:\Localhost\Service\AllowRemoteAccess -value true

13. In the Winrs section, if the parameter **AllowRemoteShellAccess** is set to false, execute the following command:

Set-Item WSMan:\Localhost\Winrs\AllowRemoteShellAccess -value true

14. If you are configuring this Windows server for unencrypted communication and the parameter **AllowUnencrypted** (in the Service section) is set to *false*, execute the following command:

Set-Item WSMan:\Localhost\Service\AllowUnencrypted -value true

15. If you are configuring this Windows server for unencrypted communication, verify that "HTTP = 5985" appears in the DefaultPorts section.

NOTE: ScienceLogic recommends using encrypted communication, particularly if you are also using an Active Directory account. Using an Active Directory account for encrypted authentication enables you to use Kerberos ticketing for authentication.

- If you are configuring this Windows server for encrypted communication, verify that "HTTPS = 5986" appears in the DefaultPorts section.
- 16. If you are using an Active Directory account to communicate with this Windows server and in the Auth section, the parameter **Kerberos** is set to *false*, execute the following command:

Set-Item WSMan:\Localhost\Service\Auth\Kerberos -value true

NOTE: ScienceLogic recommends using an Active Directory account.

17. If you are using a local account to communicate with this Windows server and in the Auth section, the parameter **Basic** is set to false, execute the following command:

Set-Item WSMan:\Localhost\Service\Auth\Basic -value true

18. IdleTimeout is set to 7200000 milliseconds (2 hours) by default. If an issue occurs with scheduled PowerShell monitoring and a process remains on a Windows device, it will therefore remain for up to 2 hours before being removed. To reduce the IdleTimeout and have Windows shut down idle WinRM processes after a shorter time period, execute the following command:

```
winrm s winrm/config/winrs '@{IdleTimeout="600000"}'
```

This command will change the timeout to 10 minutes (600000 ms).

NOTE: When changing IdleTimeout, ensure that no other applications or utilities need a higher timeout for WinRM sessions.

Option 3: Using a Group Policy to Configure Windows Remote Management

You can use a group policy object (GPO) to configure the following Windows Remote Management settings on Windows Server 2012 or Windows Server 2016:

- A registry key to enable Local Account access to Windows Remote Management
- Firewall rules
- Certificates
- HTTP and HTTPS listeners, including authentication and encryption settings
- Service start and recovery settings

To create the group policy object, perform the following steps:

- 1. Log in to the CA server as an administrator.
- 2. Right-click on the PowerShell icon in the taskbar and select Run as Administrator.
- 3. At the PowerShell prompt, use the change directory (CD) command to navigate to a folder where you can create new files.
- 4. Save the root Certification Authority certificate to the local directory by executing the following command:

certutil.exe -ca.cert ca_name.cer

C:\Users\EM7Admin\Documents>certutil -ca.cert ca_name.cer CA cert[0]: 3 Valid CA cert[0]: BEGIN CERTIFICATE MIIDpTCCA02gAwIBAgIQHAmGt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ MRUWEwYKCZImiZPyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/IsZAEZFgINU1RMMDEy UjIxJTAjBgNVBAMTHE1TVEwwMTJSMilUTDAxMIJyLURDLTAxLUNBLTEwHhcMMTOw NDEIMTYINTQlwhchMrkwNDEIMTCwNTQIWjBZMRUWEWYKCZImiZPyLGQBGRYFbG9j YWwxGTAXBgoJkiaJk/IsZAEZFgINU1RMMDEyUjIXJTAjBgNVBAMTHE1TVEwwMTJS MilUTDAxMIIyLURDLTAxLUNBLTEwggEiMAOGCSqGSIB30QEBAQUAA41BDAwaggEK AAIBAQCmsPONZQIJA5pxqI9ZrofUCZFaa6IS5pG0JWiit+risfY4g1RqVFvc3mmQK TKO0WqeiuNAuh11fYFIDs0RNSOFHgUNgrasdrvugSPL/V23VDH2dqjHaDd6azY 7CcWfD6uu3oV0aZU9Sgt4HEymPU14QkGuZ1n4UTX1depCA0N37oyNkOQg0JLUutp Q816YdKbYaU0WwyKnvS0osQpqAFSdFW7rgt80bIXf9F2n13yuwogEpfeq+E8UH4 JGmtOpSZk7hsFDMxXkvRhdPugH7rIONGia0xy0VuVQffiK748LiE/QveX73wBo 7XLVsMSbWNo9SNxrf8/hiUTJ0pOnAgMBAAGjaTBnMBMGCSSGAQQBgjCUAgQGHgQA QWBBMA4GAlUdDwEB/wQEAwIBbjAPBgNVHMMBAf8EBTADAQH/MBOGALUdDgQWBBR9 QjsBuyfqH2Prforx0g/291ozWDAQBgkrBgEEAYI3FQEEAWIBADANBgkqNiG9SNOB AQUFAAOCAQEATSkQpaWpO6iOIT1398051HbT1n6AV/GiZURNRAWLKAxguEdha R/+1RL/qkNXJeqjpDAFsz22EIvei0KVCIbwEXeKePZnQG1ujr2FLRbUWt+oA0/ES G4rxLTw//q4s0HKSJmRYCXJ0zDK8zFH0ZADv/Trrn6CEMxYaB6quQFzTQmSMbUK troOgF270W29LG2E7TNn10X0xKEQ1QFR8EPFkctY72/+bVFV8V3YJjdAm/42g 4hjdX04PGIADj0Bg2srX+01tx8mAMjA/UdMg2kvU0m0dP6h17BqJJ08umJxPmfQI vWF1gNeTUNHfTYUJBERZQhLhK6rkAnHw== END CERTIFICATE CertUtil: -ca.cert command completed successfully. C:\Users\EM7Admin\Documents>_	

TIP: You will import this certificate into the new group policy in step 21.

- 5. Exit the command prompt.
- 6. Log in to a domain controller in your Active Directory forest and navigate to the System Manager dashboard.
- 7. Click the **Tools** menu, then select Group Policy Management.

E.	Server Manager	- 0 ×
Contraction Contracti	Configure this local server	
 DNS ■ File and Storage Services ▷ ■ IIS 	2 Add roles and features 3 Add other servers to manage 4 Create a server group LEARN MORE	Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management Internet Information Services (IIS) Manager IGCSI Initiator Local Security Policy ODBC Data Sources (32-bit) DRDR DR DR DR DR DR DR
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers total: 1 AD CS 1 Manageability AD DS 1 Events Services Performance BPA regultr	ODBC Data Sources (64-bit) Performance Monitor Resource Monitor Services Services Services Services Services Services Services Windows Firewall with Advanced Security Performance Windows Memory Diagnostic

8. On the **Group Policy Management** page, in the left panel, right-click the domain name where you want the new group policy to resideand then select Create a *GPO* in this domain and Link it here.

		Group Policy M	anagement		_ 0 ×	
Window Help					- 5	
Q 7 1						
ment	Group Policy	Objects in MSTL012R2.local				
A Forest: MSTL012R2.local A Domains A MSTL012R2 local		Contents Delegation				
		•	GPO Status	WMI Filter	Modfied	
Create a GPO in this domain	, and Link it here	trollers Policy	Enabled	None	3/19/201	
Link an Existing GPO		Cy Management Policy	Enabled All settings disabled	None	2/4/2014	
Block Inheritance		Hundgenent roley	All settings disabled	None	4/16/20	
Group Policy Modeling Wiza	ard					
New Organizational Unit						
Search						
Change Domain Controller						
Remove						
Active Directory Users and C	omputers					
New Window from Here						
Refresh						
Properties						
Help						
	Window Help Window Help Constant Create a GPO in this domain Link an Existing GPO Block Inheritance Group Policy Modeling Wizz New Organizational Unit Search Change Domain Controller Remove Active Directory Users and C New Window from Here Refresh Properties Help	Window Help	Window Help	Window Help	Window Help Intent Corterts Delegation Create a GPO in this domain, and Link it here Intent Link an Existing GPO Block Inheritance Group Policy Modeling Wizard New Organizational Unit Search Change Domain Controller Remove Active Directory Users and Computers Help	

9. In the left panel, right-click the new group policy and select *Edit*. The **Group Policy Management Editor** page for the new Windows Remote Management group policy appears.

4		Group Policy Ma	anagement		- 0 ×
📓 File Action View Wine	dow Help				- 5
Group Policy Management Group Policy Management Group Policy Management Market MSTL012R2.local Market MSTL012R2.local Market Management Policy PowerShell Remote Management Policy Market Management Policy Den Edit	Group Policy Objects in MSTL012R2.local Cortexts Delegation Name Default Domain Controllers Policy Default Domain Policy PowerShell Reintet Management Policy WinRM Policy WinRM Policy WinRM Policy	GPO Status Enabled Enabled Al settings disabled Enabled Mastering disabled	WMI Fiter None None None None	Modified 3/19/201 2/4/2014 4/17/201 4/17/201	
P i forcu Ent P i VM ✓ San P i Stas Stas Group Polic Group Polic Re Re Re Re	orced k Fnabled k Fnabled w Window from Here lete ete freh lp		, a source right desided		41020
		٤	н		×

 In the left panel, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > System Services. In the right panel, locate the Windows Remote Management (WS-Management) service. Right-click the service, then select Properties.

	Group Pol	icy Management Editor			- 0 ×
File Action View Help					
🗢 🔿 🙍 🗶 🗃 🗟 🖬					
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	Service Name		Startup	Permission	^
4 👰 Computer Configuration	User Access Logging Service		Not Defined	Not Defined	
⊿ 🦳 Policies	User Profile Service		Not Defined	Not Defined	
Software Settings	Virtual Disk		Not Defined	Not Defined	
⊿ 🚞 Windows Settings	Volume Shadow Copy		Not Defined	Not Defined	
Name Resolution Policy	W3C Logging Service		Not Defined	Not Defined	
Scripts (Startup/Shutdown)	Windows Audio		Not Defined	Not Defined	
A Security Settings	Windows Audio Endpoint Builder		Not Defined	Not Defined	
Account Policies	Windows Color System		Not Defined	Not Defined	
Local Policies	Windows Connection Manager		Not Defined	Not Defined	
Event Log	Windows Driver Foundation - User	mode Driver Framework	Not Defined	Not Defined	
Kestricted Groups	Windows Encryption Provider Host	Service	Not Defined	Not Defined	
Desister	Windows Error Reporting Service		Not Defined	Not Defined	
Eile Sustem	Windows Event Collector		Not Defined	Not Defined	
Wired Network (IEEE 802 3) Policies	Windows Event Log		Not Defined	Not Defined	
Windows Firewall with Advanced Security	Windows Firewall		Not Defined	Not Defined	
Network List Manager Policies	Windows Font Cache Service		Not Defined	Not Defined	
Wireless Network (IEEE 802.11) Policies	Windows Installer		Not Defined	Not Defined	
Public Key Policies	Windows Management Instrument	ation	Not Defined	Not Defined	
Software Restriction Policies	Windows Modules Installer		Not Defined	Not Defined	
Network Access Protection	Windows Process Activation Servic	e	Not Defined	Not Defined	
Application Control Policies	Windows Remote Management	(tananant)	Not Defined	Not Defined	
IP Security Policies on Active Directory (MSTL012F)	Windows Store Service (WSServi	Properties	Not Defined	Not Defined	
Advanced Audit Policy Configuration	Windows Time	Help	Not Defined	Not Defined	
Policy-based QoS	Windows Update	1.000	Not Defined	Not Defined	
Administrative Templates: Policy definitions (ADMX files)	WinHTTP Web Proxy Auto-Discove	ry Service	Not Defined	Not Defined	
Preferences	Wired AutoConfig	·	Not Defined	Not Defined	_
4 💰 User Configuration	WMI Performance Adapter		Not Defined	Not Defined	=
Policies	Workstation		Not Defined	Not Defined	
p Preferences	World Wide Web Publishing Servic	e	Not Defined	Not Defined	
					~

11. The Windows Remote Management (WS-Management) modal page appears. Select the Define this policy setting check box and the Automatic radio button, then click [OK].

<u>J</u>	Group Policy Management Editor	r		_ 0 ×
File Action View Help				
🗢 🔿 🙍 🗙 🗟 🗟 🖬 🖬				
WinRN Policy (TL012R-2-COLINSTL012R2.LOCAL] Policy WinRN Policy (TL012R-2-COLINSTL012R2.LOCAL] Policy Dolicies Software Settings MinRN Policy (TL012R-2-COLINSTL012R2.LOCAL] Policy Software Settings MinRN Policies Software Settings MinRN Policies MinRN Policies	Service Name User Access Logging Service User Profile Service VirtualTisk Virt	Startup Not Defined Not Defined Not Defined	Permission Not Defined Not Def	
 ▷ Preferences ⊿ ³ User Configuration ▷ ²⁰ Policies 	Wired AutoConfig	Not Defined Not Defined	Not Defined Not Defined	1
> Preferences	Workstation	Not Defined Not Defined	Not Defined Not Defined	

12. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security - LDAP > Inbound Rules. In the right panel, right-click and select New Rule.

File Action View Help	Profile o items to she	Enabled	Action w.	Override	Program	Local Address	Remot
Image: Software Settings Image: Software Settings Image: Software Settings <th>Profile b items to she</th> <th>Enabled ow in this view</th> <th>Action</th> <th>Override</th> <th>Program</th> <th>Local Address</th> <th>Remot</th>	Profile b items to she	Enabled ow in this view	Action	Override	Program	Local Address	Remot
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy ∧ ▲ Computer Configuration ∧ ▲ Dolicies Policies ▶ Olicies Software Settings ▲ Windows Settings ∧ ▲ Windows Settings ∧ ▲ Security (Statings) ∧ ▲ Security Settings ∧ ▲ Local Policies ∧	Profile b items to she	Enabled	Action w.	Override	Program	Local Address	Remot
b III Event Log Control Cont							
Inbound Rules New Kulc Outbound Rules Filter by Profile Connection Security Rules Filter by Sate Wireless Network (IEE BOS) Filter by Sate P Public Key Policies P Software Restriction Policies P Software Restriction Policies P Software Restriction Policies P Polic Key Policies P Refresh View Line up Icons P Policy-Dased QoS P Administrative Templates: Policy definitions (ADMX fr.v.	> > >						

13. The **New Inbound Rule Wizard** modal page appears. Click the **Predefined** radio button, select Windows *Firewall Remote Management* from the list, and then click **[Next]**.

J		Group Policy Man	agement Editor						- 0	x
tile Action	View Help									
WinRM P	2	New Inbound Rule Wizard	×	Profile	Enabled	Action	Override	Program	Local Address	Rem
⊿ 🛄 Po ▷ 📫	Rule Type Select the type of firewall rule	to create.		ems to she	ow in this vie	w.				
Þ	Steps:	What turns of rules would you like to create?								
4	 Rule Type Predefined Rules 	This get of the money of the creater								
	 Action 	Program Rule that controls connections for a program. Pot Rule that controls connections for a TCP or UDP port. Predefined:								
		Windows Firewall Remote Management	~							
		Rule that controls connections for a Windows experience. Custom Custom rule.								
¢		< Back Ne	kt > Cancel							

14. Select the Windows Firewall Remote Management (RPC) and Windows Firewall Remote Management (RPC-EPMAP) check boxes, then click **[Next]**.

J		G	roup Policy	Manageme	ent Editor							-	j x
File Action	View Help												
							1						
WinRM Pe	#	New Inbound Rule Wizard				×	Profile	Enabled	Action	Override	Program	Local Addres	Remot
⊿ 🛄 Po ▷ 🚞 ⊿ 🚞	Predefined Rules Select the rules to be created for t	this experience.					ems to sho	w in this view	Ν.				
Þ	Steps:												
4	Rule Type	Which rules would you like to create?											
	Predefined Rules	The following rules define network connectivity requi	rements for the s	selected predefir	ed group.								
	 Action 	Rules that are checked will be created. If a rule alreated the existing rule will be overwritten.	idy exists and is	checked, the co	intents of								
		Name	Rule Exists	Profile	Desc								
		Windows Firewall Remote Management (RPC	No	All	Inbou								
		Vindows Frewall Remote Management (RPC)	No	AI	Inbou								
		K III			>								
4 4 4		E	< Back	Next >	Cancel								

15. Select the Allow the connection radio button, then click [Finish].

	Group Policy Management Edit	or							X
RM Pe	New Inbound Rule Wizard	×	Profile	Enabled	Action	Override	Program	Local Address	Rem
Po Action Specify the action to be ta	ken when a connection matches the conditions specified in the rule.		ems to sho	ow in this vie	W.				
 Steps: Rule Type Predefined Rules Action 	What action should be taken when a connection matches the specified conditions? Image: Contract on the connection is the second with IPsec as well as those are not. Image: Contract on the connection is the second with IPsec as well as those are not. Image: Contract on the second with IPsec as well as those are not. Image: Connection is the second with IPsec as well as those are not. Image: Connection is the second with IPsec as well as the connection Second with the not. Image: Connection is the connection is the connection in the connection Second with the not. Image: Connection is the connection is the connection in the connection is the connecon is the connection is the connection is t								

16. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Automatic Certificate Request Settings. In the right panel, right-click and select New > Automatic Certificate Request.

	Group Policy Management Editor		
Action View Help			
	na in the statement	and the second sec	
Windows Settings Windows Settings Windows Settings Scripts (Startup/Shutdown) Scripts (Startup/Shutdown	Automatic Certificate Request	no items to show in this view. Automatic Certificate Request	

17. The Automatic Certificate Request Setup Wizard modal page appears. Click [Next].
| Automatic Certificate Request Setup Wizard | Group Policy Management Editor | - 0 X |
|---|--|-------|
| Welcome to the Automatic
Certificate Request Setup
Visual helps you set up automatic certificate requests
for computers.
Using advantic part of certificate removes, an administrator can
seedy which types of certificate can be automatically
requested by a computer.
To continue, click Next. | request There are no items to show in this view. | |
| < BitLocker Drive Encryption BitLocker Drive Encryption Network Unlock Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies Network Access Protection Application Control Policies BitLocker Drive Directory (MSTLD V M BitLocker Drive Directory (MSTLD V M Software Restriction Policies BitLocker Control Policies Software Restriction Policies Methods Software Restriction Policies Software Restrestriction Software Restriction Software Restriction | | |

18. Select the Computer certificate template. Click [Next], and then click [Finish].

Hatomatic certif	ficate Request Setup Wizard	Group Policy Mar	agement Editor		_ 0
ertificate Template The next time a computer logs on, a provided.	a certificate based on the template you select is		-		
A certificate template is a set of pre- computers. Select a template from the Certificate templates:	defined properties for certificates issued to he following list.		There are no items	to show in this view.	
Name	Intended Purposes				
Computer Domain Controller Enrollment Agent (Computer) IPSec	Client Authentication, Server Authentication Client Authentication, Server Authentication Certificate Request Agent IP security IKE intermediate				
< III	>				
		_			
	< Back Next > Cancel]			
BitLocker Drive BitLocker Drive Automatic Cert Trusted Root C Interprise Trust Interprise Trust Untursted Cert Outsust Cert	<pre></pre>	1			

19. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration
 > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root
 Certification Authorities. In the right panel, right-click and select Import.



20. The Certificate Import Wizard modal page appears. Click [Next].

J	Group Policy Management Editor			Ŀ	- 0 ×
File Action View Help					
	· · · · · · · · · · · · · · · · · · ·	·	Friendly News	Chatara	Contificante Te
Vindows Settings	🖉 🖉 Certificate Import Wizard	riew.	Friendly Name	Status	Certificate Te
Count Policies Event Log Event	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate stree. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. Store Location				
Encrypting File System Data Protection BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc	Current User O Local Machine				
Automatic Certificate Request Settings Trusted Root Certification Authorities Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Tusted Bench	To continue, dick Next.				
Software Restriction Policies Network Access Protection	Next Cancel				
Application Control Policies B IP Security Policies on Active Directory (MSTLO	< III				>

21. Browse to the Certification Authority certificate that you saved to your local directory in step 4, then click **[Next]**.



22. Select the **Place all certificates in the following store** radio button, then select the Trusted Root Certification Authorities certificate store and click **[Next]**.

	Group Policy Management Editor		- 0 X
Action View Help			
Windows Settings Mame Resolution Policy Scripts (Startup/Shutdown) Scripts (Startup	Certificate Import Wizard Certificate Store Certificate Store Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Place all certificates the certificate store based on the type of certificate. Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browne	ended Purposes Friendly Nam	e Status Certificate T
Intermediate Certification Authorities Intrusted Gentification Authorities Intrusted Gentificates Intrusted Gentificates Intrusted Gentificates Intrusted Gentificates Intrusted Gentification Policies Intermediate Access Protection Intermediate Deficies on Active Directory (MSTLC) Intermediate Directory (MSTLC	Nest Cancel		

23. Click [OK] to confirm that the certificate was successfully imported, and then click [Finish].

J	Group Policy Management Editor			- 0	x
File Action View Help					
▲ Windows Settings ▶ Manne Resolution Policy Scripts (Startup/Shutdown) ▲ Security Settings	€ 🦻 Certificate Import Wizard	ended Purposes Fr riew.	iendly Name Stat	us Certifica	ite T
 ▷ Account Policies ▷ a Local Policies ▷ a Event Log ▷ a Restricted Groups ○ System Services ▷ a Segistry ▷ a File System 	Completing the Certificate Import Wizard The certificate will be imported after you click Finish.				
J Windows Firewall with Advanced Security Windows Firewall with Advanced Security Network IUSK Manager Policies Wireless Network (IEEE 802.1) Policies Wireless Network (IEEE 802.1) Policies Dublic Key Policies Dublic Key Policies Dublic Key Policies Bercypting File System Data Protection BitLocker Drive Encryption BitLocker Drive Encryption Automatic Cardicate Benergit Cardicate	Tou have specified the following settings: Contract State State by User Content Certificate File Name C: Users (EM7Admin / Documents) ca_name.cer				
Trusted KoetTruicate request settings Trusted KoetTruicate not Authorities Intermediate Certification Authorities Trusted Publishers Untrusted Publishers Trusted People Trusted People Software Restriction Policies	Finish Cancel				
Original Control Policies Original Control Policies Original Control Policies Original Control Policies on Active Directory (MSTL0 Original Control Policies on Active Directory (MSTL0 Original Control Policies on Active Directory (MSTL0 Original Control Policies	v <				

24. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration
 Policies > Administrative Templates > Network > Network Connections > Windows Firewall
 > Domain Profile. In the right panel, right-click Windows Firewall: Define inbound port exceptions and select Edit.

	Group Pol	icy Management Editor			_ 0
Action View Help					
🔶 🙍 📷 🔽 📰 🔻					
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	🚊 Domain Profile				
Computer configuration	Windows Firewall: Define inbound	Setting		State	Comment
b Software Settings	port exceptions	🗄 Windows Firewall: Allow local progra	am exceptions	Not configured	No
Vindows Settings		🗄 Windows Firewall: Define inbound p	rogram exceptions	Not configured	No
Administrative Templates: Policy definitions (ADMX fi	Edit policy setting	🖹 🗈 Windows Firewall: Protect all networ	k connections	Not configured	No
Control Panel	Requirements:	📰 Windows Firewall: Do not allow exce	ptions	Not configured	No
4 Network	At least Windows XP Professional	📰 Windows Firewall: Allow inbound fil	e and printer sharing ex	Not configured	No
Background Intelligent Transfer Service (BITS)	with SP2	Windows Firewall: Allow ICMP except	tions	Not configured	No
BranchCache	0.10	Windows Firewall: Allow logging		Not configured	No
DirectAccess Client Experience Settings	Allows you to view and change	🗄 Windows Firewall: Prohibit notificati	ons	Not configured	No
DNS Client	the inbound port exceptions list	Windows Firewall: Allow local port e	xceptions	Not configured	No
Hotspot Authentication	defined by Group Policy. Windows	Windows Firewall: Define inbound	art excentions	Alot configured	No
Lanman Server	Firewall uses two port exception	Windows Firewall: Allow inbound	Edit	lot configured	No
Link-Laver Topology Discovery	lists: one is defined by Group	Windows Firewall: Allow inbound	Filter On	lot configured	No
Microsoft Peer-to-Peer Networking Services	defined by the Windows Firewall	Windows Firewall: Prohibit unica	Eilter Ontions	lot configured	No
A 📔 Network Connections	component in Control Panel.	Windows Firewall: Allow inhound	Part options	lot configured	No
⊿ Provide A Strategy A Strategy A A A A A A A A A A A A A A A A A A A			Re-Apply Filter	lot configured	140
Domain Profile	If you enable this policy setting,		All Tasks	•	
Standard Profile	you can view and change the		Help		
Network Connectivity Status Indicator	defined by Group Policy. To view		Theip		
Network Isolation	this port exceptions list, enable the				
Offline Files	policy setting and then click the				
QoS Packet Scheduler	Show button. To add a port,				
SNMP	syntax, click the Show button. In				
SSL Configuration Settings	the Show Contents dialog box				
TCPIP Settings	type a definition string that uses				
Windows Connect Now	the syntax format. To remove a				
Windows Connection Manager	port, click its definition, and then				
WLAN Service	definition, remove the current	/			
N 🛅 WWAN Service	definition from the list and add a				
III >	Extended / Standard /				

- 25. The Windows Firewall: Define inbound port exceptions modal page appears. Under Options, click [Show].
- 26. The **Show Contents** modal page appears. Enter the following values:

[Group Policy Management Editor	- 0
Action View H	Se Windows F	irewall: Define inbound port exceptions	
WinRM Policy (TL012	Windows Firewall: Define inbound port e	Coppions Previous Setting Next Setting	2
Computer Config	O Not Configured Comment:	∧ State	Comment
D Software S	Enabled	xceptions Not configured	No
Windows		am exceptions Not configured	No
🔺 📔 Administr	Supported on:	INCL VD. C. L. L. C.	NO
Contro	ALI	Show Contents	No
⊿ 🦲 Netwo		Show contents	No
	Options:	Not configured	No
Dir		Verine port exceptions: Not configured	No
DN	Defer and marking a	Value Not configured	No
🚞 Ho	Define port exceptions: Snow	5985:TCP:*tenabled:WSMan Not configured	No
🧾 Lar	Specify the port to open or block.	9986:TCP:*tenabled:WSMan tration exc Not configured	No
🧾 Lin	Custom	* exceptions Not configured	No
D 🧮 Mi	Syntax:	Iticast or Not configured	No
⊿ 🚞 Ne	<port>:<transport>:<scope>:<status>:<</status></scope></transport></port>	k exceptio Not configured	No
⊿ 📔	<port> is a decimal port number</port>		
	<transport> is either "TCP" or "UDP"</transport>		
🧮 Ne	<scope> is either "*" (for all networks) o</scope>		
Off	a comma-separated list that contains		
þ 🧾 Qa	any number or combination of these:	OK Carcel	
🧮 SN	IR addresses such as 10.0.0.1		
🚞 SSI	ir addresses, such as 10.0.0.1	also enable the "Windows Firewall: Allow local port exceptions"	
TC	Subnet descriptions, such as 10.2.3.0/2	policy setting.	
WI WI		If you disable this policy setting, the port exceptions list defined	
N M			
6 📑 W		OK Cancel Apply	

- 5985:TCP:*:enabled:WSMan
- 5986:TCP:*:enabled:WSMan
- 27. Click [OK], then click [OK] again.
- 28. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client. In the right panel, double-click the Allow Basic authentication setting.

	Group Policy Management Editor	_ 0 X
File Action View Help	Se Allow Basic authentication	
← ⇒ 2 🗊 🖻 🛛 🗊 🍸	Allow Basic authentication	Setting Next Setting
Smart Card Sound Recorder Syncy pour settings Tablet PC Tablet	Not Configured Comment: Enabled Disabled Supported on: At least Windows Vista Options: Help: Hel	Setting Next Setting International Internati
		OK Cancel Apply
< III > \Extended		
7 setting(s)		

29. Select the **Enabled** radio button, then click **[OK]**.

- 30. Repeat steps 28 and 29 for the Allow unencrypted traffic setting.
- 31. Double-click the **Trusted Hosts** setting. Select the **Enabled** radio button, enter an asterisk (*) in the **TrustedHostsList** field (under **Options**), and then click **[OK]**.

	Group Policy Management Editor	d x
File Action View Help	F Trusted Hosts	
← → 2 m → 2 m ▼ Smart Card Sound Recorder Sync your settings	Trusted Hosts Previous Setting Next Setting O Not Configured Comment: A	
Task Scheduler Task Scheduler Windows Calendar Windows Color System Windows Defender Windows Defender	C Enabled C Disabled Supported on: At least Windows Vista At least Windows Vista	
↓ Windows Strof Reporting manage ↓ Windows Strof Reporting manage ↓ Windows Strof Reporting Remote I ↓ Windows Logan Options Uses the I ↓ Windows Media Trustelf ↓ Windows Media Digital Rights Management If you en ↓ Windows Media Parente ↓ Windows Media Center ↓ Windows Messenger Trustelf ↓ Windows Messenger Gestinati ↓ Windows Reinbell The Winf ↓ Windows Reinbell The Winf ↓ Windows Remote Management (WinRM) Windows Update ↓ Windows Update palety at the parente work the palety at the states ↓ Windows Update meds to you must work blots loc ↓ Windows Lipdate meds to you must work blots loc	Options: Help: No TrustedHostsList: This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses the list specified in TrustedHostsList to determine if the destination host is a trusted entity. Image: The specified in TrustedHostsList to determine if the destination host is a trusted entity. Image: TrustedHostsList to determine if the destination host is a trusted entity. Configure the trusted hosts by a comma separated list If you enable this policy setting, the WinRM client uses the list sectified in TrustedHostsList to determine if the destination host is a trusted entity. The WinRM client uses this list when neither HTTPS how Kenters are used to authenticate the identity of the host. Image: Trusted entity. The WinRM client uses the list specified in TrustedHostsList to determine if the destination host is a trusted entity. The WinRM client uses this list when neither HTTPS how Kenters are used to authenticate the identity of the host. Image: Trusted entity. The WinRM client uses the list of trusted hosts, you must configure the list of trusted hosts locally on each computer. Image: Trusted entity of trusted hosts locally on each computer. Image: Trusted entity of trusted hosts locally on each computer.	
▶ ☐ Preferences ▲ % User Configuration ▲ 1000 End (1000 End (1000E	Cancel Apply	

32. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. In the right panel, double-click the Allow Basic authentication setting.

<u>I</u>	Group Policy Management Editor	_ 0 X
File Action View Help	Allow Basic authentication	_ D X
← → 2 III → II → II → Vii Smart Card Sound Recorder	Allow Basic authentication Previous Setting Next S	etting ment
Sync your settings Tablet PC Tablet PC Tablet PC Windows Calendar Windows Calendar Windows Color System Windows Color System Windows Defender Windows Defender Windows Installer Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Payaer Windows Medianger Windows Media	Not Configured Comment Enabled Disabled Supported on: At least Windows Vista Options: Help: This policy setting allows you to manage Remote Management (WinRM) service ac authentication from a remote client. If you enable this policy setting and the setting the V Basic authentication from a remote client. If you disable or do not configure this	whether the Windows spolicy setting, the whether the Vine accepts s
Windows Yowershell Windows Remote Management (WinRM) Windows Remote Management (WinRM) Windows Remote Shell Windows Remote Shell Image Shell Windows Remote Shell Image Shell Windows Update Image Shell Windows Update Image Shell Windows Remote Shell Image Shell Windows Update Image Shell Windows Update Image Shell Image Shell	vinnu sevice does not accept basic autr remote client.	Cancel Apply

33. Select the **Enabled** radio button, then click **[OK]**.

- 34. Repeat steps 32 and 33 for the Allow unencrypted traffic setting.
- 35. Double-click the **Allow remote server management through WinRM** setting. Select the **Enabled** radio button, enter an asterisk (*) in the **Pv4 filter** and **Pv6 filter** fields (under **Options**), and then click **[OK]**.

File Atlow remote server management through WinRM Image: Comment: Comment		Group Policy Management Editor – 🗖 🗴
Allow remote server management through WinRM Previous Setting Previous Setting Allow remote server management through WinRM Previous Se	File Action View Help	Allow remote server management through WinRM -
b Tablet PC Tablet PC Task Scheduler Windows Collendar Disabled Windows Event Reperince Improvement F Disabled Windows Mail Descriptio Windows Mail Descriptio Windows Media Digital Rights Management Pv6 filter: Windows Media Digital Rights Management Windows Molligit Center Windows Media Digital Rights Management Windows Molligit Center Windows Renote Management (WinRM) Kenvice automatically iterus on on the WinRM service automatically iterus on on the HTP transport over the default HT port. Windows Remote Management (WinRM) To allow WinR service automatically iterus on on the WinRM service automatically iterus on on the HTP transport over the default HT port. Windows Remote Shell To allow VinRM service automatically iterus on on the HTP transport over the default HT port. Windows Remote Shell To		Allow remote server management through WinRM Previous Setting Next Setting ment
p Windows Detering Description No Windows Intaller This policy options Pol File No Windows Intaller Pol File Pol File No Windows Mail Pol File Pol File File No Windows Media Objata Rights Management Pol File Pol File File No No Windows Media Objata Rights Management Pol File Pol File Pol File	Tablet PC Tablet PC Task Scheduler Windows Color System Windows Customer Experience Improvement F	
A IS User Configuration regardless	▶ Windows Defender Descripti ▶ Windows Fore Reporting This polinas Windows Isrataller Bernote I Windows Mail Service a Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management HTPP treit Windows Remote Management (WinRM) Windows Remote Management (WinRM) Windows Remote Shell Windows Update Windows Update Port 5383 Workplace Join Windows Cleater Workplace Join Windows Update Workplace Join Windows Update Workplace Join Windows Update Workplace Join Windows Update Workplace Join Windows Cleater Windows Digits Windows Cleater <td>Options: Help: Pv4 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv0 filter: This policy setting the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port. Hype *** to allow messages from any IP address, or eave the If you called this policy setting, the WinRM service automatically is the default HTTP port. If you finable to listen on no IP address. You can pecify one To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting, the WinRM service will not respond to request from a remote computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of WinRM respond to request from a remote computer, regardless of WinRM respond to request from a remote computer, regardless of WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of WinRM service will not respond to request from a remote computer, regardlesses, lif specifies one or more ranges of IP4 addresses,</td>	Options: Help: Pv4 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv6 filter: This policy setting allows you to manage whether the Windows Pv0 filter: This policy setting the WinRM service automatically listens on the network for requests on the HTTP transport over the default HTTP port. Hype *** to allow messages from any IP address, or eave the If you called this policy setting, the WinRM service automatically is the default HTTP port. If you finable to listen on no IP address. You can pecify one To allow WinRM service to receive requests over the network, configure the Windows Firewall policy setting, the WinRM service will not respond to request from a remote computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of WinRM respond to request from a remote computer, regardless of WinRM respond to request from a remote computer, regardless of WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of whether or not any WinRM listenes are computer, regardless of WinRM service will not respond to request from a remote computer, regardlesses, lif specifies one or more ranges of IP4 addresses,

36. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Policies > Administrative Templates: Policy Definitions > Windows Components > Windows Remote Shell. In the right panel, double-click on Specify Idle Timeout:

File Action View Help	Specify idle Timeout	×	
> Windows Defender Activitus > Windows Defender Sploit Guard > Windows Defender SmithsTsreen > Windows Env Reporting Windows Intellie for Business Windows Intellier Windows Intellier Windows Installer Windows Melia Digital Rights Management Windows Media Digital Rights Management Windows Media Digital Rights Management Windows Media Projetal Rights Management Windows Media Projetal Rights Management Windows Media Projetal Rights Management Windows Remote Shell Windows Remote Shell Windows Remote Shell Windows Update > Windows Update > Windows Security > Windows Update Windows Update Windows Update Windows Update Windows Indiages > Windows Indiages > Windows Control > Windows Intellier	Not Configured Comment: Enabled Disabled Supported on: Options: IdleTimeout 900000 E	Previous Setting Next Setting At least Windows Vista Help: Help: This policy setting configures the maximum time in milliseconds remote shell will say open without any user activity until it is automatically deleted. Any value from 0 to 0x/FFFFFFF can be set. A minimum of 60000 milliseconds (1 minute) is used for smaller values. If you enable this policy setting, the server will wait for the specified amount of time since the last received message from the client before terminating the open shell. If you do not configure or disable this policy setting, the default value of 900000 or 15 min will be used.	Commen No No No No
7 setting(s)			
Performance BPA results			
		OK Cancel 55557	

Adjust the setting to meet your requirements. Using the value of 900000 in the image will set the timeout to 15 minutes. Once you have entered your timeout value in milliseconds, click the *Enabled* radio button and then click **[OK]**.

NOTE: When changing IdleTimeout, ensure that no other applications or utilities need a higher timeout for WinRM sessions.

37. In the Windows Remote Shell folder, in the right panel, double-click on MaxConcurrentUsers:

9		Ma	axConcurrentUsers
MaxConcurrentU:	sers		Previous Setting Next Setting
 Not Configured Enabled Disabled 	Comment:		~
	Supported on:	At least Wind	lows Vista
Options:			Help:
MaxConcurrentUsers	4d		This policy setting configures the maximum number of users able to concurrently perform remote shell operations on the system. The value can be any number from 1 to 100. If you enable this policy setting, the new shell connections are rejected if they exceed the specified limit. If you disable or do not configure this policy setting, the default number is five users.

Enter "40" in the **MaxConcurentUsers** field. Once you have entered your value, click the **Enabled** radio button and then click **[OK]**.

38. You can skip this step if you already have a group policy in place for this setting. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Preferences
 > Windows Settings > Registry. In the right panel, right-click and select New > Registry Item. In the New Registry Properties modal page, edit the values in one or more of the following fields:

NOTE: This step is required only if the user account is **not** a domain account and **not** the built-in local administrator account.

- Action. Select Create.
- Hive. Select HKEY_LOCAL_MACHINE.
- Key Path. Enter "SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system".
- Value name. Enter "LocalAccountTokenFilterPolicy".
- Value type. Enter "REG_DWORD".
- Value data. Enter "1".
- Base. Select Decimal.
- 39. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Preferences > Control Panel Settings > Services. In the right panel, right-click and select New > Service.



40. In the New Service Properties modal page, edit the values in one or more of the following fields:

Group Policy Management Editor	D X
File Action View Help	
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy ▲ Computer Configuration ▲ Policies ▶ Software Settings ▶ Mindows Settings ▶ Windows Settings ▶ Windows Settings ▶ Windows Settings ▶ Order Options ▶ Dexices ▶ Devices ▶ Devices <th></th>	
< III > Preferences / Extended \ Standard /	
Services	

- Startup. Select No change.
- Service name. Enter "WinRM".
- Service action. Select Start service.
- Wait timeout if service is locked. Select 30 seconds.
- Log on as. Select No change.
- 41. Click the **[Recovery]** tab, then edit the values in one or more of the following fields:

Group Policy Management Editor	_ 0 ×
File Action View Help	
WinRM Policy (TL012R2-DC-01.MSTL012R2.LOCAL] Policy WinRM Policy (TL012R2-LOCAL] Policy Software Settings Software Settings Software Settings Preferences Windows Settings Control Panel Settings Devices Devices Devices Devices Preferences Network Options Preferences Network Options Poincies Soldeduel Tasks Second failure: Restart the Service Scheduled Tasks Second failure: Restart the Service after: Scheduled Tasks Second failure: Restart the Service after: Program: Poor and Program: Poor and Preferences <th>Interactive Recovery</th>	Interactive Recovery
III > \\ Preferences ∠Extended > Standard / Services	

• First failure. Select Restart the Service.

- Second failure. Select Restart the Service.
- Subsequent failures. Select Restart the Service.
- Restart fail count after. Select 0 days.
- Restart service after. Select 1 minute.
- 42. Click the **[OK]** button.
- 43. To enforce your group policy, in the left panel of the Group Policy Management Editor page, navigate to Forest > Domains > [your local domain] > PowerShell Remote Management Policy. In the PowerShell Remote Management Policy panel on the right, right-click the local domain name under The following sites, domains, and OUs are linked to this GPO and select Enforced.

12	Group Policy Management	- 0 ×				
🛃 File Action View Window Help		_ 8 ×				
Group Policy Management Group Policy Management Group Policy Management Momains MSTL012R2.local MSTL012R2.local Default Domain Policy PowerShell Remote Management Policy	PowerShell Remote Management Policy Scope Details Settings Delegation Unks Display links in this location: MSTL012R2.local The following sites, domains, and OUs are linked to this GPO: Control of the control					
WinRM Policy	Location Enforced Link Enabled Path					
Domain Controllers	MSTL012R2 Incal No Yes MSTL012R2 Incal					
 ▷ Group Policy Objects ▷ Suther GPOs ▷ Stater GPOs ▷ State GPOs ▷ Group Policy Modeling ☑ Group Policy Results 	Enforced Uink Enabled Delete Link(s)					
	Security Hiltering					
	In electings in this GPO can only apply to the following groups, users, and computers:					
	Name					
	Add Propetites					
	WMI Filtering This GPO is linked to the following WMI filter:					
	chone> V Open					

44. To enable your group policy, in the left panel of the Group Policy Management Editor page, navigate to Forest > Domains > [your local domain] > Group Policy Objects > WinRM Policy. Right-click WinRM Policy, then select GPO Status > Enabled.

2				Group Policy M	anagement		- 0 ×	
🚮 File Action View Windo	ow Help						_ 8	
🗢 🔿 🖄 📅 🖏 🖬 🗡	Q 🛛 🖬							
Group Policy Management		WinRM P	olicy					
Forest: MSTL012R2.local Generation Domains		Scope Details Settings Delegation Status						
		Links						
Default Domain	MSTL012R2.local Jofault Domain Policy J PowerShell Remote Management Policy		Display links in this location: MSTL012R2.local					
PowerShell Ren			The following sites, domains, and OUs are linked to this GPO:					
WinRM Policy Domain Controllers		Location Friend Link Enabled Path						
		🚔 MSTL	012R2.local	No	Yes	MSTL012R2.local		
Default Don								
📑 Default Don	nain Policy							
PowerShell	Remote Management Polic							
WinKM Pole	Edit							
WMI Filters	GPO Status	× 🗸	Enabled					
D Starter GPOs	Back Up		User Configuration	on Settings Disabled				
Sites	Restore from Backup		Computer Configuration Settings Disabled computers: All Settings Disabled					
Group Policy Result	Import Settings							
	Save Report	nei	nicated users					
	View							
	New Window from Here							
	Com							
	Delete							
	Rename							
	Refresh	Au	0	Properaes				
	Help	lte	Itering					
	1.00	O is linked to the following WMI filter:						
/		<none></none>		*	Open			
N	/	<u> </u>						
li settings enabled								

Configuring an HTTPS Listener with GPO Configuration

If you are using an HTTPS listener, you cannot create the listener and start it on the monitored device within group policy object (GPO) configuration. This can be done by using a startup script or an immediate task in the group policy, or by running a command manually or on the remote management tool on the device to be monitored. This command needs to be run only once as the HTTPS listener will automatically start once configured.

To perform this configuration within the group policy, perform the following steps:

1. Run the following command on the device you want to monitor:

```
winrm quickconfig -transport:https -force
```

This command will select the first available certificate enabled for server authentication. If you have multiple, valid server authentication certificates installed on your device, you will need to specify the thumbprint of the certificate and use the following command instead:

```
New-Item -Path WSMan:\LocalHost\Listener -Transport HTTPS -Address *
-CertificateThumbPrint "<CertThumbprint>" -Force
```

NOTE: The thumbprint should not contain spaces.

Using Forward and Reverse DNS for Windows Remote Management

When using Active Directory accounts for PowerShell monitoring, Kerberos and Windows Remote Management (WinRM) are used to connect to Windows devices and execute PowerShell code on those devices. Kerberos is

used to request a ticket for authentication to the Windows device, and WinRM is used to execute code on the Windows device.

In a Windows Active Directory configuration, Kerberos needs to be able to communicate with the target Windows device and the Active Directory Domain Controller to verify credentials and issue a ticket for authentication. Kerberos refers to a Windows Domain as a "realm" and an Active Directory Server as a "kdc" (Key Distribution Center).

For this process, it is important that forward and reverse lookup is working for all systems involved. Forward lookup translates a host to an IP address; reverse lookup translates an IP address to a host.

This can be managed through DNS, where a forward lookup is handled through an "A" record in a forward lookup zone, and reverse lookup through a "PTR" record in a reverse lookup zone. A utility such as "nslookup" will work correctly only if the DNS record (a PTR record, in this case) is present.

Where DNS is not available or reliable, it is possible to use the hosts file (/etc/hosts) instead. SL1 uses Python, which in turn can use the hosts file to provide both forward and reverse lookup. However, this approach means a higher level of server management because the hosts files on multiple Data Collector servers would need to be kept in sync. Additionally, where Concurrent PowerShell is used, the hosts files within the Docker containers would need to be updated.

Without a reliable forward and reverse lookup mechanism in place, Kerberos may not be able to validate credentials and issue a ticket for access to a Windows Device, which in turn would mean that access over WinRM to the device would be rejected.

Step 4: (Optional) Configuring a Windows Management Proxy

If SL1 cannot execute PowerShell requests directly on a Windows server, you can optionally configure an additional Windows server to act as a proxy for those PowerShell requests. To use a proxy, you must configure at least two Windows servers:

- A target server that SL1 cannot communicate with directly.
- A proxy server that SL1 will communicate with to execute PowerShell requests on the target server.

NOTE: When monitoring a Windows device using a proxy, the account specified in the credentials is used to access both the proxy server and the target device. This account must have the correct access rights to be used on both servers. If multiple Active Directory domains are used, a trust relationship must be in place that allows the specified account access to the servers in both domains.

To configure the target and proxy servers, perform the following steps:

- Configure a user account that SL1 will use to connect to the proxy server and the proxy server will use to connect to the target server. The user account can either be a local account or an Active Directory account; however, the user account must have the same credentials on the target and proxy servers and be in the Local Administrator's group on both servers.
- If you have created a local user account on the Windows Server instead of an Active Directory account, you
 must configure encrypted communication between SL1 and the Windows server. To do this, you must
 configure a Server Authentication certificate.

- 3. Configure Windows Remote Management on the target server and the proxy server.
- 4. Log in to the proxy server as an administrator.
- 5. Open the PowerShell command window.
- 6. Right-click on the PowerShell icon in the taskbar and select Run as Administrator.
- 7. Execute one of the following commands on the proxy server to allow the proxy server to trust one or more target servers:
 - To allow the proxy server to trust all servers (not recommended), execute the following command:

```
Set-Item WSMan:\Localhost\Client\TrustedHosts -value *
```

• To allow the proxy server to trust only specific target servers, execute the following command, inserting a list that includes the IP address for each target server. Separate the list of IP addresses with commas.

```
Set-Item WSMan:\Localhost\Client\TrustedHosts -value <comma-
delimited-list-of-target-server-IPs>
```

NOTE: The following step is required only if the user account is **not** a domain account and **not** the built-in local administrator account.

8. Execute the following command on the proxy server to configure the LocalAccountTokenFilterPolicy:

```
New-ItemProperty
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -
Name "LocalAccountTokenFilterPolicy" -Value 1 -PropertyType "DWORD"
```

- **NOTE**: If the proxy server is in a different Windows domain (domain A) than the target servers (domain B), and the proxy server uses a user account from Active Directory, and Active Directory is in the same Windows domain as the target servers (domain B), you must perform the following to allow the proxy server to send PowerShell commands to the target servers:
 - On the domain controller for each domain (domain A and domain B), create new forward-lookup zones and reverse-lookup zones that allow name resolution to work between the two domains.
 - On the domain controller for each domain (domain A and domain B), create a non-transitive realm trust between the two domains.
 - Login to the proxy server and add the Active Directory account (from domain A) to the Local Administrator's group for the proxy server. You should be able to select the account on the proxy server after you create the non-transitive realm trust between the two domains.

Step 5: (Optional) Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously

You can optionally execute a series of commands that will allow SL1 to increase the default maximum number of PowerShell Dynamic Applications that can run simultaneously.

To do so:

- 1. Determine the number of Dynamic Applications that will be used to monitor the Windows server. Multiply this number by three.
- 2. Open a PowerShell command prompt. Log in as an Administrator.
- 3. At the prompt, execute the following commands:

Set-Item WSMan:\Localhost\Shell\MaxShellsPerUser -value <number you calculated in step 1>

Set-Item WSMan:\Localhost\Service\MaxConcurrentOperationsPerUser value <number you calculated in step 1>

Restart-Service WinRM

4. Repeat these steps on each Windows server that will be monitored by SL1.

Optional PowerShell CLI Parameters

You can use the following parameters in PowerShell for the associated reasons:

- -NoProfile. Does not load the PowerShell profile.
- -NoLogo. Hides the copyright banner at startup.
- -NonInteractive. Does not present an interactive prompt to the user.

To enable concurrent PowerShell collection to use one of these parameters:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- If this row does not already exist in the master.system_custom_config table, enter the following in the SQL Query field:

```
INSERT INTO master.system_custom_config (`powershell_prefix_setting`,
`<PREFIX INTEGER>`)
```

where:

<*PREFIX*> is an integer that represents one of the prefix values described above. The integers are as follows:

- 0. Disabled
- 1. -NoProfile
- 2. -NoLogo
- 3. -NoProfile and -NoLogo
- 4. -NonInteractive
- 7. -NoProfile, -NoLogo, and -NonInteractive

For example, if a user wanted to configure their PowerShell Data Collector to not load their PowerShell profile, they would enter the following into the **SQL Query** field:

```
INSERT INTO master.system_custom_config (`powershell_prefix_setting`,
`1`)
```

3. If this row already exists in the master.system_custom_config table, enter the following in the SQL Query field:

```
UPDATE master.system_custom_config SET field_value = 1 WHERE field =
`powershell prefix setting`
```

4. After you have entered the command in the **SQL Query** field, click the **[Go]** button. Your changes will be picked up with the next batch of jobs that are processed.

© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC[™] AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic[™] has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic[™] assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic[™] may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and [™] symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic[™]
- EM7[™] and em7[™]
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management[™]

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: <u>legal@sciencelogic.com</u>. For more information, see https://sciencelogic.com/company/legal.



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010