

Microsoft Automation PowerPacks

Microsoft Hyper-V Automation PowerPack version 101

Windows PowerShell Automations PowerPack version 103

Table of Contents

Introduction	
Microsoft Automation PowerPacks	
Windows PowerShell Automations	
What is the Windows PowerShell AutomationsPowerPack?	. 7
Installing the Windows PowerShell AutomationsPowerPack	
Standard Automation Policies	
Authentication for Windows Devices with the Windows PowerShell Automations PowerPack	
Creating a Credential for Windows PowerShell	
Creating Custom Windows PowerShell Automation Policies	
Creating a Custom Action Policy	.12
Customizing Automation Actions	
Creating a New Windows PowerShell Automation Action	
Microsoft Hyper-V Automation	. 18
What is the Microsoft Hyper-V Automation PowerPack?	
Prerequisites	. 19
Installing the Microsoft Hyper-V Automation PowerPack	.19
Standard Automation Policies	
Credential for Hyper-V Automation	24
Creating and Customizing Hyper-V Automation Policies	.24
Creating a Custom Action Policy for Hyper-V	
Customizing Automation Actions	.24
Creating a New Microsoft Hyper-V Automation Action	26
Configuring Device Credentials	
Creating a Credential	
Creating and Customizing Automation Policies	
Prerequisites	
Creating an Automation Policy	
Customizing an Automation Policy	
Removing an Automation Policy from a PowerPack	
Run Book Variables	
Run Book Variables	
Configuring Windows Servers for Monitoring with PowerShell	
Prerequisites	
Configuring PowerShell	
Step 1: Configuring the User Account for the ScienceLogic Platform	
Option 1: Creating an Active Directory Account with Administrator Access	
Option 2: Creating a Local User Account with Administrator Access	
Option 3: Creating a Non-Administrator User Account	
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	
Creating a User Group and Adding a User in Active Directory	
Setting the Session Configuration Parameters and Group Permissions	
Creating a PowerShell Credential	
Step 2: Configuring a Server Authentication Certificate	
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	
Step 3: Configuring Windows Remote Management	
Option 1: Using a Script to Configure Windows Remote Management	
Option 2: Manually Configuring Windows Remote Management	.61

Option 3: Using a Group Policy to Configure Windows Remote Management	64
Step 4: (Optional) Configuring a Windows Management Proxy	82
Step 5: (Optional) Increasing the Number of PowerShell Dynamic Applications That Can Run	
Simultaneously	83

Chapter

Introduction

Overview

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

TIP: These PowerPacks require a subscription to one of the following solutions:

- Datacenter Automation Enrichment PowerPack
- 2020 Pricing Advanced and Premium Packages

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 PowerPacks

Microsoft Automation PowerPacks

This manual describes content from the following PowerPack versions:

- Microsoft Hyper-V Automation, version 100
- Windows PowerShell Automations, version 103

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?	7
Installing the Windows PowerShell AutomationsPowerPack	7
Standard Automation Policies	8
Authentication for Windows Devices with the Windows PowerShell Automations PowerPack	11
Creating a Credential for Windows PowerShell	12
Creating Custom Windows PowerShell Automation Policies	12
Creating a Custom Action Policy	12
Customizing Automation Actions	14
Creating a New Windows PowerShell Automation Action	16

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 Remote 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.)

To download and install a PowerPack:

- 1. Download the PowerPack from the ScienceLogic Customer Portal.
- 2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. In the **PowerPack Manager** page, click the **[Actions]** button, then select Import PowerPack.

4. The Import PowerPack dialog box appears:

Import	PowerPack™	×
L	Browse for file Browse icense: Import	

- 5. Click the [Browse] button and navigate to the PowerPack file.
- 6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** 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 Remote PowerShell Request", which is supplied in the PowerPack.

Editing PowerPack™ Windo	ws Po	werShell Automations										
▼ Manage PowerPack [™]	Emb	edded Run Book Policies [5]										
Properties		Automation Policy Name *	ID	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited	
Build / Export				All 🔻	All	•					All	•
Features / Benefits	1.	A Windows PowerShell: Run CPU & Me	117	Enabled	System		All	1	1	em7admin	2019-11-19 10:28:41	6
Technical Notes	2.	A Windows PowerShell: Run CPU Diagr	115	Enabled	System		All	2	1	em7admin	2019-11-19 10:28:40	
Documentation		A Windows PowerShell: Run Disk I/O Di		Enabled	System		All	3	1	em7admin	2019-11-19 10:28:41	6
 Contents 		A Windows PowerShell: Run Memory D		Enabled	System		All	3	1	em7admin	2019-11-19 10:28:41	
Dynamic Applications	5.	A Windows PowerShell: Run Print Job E	119	Enabled	System		All	1	1	em7admin	2019-11-19 10:28:41	
Event Policies												
Device Categories												
Device Classes												
Device Templates												
Device Groups												
Reports												
Dashboard Widgets												
Dashboards	Avai	ilable Run Book Policies [0]										
Dashboards SL1		Automation Policy Name *	ID	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited	
Run Book Policies		Automation Folicy Name	19		All	<u>Organization</u>	- Devices	LVEIIIS	Accions	<u>Conted by</u>		
Run Book Actions												
Run Book Action Types												
Ticket Templates						No results to display	,					
Credentials												
Credential Tests												
Proxy XSL Transformations												
UI Themes												
IT Services												
Log File Monitoring												
Policies												
AP Content Objects												

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 Remote 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 NOTE: This automation policy is aligned with the Windows Automation device group. 	 Automation Utilities: Calculate Memory Size for Each Action Windows Get Largest Event Log Files Windows Get Largest 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 	Run Memory Diagnositc Commands

Automation Policy Name	Aligned Events	Automation Action
	 Major: Microsoft: Windows Pages per Second has exceeded threshold 	
	 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	5											Jude.	Evans-Mccarthy 🗸		Logic
88	1 Critic		19 Major	6 Minor	1 Not	1 tice H	0 lealthy	27 Events View All							v	View
	Q Ty	pe to s	search events					-							≡	•
-	\$		ORGANIZATION		VERIT	NAME		SAGE	AGE	TICKET I	CO		MASKED EVENTS		CLEAR	C
ė			Windows Device		Major	10.2.24.56		mple Windows CPU Event	8 days		1	÷		 Acknowledge 	× Clear	
			Windows Device	es 🧧	Major	10.2.24.56	Exan	nple Windows Memory Event	8 days		1	F		 Acknowledge 	× Clear	
			Windows Device	rs 🧲	Major	10.2.24.56	Exan	mple Windows Disk IO Event	8 days		1	+		✓ Acknowledge	X Clear	
			Windows Device	es 🧲	Major	10.2.24.56	Exan	mple Windows Disk Performa	8 days		1	F		✓ Acknowledge	× Clear	
			Example Devices	. (Major	netscaler	Devi	ice Failed Availability Check: U	7 days 15 ł		2195	+	Q Masked	✓ Acknowledge	× Clear	
			Example Devices	. (Minor	ec2-34-200	Netv	work latency exceeded thresh	3 days 15 ł		1044	+		✓ Acknowledge	× Clear	
			Linux Devices	•	Major	10.2.24.30	/: Fil	le system usage exceeded maj	2 days 19 H	5	268	+		✓ Acknowledge	× Clear	
			System	•	Major	ec2-18-217	Linu:	x File System /dev/loop0 : /sn	2 days 1 ht		491	+		✓ Acknowledge	× Clear	
			System	•	Major	System	EM7	7 major event: Dynamic applic	19 hours 3		20	+		✓ Acknowledge	× Clear	
			System	•	Major	cscol26	Swap	p memory utilization has exce	14 hours 5	9	157	+		✓ Acknowledge	× Clear	
			System	•	Major	System	Proc	ess time exceeded: Process D	1 hour 23 i		2	+		✓ Acknowledge	× Clear	
			System	•	Minor	cscol26	App:	: 91, Snippet: 112 reported a c	30 minutes		1	+		✓ Acknowledge	× Clear	
•••			System		Minor	System	Proc	ess 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.

1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-122 16:20:37 1 1913-123 16:20:37 1 1913-123 16:20:37 1 1913-123 16:20:37 1 1913-123 10:20:37 1 1913-123 10:20:20:20:20:20:20:20:20:20:20:20:20:20	Event Actions	g For Event [18263] Refresh Guide	
ukumator Policy Windows PowerShell: Run CPU Ja Memory Diagnostic Commands with HTML Dutput ran Successfully kesam Custom Command Output mandle Get-Process Soft CPU - descending Select - first 20 Format-Table - AutoSize mandle Get-Process Soft CPU - descending Select - first 20 Format-Table - AutoSize 634 07 22363 12363 123,223 214 174 0 FiftyEng 634 07 22363 12363 123,223 214 174 0 FiftyEng 634 07 22363 123,23 22,23 21400 0 vetoSide 635 07 12363 123,23 22,23 1240 0 vetoSide 636 07 12363 123,23 22,23 1240 0 vetoSide 637 17 12230 1305 123,723 123 0 o vetoSide 638 09 1236 12,723 123 0 o vetoSide 638 09 1236 12,723 123 0 o vetoSide 638 09 1236 12,73 13 0 o vetoSide 638 13 1276 1958 0 314 0 vetoSide 638 13 1276 0 vetoSide 638 13 1276 1958 0 314 0 vetoSide 638 13 1276 0 vetoSide 638 13 1276 0 vetoSide 638 13 1276 0 vetoSide 648 13 17 199 0 438 0 vetoSide 718 128 14			
dessage Custom/actionTpg (46) executed without incident command: Get+Process Sort CPU - descending Select - first 20 Format-Table - AutoSize softale WP(C) VC(C) VC			- ^
Handles NPM(K) PM(K) VEX VEX To recession 9900 1 2022 1 1 1 9900 1 213 1 1 1 1 9900 1 1 1 1 1 1 1 9101 1 <t< td=""><td>Message:CustomA</td><td>Type (448) executed without incident</td><td></td></t<>	Message:CustomA	Type (448) executed without incident	
comment comment <t< td=""><td></td><td></td><td></td></t<>			
614 67 272260 183468 185,272.64 1728 0 Mshfeng 536 62 23867 27373 66 393.05 2116 0 Saltervi 537 64 0980 202 21,32.4 4400 0 conost 638 39 159516 6314 21,633.34 440 0 schost 638 39 159516 6314 22,633.4 484 0 schost 539 6 0022 1027 11,078.36 0 Stoto 648 39 159516 6314 22,632.4 450 0 schost 539 6 0022 1027 11,078.36 0 Stoto 540 0 Stoto 541 10 508 0 886 10,596.0 556 0 services 541 10 508 0 886 10,596.0 556 0 services 541 10 508 0 886 10,596.0 576 0 services 542 10 508 0 886 10,596.0 576 0 services 543 23 3000 41552 7,141.63 4360 0 Mshryst 544 11 77 1002 1270 10,773.16 1276 0 kmlryst 545 12 14460 2623 7,64.6 576 0 services 546 10 588 0 40,595.0 12,672 31,078.0 576 0 services 547 10 578 10,573 10,573 10,573 10,574 0 schost 548 12 14460 2623 7,64.6 576 0 schost 548 12 14460 2623 7,64.6 576 0 schost 549 18 2090 4452 7,741.63 4360 0 kmlryst 540 18 2090 4452 7,741.63 4360 0 schost 541 10 5728 1468 1,905.52 10 schost 541 10 5728 1,905.57 144 0 schost 541 10 5728 1,905.57 144 0 schost 541 10 572 10 10 schost 541 10 572 10 10 schost 541 10 10 10 s	nunuics writer)		
614 67 27220 183468 183.72.64 1728 0 Mshfeng 530 6 124 330 155,646.54 0 State 0 State 531 6 12407 2733 6 572.05 2116 0 State 533 7 15551 6 5144 21,613.34 444 0 vchot 534 7 12424 4140 42,762.55 128 0 vchot 535 7 1002 1972 11,773.56 3916 0 conhot 536 7 1002 1972 11,773.56 3916 0 conhot 537 7 1002 1972 11,773.56 3916 0 vchot 538 7 12408 12407 21,1273 0 vchot 539 1 10 500 1002 10,773.10 100 0 vchot 531 12 33040 41552 7,141.05 3450 0 km ⁻ rs ⁵ 531 13 2730 1406 225 7,244.95 7 14 0 vchot 531 12 1300 1100 1000 1000 1000 1000 1000	967480 91	648 204260 217.886.92 876 0 svchost	
554 62 236572 72732 60,990,93 2216 0 sileervr 33 1 10407 2423 22,232,44 4040 0 conhot 33 4 10407 2423 22,232,44 4400 0 conhot 33 4 4080 22,232,44 4400 83 conhot 33 4 4080 22,232,44 4400 83 conhot 33 6 4080 20,72,31 220 0 conhot 33 8 4980 921 67,73 697 0 conhot 331 23 3040 41257 7,486,43 0 halfrvist 331 23 30404 4252 7,446,43 0 kalervist 331 12 3468 9,498 944<			
32 1 10072 2432 26,722.22 1040 0 vmbold 3 6 496 920 24,232.44 490 0 conhot 63 7 15552 6114 21,315.34 464 0 vchost 53 8 496 924 11,400.83 772 0 conhost 39 8 5012 9572 11,078.56 3916 0 conhost 31 10 1008 12572 7,418.65 4560 0 conhost 31 12 3 3000 41552 7,418.65 4560 0 conhost 31 12 3 3000 41552 7,7418.65 4560 0 conhost 31 12 3 3000 41552 7,7418.65 4560 0 conhost 31 12 730 4468 2,909.52 10, 148.55 276 0 kmbrst 514 11 5728 1468 2,909.52 20 0 vchost 31 1 7 100 4336 3,117.50 384 0 corss 514 11 5728 1468 2,909.52 20 0 vchost 31 8 494 9644 2,736.05 7164 0 conhost 31 8 494 9644 2,736.05 7164 0 conhost 31 8 494 9644 2,736.05 7164 0 conhost 31 8 10 7788 1468 2,909.52 20 0 vchost 31 8 10 1000 433 514 11 6 22 500 conhost 31 10 100 433 514 11 6 22 500 conhost 514 116 22 500 conhost 514 51 52 514 51 52 51	900 0	124 136 159,606.53 4 0 System	
93 8 9200 22,222,44 44980 0 context 134 71 22224 41684 20,722,52 1444 64 0 vvhost 134 72 22242 41684 20,722,52 1444 64 0 vvhost 93 6 5812 5972,51 11,078,53 5914 0 vvhost 411 17 16982 19708 16,772,31 928 0 vvhost 33 8 498 952,10,383,55 597,040,55 0 ohnost 331 23 30840 1552,7,746,53 5400 0 bimPrvSE 451 11 1460 2576,70,746,05 276,06 0 context 93 8 6984 5,974,06,97,40 0 context 15 93 8 1984 942,736,06 7164 0 context 93 8 984 942,736,06 7164 0 context 94 944 2,736,06 7164 0 context			
683 39 159516 63344 21,815.34 464 0 svchot 39 4 798 9284 11,400.88 3372 0 conhot 31 6 70 504 1905 11,073.35 100 0 svchot 33 6 998 9284 11,400.88 3372 0 conhot 34 6 10 504 9996 10,395.01 506 0 services 35 8 498 9996 11,377.5 9,967.13 604 0 lass 38 1 23 8980 177.7 9,967.13 604 0 lass 38 1 23 8980 177.7 9,967.13 604 0 lass 38 1 23 8980 177.7 9,967.13 604 0 lass 39 1 1 2776 9,967.13 604 0 lass 39 1 1 2796 35092 5,240.50 736 0 svchot 39 1 1 2796 35092 5,240.50 736 0 svchot 39 4984 9944 2,736.07 146 0 conhot 39 4984 944 2,736.07 146 0 conhot 39 4984 944 2,736.7144 0 conhot 41 ThreadCount',Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 are id ThreadCount',Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 are id ThreadCount',Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 worhout 376 5 40 1 30 0 worhout 464 33 worhout 464 33 worhout 464 33 worhout 464 13 worhout 976 14 41 20 Worhout 98 12 41 41 5 22 41 42 7 4 41 42 7 4 41 42 7 4 41 42 7 4 41 42 7 4 42 4 43 4 44 43 44 43 45 4 46 43 47 4 47			
1394 71 222.04 41604 26,762.52 1460 0 suchast 39 4 498 9324 11,400,83 9372 0 combat 39 8 5012 9672 11,078.38 9312 0 combat 39 8 5012 9672 11,078.38 9372 0 combat 39 0 4988 9632 15,458.58 976 0 combat 318 23 9080 4752 7,418.63 640 0 lass 318 123 9080 4752 7,418.63 460 combat 318 123 9040 41522 7,418.63 490 combat 314 13 5722 14602 2526 0 winbrvE 314 13 5722 14602 2527 0 winbrvE 314 13 5722 1468 2502 0 winbrvE 314 13 5722 1468 2502 0 winbrvE 314 13 5722 1468 2502 0 winbrvE 31			
93 8 988 924 11,400.88 9316 0 conhot 93 8 5012 927 11,073.83 936 0 conhot 441 11 1002 19708 10,572.31 938 0 suchost 93 10 4488 9521 10,493.8 957.13 938 0 suchost 1385 23 9390 1777 9,967.13 604 12ass 351 23 9390 1777 9,967.13 604 12ass 351 23 9390 5,717.60 8408 9264 11,967.03 313 10 7288 468 2,907.52 624 937.04 314 10 7288 468 2,909.52 622 0 suchost 514 10 5728 1468 2,909.52 622 0 suchost 500 4984 944 2,736.07 164 0 suchost 514 10 ThreadCount';Expression ={\$			
93 8 5012 9572 11.678.36 9916 0 conhost 246 10 504 9996 10.395.91 526 0 services 33 8 4988 9956 10.395.95 5076 0 conhost 348 9956 10.395.95 5076 0 conhost 348 12 23 30040 1352 7.418.63 4360 0 wmPrvSE 451 21 14460 2628 7.964.05 2276 0 WmPrvSE 451 21 1450 2628 7.964.05 736 0 sychost 348 10 5728 14688 2.909.52 692 0 sychost 348 11 5728 14688 2.909.52 692 0 sychost 349 4949 42.736.0714 0 conhost 590 18 25744 35092 5.240.50 736 0 sychost 348 11 5728 1468 2.909.52 692 0 sychost 349 4949 42.736.0714 0 conhost 591 10 5728 1468 2.909.52 692 0 sychost 34 6949 4944 2.736.0714 0 conhost 592 10 5728 1468 2.909.52 692 0 sychost 593 8 4964 9944 2.736.0714 0 conhost 594 44 2.736.0714 0 conhost 595 10 10 ThreadCount -Descending Select -first 20 596 10 ThreadCount -Descending Select -first 20 597 10 10 conhost 597 10 10 conhost 5			
441 17 1602 19708 10, \$72, 31 928 0 suchast 38 498 953 10, 348, 55 607.6 0 conhost 39 4 498 953 10, 348, 55 607.6 0 conhost 315 23 988 177.7 9,677.1 644.0 523.2 7,644.05 227.6 0 winPrvSt 314 13 147.064.05 227.6 0 winPrvSt 640.0 623.3 7,764.05 227.6 0 winPrvSt 314 13 177.09.067.13 948 0 conhost 0 conhost 0 conhost 314 14 157.23 144.08 2,090.2 524.00 0 conhost 314 16 572.2 1468 2,090.2 524.00 0 conhost 314 16 572.2 1468 2,090.4 0 conhost 0 conhost 138 23 14 109 vehost 16 0 conhost 139 8 494 94.4 2,736.00 714.0 0 conhost 139 109 105			
266 10 554 996 10, 356, 91 556 0 conbat 38 4988 906 12, 356, 907 0 conbat 1385 23 8980 17, 75 9, 967, 13 664 0 lass 1385 23 8980 17, 75 9, 967, 13 664 0 lass 1385 23 14460 2528 7, 964, 65 27, 66 0 lass 599 18 27, 944 5592 5, 240, 50 736 0 scrost 514 13 728 1468 2, 009, 52 692 0 scrost 514 14 5728 1468 2, 009, 52 692 0 scrost 514 16 5728 1468 2, 009, 52 692 0 scrost 514 16 ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 command: Get-rbrcces Select-object Name, ID, @{Name*'ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 vehost 164 33 vehost 164 33			
135 23 9980 1776 9,967.13 604 0 1sas 351 23 03004 0.523 7,418.0 0 Number State 411 21 14460 055.20 7,041.05 0 Number State 431 21 1460 055.20 7,041.05 0 Number State 431 11 1050 4363 3,117.05 0,403 3,117.05 0,404.05 0,217.05 0 Number State 0 Number State 0 Number State 0 Number State 0 0 Number State 0 0 Number State 0			
31 23 30040 41522 7,413.63 4360 0 WIMPYSE 451 21 14460 2527 0 <td>93 8</td> <td>988 9652 10,348.58 5076 0 conhost</td> <td></td>	93 8	988 9652 10,348.58 5076 0 conhost	
<pre>451 21 14460 2528 7,064.05 2276 0 WmlPrvSE 590 18 29704 3502 5,24.05 736 0 svchot 431 17 1980 4336 3,117.50 384 0 csrss 33 8 994 9644 2,736.05 716 0 conhost 0 mmadi Get Process [Select-object Name, ID, @{Name='ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 lame Id ThreadCount </pre>			
590 18 20704 35092 5;240.50 736 0 suchost 431 17 1958 436 3;10 340 0 cross 514 18 5728 14688 2,009.52 632 0 suchost 30 8 4984 5964 2,735.6714.0 0 conhost command: Get-Process Select-Object Name, ID, @{Name='ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 are 10 10 10 ytem 100 10 vohost 104 3 vohost 44 3 vohost 444 3 vohost 444 3 vohost 144 20 upstepi 172 22 owershell 5660 18 owershell 544 15 vohost 146 15 vohost 146 15 vohost 164 15 vohost 164 15 vohost 162 14			
431 17 1980 4336 3,117.50 344 0 correst 514 18 7728 1468 2,909.5 202.0 <td></td> <td></td> <td></td>			
514 18 57.28 14688 2,980.52 692 0 suchast 93 8 4984 942 736.07 146 0 conhost command: Get Process Select-Object Name, ID, @(Name='ThreadCount';Expression ={\$Threads.Count}} Sort-Object -Property ThreadCount -Descending Select -first 20 ine 1 ThreadCount 19 vchost 05 58 131 10 10 vchost 16 10 vchost 16 29 vchost 16 20 vchost 16 20 vchost 16 20 vchost 16 20 vchost 162 14 vchost 162 14 vchost 162 14 vchost 162 14			
93 8 4984 944 2,736.05 7164 0 conhost commadic Get-Forcess Select-Object Name, ID, @(Name=' ThreadCount';Expression ={\$Threads.Count}) Sort-Object -Property ThreadCount -Descending Select -first 20 ame 1 ThreadCount 109 vitem 109 109 vohat 76 58 glserv 2216 55 vohat 444 30 vohat 444 30 vohat 116 22 owershell 1476 20 owershell 1476 20 owershell 544 15 vohat 154 16 vohat 152 13 stdis 3052 13 stdis 3052 13 stdis 3052 13 Select -first 20 Format-Table -AutoSize Get 16 <td></td> <td></td> <td></td>			
Select-Object Name, ID, @(Name='ThreadCount';Expression =(\$Threads.Count})) Sort-Object -Property ThreadCount -Descending Select -first 20 Jame Id Jame 100			
poolsv 1572 13 vohst 736 13 ssdis 3952 13 command: Get-Process Sort WS -descending Select -first 20 Format-Table -AutoSize andles MPH(X) MSC - CPU(s) sdids MPL - AutoSize somids Sort WS - descending Select - First 20 Format-Table - AutoSize somids MPL - AutoSize	sychost 876 sqlservr 2216 sychost 1040 sychost 1040 sychost 884 MsMpEng 1728 sychost 1116 powershell 5660 powershell 5660 powershell 5484 sychost 928 sychost 940 WmIPrvSE 2276	- 58 55 43 33 25 25 22 20 88 18 17 16 16 16	
poolsv 1572 13 vvchost 736 13 sodis 3052 13 sommand: Get-Process Sort VB -descending Select -first 20 Format-Table -AutoSize sondis NPM(K) NS(K) CPU(s) Id SI ProcessName 967475 90 2405432 204096 217,886.97 876 0 svvchost 627 67 275096 18356 182,273.2 7128 0 HelpEng -			
ssdis 3052 13 Command: Get-Process Sort WS -descending Select -first 20 Format-Table -AutoSize Format-Table -AutoSize andles NPM(K) [NS(K) CFU(S)] Id 51 ProcessName Format-Table -AutoSize 967475 90 2405432 204096 217,805.97 876 0 svchott 627 67 275096 183566 182,273.27 12780 0 HighEng	spoolsv 1572		1
Sommand: Get-Process Sort WS -descending Select -first 20 Format-Table -AutoSize tandles NPM(K) PM(K) WS(K) CPU(s) Id SI ProcessName 967475 90 2405432 204095 217,886.97 876 0 suchost 627 67 275096 183565 182,273.25 1728 0 MHPpEng			1
andles NPM(K) PM(K) VS(K) CPU(s) Id 51 ProcessName 967475 90 2405432 204095 217,886.97 876 0 svchost 627 67 275096 18356 182,273.25 1728 0 MiNFpEng	tssdis 3052	13	1
967475 90 2465432 204096 217,886.97 876 0 svchost 627 67 275096 15356 182,273.25 1728 0 HsNPfng		(K) WS(K) CPU(s) Id SI ProcessName	
627 67 275096 183568 182,273.25 1728 0 MsMpEng			1
	627 67	096 183568 182,273.25 1728 0 MsMpEng	1.
			17
	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 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 Remote 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 ServerPowerPack* 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 Remote 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 Remote 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]
	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 ▼) arameters
<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 Remote 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 Remote 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	
Vindows Memory Diagnostic Commands [Enabled]	
Description	
Runs diagnostic commands for Memory-related events on Windows devices.	
Organization Action Type	
System] Execute Remote PowerShell Request (1.1	0)
Execution Environment Action Run Contex	đ
Default: Windows PowerShell Automations]	
Input Parameters	
<pre>{ "commands": "{\"commands\": [\"Get-Process Sort WS -descending "request_key": "", "credential_id": 0</pre>	Select -first
"request_key": "",	Select -first

The following automation actions that use the "Execute Remote 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
and Memory	Runs diagnostic commands for CPU and Memory events on Windows devices	 Get-Process Sort CPU -descending Select -first 20

Action Name	Description	<pre>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,</pre>
		 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 devices.	• Get-Process Sort WS -descending Select -first 20

Action Name	Description	Commands Run
		 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 Remote PowerShell Request" custom action type. To do this, select "Execute Remote PowerShell Request" in the Action Type drop-down 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.

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

Parameter	lnput 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.

Parameter	Input type	Description
		Get-WmiObject -Class Win32_Processor -Property DeviceID, NumberOfCores, Name, 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?	
Prerequisites	
Installing the Microsoft Hyper-V Automation PowerPack	
Standard Automation Policies	
Credential for Hyper-V Automation	24
Creating and Customizing Hyper-V Automation Policies	
Creating a Custom Action Policy for Hyper-V	
Customizing Automation Actions	
Creating a New Microsoft Hyper-V Automation Action	

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 Remote 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.)

To download and install a PowerPack:

- 1. Download the PowerPack from the <u>ScienceLogic Customer Portal</u>.
- 2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 3. In the **PowerPack Manager** page, click the **[Actions]** button, then select Import PowerPack.
- 4. The Import PowerPack dialog box appears:

l	mport PowerPack™	×
	Browse for file Browse]
	License:	
	Import	

- 5. Click the [Browse] button and navigate to the PowerPack file.
- 6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** 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 Remote PowerShell Request", which is supplied in the Windows PowerShell AutomationsPowerPack.

Technical Notes Documentation	Automation Policy Name • 1. Hyper-V: CPU & Memory Diagnostic C 6	<u>ID</u>	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited	
Features / Benefits Technical Notes Documentation			All -					ACTIONS	Edited by	Last Edited	
Technical Notes Documentation			1.00	All	•					All	۲
Documentation			Enabled	System		1 group	5	4	em7admin	2020-05-21 16:46:42	6
	 Phyper-V: Disk & Storage Diagnostic Cc 6 		Enabled	System		1 group	6	5	em7admin	2020-05-21 16:46:42	
Contents	 Hyper-V: Guests Below Threshold Diac 6 		Enabled	System		All	1	6	em7admin	2020-05-21 16:46:42	6
	 Hyper-V: Run Time Capacity Diagnosti 6 	0	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											
Dashboard Widgets											
°											
Dashboards SL1	Available Run Book Policies [0]										
Run Book Policies	Automation Policy Name •	<u>ID</u>	Policy State		Organization	Devices	Events	Actions	Edited By	Last Edited	
Run Book Actions			Ali 🔻	All	•					All	۲
Run Book Action Types											
Ticket Templates											
Credentials					No results to display.						
Credential Tests											
Proxy XSL Transformations											
UI Themes											
IT Services											
Log File Monitoring Policies											
AP Content Objects											

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 Remote 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 Microsoft: Windows Processor Queue 	 Automation Utilities: Calculate Memory Size for Each action
	 Microsoft: Windows Available Memory below threshold 	 Hyper-V Guest Status Diagnostic Commands Hyper-V Log Collection
	 Microsoft: Windows Pages per Second has exceeded threshold Microsoft: Windows Paging File has exceeded threshold 	 Datacenter Automation: Format Output as HTML

Automation Policy Name	Aligned Events	Automation Actions
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 thresholdPoller: File system usage exceeded (major) threshold	 Datacenter 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
		 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.

=	Events												Mantone 🗸	€D.scen	celogic
	1 Critical	32 Major	5 Minor	1 Notice	3 Healthy	42 Events View All									~ View
	Q Type to	o search events													= o
G	٥	ORGANIZATION		EVERITY	NAME		MESSAGE	AGE	TICKET ID	COUNT	EVENT NOTE	MASKED EVENTS	ACKNOWLEDGE	CLEAR	c
¢	· .	System		Major	PagerDut		PagerDuty DA Error: PyCURL Exception when making requ			1	Ð		 ✓ Acknowledge 	× Clear	_
	~ [System		Major	Dell EMC	Device	Example EMC Event	3 days 21 hours		1	Ð		✓ Acknowledge	X Clear	-
	~ []	Windows Devi	ces 🕻	Notice	10.2.24.5	9	Microsoft: Hyper-V Percent Virtual Machines Running is be	3 days 20 hours		5443	Ð		 Acknowledge 	X Clear	-
	× []	Example Devic	es 🛛	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	- 1
	~	Example Devic	es 🛛	Major	Test CRS-	1 165	Device Failed Availability Check: ICMP Ping	21 hours 42 minutes		261	Ð	Q Masked	 Acknowledge 	× Clear	- I
	~	Linux Devices	•	Major	10.2.24.3	1	Device Failed Availability Check: UDP - SNMP	21 hours 42 minutes		261	Ð	Q Masked	 Acknowledge 	🗙 Clear	- 1
	~	Windows Devi	ces 📢	Minor	10.2.24.5	6	CPU utilization has exceeded the threshold 75%. Current v	2 hours 47 minutes		34	Ð		 Acknowledge 	X Clear	- 1
	~	Windows Devi	ces 📢	Minor	10.2.24.5	6	Processor Queue Length has exceeded the threshold 6 Thr	1 hour 12 minutes		15	Ð		 Acknowledge 	× Clear	- 1
	~	Windows Devi	ces 🛛	Healthy	10.2.24.5	6	Network Latency below threshold	17 minutes 6 seconds		1	Ð		 Acknowledge 	× Clear	l - 1
	~	Windows Devi	ces (Healthy	10.2.24.5	6	Pages per Second is now below the threshold 200 Pages/S	13 minutes 1 second		1	Ð		 Acknowledge 	X Clear	- 1
	~	Windows Devi	ces 📢	Major	10.2.24.5	6	C:\: File system usage exceeded major threshold: Limit: 1.0	7 minutes 56 seconds	212	1	Ð		 Acknowledge 	× Clear	-
	~	Windows Devi	ces (Healthy	10.2.24.5	6	C:\: File system usage returned below critical 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 Devic	es 📢	Minor	rstlsvcsad	iu2a01	Network latency exceeded threshold: 316.63 ms.	2 minutes 13 seconds		1	Ð		 Acknowledge 	X 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 Lo	g For Event [96198]	Refresh Guide
2020-03-13 19:08:26		
Message:Snippet (365) (-V: Guests Below Threshold Diagnostic Commands action Datacenter Automation: Format Output as HTML ran Successfully executed without incident ¹ : <u>Enrichment Command Output</u>	
Command: Get-VMStatu		
ComputerName Name	State CPUUsage MemoryMB Uptime Status	
WTN_HYPERV_CVR Test	M2 Off 0 0.00.00.00 Operating pormally	
WIN-HYPERV-CYB Test	M1 Off 0 00:00:00 Operating normally	
WIN-HYPERV-CYB Test3	10 0ff 0 00:00:00 Operating normally 0ff 0 00:00:00 Operating normally	
Command: Get-VMInfo		
Name	: Test3	
CPU	: 1	
DynamicMemoryEnabled		
MemoryMinimum(MB)		
MemoryMaximum(GB)		
	: False	
	: 9.0	
ReplicationHealth		
	: Unknown	
	: Unknown	
	: Dynamic	
	: 0	
MaxSize(GB)-0	: 127	
Name	: TestVM1	
CPU DynamicMemoryEnabled	:1	
JynamicMemoryEnabled MemoryMinimum(MB)		
lemoryMinimum(MB)		
	: 1024 : False	
	: False : 9.0	
ReplicationHealth		
	: Unknown	
	: Unknown	
VHDTvpe-0	: Dynamic	
VHDSize(GB)-0	e e	
MaxSize(GB)-0	127	
Name	: TestVM2	
CPU	1	
DvnamicMemorvEnabled		
	512	
MemoryMaximum(GB)		
	: False	

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 Remote 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 Remote 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.

olicy Editor Editing Action [316] Action Name	
	Action State
Hyper-V Allocation Diagnostic Command	[Enabled]
	Description
Determines the current resource allocation health of the Hype	r-V server or cluster.
Organization	Action Type
[System]	Execute Remote PowerShell Request (1.0)
Execution Environment	Action Run Context
[Default: Microsoft Hyper-V Automation]	[Collector]
	but Parameters
<pre>"request_key": "", "credential_id": 0 }</pre>	

The following automation actions that use the "Execute Remote 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	Runs diagnostic commands to collect Hyper-V guest status and configuration information.	 Get-VMStatus Get-VMInfo Format-Table

Action Name	Description	Commands Run
Commands		
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 Remote 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.

Credential Management Credentia														Reset	Guide
														NMP Credentia	
		RO Use	RW	DA Use	_					_			Create D	latabase Crede	
Profile Name *	Organization	Use	Use	Use	Type	Credential User		Host	Port	Timeout (ms		Al	Create S	OAP/XML Host	Credenti
1. Amazon Web Services Credential	System				SOAP/XML Host	[AWS Account Access			80	2000				DAP/AD Crede	
2. Azure Credential - SOAP/XML	👔 [all orgs]				SOAP/XML Host	<ad_user></ad_user>	login.windows.net		443	60000			Create B	asic/Snippet C	
 Azure Credential - SSH/Key 	🚯 [all orgs]				SSH/Key	<subscription_id_h< td=""><td>%D</td><td></td><td>22</td><td>180000</td><td></td><td>2015-05-14</td><td>Create S</td><td>SH/Key Creder</td><td>itial</td></subscription_id_h<>	%D		22	180000		2015-05-14	Create S	SH/Key Creder	itial
 P Cisco SNMPv2 - Example 	🙀 [all orgs]				SNMP				161	1500	3	2015-05-	Create P	owerShell Cree	dential
5. A Cisco SNMPv3 - Example	👔 (all orgs)				SNMP	[USER_GOES_HERE]			161	1500		2015-05- 4			
5. 🤌 Cisco: ACI	🙀 [all orgs]			126	Basic/Snippet	admin	173.36.219.46		443	0	62	2015-05-14 1		em7admin	
Cisco: ACI Credential	👔 [all orgs]				Basic/Snippet	admin	198.18.133.200		443	0	61	2015-05-14 1		em7admin	
Cloudkick - Example	🙀 [all orgs]				Basic/Snippet	[SECURITY KEY GOES			443	5000	9	2015-05-14 1		em7admin	
 PCUCM PerfmonService 8.0 Example 	🙀 (all orgs)				SOAP/XML Host		%D		8443	2000	4	2015-05-14 1	1:25:12	em7admin	
. 🤌 EM7 Central Database	🙀 [all orgs]				Database	root	localhost		7706	0	51	2015-05-14 1	1:26:41	em7admin	
A EM7 Collector Database	[all orgs]				Database	root	%D		7707	0	14	2015-05-14 1	1:25:43	em7admin	
A EM7 DB	(all orgs)				Database	root	%D		7706	0	35	2015-05-14 1	1:26:32	em7admin	
P EM7 DB - DB Info	(all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 1	1:26:32	em7admin	
A PEM7 DB - My.cnf	[all orgs]				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 1	1:26:32	em7admin	
A EM7 DB - Silo.conf	(all orgs)				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 1	1:26:32	em7admin	
PEM7 Default V2	(all orgs)				SNMP				161	1500	10	2015-05-14 1	1:25:42	em7admin	
P EM7 Default V3	(all orgs)				SNMP	em7defaultv3			161	500	11	2015-05-14 1	1:25:42	em7admin	
A EMC - Example	(all orgs)				Basic/Snippet	root	%D		443	10000	15	2015-05-14 1	1:25:47	em7admin	
A GoGrid - Example	(all orgs)				Basic/Snippet	(SECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 1	1:25:51	em7admin	
. PIPSLA Example	(all orgs)				SNMP				161	1500	5	2015-05-14 1	1:25:14	em7admin	
P LifeSize: Endpoint SNMP	(all orgs)				SNMP	control			161	3000	18	2015-05-14 1	1:25:58	em7admin	
2. A LifeSize: Endpoint SSH/CLI	[all orgs]				Basic/Snippet	auto	%D		22	3	17	2015-05-14 1	1:25:58	em7admin	
A Local API	(all orgs)				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 1	1:26:11	em7admin	
NetApp 7-mode	(all orgs)				Basic/Snippet	root	%D		443	3000	24	2015-05-14 1	1:26:20	em7admin	
A NetApp w/SSL Option	(all orgs)				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 1	1:26:20	em7admin	
NetApp w/SSL Option Off	all orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 1	1:26:20	em7admin	
A Nexus netconf	(all orgs)				Basic/Snippet		%D		22	10000	6	2015-05-14 1	1:25:16	em7admin	
8. A Nexus snmp	(all orgs)				SNMP				161	10000	7	2015-05-14 1	1:25:16	em7admin	
Polycom - Advanced	all orgs]				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 1	1:26:24	em7admin	
. Polycom - CDR	all orgs]				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 1	1:26:24	em7admin	
1. @ Polycom - Interface	(all orgs)				SOAP/XML Host	admin	%D		80	20000	29	2015-05-14 1	1:26:24	em7admin	
ewing Page: 11			_	_							_	[Select Ac	tion		Go

4. The **Credential Editor** page appears, where you can define the following fields:

Credential Editor	×
Create New PowerShell Credential	Reset
Basic Settings Profile Name	Account Type
Hostname/IP	[Active Directory] ▼ Timeout(ms)
Username	Password
Encrypted Port [yes]	PowerShell Proxy Hostname/IP
Active Directory Settings Active Directory Hostname/IP	Domain
Save	

- **Profile Name**. Name of the credential. Can be any combination of alphanumeric characters.
- Hostname/IP. Hostname or IP address of the device from which you want to retrieve data.
 - 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.

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.
 - *n*o. 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.
- 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.
- **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	32
Creating an Automation Policy	
Customizing an Automation Policy	
Removing an Automation Policy from a PowerPack	

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 Remote 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.

Automation Policy Editor Editin	g Automation P	olicy [71]		Reset
Policy Name Windows PowerShell: Run Memory Diagnos	Policy Type	Policy St		Organization
Criteria Logic	Match Logic		Match Syntax	(,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
[and no time has elapsed] (since the first occurrence.]	Repea			With
[and event is NOT cleared] [and all times are valid] Tigger on Child Rollup	[Only once]	▼ Intities other than device	Device Groups	▼ ets, etc.)
Available Device Groups		Aligned Device Grou		
AWS EC2 Instances LayerX Appliances Microsoft Azure: Storage Disks Microsoft Azure: Virtual Machines Servers SL1 Appliances	22			*
Available Events [3158] Critical: AKCP: AC Voltage sensor det [3167] Critical: AKCP: DC Voltage sensor Lio [3168] Critical: AKCP: DC Voltage sensor Lo [3157] Critical: AKCP: DY contact Sensor LC [3163] Critical: AKCP: Smoke Detector Alert!	h Critical w Critical w Critical	[2916] Major: Micros [2918] Minor: Micros	soft: Windows Available soft: Windows Pages p soft: Windows Paging F	er Second has exce
[3161] Critical: AKCP: Water Sensor has dete	ected water	Aligned Actions		*
SNMP Trap [1]: SL1 Event Trap Snippet [5]: Automation Utilities: Calculate Mr Snippet [5]: AWS: Disable Instance By Tag Snippet [5]: AWS: Object Testance Configur Snippet [5]: AWS: Get EC2 Instance Configur Snippet [5]: AWS: Merge Physical with Comp	ration	1. Snippet [5]: Autor 2. Execute Remote 3. Snippet [5]: Data	mation Utilities: Calcula PowerShell Request [1 center Automation: For	05]: Windows
	Save	Save As		

- 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 Remote 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:

utomation Policy Editor Editin	ng Automation P	'olicy [119]		Res	et
Policy Name	Policy Type	Policy State	Policy Priority	Organizatio	n
Windows PowerShell: Run Print Job Error Di	[Active Events] 🔻	[Enabled]	[Default] 🔻	[System]	•
Criteria Logic	Match Logic		Match Syntax		
[Severity >=] ▼ [Minor,] ▼	[Text search]				
[and no time has elapsed]	Repe	at Time	Δlic	an With	
[since the first occurrence,]	[Only once]	•			•
[and event is NOT cleared]			vices (organizations, as		
Trigger on Child Rollup					
vailable Devices		Aligned Devices			
		(All devices)			
Bananaquit AWS: Service: JEM-Virtual	_				
Cardinal		x			-
vailable Events		Aligned Events			
		[5107] Minor: Mic	rosoft: Windows Print Jo	b Errors exceeded	t 🛓
[3186] Critical: AKCP: AC Voltage sensor de	tects no current 🔺	<u> </u>			
[3195] Critical: AKCP: DC Voltage sensor Hi [3196] Critical: AKCP: DC Voltage sensor Lo	-	x			-
vailable Actions	W Childai	Aligned Actions			
			te PowerShell Request	[111]: Windown	
Snippet [5]: Enrichment: Util: Format Comma			richment: Util: Format C		1
Snippet [5]: Enrichment: Util: Load Work Inst	ructions =	«			
Snippet [5]: Enrichment: Wireless: Anchor Si	how Commands 🍸	`		Ψ.	Ļ

- 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 (
- 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.

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).

This appendix covers the following topics:

Run Book Variables

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	
%К	Asset	Asset Floor	
%P	Asset	Asset plate	
%р	Asset	Asset panel	
%q	Asset	Asset zone	
%Q	Asset	Asset punch	
%U	Asset	Asset rack	
%u	Asset	Asset shelf	
%v	Asset	Asset tag	
%w	Asset	Asset model	

Variable	Source	Description		
%W	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 the value that matches the <i>Identifier Pattern</i> field in the event definition.		
%Т	Dynamic Alert	Value returned by the Threshold function in a Dynamic Application Alert.		
%∨	Dynamic Alert	Value returned by the Result function 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 name 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.		

Variable	Source	Description
%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 • 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	Timestamp of when event was deleted.
%6	Event	Timestamp for event becoming active.

Variable	Source	Description		
%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	Timestamp of last event occurrence.		
%D	Event	Timestamp of first event occurrence.		
%e	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		
%Х	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		
%Е	Event Policy	External ID from event policy		
%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.		

Variable	Source	Description		
%G	Event Policy	Event 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		
%C	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,		
%t	Ticket	%7 represents severity (for previous versions of SL1).		
/01				

Appendix

B

Configuring Windows Servers for Monitoring with PowerShell

Overview

The following sections describe how to configure Windows Server 2016, 2012, 2012 R2, or 2008 R2 for monitoring by SL1 using PowerShell:

Prerequisites	46
Configuring PowerShell	46
Step 1: Configuring the User Account for the ScienceLogic Platform	47
Option 1: Creating an Active Directory Account with Administrator Access	47
Option 2: Creating a Local User Account with Administrator Access	48
Option 3: Creating a Non-Administrator User Account	48
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	50
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	50
Creating a User Group and Adding a User in Active Directory	. 50
Setting the Session Configuration Parameters and Group Permissions	.51
Creating a PowerShell Credential	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	55
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	
Step 3: Configuring Windows Remote Management	55
Option 1: Using a Script to Configure Windows Remote Management	

Option 2: Manually Configuring Windows Remote Management	61
Option 3: Using a Group Policy to Configure Windows Remote Management	64
Step 4: (Optional) Configuring a Windows Management Proxy	82
Step 5: (Optional) Increasing the Number of PowerShell Dynamic Applications That Can Run	
Simultaneously	83

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.

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 Microsoff'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 2008, click [Start], right-click [Computer], click [Manager], and then expand [Configuration].
 - 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. In the Management console, go to System Tools > Local Users and Groups > Groups.
- 16. 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].
- Perform steps 16-20 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"

23. 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.

24. 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.

roup or user names:	AD DCContine	Constant
Administrators (MSTESTLAB-H) Remote Management Users (M	/01\Administrat	ors)
	Add	Bemove
ermissions for PSSession reators	Allow	Deny
Full Control(All Operations)	~	
Read(Get,Enumerate,Subscribe)		
Write(Put.Delete.Create)		
Execute(Invoke)		
Special permissions		
or special permissions or advanced ick Advanced	settings,	Advanced

- 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.

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:

- You have created an Active Directory user account on the Windows Server to allow communication between SL1 and the server. In this scenario, Active Directory will use Kerberos and AES-256 encryption to ensure secure data transfer and authentication, which means you do not need to configure a self-signed Server Authentication Certificate. You can skip this section and proceed to Step 3.
- You have created a *local account* on the Windows Server that uses Basic Auth to allow communication between SL1 and the server, and 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.
- You have created a *local account* on the Windows Server that uses Basic Auth to allow communication between SL1 and the server, and your network *does not include a Microsoft Certificate server*. In this scenario, you must configure a self-signed 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: Self-signed certificates are appropriate for use on a trusted network, such as a LAN that includes both a ScienceLogic Data Collector and the Windows Server to be monitored.

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:

or ^ soft Cor	1	Console Root	Edit Extensions
			Remove
soft Cor			
soft Cor 😑			
soft Cor			Move Up
soft Cor			Move Down
soft Cor	Add >		Hove Down
soft and			
soft Cor			
soft Cor 🖕			Advanced
~ -		L	
	oft Cor oft Cor	oft Cor oft Cor oft and oft Cor oft Cor oft Cor oft Cor oft Cor oft Cor oft Cor oft Cor	oft Cor oft Cor oft and oft cor oft Cor

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

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

Certificates snap-in		x
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.
- 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, see:

https://msdn.microsoft.com/library/windows/desktop/aa386968.aspx

• For details on creating a self-signed certificate with MakeCert and installing the certificate in the Trusted Root Certification Authorities store, see:

https://msdn.microsoft.com/en-us/library/ms733813%28v=vs.110%29.aspx

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:

https://docs.microsoft.com/en-us/powershell/module/pkiclient/newselfsignedcertificate?view=win10-ps

• You can use the **Export-PfxCertificate** command to export the private certificate. For information on the **Export-PfxCertificate**, see:

https://docs.microsoft.com/en-us/powershell/module/pkiclient/export-pfxcertificate?view=win10-ps

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 on the ScienceLogic portal 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 Services, 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:

- Log in to the ScienceLogic portal, go to Downloads > Miscellaneous, and download the PowerShell script named WinRM Configuration Wizard Script (winrm_configuration_wizard.ps1). The link is : https://portal-cdn.sciencelogic.com/powerpackextras/5819/18486/winrm_configuration_wizard.zip
- 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.ps1* 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.ps1.
- 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>

The user account you wish to use for SL1 collection must be specified with the -user command-line 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

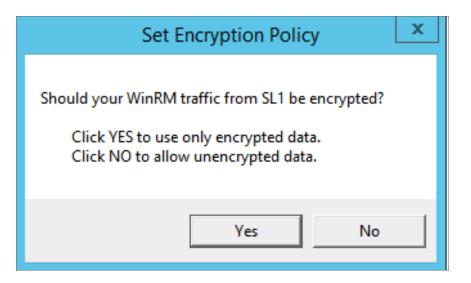
10. If you start the script without using the -silent command-line argument, the **WinRM Installation Wizard** modal page appears. Click **[OK]**.

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 page appears. Select the appropriate choice for your environment.

Windows Account Type
Will you be using an Active Directory domain account? Click YES to enable Kerberos Authentication. Click NO to enable Basic Authentication.
Yes No

12. The Set Encryption Policy modal page 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 page 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 **Set Ports for WinRM Traffic** modal page 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	:
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]

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

Set HT	TP/HTTPS Ports	_ □	x
New HTTP port:	5985		
New HTTPS port:	5986		
		ОК	

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

Set HTTPS Thumbprint	C
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.

17. The **Confirm Settings** modal page appears. If the settings are as you specified, click **[OK]**.

Confirm Settings	ĸ
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]

18. The **Complete** modal page 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.	
OK Cancel	

19. 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.
- 2. Right-click on the PowerShell icon in the taskbar or the Start menu, and select Run as Administrator.
- 3. Execute the following command:

Get-ExecutionPolicy

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

Set-ExecutionPolicy RemoteSigned

- 5. Enter "Y" to accept.
- Execute the following command: winrm quickconfig
- 7. Enter "Y" to accept.
- If you are configuring this Windows server for encrypted communication, execute the following command: winrm quickconfig -transport:https
- 9. Enter "Y" to accept.
- 10. Execute the following command:

winrm get winrm/config

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

```
Config
  . . .
  Client
     . . .
     Auth
       Basic = true
        . . .
       Kerberos = true
       . . .
     . . .
  Service
     . . .
     AllowUnencrypted = false
     . . .
     DefaultPorts
       HTTP = 5985
       HTTPS = 5986
     . . .
     AllowRemoteAccess = true
  Winrs
     AllowRemoteShellAccess = true
     . . .
```

11. In the Service section, if the parameter AllowRemoteAccess 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

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

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

13. 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

14. 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.

- 15. 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

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 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 MIIDpTCCAo2gAwIBAgIQHAmGt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/IsZAEZFg1NUlRMMDEy UJIJTJAJBgNVBAMTHEITVEwwHJJSMilUTDAxMIJL/URDLTAXLUNBLTEwHhcMMTQw NDEIMTYINTQ1WhcNMTkwNDEIMTcwNTQ1WjBZMRUwEwYKCZImiZPyLGQBGRYFbG9j YWwxGTAXBgoJkiaJk/IsZAEZFg1NUlRMMDEyUJIXJTAjBgNVBAMTHEITVEwwHTJS MIUTDAxMIJYURDLTAxLUNBLTEwggE1MAOCCSqGSIbJDQEBAQUAA41BDwAwgEK AoIBAQCmsP0NZQIJA5pxq19ZrofUCZFaoBISpG0IyMiit+risfVAG1RgVFvC3mQK TKoOWqeiuNAuhl1fYFIhOsORN50FHgUNgrasdrvugSPL/oV23VDH2dqjHaDd6azY 7CcWfD6uu30V0aZU9Sgt4HEymPU14QKGuz1n4UTXIdepCAoN37oyNkoQgOLLUutp Q81i6YdkbYaU0wWyKnvS0osQpqAF5dFW7rgt80bIXf9F2n13yuwogEpFeQ+E8UH4 JGmtOpSZt7hsFDMXKkvRhdPugH7rIONG1a0xyoVUUVqfiiK7X8LiE/Qve0X73wBo 7XLVsMSbWNo95Nxnf8/hiUTJ0pOnAgMBAAGjaTBnMBMGCSsGAQQBgjcUAgQGHgQA QWBBMA4GALUdDwEB/wQEAwIBhjAPBgNVHRMBAf8EETADAQH/MBOGALUdDgQWBBR9 QjSBuyfql2Prforx0g/29102uDAQBgksFgEAYISPEEAwIBADANBgkqhki69w0B AQUFAA0CAQEATSkQpaWp06i0TT+13980IS1HbT1n6AyVGizU2MnRAWLKAxguEdha R/+1RL/qkNXJeqjpDAFsz22EIvei0KVCIbwEXeKePZNQG1ujr2FLRbWWt+0A0/ES G4rxLIw//4sOHK5JmRYCXJ02DK8zrH0ZADV/Trn6CEWxYB6GAQUFZTQsm9WbUK trDopF270DW29LGZ6z7TNn10XoKxEqUqCfR8EFFkctYrZ/+bNFV8V3YJjdAm/42g 4hjdX04PGIhDj0Bg2srX+01tx8mAMjAvUdNg2kvU0m0dP6h17BqJJ08umJxPmfQI VWF1gMeTUNHfTYUJJdEeRZQhLhK6rkAnHw== END CERTIFICATE CertUtil: -ca.cert command completed successfully.	211	Administrator: Command Prompt	
	A cert[0]: 3 Valid A cert[0]: BEGIN CERTIFICATE: IIIDpTCCAo2gAwIBAgIQHAr IRUWEwYKCZImi2PyLGQBGR IJIXJTAjBgNVBAMTHE1TVEN IDEIMTYINTQ1WhCNNTKwNDB MWxGTAXBgoJkiaJk/IsZAB iiUTDAxMIJyLURDLTAXLU NOBAQCmSPONZQIJA5pxq1 KoOWqeiuNAuh11fYFIhOs(CcWfD6uu30V0aZU9Sgt4HE 81i6YdkbYaU0wWyKnvS0o 81i6YdkbYaU0wWyKnvS0o 80f0p5Zk7hsFDMxXkvRhdf XLVSMSbWN09SNxnf8/hiU WBBMA4GA1UdDwEB/wQEAW 1jsBuyfqH2Prforx0g/z910 QUFAAOCAQEATSkQpaWp06 //+TRL/qkNXJeqjpDAFsz2; 4rxLIW/q4S0HKSJmRYCX: rDogF270DW29LGZ6z7TNn thjdX04PG1hDj0Bg2srX+0 WF1gNeTUNHFTyuJdEeR70 END CERTIFICATE certUtil: -ca.cert com	ngt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ /FbG9jYWwxGTAXBgoJkiaJk/IsZAEZFg]NU1RMMDEy wMTJSMi1UTDAxMIIyLURDLTAxLUNBLTEwHhcNMTQw ilmTcwNTQ1WjBZMRUwEwYKCZImiZPyLGQ8GRYFbG9j iZFg]NU1RMMDEyUjIXJTAjBgNVBAMTHE1TVEwwMTJS WBLTEwggEiMA0GCSqGSIbJ0QEBAQUAAHBDwAwggEK 22rofUCZFaoBISpG0IyMiit+risfVA4JIBOwAwggEK 22rofUCZFaoBISpG0IyMiit+risfVA4JIRVFvc3mQK DRNSOFHgUNgrasdrvugSPL/oV23VDH2dqjHaDd6azY symPU14QkGu21n4UTXIdepCAoN370yNkoQg01LUutp sQpqAFSdFW7rgt8ObIXf9F2n13yuwogEpfeQ+E8UH4 YugH7rIONGia0xyoVuUVqfiiK748LiE/Qve0X73wBo JODOnAgMBAAGjaTBnMBMGCSsGAQQBgjcUAgQGHqQA EBhjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBR9 20WDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B 10T+13980Is1HbT1n6AyVGizU2MnRAWLKAxguEdha 2EIveiOKVCIbwEXeKePZNQG1uj7FLRbUWt+oA0/ES JoDZbK8rH0ZADv/TTrn6CEWxYB6GJ008umJxPmfQI 2hLhK6rkAnHw== 	

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.

<u>k</u>			Server Ma	anager			- 0
<u> </u>	lanager • Dashboa						CO Manage Tools View Help Active Directory Administrative Center Active Directory Domains and Trusts
Dashboard Local Server All Servers All Servers AD CS AD DS DNS File and Storage Services P IIS	QUICK START	Configu 2 Add ro 3 Add ot	re this local se les and features her servers to ma a server group			Active Directory Module for Windows PowerShell Active Directory Sites and Services Active Directory Users and Computers ADSI Edit Certification Authonity Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management	
	LEARN MORE ROLES AND SERVER GROU Roles: 5 Server groups: 1						Internet Information Services (IIS) Manager ISCSI Initiator Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor
	AD CS	1	AD DS	1	e	DNS	 Resource Monitor Security Configuration Wizard Services
	Manageability Events Services Performance BPA results		 Manageability Events Services Performance RPA results 		•	Manageability Events Services Performance BPA results	Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security 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.

1			Group Policy Ma	anagement		- 0 ×
File Action View						_ # ×
🗢 🏟 🖄 📰 📋						
Group Policy Manager		Group Policy Contents Delega	Objects in MSTL012R2.local			
⊿ B Domains ⊿ MSTL012R2	local	Name	*	GPO Status	WMI Filter	Modified
🛒 Defa	Create a GPO in this domain, a	and Link it here	trollers Policy	Enabled	None	3/19/201
Powe Dom	Link an Existing GPO Block Inheritance		cy Management Policy	Enabled All settings disabled All settings disabled	None None None	2/4/2014 4/17/201 4/16/201
⊳ 📑 Grou ⊳ 🕞 WMI ⊳ 🛅 Start	Group Policy Modeling Wizard New Organizational Unit	ł				
Image: Sites Big Group Polic Compared Compare	Search Change Domain Controller Remove Active Directory Users and Co	mputers				
	New Window from Here					
	Refresh					
	Properties					
	Help					
		<		10		2
Create a GPO in this doma	in and link it to this container					

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.

		Group Policy Ma	nagement		- 0 ×
File Action View					_ 8
- 🔿 🖄 📰 📋					
Group Policy Managen		Group Policy Objects in MSTL012R2.local Contents Delegation			
	Domain Policy Iell Remote Management Policy	Name	GPO Status Enabled Enabled Al settings disabled All settings disabled	W/MI Filter None None None None	Modifie 3/16/2 4/17/2 4/17/2 4/16/2

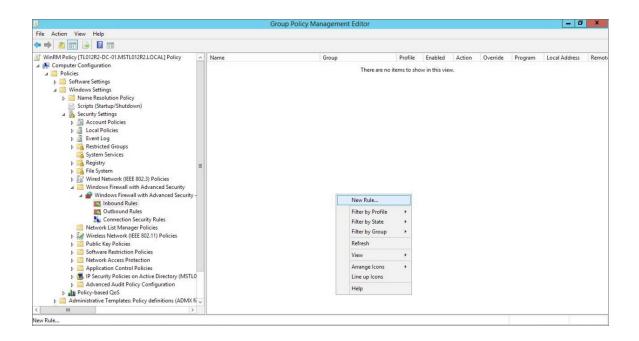
 In the left panel, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > System Services. In the right panel, locate the Windows Remote Management (WS-Management) service. Right-click the service, then select Properties.

Group Policy Management Editor							
ile Action View Help							
• 🔿 🙍 🔀 🚍 😹 🛛 🖬							
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	Service Name		Startup	Permission			
	🗱 User Access Logging Service		Not Defined	Not Defined			
	User Profile Service		Not Defined	Not Defined			
	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 Accal Policies	Windows Color System		Not Defined	Not Defined			
- Call	Windows Connection Manager		Not Defined	Not Defined			
Event Log Restricted Groups	Windows Driver Foundation - User	-mode Driver Framework	Not Defined	Not Defined Not Defined Not Defined Not Defined			
System Services	Windows Encryption Provider Host	Service	Not Defined				
A Registry	Windows Error Reporting Service		Not Defined	Not Defined			
File System	Windows Event Collector		Not Defined	Not Defined Not Defined			
	Windows Event Log		Not Defined	Not Defined			
	Windows Firewall		Not Defined	Not Defined			
	Windows Font Cache Service		Not Defined	Not Defined			
	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 Service	e	Not Defined	Not Defined			
Application Control Policies	Windows Remote Management	(C Managamant)	Not Defined	Not Defined			
IP Security Policies on Active Directory (MSTL012F)			Not Defined	Not Defined			
Advanced Audit Policy Configuration	Windows Time	Help	Not Defined	Not Defined			
Policy-based QoS	Windows Update		Not Defined	Not Defined			
Administrative Templates: Policy definitions (ADMX files)	WinHTTP Web Proxy Auto-Discovery Service		Not Defined	Not Defined			
Preferences	Wired AutoConfig			Not Defined			
5 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			
ш >			Description of the Des				

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].

J	Group Policy Management	Editor		- 🖬 X
File Action View Help				
🗢 🔿 🙍 📷 💥 🗟 🗟 🖬				
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Computer Configuration	Service Name	Startup Not Defined	Permission Not Defined	^
Policies Policies Software Settings Mindows Settings	User Profile Service	Not Defined	Not Defined	
Marne Resolution Policy Scripts (Startup/Shutdown) By Security Settings	W30 Security Policy Setting		Not Defined Not Defined Not Defined	
 Account Policies Local Policies Event Log Restricted Groups 	Windows Remote Management (WS-Mana Windows Remote Management (WS-Mana	generic	Not Defined Not Defined Not Defined	
 A restricted oroups System Services Registry Refite System 	Win Win Win Win Automatic		Not Defined Not Defined Not Defined	
Wired Network (IEEE 802.3) Policies Windows Firewall with Advanced Security Network List Manager Policies	Win Manual Win Disabled		Not Defined Not Defined Not Defined	
Wireless Network (IEEE 802.11) Policies Public Key Policies Software Restriction Policies	Win Edit Security		Not Defined Not Defined Not Defined	
 Metwork Access Protection Application Control Policies IP Security Policies on Active Directory (MSTL012F 	Win Win		Not Defined Not Defined	
Advanced Audit Policy Configuration Policy-based QoS	Win OK Ca Win Win Win Windows Update	Not Defined	Not Defined Not Defined Not Defined	-
Administrative Templates: Policy definitions (ADMX files) A files Second	WinHTTP Web Proxy Auto-Discovery Service Wired AutoConfig WMI Performance Adapter	Not Defined Not Defined Not Defined	Not Defined Not Defined Not Defined	=
Policies Preferences	Workstation World Wide Web Publishing Service	Not Defined Not Defined	Not Defined	Ļ

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.



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 Management Ed	itor						- 0	x
File Action	View Help									
🗢 🌳 🖄	🖬 🖻 🖪 🖬									
WinRM Pe	@	New Inbound Rule Wizard	×	Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ 🚰 Po ▶ 🛱 ⊿ 🚰	Rule Type Select the type of firewall rule	to create.		ems to shov	w in this view	Ν.				
Þ	Steps:									
⊿	Rule Type	What type of rule would you like to create?								
	Predefined Rules									
	 Action 	Program Rule that controls connections for a program. Port Rule that controls connections for a TCP or UDP port. Predefined:								
		I	~							
		Rule that controls connections for a Windows experience. O Custom Custom rule.								
¢		< Back Next > C	ancel							

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

J		C	Group Policy	Manageme	ent Editor							- 0	x
	View Help												
🗢 🔿 🖄						x	Profile	Enabled	Action	Override	0	Local Address	Remot
A 🛃 Comp								w in this vie		Override	Program	Local Address	Kemot
🔺 🧮 Po	Predefined Rules						ems to sho	w in this vie	w.				
	Select the rules to be created for this experience.												
Þ	Steps:												
4	Rule Type	Which rules would you like to create?	Which rules would you like to create?										
	Predefined Rules	The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of											
	Action	Rules that are checked will be created. If a rule alreat the existing rule will be overwritten.	ady exists and is	checked, the co	ntents of								
		Rules:	Rule Exists	Profile	Desc								
		Windows Firewall Remote Management (RPC		All	Inbou								
		✓ Windows Firewall Remote Management (RPC)	No	All	Inbou								
		< III			>								
Þ Þ 🚞			< Back	Next >	Cancel								
< 1		L			Sanoor	_							
						_							

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

J		Group Policy Management Editor							- 6) X
File Action	View Help									
	🖬 🔒 🔽 🖬									
WinRM Pe	2	New Inbound Rule Wizard	x	Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ 💭 Po ▷ 🛄 ⊿ 🛄 ▷		when a connection matches the conditions specified in the rule.		ems to sho	ow in this vie	w.				
A A	Sleps: a Rule Type b Predefined Rules a Action	What action should be taken when a connection matches the specified conditions?								
¢		< Back Finish Cance								

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 Pol	icy Management Editor		_ 0 ×
File Action View Help				
* * 2 📰 @ 🖻 🖬 🖬				
⊿ 🧾 Windows Settings 📃 ∧	Automatic Certificate Request	•		-
▶ Name Resolution Policy ■ Scripts (Startup/Shutdown) ■ ■ ■		There	are no items to show in this view.	
Encrypting File System Data Protection		New	Automatic Certificate Request]
BitLocker Drive Encryption		Refresh	-	
BitLocker Drive Encryption Network Unlock Automatic Certificate Request Settings		View		
Trusted Root Certification Authorities Enterprise Trust		Arrange Icons		
Intermediate Certification Authorities		Help		
Induced Publishers Induced Publishers Induced Certificates Induced People is Software Restriction Policies is Software Restriction is Software Restriction is Restriction Control Policies is IP Security Policies on Active Directory (IMSTLO iff policies on Active Directory (IMSTLO iff policies on Active Directory (IMSTLO			_	

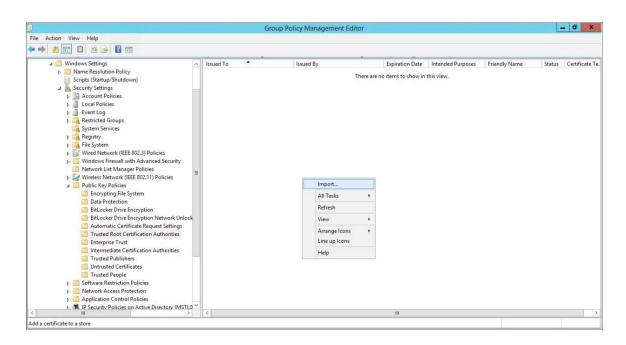
17. The Automatic Certificate Request Setup Wizard modal page appears. Click [Next].

Automat	tic Certificate Request Setup Wizard	Group Policy Management Editor	- 0 X
	Welcome to the Automatic Certificate Request Setup Wizard This wizard helps you set up automatic certificate requests for computer. Using automatic certificate requests, an administrator can specify which yous of certificate can be automatically requested by a computer.	request There are no items to show in this view.	
 Bitl.cc Auton Truster Intern Truster Intern Truster Software Software Application 	< Back Neet > Cancel ker Drive Encryption cker Drive Encryption Network Unlock cker Drive Encryption Network Unlock natic Certificate Request Settings cker Drive Encryption Network Unlock cker Drive Encryption Network Unlock atic Certification Authorities cker Drive Encryption Network Unlock cker Drive Encryption Network Unlock ate Certification Authorities cker Drive Driv		

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

	cate Request Setup Wizard	x Group Policy Man	agement Editor		- 0
Certificate Template The next time a computer logs on, a provided.	certificate based on the template you select is	equest •			
A certificate template is a set of pred computers. Select a template from th Certificate templates:	efined properties for certificates issued to e following list.		There are no iten	ns to show in this view.	
Name Computer Domain Controller Enrollment Agent (Computer) IPSec	Intended Purposes Client Authentication, Server Authentication Client Authentication, Server Authentication Certificate Request Agent IP security IKE intermediate				
۲. III	>				
📑 BitLocker Drive E	< Back Next > Cancel ncryption ncryption Network Unlock				
	icate Request Settings tification Authorities tification Authorities				
 Intermediate Cer Trusted Publishe Untrusted Certifi Trusted People Software Restriction Network Access Pro 	cates Policies				

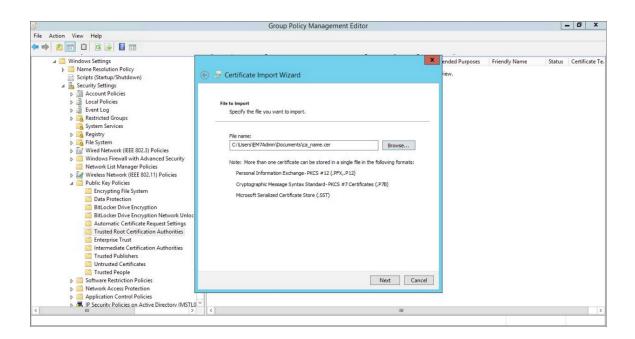
19. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration
 > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification
 Authorities. In the right panel, right-click and select Import.



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

	Group Policy Management Editor		- 0 ×
ile Action View Help			
▲ ▲ Windows Settings ▶ ▲ Name Resolution Policy ➡ Scripts (Startup/Shutdown)	🔰 🖉 Certificate Import Wizard	ended Purposes Friendly Name	Status Certificate Te
 J Security Settings A Account Policies J J Local Policies J Local Policies J Restricted Groups 	Welcome to the Certificate Import Wizard		
iii System Services ▷ iii Registry ▷ iii System	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.		
Wired Network (IEEE 802.3) Policies Mindows Firewall with Advanced Security Network List Manager Policies Metwork List Manager Policies	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.		
Wireless Network (IEEE 802.11) Policies Public Key Policies	Store Location		
Encrypting File System	O Current User		
Data Protection BitLocker Drive Encryption	Local Machine		
Bit Ocker Unive Encryption Bit Ocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Dublichers	To continue, dick Next.		
Untrusted Certificates			
Trusted People	Next Cancel	1	
Network Access Protection	INEXT Caller		
Application Control Policies			
b R. IP Security Policies on Active Directory (MSTL0)			

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



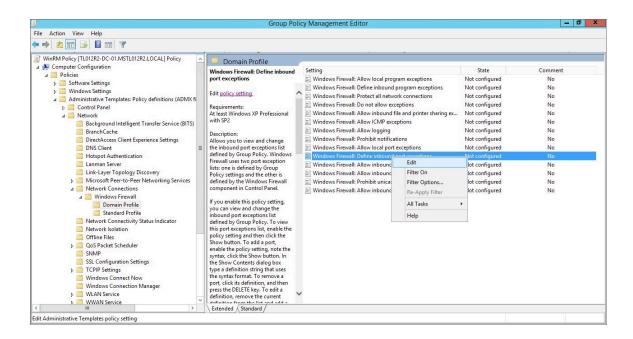
22. Select the **Place all certificates in the following store** radio button, then select the *Trusted Root Certification Authorities* certificate store and click [Next].

L.	Group Policy Management Editor			Ŀ	- 0	x
File Action View Help						
⊿ 📑 Windows Settings ▷ 🗃 Name Resolution Policy 📓 Scripts (Startup/Shutdown)	Certificate Import Wizard					
Security Settings Barrow Account Policies Dail Local Policies Dail Event Log Dail Restricted Groups Gystem Services	Certificate Store Certificate stores are system areas where certificates are kept.					
System services System services System services System S	Windows can automatically select a certificate store, or you can specify a location for Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse					
Trusted People Carlot Content of the second	Next Cancel					
Application Control Policies A	v (III					>
						-

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

9	Group	Policy Management Editor			Ŀ	- 🗇 X
File Action View Help						
◆ ◆ ≥ 🗊 🛍 @ ≥ 🛛 🖬						
 Windows Settings Name Resolution Policy Scripts (Startup/Shutdown)) 📀 🎐 Certificate Import Wi	ended Purposes	Friendly Name	Status	Certificate T	
 Jaccount Policies Jaccount Policies Jaccount Policies Jaccount Policies Jaccount Count Policies Jaccount Count Policies 	Completing the C	ertificate Import Wizard				
Case System Services ▷ Case Registry ▷ Case File System	The certificate will be import					
Windows Firewall with Advanced Security Windows Firewall with Advanced Security Wireless Network (IEEE 802.11) Policies Wireless Network (IEEE 802.11) Policies Wireless Network (IEEE 802.11) Policies Date Protection		Ny User Jon 1970 - Certification Authorities Certificate C: Users EM7Admin/Documents/cs_name.cer				
BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authorities Interprise Trust Interprise Trust						
		Finish Can	cel			
< װ >	<	ш				

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.

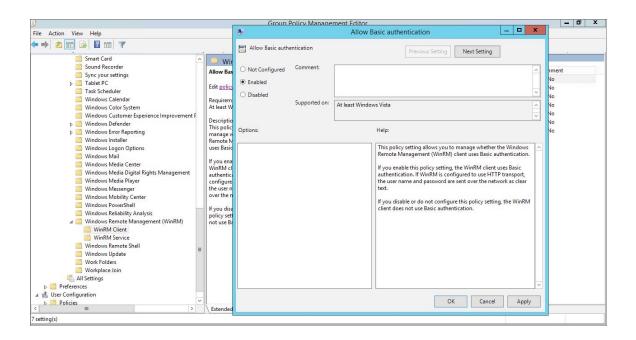


25. The Windows Firewall: Define inbound port exceptions modal page appears. Under Options, click [Show].

26. The **Show Contents** modal page appears. Enter the following values:

		Group Policy Management Editor	– 0 ×
File Action View H	Windows F	rewall: Define inbound port exceptions	
🔶 🌩 🙎 📰 🗟	Windows Firewall: Define inbound port e	reptions Previous Setting Next Setting	
⊿ A Computer Config ⊿ Policies	O Not Configured Comment:	^ xceptions	State Comment Not configured No
▷ Software Softwa	Enabled Disabled	am exceptions nnections	Not configured No Not configured No
⊿ 📫 Administr ▷ 📫 Contro ⊿ 📬 Netwo	Supported on: At le	st Windows XP Professional with SP2	Not configured No
Bai Bai Bra Dir	Options:	Define port exceptions:	Not configured No Not configured No Not configured No
DN Ho	Define port exceptions: Show	Value 5985.TCP:*enabled:WSMan	Not configured No Not configured No
i≣ Lar i≊ Lin ⊳i≣ Mi	Specify the port to open or block. Syntax:	* exception	Not configured No ns Not configured No
▶ 🧾 Mi ⊿ 🗂 Ne ⊿ 🦳	<pre><port>:<transport>:<scope>:<status>:< < <</status></scope></transport></port></pre>		Not configured No Not configured No
Ine Ine Ine Infi Infi Infi Infi Infi Infi Infi Infi	<transports "tcp"="" "udp"<="" either="" is="" or="" p=""> <scope> is either "*" (for all networks) or a comma-separated list that contains any number or combination of these:</scope></transports>	OK Cancel	
≦ SN SSI D TC Wi Wi Wi	IP addresses, such as 10.0.0.1 Subnet descriptions, such as 10.2.3.0/2.	also enable the "Windows Firewall: Allow local port exceptions"	
⊳ 🛄 WL ⊳ 🗎 W < 🔋 Ⅲ		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.



- 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]**.

<u>I</u>	Group Policy Mapagement Editor	- 0 X
File Action View Help	Trusted Hosts	
	Trusted Hosts Previous Setting Next Setting	
	ed + O Not Configured Comment: mm Image: Second	int
Windows Logon Options Windows Mail Windows Mail Windows Mail Windows Media Center Windows Media Digital Rights Management Windows Media Player Windows Mobility Center Windows Mobility Center Windows Remote Management (WinRM) Windows Update Wondows Wondows Update	and solution Interface state Syntax: syntax: If you enable this policy setting the WinRM client uses the list entry. and syntax: If you enable this policy setting the WinRM client uses the list specified in TrustadHostList to determine if the destination host is a trusted entry. and foot names. You can use wildcards (") but only on wildcard is allowed in a host name pattern. If you disable or do not configure this policy setting and the WinRM client uses the ist when enther thost. dist dist all host names that do not contain a period (.). If you disable or do not configure the list of trusted hosts locally on each computer. to to to to to to to the list of trusted hosts locally on each computer. If you disable of trusted hosts locally on each computer.	
b Policies Control Contro Control Control Control Control Control Control Con		
7 setting(s)		

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>.</u>	Group	Policy Manage	ment Editor			- 0 X
File Action View Help			Allow B	lasic authentication	_ 🗆 X	
← → 2 III → II → II → Win Smart Card Sound Recorder Allow Bas	Allow Basic auth	entication Comment:		Previous Setting Next Setting	<u> </u>	ment
Sync your setting: Allow Bas > Table PC Edit golicy: Table PC Task Scheduler Windows Calendar Requirem Windows Color System Description > Windows Defender Description > Windows Golor Options This policy Windows Media Center Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows MediaPlayer Windows MediaPlayer Windows Workplate Windows Remote Admagement (WinRM) Windows Update Windows Remote Solid Windows Vipdate Windows Remote Solid Workplace Join Workplace Join Workplace Join Windows Media Player Workplace Join Workplace Join Workplace Join Windows Media Player Workplace Join	 Not Configured Enabled Disabled 	Supported on:	At least Window	Help: This policy setting allows you to manage whell femote Management (WinRM) service accepts suthentication from a remote client. If you mable this policy setting, the WinRM Basic authentication from a remote client. WinRM service does not accept Basic authentic remote client.	Basic I service accepts :y setting, the ation from a	40 40 40 40 40 40 40 40 40 40 40 40 40 4
< POILES III > Extended				OK Cano	el 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]**.

	Group Policy Management Editor	- 0 ×
File Action View Help	Allow remote server management through WinRM - 🗖 🗙	
	Allow remote server management through WinRM Previous Setting Next Setting	
Smart Card Sound Recorder Sync, your settings b Tablet PC Tablet PC Windows Calendar Windows Color System Windows Color System Windows Color System Windows Color System Windows Defender b Windows Media Pigner Windows Media Digital Rights Management Windows Remote Shell Windows Update Windows Update Windows Update Work Folders Work Fo	Image: Section of Previous Section Previous Previous Section Previous Section Previous Section Previous Section Pre	
C III Extended	d OK Cancel Apply	
IU setting(s)		

36. 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 ltem.

	Group Pol	icy Management Edito	r		- 0	X
File Action View Help						
🗢 🔿 🙍 🛅 🚔 🙆 📾 📓 🖬 🚳 🛇 🔸						
 WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Computer Configuration Policies Software Settings Software Settings Preferences Preferences IniFiles Folders IniFiles Software Settings Network Shares Software Settings Software Settings Network Shares Software Settings Software Settings Preferences Network Shares Software Settings Software Settings Software Settings Software Settings Software Settings Software Settings 	Processing (*) Processing (*)	Name C	Order Action Hive There are no New + All Tasks + Paste Refresh View + Arrange Icons + Line up Icons Help	Key I Items to show in this view. Registry Item Collection Item Registry Wizard	Value Name	Тур
< III >		1				
< III > Add a new registry item	│ Preferences │ Extended 〉 Standard	1				
Aud a new registry item						

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

1		Gr	oup Policy Manageme	ent Editor			- 0	x
File Action View Help								
🗢 🏟 📶 📋 📾 🙆 📓 🖬								
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy A Policies b Software Settings Computer Configuration b Software Settings		Registr	V New Registry Prope	rtion	Hive	Key	Value Name	Тур
	Pre	General Common		v	ere are no iten	ns to show in this view.		
 ➢ Folders ➢ Ini Files ☞ Registry ➢ Network Shares ➢ Nortcuts ➢ Control Panel Settings 	De	Hive: Key Path: Value name	HKEY_LOCAL_MACHINE SOFTWARE/Microsoft\Win LocalAccountTokenFilterPo					
a g ⁰ ₈ User Configuration N	Nd	Value type: Value data:	REG_DWORD	×				
				Base O Hexadecimal O Decimal				
			DK Cancel	Apply Help	111			>
< װ > >	Preferen	ices (Extended)	Standard /					
Registry								

- 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.
- 38. Click the [OK] button.
- 39. Repeat steps 36-38 to make an additional registry change to increase the maximum number of users who can access Windows Remote Management. In the New Registry Properties modal page, edit the following values:
 - Action. Select Create.
 - Hive. Select HKEY_LOCAL_MACHINE.
 - Key Path. Enter "SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\".
 - Value name. Enter "WinRS!MaxConcurrentUsers".
 - Value type. Enter "REG_DWORD".
 - Value data. Enter "0x64 (100)".
 - Base. Select Decimal.

40. 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.

	Group Pol	icy Managemer	nt Editor				_ (0
File Action View Help								
• 🔿 🙍 🛅 🖶 🍳 💀 🛛 🖬 🖄 🛇 🔸								
 WinRM Policy [TL012R2-DC-01.MSTL012R2LOCAL] Policy Computer Configuration Policies Software Settings Software Settings Administrative Templates: Policy definitions (ADMX files) Perferences Windows Settings Octoral Panel Settings Devices Devices Devices Devices Devices Devices Network Options Network Options 	Processing (*)	Name	Order Action T	Startup here are no item	- Account is to show in this	Interactive	Recovery	
	No policies selected		All Tasks Paste Refresh View Arrange Icons Line up Icons Help	> >	4			
(III >	♦ Preferences	/						

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

Group Policy Management Editor	- 0 X
File Action View Help	
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Software Settings Software Settings Software Settings Windows Settings Order Consultance Preferences Devices Devices Devices Devices Policies Devices Policies Devices Policies Policies Service name: Windows Settings Service name: Windows Settings Policies Devices Policies Devices Policies Policies Policies Service and Groups Network Options Policies Service formination Policies Service formiguration Policies Policies Policies Policies Policies Policies Policies Policies	Interactive Recovery ew.
< 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.
- 42. Click the **[Recovery]** tab, then edit the values in one or more of the following fields:

<u>I</u>	Group Policy Management Editor	- 0 X
File Action View Help		
WinPM Policy (TL01282-DC-01 MSTL01282 LOCAL) Policy	Pr New Service Properties Startup Account Interactive R Select the computer's response if this service fails. First failure: Restart the Service V Subsequent failures: Restart the Service V Subsequent failures: Restart the Service V Restart fail count after: 1 @ days Restart service after: 1 @ minutes Program: Command line parameters: Append fail count to end of command line (fail=%1%) Restart Computer Options OK Cancel Apply	ecovery
< 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.
- 43. Click the **[OK]** button.

44. 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.

<u>.</u>	Group Policy Management	- 0 X
🔣 File Action View Window Help		_ 8 ×
🗢 🔿 🙍 💽 🙆 🖬		
Group Policy Management Group Policy Management Mission Porest: MSTU01282.local Mission MSTU01282.local Mission PowerShell Remote Management Policy Mission PowerShell Remote Management Policy Mission Policy Objects Mission Policy Objects Mission Policy Modeling Group Policy Results	PowerShell Remote Management Policy Scope Details Statings Delegation Unics Deplay links in this location: MSTLD12R2.local The following stee, domains, and OUs are linked to this GPO: Location Enforced Unic Enforced Vis MSTLD12R2.local No Yes MSTLD12R2.local MSTLD12R2.local No Yes MSTLD12R2.local Security Filtering The satings in this GPO can only apply to the following groups, users, and computers: Name Authenticated Users	✓
	Add Properties	
	WMI Filtering This GPO is Inked to the following WMI filter: frame=> Copen Cop	
	I wiev + vjen	

45. 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.

Group Policy Management							- 0 ×
📓 File Action View Window Help							_ 8 ×
Group Policy Management		WinRM Policy Scope Details Settings Delegation Status Links Deploy links in this location: MSTL012R2.local The following ates, domains, and OUs are linked to this GPO. MSTL012R2.local					v]
▷ a Domain Contro	jects ain Controllers Policy ain Policy temote Management Polic	Location	L012R2.local	Enforced No	Link Enabled Yes	Path MSTL012R2.local	
→ WinfM S → WMI Filters → Starter GPOs → Stres Group Policy Result	Edit						
	GPO Status	+ v	/ Enabled				
	Back Up Restore from Backup Import Settings Save Report	TIC	User Configuration Settings Disabled Computer Configuration Settings Disabled All Settings Disabled Henucated Oseis		computers:		
	View New Window from Here	٠					
	Copy Delete Rename Refresh			nove Properties			
	Help	Rering O is linked to the following WMI filter:					
<	>	<none></none>		*	Open		
All settings enabled							

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.

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.
- 2. 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>
```

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.

© 2003 - 2020, 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: legal@sciencelogic.com



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

International: +1-703-354-1010