ScienceLogic

Monitoring Windows Systems with PowerShell

SL1 version 12.2.0 (Document revision 1)

Table of Contents

Introduction	7
Monitoring Windows Devices in the ScienceLogic Platform	8
What is SNMP?	8
What is PowerShell?	8
PowerPacks	9
Configuring Windows Systems for Monitoring with SNMP	10
Configuring SNMP for Windows Server 2016 and Windows Server 2012	11
Configuring Ping Responses	.11
Installing the SNMP Service	. 12
Configuring the SNMP Service	.17
Configuring the Firewall to Allow SNMP Requests	. 22
Configuring Device Classes for Windows Server 2016 and Windows 10	22
Manually Align the Device Class	23
Edit the Registry Key	. 23
Configuring SNMP for Windows Server 2008	.24
Configuring Ping Responses	. 24
Installing the SNMP Service	. 25
Configuring the SNMP Service	. 28
Configuring the Firewall to Allow SNMP Requests	. 33
Configuring Windows Servers for Monitoring with PowerShell	. 34
Prerequisites	. 34
Configuring PowerShell	35
Step 1: Configuring the User Account for the ScienceLogic Platform	35
Option 1: Creating an Active Directory Account with Administrator Access	36
Option 2: Creating a Local User Account with Administrator Access	. 36
Option 3: Creating a Non-Administrator User Account	. 37
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	39
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	. 39
Creating a User Group and Adding a User in Active Directory	. 39
Setting the Session Configuration Parameters and Group Permissions	40
Optional: Configuring the User Account for Access to Windows Failover Cluster	40

Step 2: Configuring a Server Authentication Certificate	40
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	41
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	44
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	44
Step 3: Configuring Windows Remote Management	44
Option 1: Using a Script to Configure Windows Remote Management	44
Option 2: Manually Configuring Windows Remote Management	50
Option 3: Using a Group Policy to Configure Windows Remote Management	54
Configuring an HTTPS Listener with GPO Configuration	72
Using Forward and Reverse DNS for Windows Remote Management	72
Step 4: Configuring a Windows Management Proxy	73
Risk of Password Exposure	75
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously \ldots	75
Optional PowerShell CLI Parameters	76
Dynamic Applications for Windows Devices	77
SNMP Dynamic Applications for Windows Devices	77
PowerShell Dynamic Applications	78
Microsoft: Active Directory Server	78
Microsoft: DHCP Server	79
Microsoft: DNS Server	79
Microsoft: Exchange Server	79
Microsoft: Exchange Server 2010	80
Microsoft: Hyper-V Server	81
Microsoft: IIS Server	82
Microsoft: Lync Server 2010	82
Microsoft: SharePoint Server	83
Microsoft: Skype for Business	83
Microsoft: SQL Server	84
Microsoft: Windows Server	84
Microsoft: Windows Server Event Logs	86
Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows Servers	

Error Messages for PowerShell Collection	
Relationships with Other Types of Component Devices	
Creating Credentials and Discovering Windows Devices	
Creating an SNMP Credential	91
Creating an SNMP Credential in the SL1 Classic User Interface	93
Creating a PowerShell Credential	
Creating a PowerShell Credential in the SL1 Classic User Interface	
Testing Windows Credentials	
SNMP Credential Test	
PowerShell Credential Test	
Running a Windows Credential Test	
Running a Windows Credential Test in the SL1 Classic User Interface	
Adding Devices Using Unguided Discovery	
Discovering Windows Server Clusters	
Discovering Windows Server Clusters in the SL1 Classic User Interface	110
Discovering Devices with the Microsoft: Windows Server Discovery Template	110
Discovering Component Devices on Hyper-V Systems	
Viewing Component Devices	
Manually Aligning the Microsoft: Print Server Dynamic Application	114
Using Microsoft PowerPacks	115
Microsoft: DHCP Server PowerPack	115
Add User to DHCP Users Group	115
Microsoft: Windows Server PowerPack	116
Prerequisites	116
Monitoring Windows Services and Processes with PowerShell	
Monitoring Windows Processes	116
Monitoring Individual Windows Services via Internal Collections	116
Monitoring Automatic Services with the Microsoft: Windows Server Service Configuration	,
Restarting Automatic Windows Services Using the Run Book Automation Policy	117
Excluding Automatic Services	117
Viewing the List of Excluded Services	118

Adding an Excluded Service for All Devices	118
Adding an Excluded Service for a Single Device	118
Removing an Excluded Service	119
Monitoring Windows Server Services with Monitoring Policies	119
Granting Access To Services	120
Concurrent PowerShell Collection	121
Prerequisites	122
Scope	122
Enabling and Disabling Concurrent PowerShell for Collector Groups	123
Enabling and Disabling Concurrent PowerShell on All Collector Groups	123
Enabling and Disabling Concurrent PowerShell on a Specific Collector Group	123
The SL1: Concurrent PowerShell Monitoring PowerPack	124
Configuring the SL1: Concurrent PowerShell Monitoring PowerPack for Military Unique Deployment (MUD) Environments	124
Configuring the Sudo Config File	124
Configuring the ScienceLogic: PowerShell Service Log Parser Dynamic Application	124
Aligning the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application	125
Manually Aligning the Dynamic Application	126
Configuring the Device Template	127
Applying the Device Template	127
Aligning the "ScienceLogic: PowerShell Collector Performance" Dynamic Application	128
Enabling HTTPS Between SL1 and the PowerShell Data Collector	129
Enabling and Disabling the Python PowerShell Remoting Protocol Client	130
Optional PowerShell CLI Parameters	130
Users with Windows 2008 R2 Servers or Windows 2012 Servers	131
Scale Recommendations	132
Additional Scale Tips	132
Executing the SL1 Agent with Windows PowerShell	133
What is an SL1 Agent?	133
Agent-Compatible PowerPacks	134
The Credential for the SL1 Agent	134
Configuring the SL1 Agent Device Templates	135

Windows Dashboards	
Installing the Microsoft Server Dashboards	
Microsoft: Active Directory Server Performance	
Microsoft: DNS Server Performance	
Microsoft: Exchange Server 2010 Performance	141
Microsoft: Exchange Server 2013 Performance	
Microsoft: IIS Server Performance	
Microsoft: Lync Server 2010 Dashboards	
Microsoft: Lync Server 2010 Performance	
Microsoft: Lync Server 2010 Utilization	151
Microsoft: Skype for Business Dashboards	
Microsoft: Lync Server 2013 Performance	
Microsoft: Lync Server 2013 Utilization	
Microsoft: SQL Server Performance	
Troubleshooting	
Troubleshooting WinRM Error Messages	
Debugging Code 401 Errors	
Debugging Code 500 Errors	165
Troubleshooting PowerShell Error Messages	

Chapter

Introduction

Overview

This manual describes how to monitor Windows systems in SL1 using SNMP and PowerShell credentials and Dynamic Applications.

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

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

The following sections provide an overview of SNMP and PowerShell, as well as the PowerPacks you can use to monitor Windows systems in SL1.

For an introduction to PowerShell Monitoring, see the following video: https://www.youtube.com/watch?v=x7hYFK d6A.

This chapter covers the following topics:

Monitoring Windows Devices in the ScienceLogic Platform	8
What is SNMP?	8
What is PowerShell?	8
PowerPacks	9

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software, which 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.

Monitoring Windows Devices in the ScienceLogic Platform

SL1 can monitor a Windows device using the following methods:

- Requesting information from the Windows SNMP agent
- Requesting information by executing a remote PowerShell command
- Requesting information from the Windows Management Instrumentation (WMI) agent
- Requesting information using the SL1 agent

NOTE: This manual describes how to monitor Windows with SNMP and PowerShell. For more information about using WMI to monitor Windows devices, see the **Monitoring Windows with WMI** manual.

What is SNMP?

SNMP (Simple Network Management Protocol) is a set of standard protocols for managing diverse computer hardware and software within a TCP/IP network. SNMP is the most common network protocol used by network monitoring and management applications to exchange management information between devices. SL1 uses this protocol and other protocols to collect availability and performance information.

SNMP uses a server-client structure. Clients are called **agents**. Devices and software that run SNMP are agents. The server is called the **management system**. SL1 is the management system.

Most network hardware is configured for SNMP and can be SNMP-enabled. Many enterprise software applications are also SNMP-compliant. When SNMP is running on a device, it uses a standard format to collect and store data about the device and/or software. For example, SNMP might collect information on each network interface and the traffic for each interface. SL1 can then query the device to retrieve the stored data.

What is PowerShell?

Windows PowerShell is a command-line shell and scripting language for administration of Windows systems. SL1 can execute PowerShell requests on target Windows devices via WinRM (Windows Remote Management). For an overview of Windows PowerShell, see https://learn.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.3.

SL1 supports the following PowerShell versions for monitoring Windows devices:

- PowerShell 3.0
- PowerShell 4.0
- PowerShell 5.1

PowerPacks

This manual describes content from the following PowerPack versions:

- Microsoft: Active Directory Server, version 101
- Microsoft: DHCP Server, version 100
- Microsoft: DNS Server, version 100
- Microsoft: Exchange Server, version 101
- Microsoft: Exchange Server 2010, version 1.2
- Microsoft: Hyper-V Server, version 102
- Microsoft: IIS Server, version 103
- Microsoft: Lync Server 2010, version 1.0
- Microsoft: SharePoint Server, version 1.0
- Microsoft: SQL Server, version 102
- Microsoft: Windows Event Logs, version 101
- Microsoft: Windows Server, version 116
- Microsoft: Windows Server Cluster, version 103
- SL1: Concurrent PowerShell Monitoring, version 102

Chapter

2

Configuring Windows Systems for Monitoring with SNMP

Overview

The following sections describe how to configure Windows Server 2016, Windows Server 2012, and Windows Server 2008 for monitoring by SL1 using SNMP.

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

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

For an overview of configuring Windows PowerShell monitoring, see the following video: https://www.youtube.com/watch?v=23ydHZDIGpE.

This chapter covers the following topics:

Configuring SNMP for Windows Server 2016 and Windows Server 2012	
Configuring SNMP for Windows Server 200824	

Configuring SNMP for Windows Server 2016 and Windows Server 2012

To configure SNMP on a Windows server, you must:

- 1. Configure "ping" responses.
- 2. Install the SNMP service.
- 3. Configure the SNMP service.
- 4. Configure the firewall to allow SNMP requests.
- 5. Configure Device Classes. (Windows Server 2016 only)

Configuring Ping Responses

For SL1 to discover a device, including SNMP-enabled devices, the device must meet one of the following requirements:

- The device must respond to an ICMP "Ping" request.
- One of the ports selected in the **Detection Method & Port** field for the discovery session must be open on the device. If the Default Method option for the **Detection Method & Port** field is selected, SL1 scans TCP ports 21, 22, 23, 25, and 80.

The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in SL1, you must perform one of the following tasks:

- Reconfigure the firewall on the Windows Server to allow ICMP "Ping" requests. This section describes how to perform this task.
- Reconfigure the firewall on the Windows Server to allow connections to port 21, 22, 23, 25, or 80. If you have already configured your Windows Server to accept SSH, FTP, Telnet, SMTP, or HTTP connections, this task might have been completed already. You should perform this task only if you were already planning to allow SSH, FTP, Telnet, SMTP, or HTTP connections to your Windows Server.
- When you create the discovery session that will discover the Windows Server, select at least one port in the Detection Method & Port field that is open on the Windows Server. For example, if your Windows Server is configured as an MSSQL Server, you could select port 1433 (the default port for MSSQL Server) in the Detection Method & Port field.

To reconfigure the firewall on a Windows Server to allow ICMP "Ping" requests, perform the following steps:

- 1. In the Start menu search bar, enter "firewall" to open a **Windows Firewall with Advanced Security** window.
- 2. In the left pane, select Inbound Rules.
- 3. If you want SL1 to discover your Windows Server using an IPv4 address, locate the File and Printer Sharing (Echo Request ICMPv4-In) rule.
- 4. If you want SL1 to discover your Windows Server using an IPv6 address, locate the File and Printer Sharing (Echo Request ICMPv6-In) rule.

5. Right click on the rule that you located, then select *Enable Rule*:

	Window	ws Firewall with	h Advanced S	ecurity			
le Action View Help							
🔹 🗈 🖬 🔒							
Windows Firewall with Advance	Inbound Rules					Actions	
🔣 Inbound Rules	Name	Group	•	Profile	Enabled ^	Inbound Rules	
Cutbound Rules	🕜 Core Networking - Multicast Listener Qu	Core Network	ing	All	Yes	🚉 New Rule	
http://www.connection Security Rules	🕜 Core Networking - Multicast Listener Rep	o Core Network	ing	All	Yes	-	
The second secon	🕜 Core Networking - Multicast Listener Rep	o Core Network	ing	All	Yes	Tilter by Profile	
	🕜 Core Networking - Neighbor Discovery A	Core Network	ing	All	Yes	🕎 Filter by State	
	🕜 Core Networking - Neighbor Discovery S	Core Network	ing	All	Yes	Filter by Group	
	🕜 Core Networking - Packet Too Big (ICMF	Core Network	ing	All	Yes	View	
	🕜 Core Networking - Parameter Problem (I	Core Network	ing	All	Yes	VIEW	
	😨 Core Networking - Router Advertisemen	t Core Network	ing	All	Yes	🖪 Refresh	
	🕜 Core Networking - Router Solicitation (IC	Core Network	ing	All	Yes =	🔜 Export List	
	🕑 Core Networking - Teredo (UDP-In)	Core Network	ing	All	Yes	R Help	
	🕜 Core Networking - Time Exceeded (ICMF	Core Network	ing	All	Yes	The Prop	
	💿 Distributed Transaction Coordinator (RP	C) Distributed Tra	ansaction Coo	All	No	File and Printer Sharing (Echo Reque	est
	💿 Distributed Transaction Coordinator (RP	Distributed Tra	ansaction Coo	All	No	O Enable Rule	
	🔘 Distributed Transaction Coordinator (TC	Distributed Tra	ansaction Coo	All	No	K Cut	
	File and Printer Sharing (Echo R		Sharing		No		
	🕑 File and Printer Sharing (Echo R	able Rule	Sharing	All	Yes	Copy	
	🜑 File and Printer Sharing (LLMNF Cu	ut	Sharing	All	No	🔀 Delete	
	🐨 File and Printer Sharing (NB-Dat Co	ру	Sharing	All	No	Properties	
	File and Printer Sharing (NB-Na De	lete	Sharing	All	No		
	🐨 File and Printer Sharing (NB-Ses		Sharing	All	No	😰 Help	
	File and Printer Sharing (SMB-Ir	operties	Sharing	All	No		
	🜑 File and Printer Sharing (Spoole 🛛 🛛 He	elp	Sharing	All	No		
	File and Printer Sharing (Spooler Service)	File and Printe	er Sharing	All	No		
	File and Printer Sharing over SMBDirect (i File and Printe	er Sharing over	All	No		
	🔘 iSCSI Service (TCP-In)	iSCSI Service		All	No		
	Key Management Service (TCP-In)	Key Managem	nent Service	All	No		
	🜑 Netlogon Service (NP-In)	Netlogon Serv	/ice	All	No		
	🜑 Netlogon Service Authz (RPC)	Netlogon Serv	/ice	All	No		
	Network Discovery (LLMNR-UDP-In)	Network Disco	overy	All	No		
	🜑 Network Discovery (NB-Datagram-In)	Network Disco	overy	All	No		
	Network Discovery (NB-Name-In)	Network Disco	overy	All	No		
	Network Discovery (Pub-WSD-In)	Network Disco	overy	All	No 🗸	-	
III >	< III				>		

Installing the SNMP Service

To install the SNMP service on a Windows 2012 Server or Windows 2016 Server, perform the following steps:

- 1. Open the Server Manager utility.
- 2. In the upper-right of the window, select [Manage] > Add Roles and Features. The Add Roles and Features window is displayed.

3. If the server does not skip the **Before you begin** page, click the **[Next >]** button to manually skip it. The **Select installation type** page is displayed:

B	Add Roles and Features Wizard	x
Select installation	type destination servination s	
Before You Begin Installation Type	Select the installation type. You can install roles and features on a running physical computer or virte machine, or on an offline virtual hard disk (VHD).	ual
Server Selection Server Roles	Role-based or feature-based installation Configure a single server by adding roles, role services, and features.	
Features Confirmation	 Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-base or session-based desktop deployment. 	ased
Results		
	< Previous Next > Install Cance	:

4. Click the [Next >] button to continue with Role-based or feature-based installation. The Select destination server page is displayed:

A	Add Role	es and Features V	Vizard	_ 🗆 X
Select destination	n server			NATION SERVER N-3UGJKS2COLQ
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a virtua Select a server from t Select a virtual hard d Server Pool Filter:	he server pool	to install roles and features.]
Confirmation Results	Name WIN-3UGJKS2COLQ	IP Address 10.100.100.22	Operating System Microsoft Windows Server 2012 R2 Stan	dard
		Server Manager. Off	dows Server 2012, and that have been adde line servers and newly-added servers from	
		< Pre	vious Next > Install	Cancel

- 5. Ensure the Windows 2012 server or Windows 2016 Server is selected and then click the **[Next >]** button. The **Select server roles page** is displayed.
- 6. Click the **[Next >]** button without selecting any additional roles. The **Select features** page is displayed:

B	Add Roles and Features Wizard	_ D X
Select features		DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin Installation Type	Select one or more features to install on the selected server. Features	Description
Server Selection Server Roles Features Confirmation Results	NET Framework 3.5 Features ^ Image: Installed installow installed installed installadied installed installed install	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	Ink and Handwriting Services	Install Cancel

7. Select the SNMP Service checkbox. The following confirmation window is displayed:

b	Add Roles and Features Wizard	x
1	Add features that are required for SNMP Service? The following tools are required to manage this feature, but do not ave to be installed on the same server.	
	▲ Remote Server Administration Tools	7
	▲ Feature Administration Tools	
	[Tools] SNMP Tools	
l	✓ Include management tools (if applicable) Add Features Cancel	

- 8. Click the [Add Features] button.
- 9. In the Select features page, expand SNMP Service and select the SNMP WMI Provider checkbox.

10. Click the [Next >] button. The Confirm installation selections page is displayed:

Ē.	Add Roles and Features Wizard	_ D X
Confirm installati	on selections	DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin	To install the following roles, role services, or features on selected server, click I	nstall.
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be displayed on this pag	3
Server Roles	been selected automatically. If you do not want to install these optional feature their check boxes.	s, click Previous to clear.
Features	-	
Confirmation Results	Remote Server Administration Tools Feature Administration Tools SNMP Tools SNMP Service SNMP WMI Provider	
	Export configuration settings Specify an alternate source path	
	< Previous Next >	Install Cancel

- 11. Click the [Install] button.
- 12. After the installation is complete, click the **[Close]** button.

Configuring the SNMP Service

To configure the SNMP service on a Windows 2012 Server or Windows 2016 Server, perform the following steps:

NOTE: If you recently installed the SNMP service, you must wait for the **Server Manager** window to refresh to allow the SNMP service snap-in to be added. You can manually refresh the **Server Manager** window by closing the **Server Manager** and then re-opening the **Server Manager**.

1. In the upper-right of the **Server Manager** window, select **[Tools]** > Services. The **Services** window is displayed.

2. In the **Services** window, right-click on *SNMP* Service, and then select *Properties*. The **SNMP** Service **Properties** window appears:

SNMP	Service Properties (Local Computer) 💦 💌
General Log On	Recovery Agent Traps Security Dependencies
Service name:	SNMP
Display name:	SNMP Service
Description:	Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.
Path to executabl C:\Windows\Syst	
Startup type:	Automatic 🗸
Service status:	Running
Start	Stop Pause Resume
You can specify th from here.	ne start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

3. In the **Startup type:** field, select Automatic.

4.	Select the	[Security]	tab.	The security	y settings	are displayed:	
----	------------	------------	------	--------------	------------	----------------	--

SI	NMP Se	rvice P	ropert	ies (Lo	cal Con	nputer) 🛛 🗙
General Lo	g On R	ecovery	Agent	Traps	Security	Dependencies
✓ Send a	uthenticat	ion trap				
Accepte	d commur	nity name	s			
Comm	iunity	-		Rig	nts	
					-	
l l	Add		Edi	t	Remo	ive
O Acc	ept SNMP	nackets	from any	host		
	ept SNMF					
local		F				
	Add		Edit		Remo	ve
			OK	(Cancel	Apply

5. In the Accepted community names panel, click the [Add...] button. The SNMP Service Configuration pop-up window is displayed:

SNMP Service Properties (Local Computer)
General Log On Recovery Agent Traps Security Dependencies
Send authentication trap
Accepted community names
Community Rights
SNMP Service Configuration
Community rights: Add READ ONLY Community Name: Cancel
Add Edit Remove
OK Cancel Apply

- 6. Enter a value in the following fields:
 - Community rights. Select one of the following options from the drop-down list:
 - READ ONLY. Select this option to allow SL1 to request information from this Windows 2012 Server or Windows 2016 Server using this SNMP community string. This option does not allow SL1 to perform write operations on this Windows 2012 Server or Windows 2016 Server using this SNMP community string.
 - READ WRITE. Select this option to allow SL1 to request information from this Windows 2012 Server or Windows 2016 Server and to perform write operations on this Windows 2012 Server or a Windows 2016 Serve using this SNMP community string.

- **Community name**. Enter the SNMP community string that SL1 will use when making SNMP requests to this Windows 2012 Server or Windows 2016 Server. When you create a credential for this Windows 2012 Server or Windows 2016 Server in SL1, you will enter this community string in one the following fields in the **Credential Editor** modal page:
 - SNMP Community (Read-Only). Enter the SNMP community string in this field if you selected READ ONLY in the **Community rights** drop-down list.
 - SNMP Community (Read/Write). Enter the SNMP community string in this field if you selected READ WRITE in the **Community rights** drop-down list.
- 7. Click the **[Add]** button to add the community string to the list of community strings this Windows 2012 Server or Windows 2016 Server accepts.
- 8. In the Accept SNMP packets from these hosts panel, click the Add... button. The SNMP Service Configuration pop-up window is displayed:

SNI	MP Service	Propert	ties (Lo	ocal Con	nputer) 🛛 🗙
General Log	On Recovery	Agent	Traps	Security	Dependencies
💽 Send auti	hentication trap	ı			
Accepted	community nar	nes			
Commun	nity		Rig	hts	
public			REA	AD ONLY	
	SNMP	Service	Config	guration	×
Host n	ame, IP or IPX	address:			Add Cancel
	Add	Edi		Remo	we
		10	<	Cancel	Apply

- 9. In the *Host name, IP or IPX address* field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.
- 10. Click the **[Add]** button to add the appliance to the list of authorized devices.
- 11. If you are using SL1 with a distributed architecture, repeat steps 8–10 for each Data Collector in the collector group that will monitor this server.
- 12. Click the [Apply] button to apply all changes.

Configuring the Firewall to Allow SNMP Requests

To configure the Windows Firewall to allow SNMP requests on a Windows 2012 server or Windows 2016 Server, perform the following steps:

- 1. In the Start menu search bar, enter "firewall" to open a Windows Firewall with Advanced Security window.
- 2. In the left pane, click Inbound Rules.
- 3. Locate the two SNMP Service (UDP In) rules.
- 4. If one or both of the rules is not enabled, right-click on the rule and then select Enable Rule:

		Win	ndows F	irewall with Adv	anced Sec	urity					_ 0	
le Action View Help												
🔿 🖄 🖬 🗟 🖬												
Windows Firewall with Advance	Inbound Rules									H.	Actions	
🗱 Inbound Rules	Name	Group		Profile	Enabled	Action	Override	Program	Local Address		Inbound Rules	
Cutbound Rules	Remote Event Log Management (RPC-EP	Remote Event Log Ma	anage	All	No	Allow	No	%System	Any	П	New Rule	-
Lonnection Security Rules	Remote Event Monitor (RPC)	Remote Event Monito	or	All	No	Allow	No	%System	Any		-	
s wonitoring	Remote Event Monitor (RPC-EPMAP)	Remote Event Monito	or	All	No	Allow	No	%System	Any		Filter by Profile	
	Remote Scheduled Tasks Management (Remote Scheduled Ta	isks M	All	No	Allow	No	%System	Any		Y Filter by State	
	Remote Scheduled Tasks Management (Remote Scheduled Ta	isks M	All	No	Allow	No	%System	Any		Filter by Group	
	Remote Service Management (NP-In)	Remote Service Mana	gement	All	No	Allow	No	System	Any		View	
	Remote Service Management (RPC)	Remote Service Mana	gement	All	No	Allow	No	%System	Any		view	
	Remote Service Management (RPC-EPM	Remote Service Mana	gement	All	No	Allow	No	%System	Any		Refresh	
	Inbound Rule for Remote Shutdown (RP	Remote Shutdown		All	No	Allow	No	%system	Any		🔿 Export List	
	Inbound Rule for Remote Shutdown (TC	Remote Shutdown		All	No	Allow	No	%system	Any		Help	
	Remote Volume Management - Virtual D	Remote Volume Man	ageme	All	No	Allow	No	%System	Any		I riep	
	Remote Volume Management - Virtual D	Remote Volume Man	ageme	All	No	Allow	No	%System	Any		SNMP Service (UDP In)	
	Remote Volume Management (RPC-EPM	Remote Volume Man	ageme	All	No	Allow	No	%System	Any		O Enable Rule	
	Routing and Remote Access (GRE-In)	Routing and Remote	Access	All	No	Allow	No	System	Any		-	
	Routing and Remote Access (L2TP-In)	Routing and Remote	Access	All	No	Allow	No	System	Any		of Cut	
	Routing and Remote Access (PPTP-In)	Routing and Remote	Access	All	No	Allow	No	System	Any		🗎 Сору	
	Secure Socket Tunneling Protocol (SSTP	Secure Socket Tunnel	ing Pr	All	No	Allow	No	System	Any		🔀 Delete	
	SNMP Service (UDP In)	SNMP Service		Domain, Public	Yes	Allow	No	%System	Any		Properties	
	SNMP Service (UDP In)			Private, Public		Allow		%System	Any			
	SNMP Trap Service (UDP In)	Enable Rule		Private, Public	No	Allow	No	%System	Any	11	👔 Help	
	SNMP Trap Service (UDP In)	Cut		Domain	No	Allow	No	%System	Any	ы		
	TPM Virtual Smart Card Managemen	Сору	rd Ma	Domain	No	Allow	No	%System	Any		1	
	TPM Virtual Smart Card Managemen	Delete	rd Ma	Private, Public	No	Allow	No	%System	Any			
	TPM Virtual Smart Card Managemen	,	rd Ma	Domain	No	Allow	No	%System	Any	≡		
	TPM Virtual Smart Card Managemen	Properties	rd Ma	Private, Public	No	Allow	No	%System	Any			
	Virtual Machine Monitoring (DCOM-	Help	itoring	All	No	Allow	No	%System	Any			
	Virtual Machine Monitoring (Echo Reque	Virtual Machine Moni	itoring	All	No	Allow	No	Any	Any	П		
	Wirtual Machine Monitoring (Echo Reque	Virtual Machine Moni	itoring	All	No	Allow	No	Any	Any			
	Wirtual Machine Monitoring (NB-Session	Virtual Machine Moni	itoring	All	No	Allow	No	Any	Any	÷		
										الشار		

Configuring Device Classes for Windows Server 2016 and Windows 10

There is a known problem with the Microsoft OID that contains the version number for the operation system. This problem prevents SL1 from using SNMP to automatically align device classes to Windows 10 devices and Microsoft Server 2016 devices.

Because Microsoft has deprecated support of SNMP on Microsoft Server 2016 and Windows 10, users who want to use SNMP to monitor Windows 10 and Microsoft Server 2016 should use one of these workarounds:

- After discovering a Microsoft Server 2016 or Windows 10 device, manually align the device class and disable nightly auto-discovery
- Edit the registry key

Both workarounds are described in the following sections.

Manually Align the Device Class

After discovering Microsoft Server 2016 devices and Windows 10 devices, you can manually align a device class with the discovered devices. To preserve your manual changes, you must disable nightly auto-discovery for those devices. You can manually align the discovered devices with one of these device classes:

- Windows Server 2016
- Windows Server 2016 Domain Controller
- Windows 10 Workstation

For details on manually assigning a device class to a device, follow the steps in the section on Manually Changing the Device Class for a Device in the **Device Management** manual chapter on Managing Device Classes and Device Categories. For details on disabling nightly auto-discovery for a device, see the section on Maintaining the New Device Class During Auto-Discovery in the **Device Management** manual chapter on Managing Device Classes and Device Categories.

Edit the Registry Key

You can log in to the device that you want to monitor and manually edit the Windows Registry Key "HKEY_ LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion". You can define the value CurrentVersion as either "2016" or "10.0". To do this:

- 1. Click the Start menu and choose Run.
- 2. In the Run dialog box, type regedit and then click OK.
- 3. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
- 4. In the right pane, double click on the Default key.
- 5. Enter the appropriate value:
 - For Microsoft Server 2016, change the Value to 2016
 - For Windows 10, change the Value to 10.0

Configuring SNMP for Windows Server 2008

To configure SNMP on a Windows 2008 Server, you must:

- 1. Configure "ping" responses.
- 2. Install the SNMP service.
- 3. Configure the SNMP service.
- 4. Configure the firewall to allow SNMP requests.

Configuring Ping Responses

For SL1 to discover a device, including SNMP-enabled devices, the device must meet one of the following requirements:

- The device must respond to an ICMP "Ping" request.
- One of the ports selected in the **Detection Method & Port** field for the discovery session must be open on the device. If the *Default Method* option for the **Detection Method & Port** field is selected, SL1 scans TCP ports 21, 22, 23, 25, and 80.

The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in SL1, you must perform one of the following tasks:

- Reconfigure the firewall on the Windows Server to allow ICMP "Ping" requests. This section describes how to perform this task.
- Reconfigure the firewall on the Windows Server to allow connections to port 21, 22, 23, 25, or 80. If you have already configured your Windows Server to accept SSH, FTP, Telnet, SMTP, or HTTP connections, this task might have been completed already. You should perform this task only if you were already planning to allow SSH, FTP, Telnet, SMTP, or HTTP connections to your Windows Server.
- When you create the discovery session that will discover the Windows Server, select at least one port in the Detection Method & Port field that is open on the Windows Server. For example, if your Windows Server is configured as an MSSQL Server, you could select port 1433 (the default port for MSSQL Server) in the Detection Method & Port field.

To reconfigure the firewall on a Windows Server to allow ICMP "Ping" requests, perform the following steps:

- 1. In the Start menu search bar, enter "firewall" to open a Windows Firewall with Advanced Security window.
- 2. In the left pane, select Inbound Rules.
- 3. If you want SL1 to discover your Windows Server using an IPv4 address, locate the File and Printer Sharing (Echo Request ICMPv4-In) rule.
- 4. If you want SL1 to discover your Windows Server using an IPv6 address, locate the File and Printer Sharing (Echo Request ICMPv6-In) rule.

5. Right click on the rule that you located, then select *Enable Rule*:

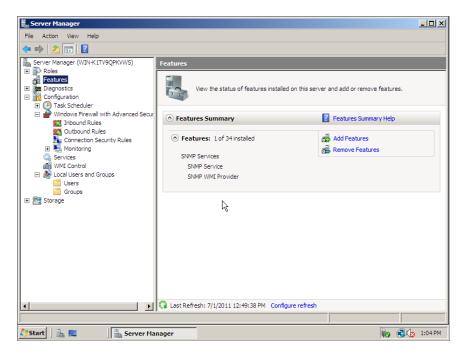
Connection Security Rules	nbound Rules Vame Core Networking - Multicast Listener Qu. Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery S Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I. Core Networking - Router Advertisement Core Networking - Router Advertisement Core Networking - Router Advertisement Core Networking - Router Solicitation (IC Core Networking - Teredo (UDP-In)	Core Network Core Network Core Network Core Network Core Network Core Network Core Network	king king king king king king	Profile All All All All All All All	Enabled ^ Yes Yes Yes Yes Yes Yes Yes Yes	Actions Inbound Rules	
Windows Firewall with Advance In Doubound Rules Outbound Rules Connection Security Rules Monitoring	Vame Core Networking - Multicast Listener Qu. Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery A Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I, Core Networking - Rourter Advertisement Core Networking - Rourter Solicitation (IC	Core Network Core Network	king king king king king king	Ali Ali Ali Ali Ali Ali	Yes Yes Yes Yes Yes Yes	Inbound Rules Imbound Rule Imbound Rule<	
Connection Security Rules	Vame Core Networking - Multicast Listener Qu. Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery A Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I, Core Networking - Rourter Advertisement Core Networking - Rourter Solicitation (IC	Core Network Core Network	king king king king king king	Ali Ali Ali Ali Ali Ali	Yes Yes Yes Yes Yes Yes	Inbound Rules Imbound Rule Imbound Rule<	
Outbound Rules Connection Security Rules Monitoring	Core Networking - Multicast Listener Qu. Core Networking - Multicast Listener Rep Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery A Core Networking - Packet Too Big (ICMP Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I, Core Networking - Router Advertisement Core Networking - Router Solicitation (IC	Core Network Core Network	king king king king king king	Ali Ali Ali Ali Ali Ali	Yes Yes Yes Yes Yes Yes	 Wew Rule Filter by Profile Filter by State Filter by Group 	
Connection Security Rules	Core Networking - Multicast Listener Rep Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery S Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I. Core Networking - Router Advertisement Core Networking - Router Advertisement	Core Network Core Network Core Network Core Network Core Network Core Network Core Network	king king king king king king	Ali Ali Ali Ali Ali	Yes Yes Yes Yes Yes	 Wew Rule Filter by Profile Filter by State Filter by Group 	
Monitoring	Core Networking - Multicast Listener Rep Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery S Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I. Core Networking - Rauter Advertisement Core Networking - Rauter Advertisement	Core Network Core Network Core Network Core Network Core Network Core Network	king king king king king	All All All All	Yes Yes Yes Yes	 Filter by Profile Filter by State Filter by Group 	
	Core Networking - Neighbor Discovery A Core Networking - Neighbor Discovery S Core Networking - Packet Too Big (ICMP Core Networking - Parameter Problem (I. Core Networking - Router Advertisement Core Networking - Router Advertisement Core Networking - Router Solicitation (IC	Core Network Core Network Core Network Core Network Core Network	king king king king	All All All	Yes Yes Yes	 Filter by State Filter by Group 	
	9 Core Networking - Neighbor Discovery S 9 Core Networking - Packet Too Big (ICMP 9 Core Networking - Parameter Problem (I. 9 Core Networking - Router Advertisement 9 Core Networking - Router Solicitation (IC	Core Network Core Network Core Network Core Network	king king king	All All	Yes Yes	Y Filter by Group	
	© Core Networking - Packet Too Big (ICMP © Core Networking - Parameter Problem (I. © Core Networking - Router Advertisement © Core Networking - Router Solicitation (IC	Core Network Core Network Core Network	king king	All	Yes		
	Core Networking - Parameter Problem (l. Core Networking - Router Advertisement Core Networking - Router Solicitation (IC	Core Network Core Network	king				
	Core Networking - Router Advertisement Core Networking - Router Solicitation (IC	Core Network	-	All	Yes	View	
	Core Networking - Router Solicitation (IC		kina				
		Core Network		All	Yes	💿 Refresh	
	🖉 Core Networking - Teredo (UDP-In)		king	All	Yes =	📑 Export List	
		Core Network	king	All	Yes =	Help	
	Ore Networking - Time Exceeded (ICMP)	Core Network	king	All	Yes	I Help	
	Distributed Transaction Coordinator (RPC) Distributed Tr	ransaction Coo	All	No	File and Printer Sharing	(Echo Request
	Distributed Transaction Coordinator (RP.	. Distributed Tr	ransaction Coo	All	No	O Enable Rule	
	Distributed Transaction Coordinator (TC.	Distributed Tr	ransaction Coo	All	No	-	
	File and Printer Sharing (Echo R		Sharing	All	No	of Cut	
	File and Printer Sharing (Echo R En	able Rule	Sharing	All	Yes	🗈 Copy	
	File and Printer Sharing (LLMNF Cu	t	Sharing	All	No	🔀 Delete	
	File and Printer Sharing (NB-Dat Co	pv.	Sharing	All	No	Properties	
	City and Deleters Charles - (ND, No.	r <i>y</i> lete	Sharing	All	No		
	File and Printer Sharing (NB-Ses	lete	Sharing	All	No	🛛 🕜 Help	
	File and Printer Sharing (SMB-Ir Pro	operties	Sharing	All	No		
	File and Printer Sharing (Spoole He	lp	Sharing	All	No		
	File and Printer Sharing (Spooler Service -	File and Print	er Sharing	All	No		
	File and Printer Sharing over SMBDirect (i	File and Print	er Sharing over	All	No		
	iSCSI Service (TCP-In)	iSCSI Service		All	No		
	Key Management Service (TCP-In)	Key Managen	ment Service	All	No		
	Netlogon Service (NP-In)	Netlogon Ser	vice	All	No		
	Netlogon Service Authz (RPC)	Netlogon Ser	vice	All	No		
	Network Discovery (LLMNR-UDP-In)	Network Disc	overy	All	No		
	Network Discovery (NB-Datagram-In)	Network Disc	overy	All	No		
	Network Discovery (NB-Name-In)	Network Disc	overy	All	No		
	Network Discovery (Pub-WSD-In)	Network Disc		All	No 🗸		
III > <					>		

Installing the SNMP Service

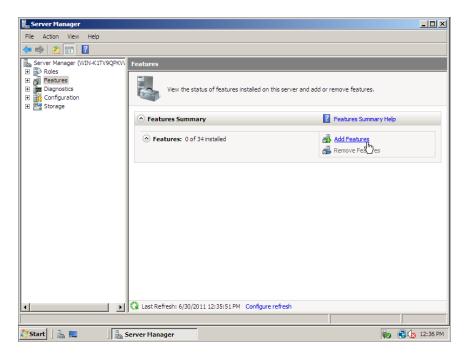
To install the SNMP service on a Windows 2008 Server, perform the following steps:

1. Open the Server Manager utility.

2. In the left pane of the Server Manager window, select Features. The Features Summary is displayed:



 If the Features Summary displays "SNMP Service" and "SNMP WMI Provider" in the list of installed services (as shown above), you can skip to the section on configuring the SNMP service. If "SNMP Service" and "SNMP WMI Provider" are not included in the list of installed services, select Add Features:



4. In the **Select Features** window, select SNMP Services:

Select Features Confination Progress Results Benerote Differential Compression Benerote Server Administration Tools Borney Benerote Simple TCP/IP Services Simple Server Benerote Server Manager Benerote Server Manager Windows Internal Database Windows Server Backup Features Windows Servere Backup Features Windows Servere Backup Features <	Add Features Wizard		×
Confirmation Features: Description: Progress Quality Windows Audio Video Experience Simple Network Management Protocol Results Remote Assistance Simple Network Management Protocol Results Remote Assistance Simple Network Management Protocol B Remote Server Administration Tools Service and SMMP WMI Provider. B Remote Server Administration Tools Service and SMMP WMI Provider. B Service Server Administration Tools Service and SMMP WMI Provider. B Storage Manager System for UIDX-based Applications Tehet Clent Tehet Clent Tehet Clent Tehet Server Windows Provershell B Windows Server Badup Features Windows Server Windows Server Windows Server Windows Server Windows Server Video Server	Select Features		
< Previous Next > Install Cancel	Confirmation Progress	Eeatures: Quality Windows Audio Video Experience Remote Assistance Remote Differential Compression Remote Server Administration Tools Removable Storage Manager RPC over HTTP Proxy Simple TCP/IP Services Storage Manager ftb/SANs Subsystem for UNIX-based Applications Terhet Clent Windows Internal Database Windows Process Activation Service Windows System Resource Manager Windows System Resource Manager Windows Service Backup Features Windows Service Windows Service Service </th <th>Simple Network Management Protocol (SMMP) Services includes the SNMP Service and SNMP WMI Provider.</th>	Simple Network Management Protocol (SMMP) Services includes the SNMP Service and SNMP WMI Provider.

5. Click the **[Next >]** button. The **Confirm Installed Selections** window is displayed with "SNMP Service" and "SNMP WMI Provider" in the list of features that will be installed:

Add Features Wizard		×
Confirm Installat	tion Selections	
Features Confirmation Progress Results	To install the following roles, role services, or features, click Install. Informational message below This server might need to be restarted after the installation completes. SIMP Services SIMP WHI Provider 	
	< Previous Next > Instal Cancel	

6. Click the **[Install]** button. After the installation is completed, the **Installation Results** window will be displayed:

Add Features Wizard	2
Installation Res	ults
Features Confirmation Progress Results	The following roles, role services, or features were installed successfully: I warning message below I warning message below Control Panel to check for updates. Control Panel to check for updates. SIMP Service Installation succeeded Following features were installed: SIMP Service SIMP Service SIMP Service SIMP Service Print, e-mail, or save the installation report
	< Previous Next > Close Cancel

7. Click the **[Close]** button.

Configuring the SNMP Service

To configure the SNMP service on a Windows 2008 Server, perform the following steps:

NOTE: If you recently installed the SNMP service, you must wait for the **Server Manager** window to refresh before it will display the SNMP service snap-in. You can manually refresh the **Server Manager** window by closing the **Server Manager** and then re-opening the **Server Manager**.

1. In the left pane of the Server Manager window, expand the Configuration section, and then select Services.

2. In the list of services, right-click on SNMP Service, and then select Properties. The **SNMP Service Properties** window appears:

SNMP Service Prop	erties (WIN-K1TV9QPKVW5)	X
General Log On	Recovery Agent Traps Security Dependencies	_
Service name:	SNMP	
Display name:	SNMP Service	
Description:	Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.	
Path to executable C:\Windows\Syste		
Startup type:	Automatic	
Help me configure	service startup options.	
Service status:	Started	
Start	Stop Pause Resume	
You can specify th from here.	e start parameters that apply when you start the service	
Start parameters:		
	OK Cancel Apply	

3. In the **Startup type:** field, select Automatic.

4. Select the **[Security]** tab. The security settings are displayed:

SNMP Service Properties (W	IN-K1TV9QI	PKVWS))		2	×
General Log On Recovery	Agent Tra	aps Se	ecurity	Dependen	cies	
						T
Send authentication trap						L
Accepted community name	es				_	L
Community		Rights			_	L
						L
						L
						L
Add	Edit		Remov			L
Add	Edit		Hemov	/e		L
C Accept SNMP packets	s from any ho	st				L
- Accept SNMP packet	-				L.	L
localhost						L
						L
						L
						L
Add	Edit		Remov	e		L
						L
Leam more about SNMP						L
	ОК		Cancel	I A	\pply	1

5. In the Accepted community names panel, click the [Add...] button. The SNMP Service Configuration pop-up window is displayed:

SNMP Service Properties (WIN-K1TV9QPKVWS)	×
General Log On Recovery Agent Traps Security Dependencies	
Send authentication trap	
Accepted community names	
Community Rights	
SNMP Service Configuration	
Community rights: Add	
READ ONLY	
Community Name:	
public	
Add Edit Remove	
Leam more about <u>SNMP</u>	
OK Cancel Apply	

- 6. Enter a value in the following fields:
 - Community rights. Select one of the following options from the drop-down list:
 - READ ONLY. Select this option to allow SL1 to request information from this Windows 2008 Server using this SNMP community string. This option does not allow SL1 to perform write operations on this Windows 2008 Server using this SNMP community string.
 - *READ WRITE*. Select this option to allow SL1 to request information from this Windows 2008 server and to perform write operations on this Windows 2008 Server using this SNMP community string.

- **Community name**. Enter the SNMP community string that SL1 will use to make SNMP requests to this Windows 2008 Server. When you create a credential for this Windows 2008 Server in SL1, you will enter this community string in one the following fields in the **Credential Editor** modal page:
 - SNMP Community (Read-Only). Enter the SNMP community string in this field if you selected *READ ONLY* in the **Community rights** drop-down list.
 - SNMP Community (Read/Write). Enter the SNMP community string in this field if you selected *READ WRITE* in the **Community rights** drop-down list.
- 7. Click the **[Add]** button to add the community string to list of community strings this Windows 2008 Server accepts.
- 8. In the Accept SNMP packets from these hosts panel, click the Add... button. The SNMP Service Configuration pop-up window is displayed:

SNMP Service Properties (WIN-2TVE5CD1762)
General Log On Recovery Agent Traps Security Dependencies
Send authentication trap
Accepted community names
Community Rights
cOsmOs READ ONLY
SNMP Service Configuration
bbA
Host name, IP or IPX address:
Add Edit Remove
Learn more about <u>SNMP</u>
OK Cancel Apply

- 9. In the *Host name, IP or IPX address* field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.
- 10. Click the [Add] button to add the appliance to the list of authorized devices.

- 11. If you are using SL1 with a distributed architecture, repeat steps 8–10 for each Data Collector in the collector group that will monitor this server.
- 12. Click the [Apply] button to apply all changes.

Configuring the Firewall to Allow SNMP Requests

To configure the Windows Firewall to allow SNMP requests on a Windows 2008 server, perform the following steps:

- 1. In the Start menu search bar, enter "firewall" to open a **Windows Firewall with Advanced Security** window.
- 2. In the left pane, click Inbound Rules.
- 3. Locate the two SNMP Service (UDP In) rules.
- 4. If one or both of the rules is not enabled, right-click on the rule and then select *Enable Rule*:

<i>a</i>		Windows	Firewall with Ad	/anced Sec	urity					- 0	x
File Action View Help											
🔶 🧼 🙇 📰 📄											
P Windows Firewall with Advance Inbound Rules									17	Actions	
🔣 Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address	1	Inbound Rules	
Cutbound Rules	Remote Event Log Management (RPC-EP	Remote Event Log Manage	All	No	Allow	No	%System	Any		New Rule	
L Connection Security Rules	Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System	Any	112	-	
Monitoring	Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System	Any	11	Filter by Profile	•
	Remote Scheduled Tasks Management (Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	U:	Filter by State	•
	Remote Scheduled Tasks Management (Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	١ŀ	Filter by Group	•
	Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	No	System	Any			
	Remote Service Management (RPC)	Remote Service Management	All	No	Allow	No	%System	Any		View	•
(Ren	Remote Service Management (RPC-EPM	Remote Service Management	All	No	Allow	No	%System	Any	G	Refresh	
	Inbound Rule for Remote Shutdown (RP	Remote Shutdown	All	No	Allow	No	%system	Any		Export List	
	Inbound Rule for Remote Shutdown (TC	Remote Shutdown	All	No	Allow	No	%system	Any		? Help	
@ Re Ø Re	Remote Volume Management - Virtual D	Remote Volume Manageme.	. All	No	Allow	No	%System	Any		- Help	
	Remote Volume Management - Virtual D	Remote Volume Manageme.	. All	No	Allow	No	%System	Any		SNMP Service (UDP In)	
	Remote Volume Management (RPC-EPM	. Remote Volume Manageme.	. All	No	Allow	No	%System	Any		C Enable Rule	
	Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow	No	System	Any		-	
	Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No	System	Any		🥻 Cut	
	Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No	System	Any		Сору	
	Secure Socket Tunneling Protocol (SSTP	Secure Socket Tunneling Pr	All	No	Allow	No	System	Any		🗙 Delete	
	SNMP Service (UDP In)	SNMP Service	Domain, Public	Yes	Allow	No	%System	Any		Properties	
	SNMP Service (UDP In)	Enable Rule	Private, Public		Allow		%System	Any			
	SNMP Trap Service (UDP In)	Enable Kule	Private, Public	No	Allow	No	%System	Any	Ш	? Help	
	SNMP Trap Service (UDP In)	Cut	Domain	No	Allow	No	%System	Any	11.		
	TPM Virtual Smart Card Managemen	Copy ard Ma	Domain	No	Allow	No	%System	Any	Ш.		
	TPM Virtual Smart Card Managemen	Delete ard Ma	Private, Public	No	Allow	No	%System				
	TPM Virtual Smart Card Managemen	ard Ma	Domain	No	Allow	No	%System	Any			
	TPM Virtual Smart Card Managemen	Properties and Ma	Private, Public	No	Allow	No	%System	Any			
	Wirtual Machine Monitoring (DCOM-	Help itoring	All	No	Allow	No	%System	Any	Ш.		
	Wirtual Machine Monitoring (Echo Reque		All	No	Allow	No	Any	Any			
	 Virtual Machine Monitoring (Echo Reque Virtual Machine Monitoring Virtual Machine Monitoring (NB-Session Virtual Machine Monitoring 		All	No	Allow	No	Any	Any			
			All	No	Allow	No	Any	Any			
< III >	< III III III										
Enable Rule	h •										
hubic nuic											

Chapter



Configuring Windows Servers for Monitoring with PowerShell

Overview

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

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

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

This chapter covers the following topics:

Prerequisites	34
Configuring PowerShell	35
Step 1: Configuring the User Account for the ScienceLogic Platform	35
Step 2: Configuring a Server Authentication Certificate	40
Step 3: Configuring Windows Remote Management	44
Step 4: Configuring a Windows Management Proxy	. 73
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	. 75
Optional PowerShell CLI Parameters	76

Prerequisites

Before configuring PowerShell, ensure the following:

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

Configuring PowerShell

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

- 1. **Configure a user account** that SL1 will use to connect to the Windows Server. The user account can either be a local account or an Active Directory account.
- **TIP**: For ease of configuration, ScienceLogic recommends using an Active Directory account that is a member of the local Administrators group on the Windows Server.
- Configure a Server Authentication Certificate to encrypt communication between SL1 and the Windows Server.
- 3. Configure Windows Remote Management.
- 4. Optionally, configure a Windows server as a Windows Management Proxy.

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

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

Step 1: Configuring the User Account for the ScienceLogic Platform

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

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

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

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

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

- Microsoft Exchange Server
- Hyper-V Servers
- **NOTE:** In SL1 versions 11.3.0 and later, a newer Kerberos library is used that allows for message encryption over HTTP. This feature is on by default and may eliminate the need for you to configure an HTTPS certificate depending on your security requirements. When the *Encrypted* field is toggled on or off in the PowerShell credential, it determines if the HTTPS port is used (Yes) or not (No). Encryption is on by default.

Option 1: Creating an Active Directory Account with Administrator Access

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

After creating your Active Directory account:

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

Option 2: Creating a Local User Account with Administrator Access

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

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

After creating your local user account with Local Administrator access:

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

Option 3: Creating a Non-Administrator User Account

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

After creating your domain user account or local user account:

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

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

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

winrm configsddl default

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

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

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

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

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

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

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

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

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

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

If you use SL1 to monitor Microsoft Exchange Servers:

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

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

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

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

Creating a User Group and Adding a User in Active Directory

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

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

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

Setting the Session Configuration Parameters and Group Permissions

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

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

Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell

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

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

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

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

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

Step 2: Configuring a Server Authentication Certificate

NOTE: In SL1 versions 11.3.0 and later, a newer Kerberos library is used that allows for message encryption over HTTP. This feature is on by default and may eliminate the need for you to configure an HTTPS certificate depending on your security requirements. When the *Encrypted* field is toggled on or off in the PowerShell credential, it determines if the HTTPS port is used (Yes) or not (No). Encryption is on by default.

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

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

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

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

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

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

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

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

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

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

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

nap-in	Vendor	*	Console Root	Edit Extensions
ActiveX Control Authorization Manager Certificates Component Services Computer Managem Device Manager Disk Management Event Viewer Folder	Microsoft Cor Microsoft Cor	II	dd >	Remove Move Up Move Down
Group Policy Object IP Security Monitor IP Security Policy M Link to Web Address	Microsoft Cor Microsoft Cor	Ŧ		Advanced

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

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

This snap-in will always manage certificates for: My user account Service account Computer account
 My user account Service account
Service account
0
Computer account
< Back Finish Cancel

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

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

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

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

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

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

Step 3: Configuring Windows Remote Management

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

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

There are three ways to configure Windows Remote Management:

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

Option 1: Using a Script to Configure Windows Remote Management

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

To use the PowerShell script, perform the following steps:

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

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

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

8. After the warning text, select Y.

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

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

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

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

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

help .\winrm_configuration_wizard.ps1 -full

The most common way to run the script is silently:

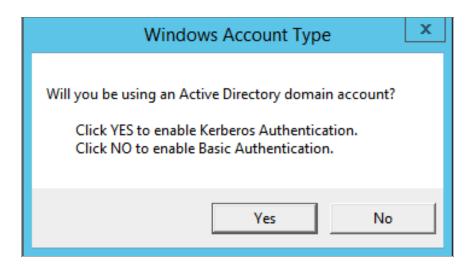
```
.\winrm_configuration_wizard.ps1 -user <domain>\<username> -
silent
```

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

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

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

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



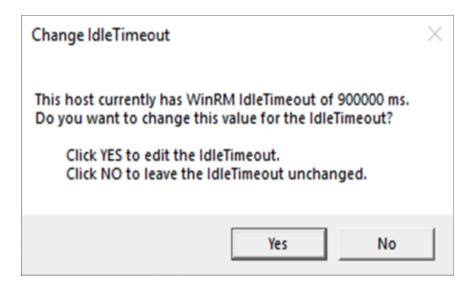
12. The Set Encryption Policy modal appears. Select the appropriate choice for your environment.



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

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

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



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

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

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

Set H	TTP/HTTPS Ports	_ □	X
New HTTP port:	5985		
New HTTPS port:	5986		
		ОК	

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

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

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

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

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

Complete				
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				

20. Exit the PowerShell session.

Option 2: Manually Configuring Windows Remote Management

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

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

Get-ExecutionPolicy

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

```
Set-ExecutionPolicy RemoteSigned
```

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

winrm quickconfig

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

winrm quickconfig -transport:https

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

winrm get winrm/config

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



12. In the Service section, if the parameter *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

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

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

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

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

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

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

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

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

NOTE: ScienceLogic recommends using an Active Directory account.

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

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

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

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

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

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

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

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

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

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

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

certutil.exe -ca.cert ca_name.cer

:\Users\EM7Admin\Documents>certuti] -ca.cert ca_name.cer A cert[0]: 3 Valid A cert[0]: BEGIN CERTIFICATE IIIDDTCCAo2gAwIBAgIQHAmGt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ RUWEWYKCZImiZPyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/ISZAEZFg]NU1RMDEy jiJJTAjBgNVBAMTHEITVEwwMTJSMi1UTDAxMlIyLURDLTAxLUNBLTEwHhcNNTQw DEIMTYINTQ1WhcNMTkwNDEIMTcwNTQ1WjBZMRUWEWYKCZImiZPyLGQBGRYFbG9j WwxGTAXBgoJkiaJk/ISZAEZFg]NU1RMNDEyUjIXJTAjBgNVBAMTHEITVEwwMTJS Ji1UTDAxMlIyLURDLTAxLUNBLTEwggEiMAOGCSqGSIb3DQEBAQUAA4IBDMawggEK KOOWqeiuNAuhllfYFIh0sORNSOFHgUNgradrugSPL/oV23VDH2dg]HaDd6azY CcwfD6uu3oV0aZU9Sgt4HEymPUl4QkGu21n4UTXIdepCA0N370yNkoQg01LUutp Bi16YdKbYaU0WwYkNrSOoSQpadFSGFW7gt8ObIXF92NJNywogEpfeQ+E8UH4 Gmt0pSZk7hsFDMxXkvRhdPugH7rIONGiaOxyoVUUVqfiiK748LiE/QveOX73wBo XLVsMSbWNo9SNxnf8/hiUTJOpOnAgMBAAGjaTBMMBMCCSGAQBgjCUAgQGHuQA WBBMA4GALUdDwE6/wQEAwIBhjAPBgNVHRMBAf8EBTADAQH/MB0GALUdDgQWBBR9 jjsBuyfqH2PrforxOq/z9102wDAQBgkrBgEEAYI3FQEEAWIBADANBgkqhkiG9w0B QUFAAOCAQEATSKQpaWpO6iOIT+1398051bHT1n6ayVGi2UZMBAANBgkqhkiG9w0B QUFAAOCAQEATSKQpaYDoE3ZTTNIOXKxEqUQCFR8EPFAZJYWABGqUQEZTQs99WbUK rD0gFZ7C0HXSJmRYCXJ02DK8zrH0ZADV/TTrn6CEWxYaB6qUQEZTG99WbUK rD0gFZ7C0HXSJmRYCXJ02DK8zrH0ZADV/TTrn6CEWxYaB6qUQEZg99WbUK rD0gFZ7C0H29LCZ6ZTTNIOXKxEqUQCFR8EPFACTYZ/+bNFV8V3YJjdAm/42g hjdX04PG1hDj0Bg2srX+01tx8mAMjAVUdNg2kvU0m0dP6h17BqJJ08umJxPmFQI WF19NeTUNHTYW1JdEeR7QhLhK6rkAnHw== END CERTIFICATE eretUti]: -ca.cert command completed successfully.
:\Users\EM7Admin\Documents>_

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

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

<u>الم</u>	Server Manager	_ 0 ×
Server M Server M Local Server All Servers	lanager • Dashboard welcome to server manager	
 R AD CS I AD DS DNS File and Storage Services ▷ IIS 	QUICK START 2 Add roles and features 3 Add other servers to manage WHATS NEW 4 Create a server group	Certification Authority Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer Group Policy Management Internet Information Services (IIS) Manager ISCSI Initiator
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers total: 1 AD CS 1 Image: AD CS 1	Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor Security Configuration Wizard Services
	Image ability Image ability Image ability Image ability Events Events Events Services Services Services Performance Performance Performance RPA results RPA results RPA results	y 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.

-			Group Policy M	anagement		- 🗆 🗙
File Action View	Window Help					
🗢 🔿 🖄 📅 📋	Q 7 1					
Group Policy Manage		Group Policy	Objects in MSTL012R2.local			
Forest: MSTL012R Domains	2.local	Contents Delega	Contents Delegation			
A MSTL012R	2 local	Name	• •	GPO Status	WMI Filter	Modified
Defa	Create a GPO in this domai	in, and Link it here	trollers Policy	Enabled	None	3/19/201
Powe	Link an Existing GPO		Cy Management Policy	Enabled All settings disabled	None	2/4/2014 4/17/201
⊳ 💼 Dom ⊳ 🎲 Grou	Block Inheritance		management rollcy	All settings disabled	None	4/16/201
p 📑 WMI	Group Policy Modeling Wi	zard				
D Start	New Organizational Unit					
Sites	Search					
🙀 Group Polic 😤 Group Polic	Change Domain Controller	r				
	Remove					
	Active Directory Users and	Computers				
	New Window from Here					
	Refresh					
	Properties					
	Help					
		4				
eate 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.

R		Group Policy Ma	anagement		_ 0 ×
File Action View Wind					- 8
Group Policy Management Group Noticy Management Group Noticy Management Group Noticy Management Group Noticy Group Polic Default Domais Group Polic Gr	t orced k Enabled e Report w Window from Here	Group Policy Objects in MSTL012R2.local Contents Delegation Name Default Domain Controllers Policy Default Domain Policy Work RM Reity WinRM Noticy WinRM Settings	GPO Status Enabled Enabled All settings daabled Enabled All settings disabled	WMI Filter None None None None None	Modified 3/19/201 2/4/201 4/17/201 4/17/201 4/16/201
Ref	p	٢	н		5
Open the GPO editor		1			

 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 Po	licy Management Editor			- 0
le Action View Help					
🔹 🖄 📰 💥 🖼 🕞 🔽 📷					
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	Service Name		Startup	Permission	
Nonputer Configuration	User Access Logging Service		Not Defined	Not Defined	
a 🦳 Policies	User Profile Service		Not Defined	Not Defined	
Software Settings	🙀 Virtual Disk		Not Defined	Not Defined	
Windows Settings	Volume Shadow Copy		Not Defined	Not Defined	
Name Resolution Policy	W3C Logging Service		Not Defined	Not Defined	
Scripts (Startup/Shutdown)	Windows Audio		Not Defined	Not Defined	
A 🔓 Security Settings	Windows Audio Endpoint Builder		Not Defined	Not Defined	
Account Policies Local Policies	Windows Color System		Not Defined	Not Defined	
Event Log	Windows Connection Manager		Not Defined	Not Defined	
Restricted Groups	Windows Driver Foundation - User	-mode Driver Framework	Not Defined	Not Defined	
System Services	Windows Encryption Provider Hos	t Service	Not Defined	Not Defined	
> Registry	Windows Error Reporting Service		Not Defined	Not Defined	
b 🔀 File System	Windows Event Collector		Not Defined	Not Defined	
Wired Network (IEEE 802.3) Policies	Windows Event Log		Not Defined	Not Defined	
Windows Firewall with Advanced Security	Windows Firewall		Not Defined	Not Defined	
Network List Manager Policies	Windows Font Cache Service		Not Defined	Not Defined	
Wireless Network (IEEE 802.11) Policies	🛱 Windows Installer		Not Defined	Not Defined	
Public Key Policies	Windows Management Instrumen	tation	Not Defined	Not Defined	
Software Restriction Policies	Windows Modules Installer		Not Defined	Not Defined	
Network Access Protection	Windows Process Activation Service	ce	Not Defined	Not Defined	
Application Control Policies	🙀 Windows Remote Management 🔒	(teamannant)	Not Defined	Not Defined	
IP Security Policies on Active Directory (MSTL012F	🗱 Windows Store Service (WSServi	Properties	Not Defined	Not Defined	
Advanced Audit Policy Configuration	🗱 Windows Time	Help	Not Defined	Not Defined	
Policy-based QoS	🙀 Windows Update		Not Defined	Not Defined	
Administrative Templates: Policy definitions (ADMX files) Preferences	WinHTTP Web Proxy Auto-Discov	ery Service	Not Defined	Not Defined	
User Configuration	Wired AutoConfig		Not Defined	Not Defined	
b Policies	🗱 WMI Performance Adapter		Not Defined	Not Defined	
Professional Pr	🗱 Workstation		Not Defined	Not Defined	
	World Wide Web Publishing Service	e	Not Defined	Not Defined	

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

J	Group Policy Management Edit	or		_ 0 ×
File Action View Help				
🕨 🔿 📶 🗙 🗊 🔒 🛛 🖬				
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	Service Name	Startup Not Defined	Permission Not Defined	
Policies Policies Software Settings a Windows Settings b Name Resolution Policy	🔅 User Profile Service Virtual Dick 🔅 Volu Windows Remote Management (WS-Manage	Not Defined	Not Defined Not Defined Not Defined	
Scripts (Startup/Shutdown) S	Win Win	nt)	Not Defined Not Defined Not Defined Not Defined Not Defined	
 Event Log Extincted Groups System Services Registry 	Winn [™] Winn [™] Win [™] Win [™] Win [™] Winn [™] Automatic		Not Defined Not Defined Not Defined	
Comparison of the System Comparison of the System Comparison of the System of the Syste	Win O Manual ∰Win Disabled ₩Win		Not Defined Not Defined Not Defined Not Defined	
Wireless Network (IEEE 802.11) Policies Die Public Key Policies Software Restriction Policies Metwork Access Protection	Win Edt Security Win Win Win Win Win Win		Not Defined Not Defined Not Defined Nat Defined	
 Application Control Policies IP Security Policies on Active Directory (MSTL012 Advanced Audit Policy Configuration 	F Win OK Cancel	Apply	Not Defined Not Defined Not Defined	
Jin Policy-based QoS P Administrative Templates: Policy definitions (ADMX files P Preferences g User Configuration	WinHTTP Web Proxy Auto-Discovery Service	Not Defined Not Defined Not Defined	Not Defined Not Defined Not Defined	
Policies Preferences	WMI Performance Adapter Workstation	Not Defined Not Defined Not Defined		

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

	G	roup Policy Management Editor						- 0	×
e Action View Help									
🔿 🙍 📷 🔒 🛛 🖬									
 Wind Veilor (TLD12R2-DC-01/MSTL012R2.LOCAL] Policy Computer Configuration Policies Software Settings Software Settings Software Settings Software Settings Software Settings Consection Policy Software Settings Local Policies Local Policies Local Policies Local Policies Software Settings Software Settings Software Settings Windows Strewall with Advanced Security Windows Firewall with Advanced Security Software Restriction Folicies Windows Firewall with Advanced Security Software Restriction Folicies Windows Firewall with Advanced Coreceive Firewall with Advanced Advanced Advan		Group There are New Rule Filter by Prof Filter by Stat Filter by Stat Filter by Grou Refresh View Arrange Icon Line up Icon Help	• •	Enabled ow in this vie	Action Action	Override	Program	Local Address	Rem

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]**.

IJ		Group Policy Mana	gement Editor						- 0	x
	View Help									
WinRM P	<i>2</i>	New Inbound Rule Wizard	X	Profile	Enabled	Action	Override	Program	Local Address	Remo
⊿ 🛄 Po ▷ 🗎	Rule Type Select the type of firewall rule to	o create.		ems to show	w in this vie	w.				
	Steps: a Rule Type a Predefined Rules a Action	What type of rule would you like to create? Program Rule that controls connections for a program. Pot Rule that controls connections for a TCP or UDP port. Predefined: Windows Frewall Remote Management Rule that controls connections for a Windows experience. Custom Custom rule.	V							
¢		< Back Ned	Cancel							

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

J		(Group Policy	Manageme	ent Editor							- 0	x
	View Help												
WinRM Po	@	New Inbound Rule Wizard				x	Profile	Enabled	Action	Override	Program	Local Address	Remo
⊿ 🛄 Po ▷ 🚞 ⊿ 🧰	Predefined Rules Select the rules to be created f	or this experience.					ems to sho	w in this vie	w.				
Þ	Steps:												
4	Rule Type	Which rules would you like to create?											
	Predefined Rules	The following rules define network connectivity requered to the second s	irements for the	selected predefin	ed group.								
	 Action 	Hules that are checked will be created. If a rule alreate the existing rule will be overwritten.	ady exists and is	checked, the co	intents of								
		Name	Rule Exists	Profile	Desc								
		Windows Firewall Remote Management (RPC		All	Inbou								
		☑ Windows Frewall Remote Management (RPC)	No	Al	Inbou								
		с ш			>								
¢ •		C	< Back	Next >	Cancel								

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

le Action View Help	Group Policy Management Editor							- 0	x
WinRM Po	New Inbound Rule Wizard	x	Profile	Enabled	Action	Override	Program	Local Address	Rem
Action	ken when a connection matches the conditions specified in the rule.		ems to sho	ow in this vie	w.				
 Steps: Rule Type Predefined Rules Action 	What actions should be taken when a connection matches the specified conditions? • Alon the connection The induces contentions that have been subtracticated by using Prec. Connections Subtractions are used using the settings in Prec. properties and rules in the Connection Security The node. Instructions Instructions								

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
Action View Help				
2 🖬 🖬 🖬 🖬				
		-		
⊿ 🧾 Windows Settings	Automatic Certificate Request	ð.		
Name Resolution Policy		There	are no items to show in this view.	
Scripts (Startup/Shutdown)				
Security Settings Account Policies				
 Account Policies Local Policies 				
▷ I Event Log				
Restricted Groups				
System Services				
Registry				
File System				
Wired Network (IEEE 802.3) Policies				
Windows Firewall with Advanced Security				
Network List Manager Policies				
Wireless Network (IEEE 802.11) Policies				
⊿ Public Key Policies		le contra		
Encrypting File System Data Protection		New	 Automatic Certificate Request 	
BitLocker Drive Encryption		Refresh		
BitLocker Drive Encryption Network Unlock		View	•	
Automatic Certificate Request Settings		Arrange Icons	•	
Enterprise Trust		Line up Icons		
Intermediate Certification Authorities		and the second second		
Trusted Publishers		Help		
Untrusted Certificates				
Trusted People				
Software Restriction Policies				
Network Access Protection				
Application Control Policies				
IP Security Policies on Active Directory (MSTL0)				
e a new Automatic Certificate Request object and add it to the Sec				1

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

Automatic Certificate Request Setup Wizard	Group Policy Management Editor	- 0 ×
Welcome to the Automatic Certificate Request Setup	equest • There are no items to show in this view.	

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

Certificate Tenglate Image: Certificate based on the template you select is with a computer log on, a certificate based on the template is with a certificate based on the template is with a certificate based on the template is a set of production state from the following list. A certificate template is a set of productive from the following list. Image: Certificate template is a set of productive from the following list. Certificate template: Image: Certificate template is a set of productive from the following list. Certificate template: Image: Certificate template is a set of productive from the following list. Certificate template: Image: Certificate template is a set of productive from the following list. Image: Certificate from the following list. Certificate template is a set of productive from the following list. Image: Certificate from the following list. Certificate from the following list. Image: Certificate from the following list. Cerificate from the following list. Image: Certificate from the following list. Cerificate from following list. Image: Certificate from following list. Cerificate from following list. Image: Certificate from following list. Cerificate from following list. Image: Certificate from following list. Cerificate from following list. Image: Certificate from following list. Cerificate from following list. Image: Certificate fr	Automatic Certif	icate Request Setup Wizard	Group Policy Mana	gement Editor		- 0	1 :
A cotificate template is a set of predefined properties for certificates issued to computers. Select a template if from the following list. Certificate template: Varie Intended Puposes Certificate Template: Varie Intended Puposes Certificate Request Agent (Computer) Certificate Request Register (Certification Authonities Certificate (Certification Certification Authonities Certificate Register (Certification Certification Authonities Certification Authonities Certification Authonities Certification Authonities Certification Authonities Certification Authonities Certification Authonities Certificate Register (Certificatio		certificate based on the template you select is	equest •				
Name Hended Puposes Caref Authentication, Server Authentication Doman Controller Careficate Request Agent Errollment Agent (Computer) Catificate Request Agent IPSic IP security IKE intermediate III Name III III BitLocker Drive Encryption BitLocker Drive Encryption Estinging Intermediate Catification Authonities Intermediate Catification Authonities <t< td=""><td></td><td>lefined properties for certificates issued to e following list.</td><td></td><td>There are no items t</td><td>o show in this view.</td><td></td><td></td></t<>		lefined properties for certificates issued to e following list.		There are no items t	o show in this view.		
Computer Over Authentication. Server Authentication Domain Controller Control. Server Authentication Evrollment Agent (Computer) Certificate Request Agent IP'Sec IP'security IKE intermediate M Cancel BitLocker Drive Encryption Cancel BitLocker Drive Encryption Cancel BitLocker Drive Encryption Cancel BitLocker Drive Encryption Cancel Distancer Drive Encryption Cancel Distan		Intended Purposes					
Evolment Agent (Computer) IP Sec IP Security IKE Intermediate C C BitLocker Drive Encryption BitLocker Drive Encryption BitLocker Drive Encryption Network Unlock BitLocker Drive Encryption Network Unlock Distributer Distributer Distri							
PSec PSec PSec PSec PSec PSec PSec PSec							
Image: Control of the second secon							
< Back	IPSec	IP security IKE intermediate					
< Back							
< Back							
BitLocker Drive Encryption BitLocker Drive Encryption BitLocker Drive Encryption BitLocker Drive Encryption Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Poblishers Untrusted Certificates Trusted Pople Notwork Access Protection > > Application Control Policies > > > Descutive Polisies on Active Directory (MSTL)	<	>					
BitLocker Drive Encryption Intermediate Certificates Intermediate Certificates Trusted People Difference Postoware Restriction Policies Postowark Access Protection							
BitLocker Drive Encryption BitLocker Drive Encryption BitLocker Drive Encryption BitLocker Drive Encryption Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Poblishers Untrusted Certificates Trusted Pople Notwork Access Protection > > Application Control Policies > > > Descutive Polisies on Active Directory (MSTL)							
BitLocker Drive Encryption Intermediate Certificates Intermediate Certificates Trusted People Difference Postoware Restriction Policies Postowark Access Protection							
 BitLocker Drive Encryption Network Unlock Automatic Certificate Request Settings Trusted Root Certification Authonities Enterprise Trust Intermediate Certification Authonities Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies Software Restriction Policies Security Policies on Active Directory (MSTL0.⁵⁷) 		< Back Next > Cancel					
 BitLocker Drive Encryption Network Unlock Automatic Certificate Request Settings Trusted Root Certification Authonities Enterprise Trust Intermediate Certification Authonities Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies Software Restriction Policies Security Policies on Active Directory (MSTL0.⁵⁷) 	BitLocker Drive	Encryption					
Trusted Paol Certification Authorities Trusted Publishers Trusted Publishers Trusted People Software Restriction Policies Software Restriction Policies Software Restriction Policies Software Restriction Control Policies Software Restriction Co							
Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies Del Software Restriction Polici	Automatic Certi	ficate Request Settings					
Intermediate Certification Authorities Intermediate Certification Authorities Intrusted Certificates Intrusted People Intrus							
Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies Network Access Protection P Application Control Policies Network Access Protection P Application Control Policies Network Access Protection							
Untrusted Certificates Trusted People Software Restriction Policies Mathematical Policies Mathematical Policies Software Restriction Policies Software Restrict Policies Software Restrevee S							
	Trusted Publish						
▷ Software Restriction Policies ▷ Network Access Protection ▷ Application Control Policies ▷ R. Security Policies on Active Directory (MSTL) [×]							
 ▷ In Period Control Policies ▷ In Policies on Active Directory (MSTL0^{-1/2}) 		icates					
 Application Control Policies I. P. Security Policies on Active Directory (MSTL0 × 	Trusted People						
b. ■ Psecurity Policies on Active Directory (MSTL0)	Trusted People	Policies					
	Trusted People	Policies					
	 Trusted People Software Restriction Metwork Access Pro Application Control 	Policies tection Policies					

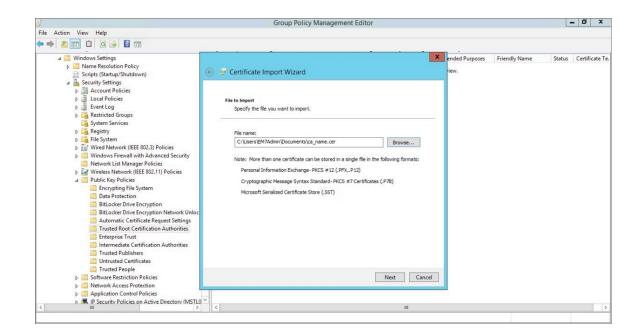
19. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration
 > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root
 Certification Authorities. In the right panel, right-click and select Import.

			Group Pol	cy Management Editor						- 0 ×
Action View Help										
🔿 🙍 🛅 📋 🙆 🔂 📷										
🛯 🧮 Windows Settings	^	Issued To	-	- Issued By		Expiration Date	Intended Purposes	Friendly Name	Status	Certificate
 Name Resolution Policy Scripts (Startup/Shutdown) Scruht Startup/Shutdown) Scruht Settings Account Policies Start Setup Local Policies Event Log System Services Square Services Registry 	_			Then	e are	no items to show in	this view.			
Gill System Wired Network (IEEE 802.3) Policies Windows Firewall with Advanced Security Network List Manager Policies Wireless Network (IEEE 802.11) Policies	Ш									
a 🔛 Public Key Policies				Import						
Encrypting File System Data Protection				All Tasks	•					
BitLocker Drive Encryption				Refresh						
BitLocker Drive Encryption Network Unlock	ć.			View						
Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust				Arrange Icons Line up Icons	٠					
Intermediate Certification Authorities				Help						
 Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies 				Look as						
Network Access Protection										
Application Control Policies	_									
IP Security Policies on Active Directory (MSTLO III)	Ľ.	<				Ш				

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

	Group Policy Management Editor			- 0 ×
File Action View Help				
▲ Windows Settings ▶ Name Resolution Policy ⊆cripts (Startury/Shutdown) ▲ Security Settings ▶ ↓ Local Policies ▶ ↓ Local Policies ▶ ▲ Restricted Groups ▲ ▲ ▲ ■ ■ ■ ■	Certificate Import Wizard Welcome to the Certificate Import Wizard This witard helps you copy certificates, certificate trust lists, and certificate revocation lists from your dak to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect date or to establish eacure network.	ended Purposes Frien	dly Name Statu	s Certificate Te
Network List Manager Policies Wireless Network (IEEE 802.11) Policies Public Key Policies Encrypting File System BitLocker Drive Encryption BitLocker Drive Encryption Key Control Network Unloc Automatic Certificate Request Settings	connections. A certificate store is the system area where certificates are kept. Store Location Current User © Local Machine To continue, dick Next.			
Trusted Root Certification Authorities Trusted Root Certification Authorities Trusted Publishers Trusted Publishers Trusted People Software Restriction Policies Application Control Policies	Next Cancel			
IP Security Policies on Active Directory (MSTL0 ~				>
· · · · · · · · · · · · · · · · · · ·			1	/

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



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

	Group Policy Management Editor		-	. 🗊 X
Action View Help				
Windows Settings Mame Resolution Policy Scripts (Startup/Shutdown) Signame Services System Services System Services Swindows Firewall with Advanced Security Windows Firewall with Advanced Security Network List Manager Policies Services Services Services Startup/Shutdown (IEEE 802.3) Policies Services Se	Certificate Import Wizard Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for who certificate. Windows can 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	ended Purposes Friendly Name	Status	Certificate 1
Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted People Software Restriction Policies Network Access Protection Paphication Control Policies P. IP Security Policies on Active Directory (MSTUL)	Next Cancel			

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

	Group Policy Management Editor			Ŀ	- 🗊 X
File Action View Help					
 ∠ Windows Settings ▷ Name Resolution Policy ≥ Scripts (Startup/Shutdown) ∠ 5 security Settings 	€ 🦻 Certificate Import Wizard	ended Purposes riew.	Friendly Name	Status	Certificate T
P Gamma Count Policies D Gamma Count Policies D Gamma Count Policies Vent Log P Restricted Groups Gamma Count Policies P Gamma Restricter P P P Gamma Restricter P P	Completing the Certificate Import Wizard The certificate will be imported after you click Finish. You have specified the following settings:				
Journal Metwork (IEE 802.3) Policies Windows Firewall with Advanced Security Network List Manager Policies Journal Metwork (IEE 802.11) Policies Public Rey Policies Dublic R	Contract store Section by User Trasted Root Certification Authorities Content Certificate File Name C:\Users\EM7Admin\Documents\ca_name.cer				
Trusted Root Certification Authonities Trusted Root Certification Authonities Trusted Publishers Trusted Publishers Trusted Publishers Trusted People Software Restriction Policies Depople D	Finish Cancel				
Application Control Policies	× (III				

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*.

a Action View Help Windby Picky [Tu13R2-DC-01.MSTL012R2L0CAL] Policy Computer Configuration b Software Settings b Softwa		Group Poli	cy Management Editor			- 0
Windby Direct (TL012R2-DC-OLINSTL012R2.LOCAL] Policy Configuration Policies Policies<	Action View Help					
 Configuration Policies Software Settings Monovs Firewalls Define induors Firewalls Allow local program exceptions. Not configured No Monovs Firewalls Define induors Firewalls Allow local program exceptions. Not configured No Monovs Firewalls Define induors Firewalls Allow local program exceptions. Not configured No Monovs Firewalls Allow local program exceptions. Not configured No Windows Firewalls Allow vibeous firewalls Allow induors Firewalls Allow local program exceptions. Not configured No Windows Firewalls Allow vibeous firewalls Allow local program exceptions. Not configured No Windows Firewalls Allow local program exceptions. Not configured No Windows Firewall Allow local program exceptions. Not configured No Windows Firewall Allow local prot exceptions is the finite on group policy. Windows Firewall Allow local pot exceptions. Not configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow local pot exceptions. Ist configured No Windows Firewall Allow inbound Firewalls Prohibution undows Firewall Allow inbound Firewalls Prohib	🔶 🙍 📷 🛛 🖬 🔻					
 Policies Software Settings Mondows Firevall: Allow local program exceptions Not configured Administrative Templates: Policy definitions (ADMX f) Administrative Templates: Policy definitions (ADMX f) Beckground Intelligent Transfer Service (BITS) BranchCache DirectAccess Client Experience Settings DirectAccess Client Experience Settings DirectAccess Client Experience Settings Link-Layer Topology Discovery Microsof Teevalt <li< th=""><th></th><th></th><th>Setting</th><th></th><th>State</th><th>Comment</th></li<>			Setting		State	Comment
b 📴 WWAN Service		port exceptions Edit policy setting, Requirements: At least Windows XP Professional with SP2 Description: Allows you to view and change the inbound port exceptions list defined by Group Policy. Windows Firewall uses two port exception lists: one is defined by Group Policy settings and the other is defined by the Windows Firewall component in Control Panel. If you enable this policy setting, you can view and change the inbound port exceptions list defined by Group Policy. To view this port exceptions list defined by Group Policy. To view this port exceptions list defined by Group Policy. To view this port exceptions list definition. To add a port, enable the policy setting, note the syntax. citck the Show button. In the Show Contents dialog box type a definition tring that uses the syntax format. To remove a port, citck its definition, and then press the DELETE key. To edit a definition; remove the current	Windows Firewall: Allow local progra Windows Firewall: Define inbound pu Windows Firewall: Define inbound pu Windows Firewall: Allow inbound file Windows Firewall: Allow inbound file Windows Firewall: Allow indows Windows Firewall: Allow logging Windows Firewall: Allow logging Windows Firewall: Allow logging Windows Firewall: Allow inbound Windows Firewall: Prohibit unical	ogram exceptions c connections stand printer sharing ex tions cceptions Edit Filter On Filter Options Re-Apply Filter All Tasks	Not configured Not configured Not configured Not configured Not configured Not configured Not configured Not configured Iot configured Iot configured Iot configured Iot configured	No No No No No No No No No No No

- 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
le Action View I	Se Windows	Firewall: Define inbound port exceptions	
🔿 🖄 📷 🗟	Windows Firewall: Define inbound port	exceptions Previous Setting Next Setting	÷
 Computer Config Policies Software ! Situation ! 	O Not Configured	State State Acceptions Not configured am exceptions Not configured	Comment No No
p → Windows	Supported on: At	nections Not configured s. Not configured Show Contents - Vindows XP Professional with SP2 Show Contents - Vindows Analysis An	No No No
⊿ Netwo Ba Bra Din	Options:	Define port exceptions: Not configured Not configured Not configured Not configured	No No No
📑 DM 🛄 Ho 📑 La	Denne port exceptions: Snow	Value Not configured 5985:TCP:*:enabled WSMan Not configured // 5985:TCP:*:enabled WSMan ration exc.	No No No
iii Lir ⊳ iii Mi	Syntax:	P 3986 ICF: shabed WSMan Proceedings of the state of	No No
⊿ <u></u> Ne ⊿ <u></u>	<port> is a decimal port number <transport> is either "TCP" or "UDP"</transport></port>	c exceptio Not configured	No
iii Ne iii Ne iii Of	<scope> is either " (for all networks) o a comma-separated list that contains</scope>		
▶ 🚞 Qa 🛄 SN 🛄 SS	IP addresses, such as 10.0.0.1	OK Cancel also enable the Windows Firewalt Allow local port exceptions	
▶ 🥌 TC 📑 Wi 🥅 Wi	< 111	24 v V V V V V V V V V V V V V	
⊳ 🛄 Wi ⊳ 🛅 W		OK Cancel Apply	

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

	Group Policy Manage	ement Editor	_ 0 X
File Action View Help	9	Allow Basic authentication	
+ + 2 🖬 🕒 🗊 🍸	Allow Basic authentication	Previous Setting Next Setting	
Smart Card Smart Card Snyc your settings P Tablet PC Task Scheduler Windows Color System Windows Color System Windows Color System Windows Customer Experince Improvement F Windows Customer Experince Improvement Windows Eror Reporting Windows Installer Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows Remote Management Windows Remote Management (WinRM) Windows Remote Management (WinRM) Windows Remote Shall Windows Remote Shall Windows Remote Management (WinRM) Windows Remote Shall Windows Remote Management (WinRM) Windows Remote Shall Windows R	Comment: Co	Previous setting Vext setting At least Windows Vista V At least Windows Vista V Help: V This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client uses Basic authentication. If WinRM is configured to use HTTP transport, the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, the WinRM client does not use Basic authentication. Voidable or do not configure this policy setting, the WinRM Client does not use Basic authentication.	hment Vo Vo Vo Vo Vo Vo
< III > Extende	d		
7 setting(s)			

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

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

	Group Policy Management Editor	- 0 X
File Action View Help	Trusted Hosts	
Smart Card Smart Card Smart Card Syncy our settings Tablet PC Tablet PC Tablet PC Windows Color System Windows Color System Windows Color System Windows Color System Windows Induler Windows Intaller	Trusted Hosts Image: Comment: Image: Comment: Image: Comment:	hent
Windows Logon Options uses the Trusted-Identination Windows Mail Trusted-Identination Windows Media Center Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows Rest Media Player Windows Media Player Windows Rest Media Player Windows Rest Management Windows Rest Management (WinRM) Windows Remote Management (WinRM) Windows Remote Management (WinRM) Windows Remote Management (WinRM) Windows Update Windows Update Workplace Join Workplace Join Workplace Join Workplace Join Windows Update Workplace Join Windows Update Workplace Join Windows Update Workplace Join Windows Develope Workplace Join Windows	Intern objects: Remote Management (WinRM) client uses the list specified in Trusted-holdstist to determine if the destination host is a trusted entity. If Configure the trusted hosts by a comma separated of the test name. You can use wildcards (') but only. o a	
< III > Extende		
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 Management Editor	0 X
File Action View Help	Allow Basic authentication	
	Allow Basic authentication Previous Setting Next Setting .	
Task Scheduler Edit policy Task Scheduler Requirem Windows Calendar Requirem Windows Cutomer Experience Improvement F Windows Cutomer Experience Improvement F	O Disabled Supported on: At least Windows Vista Vista	
	Options: Help: No No This policy setting allows you to manage whether the Windows A No No Remote Management (WinRM) service accepts Basic authentication from a remote client. A No No Basic authentication from a remote client. If you enable this policy setting, the WinRM service accepts Basic authentication from a remote client. A No WinRM service does not accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service does not accept Basic authentication from a remote client. B	
b C Policies	OK Cancel Apply	

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

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

	Group Policy Management Editor	_ 0 X
File Action View Help	Allow remote server management through WinRM -	
	Allow remote server management through WinRM Previous Setting Next Setting O Not Configured Comment:	nent
Windows Calendar Windows Color System Windows Color System Windows Customer Experience Improvement F Mindows Defender Descripti	O Disabled Supported on: At least Windows Vista V V	
▶ Windows Error Reporting This politimage Windows Itsaller manage Windows Neal error Reporting Windows Neal error Reporting Windows Media Center Hith enew Windows Media Center HITP true Windows Media Player Windows Media Player Windows Media Player Windows Media Player Windows Media Player HTP true Windows Media Player HTP true Windows Media Player Htp Windows Media Player Windows Media Player Htp Windows Media Player Windows Remote Management (WinRM) Windows Remote Management (WinRM) Windows Remote Shell Windows Vpdate Windows Remote Shell Port 5983 WorkPlace Join Windows Profeers WorkPlace Join Windows Profeers Windows Weinger Port 5983 Wer Configuration reguets Windows Diver Port 5983 Wer Configuration reguets Windows Poiloise Windows Poiloise	Pv4 filter: • This policy setting allows you to manage whether the Windows on the metwork for requests on the HTTP transport over the default items on the network for requests on the HTTP transport over the default HTTP port. • Py0 filter: • <t< td=""><td>,</td></t<>	,
Policies III Policies III Policies III Policies III Policies Policies III Policies Policies		

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

Group Policy Management Editor			
File Action View Help	💭 Specify idle Timeout	- O X	1
💠 🔶 🙍 📷 🕞 📓 💷 🖤	and developing Terrory		
Windows Defender Antvirus Windows Defender Spicio Guard Windows Elefender SmartScreen Windows Helle for Eurois Guard Windows Helle for Eurois Windows Helle for Eurois Windows Inteller Windows Inteller Windows Media Digital Rights Management Windows Remote Management (WinRM) Windows Remote Management (WinRM	Specify idle Timeout Not Configured Not Configured Disabled Disabled Supported on: At Options: IdleTimeout 900000	Previous Setting Next Setting t least Windows Vista Image: Configures the maximum time in milliseconds month of the Vistay open without any user activity until it is automatically deleted. Any value from 0 to 0x/FFFFFF can be set. A minimum of 60000 milliseconds milliseconds milliseconds or smaller values. Hy ou enable this policy setting, the sarver will wait for the specified amount of time since the last received message from the client before terminating the open shell. Hy ou enable this policy setting, the sarver will wait for the specified amount of time since the last received message from the client before terminating the open shell. Hy ou enable this policy setting, the used.	Comment No No No No No
		OK Cancel Apply	

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

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

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

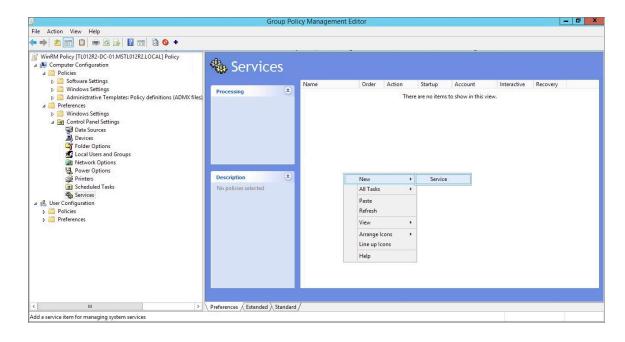
8		Max	ConcurrentUsers –	
🔠 MaxConcurrentUs	ers		Previous Setting Next Setting	
 Not Configured Enabled Disabled 	Comment:			^ ~
	Supported on:	At least Windo	ws Vista	< >
Options:			Help:	
MaxConcurrentUsers	40	× >	This policy setting configures the maximum number of able to concurrently perform remote shell operations or system. The value can be any number from 1 to 100. If you enable this policy setting, the new shell connection rejected if they exceed the specified limit. If you disable or do not configure this policy setting, the number is five users.	n the ons are
			OK Cancel	Apply

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

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

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

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



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

Group Policy Management Editor	a x
File Action View Help	
WinRM Melicy [TL01282-DC-01.MSTL01282.LOCAL] Policy WinRM Melicy [TL01282-DC-01.MSTL01282.LOCAL] Policy Performs Software Settings Mindows Settings Mindows Settings Administrative Templates: Policy definitions (ADMX Files) Preferences Devices Policies Devices Policy Control Panel Settings Devices Policy Policy definitions Service name: WinRM Melicy [TL01282-DC-01.MSTL01282.LOCAL] Policy Preferences Policy (Control Panel Settings) Devices Policy Control Panel Settings Service and Groups Service and Groups Policy Policy Options Service Seconds Policies Policies Policies Preferences Preferences Device Configuration Policies Preferences Preferences Preferences Policies Preferences Preferences	
C III Preferences / Extended / Standard /	
Services	

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

	Group Policy Management Editor	- 0 ×
File Action View Help		
* * 2 📷 📋 🗰 🛛 🖬 🖬		
 WinRM Policy [TL012R2-DC-01.MSTL012R2LOCAL] Policy Computer Configuration Policies Software Settings Administrative Templates: Policy definitions (ADMX files) Preferences Outro Panel Settings Control Panel Settings Control Panel Settings Control Panel Settings Devices Folder Options Network: Options Scheduled Tasks Services Scheduled Tasks Services Preferences Preferences 	Services New Service Properties Statup Account Interactive Recovery re are no items to show in this view. Select the computer's response if this service fails. First failure: Restart the Service Subsequent failures: Restart the Service Subsequent failures: Restart the Service Subsequent failures: Restart the Service Nu Program Program: Command line (Ifail=%1%) Restart Computer Options OK Cancel Apply Heb	
< III >	Preferences / Extended / Standard /	
Services		

• First failure. Select Restart the Service.

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

14	Group Policy Management				
🛃 File Action View Window Help					_ # ×
🗢 🔿 🙋 🖬 🧕 🖬 🖬					
Group Policy Management ▲ Group Policy Management ▲ Group Policy Management ▲ MSTL012R2.local ▲ MSTL012R2.local ▲ MSTL012R2.local ▲ Dowes field Remote Management Policy ▲ WinR Molicy ▶ Group Policy Objects ▶ Group Policy Objects ▶ Group Policy Results A Group Policy Results	PowerShell Remote Manager Scope Details Settings Delegation Unks Display links in this location:	v]			
	Location	Enforced	Link Enabled	Path	
	Security Filtering The settings in this GPO can only apply to Name	No	Yes rs, and computers:	MSTL012R2.booal	
	Add Remove WMI Filtering This GPD is linked to the following WMI (cnone)		Open		

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

<u>(</u>		Group Policy Management	- 0 ×			
File Action View Windo			- 8			
• 🔿 🖄 📅 🐴 🗊 🗙	a 1					
Group Policy Management		WinRM Policy				
A Forest: MSTL012R2.local		Scope Details Settings Delegation Status				
⊿ 👫 Domains ⊿ 🚔 MSTL012R2.local		Links				
🛒 Default Domain	Policy	Display links in this location: MSTL012R2.local	Y			
	note Management Policy	The following sites, domains, and OUs are linked to this GPO:				
 ₩inRM Policy Domain Controllers Group Policy Objects 		Location Enforced Link Enabled Path				
		MSTL012R2.local No Yes MSTL012R2.local				
📑 Default Don	nain Controllers Policy					
📑 Default Don						
VinRM Poli	Remote Management Polic					
WinRM 5 Edit P WinRM 5 GPO Status P Status Statter GPOs Back Up Back Up Back Up Back Up Back Up Save Report View New Window from He Copy Delete Rename Refresh						
	GPO Status	► 🗸 Enabled				
	Back Up	User Configuration Settings Disabled				
	Restore from Backup	Computer Configuration Settings Disabled computers:				
	Import Settings	All Settings Disabled				
	Save Report	ricinicalcu useis				
	View	•				
	New Window from Here					
	Copy					
	Rename	Add Remove Properties				
	Refresh	Add Hemove Propentes				
	Help	Itering				
		O is linked to the following WMI filter:				
	>	(none) V Open				
settings enabled	/	le.	1			

Configuring an HTTPS Listener with GPO Configuration

If you are using an HTTPS listener, you cannot create the listener and start it on the monitored device within group policy object (GPO) configuration without using a startup script or an immediate task in the group policy, or by running a command manually or on the remote management tool on the device to be monitored. This command needs to be run only once as the HTTPS listener will automatically start once configured.

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

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

winrm quickconfig -transport:https -force

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

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

NOTE: The thumbprint should not contain spaces.

Using Forward and Reverse DNS for Windows Remote Management

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

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

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

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

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

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

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

Step 4: Configuring a Windows Management Proxy

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

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

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

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

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

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

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

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

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

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

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

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

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

Risk of Password Exposure

The use of a PowerShell proxy server or PowerShell implicit remoting can expose the monitoring account password when using HTTP or when Script Block Logging is enabled.

To avoid password exposure, use the following recommendations:

- Use HTTPS instead of HTTP for PowerShell monitoring.
- The only ScienceLogic-released PowerPack that included implicit remoting is the *Microsoft: Exchange Server* PowerPack. Implicit remoting has been removed from the PowerPack as of version 101. ScienceLogic recommends either uninstalling the *Microsoft: Exchange Server* PowerPack if it is not being used, or upgrading the PowerPack to version 101.
- Do not enable Script Block Logging on the PowerShell proxy server. If Script Block Logging is required by company policy, then take extra care in restricting what users can access on that server.

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

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

To do so:

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

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

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

Restart-Service WinRM

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

Optional PowerShell CLI Parameters

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

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

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

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

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

where:

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

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

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

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

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

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

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

Chapter

4

Dynamic Applications for Windows Devices

Overview

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

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

The following sections describe the SNMP and PowerShell Dynamic Applications that SL1 uses to monitor Windows devices:

This chapter covers the following topics:

SNMP Dynamic Applications for Windows Devices	77
PowerShell Dynamic Applications	78
Relationships with Other Types of Component Devices	89

SNMP Dynamic Applications for Windows Devices

If you configure your Windows system to respond to SNMP requests from SL1, you can discover your Windows system as an SNMP device. When SL1 discovers a Windows system as an SNMP device, the platform will automatically collect the same data from the Windows system that the platform collects from most network devices. This data includes interface usage, file system usage, CPU usage, memory usage, and hardware configuration information.

In addition to the common SNMP data collection, you can install an optional agent that reports WMI information through SNMP. The following SNMP Dynamic Applications can be used to collect the information reported by the optional agent:

- MSSQL: General
- MSSQL: Memory
- MSSQL: SQL Stats

PowerShell Dynamic Applications

If you configure your Windows system to respond to PowerShell requests from SL1, you can use PowerShell Dynamic Applications to collect information from your Windows system.

All of the PowerShell Dynamic Applications include a discovery object. If you include a credential for PowerShell Dynamic Applications in the discovery session that includes your Windows system, SL1 will automatically align the appropriate PowerShell Dynamic Applications to the Windows system. For more information about creating a discovery session, see the **Discovery & Credentials** manual.

The following PowerPacks include PowerShell Dynamic Applications for Microsoft Servers.

Microsoft: Active Directory Server

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2012 R2.

The following PowerShell Dynamic Applications can be used to collect performance data from Active Directory servers:

- Microsoft: Active Directory Address Book Performance
- Microsoft: Active Directory Async Thread Queue Performance
- Microsoft: Active Directory Database Performance
- Microsoft: Active Directory Directory Services Reads Performance
- Microsoft: Active Directory Directory Services Searches Performance
- Microsoft: Active Directory Directory Services Writes Performance
- Microsoft: Active Directory DRA Performance
- Microsoft: Active Directory LDAP Performance
- Microsoft: Active Directory Security Account Management Performance
- Microsoft: Active Directory Services General Performance
- Microsoft: Active Directory Web Service Performance

Microsoft: DHCP Server

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2012.

The following PowerShell Dynamic Applications can be used to collect performance data from DHCP servers:

- Microsoft: DHCP IPv4 Performance
- Microsoft: DHCP IPv4 Scope Performance
- Microsoft: DHCP Service Performance

The following PowerShell Dynamic Applications can be used to collect configuration data from DHCP servers:

- Microsoft: DHCP IPv4 Lease Configuration
- Microsoft: DHCP IPv6 Lease Configuration
- Microsoft: DHCP Service Performance

Microsoft: DNS Server

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2012 and 2012 R2.

The following PowerShell Dynamic Applications can be used to collect performance data from DNS servers:

- Microsoft: DNS AXFR Performance
- Microsoft: DNS Dynamic Update Performance
- Microsoft: DNS IXFR Performance
- Microsoft: DNS Memory Performance
- Microsoft: DNS Notification Performance
- Microsoft: DNS Recursion Performance
- Microsoft: DNS Secure Dynamic Update Performance
- Microsoft: DNS TCP Performance
- Microsoft: DNS Total Overall Performance
- Microsoft: DNS UDP Performance
- Microsoft: DNS WINS Performance
- Microsoft: DNS Zone Transfer Performance

Microsoft: Exchange Server

The following PowerShell Dynamic Applications can be used to collect performance data from Exchange 2013 and Exchange 2016 servers:

• Microsoft: Exchange CAS ActiveSync Performance

- Microsoft: Exchange CAS Address Book Load Performance
- Microsoft: Exchange CAS Address Book Service Performance
- Microsoft: Exchange CAS Availability Service Performance
- Microsoft: Exchange CAS OWA Performance
- Microsoft: Exchange CAS Performance
- Microsoft: Exchange CAS RPC Client Access Load Performance
- Microsoft: Exchange CAS RPC Client Access Performance
- Microsoft: Exchange MBS Database Performance
- Microsoft: Exchange MBS Info Store RPC Processing Stats
- Microsoft: Exchange MBS Information Store Performance
- Microsoft: Exchange MBS Replay Log I/O Latency Requirements
- Microsoft: Exchange TPS Disk Performance
- Microsoft: Exchange TPS Transport Database Performance
- Microsoft: Exchange TPS Transport Load Assessment Stats
- Microsoft: Exchange UMS General Performance

Microsoft: Exchange Server 2010

The following PowerShell Dynamic Applications can be used to collect performance data from Exchange 2010 servers:

- Microsoft: Exchange 2010 CAS Address Book Load Performance
- Microsoft: Exchange 2010 CAS Address Book Service Performance
- Microsoft: Exchange 2010 CAS Availability Service Performance
- Microsoft: Exchange 2010 CAS OWA Performance
- Microsoft: Exchange 2010 CAS Performance
- Microsoft: Exchange 2010 CAS RPC Client Access Load Performance
- Microsoft: Exchange 2010 CAS RPC Client Access Performance
- Microsoft: Exchange 2010 MBS Client-Related Search Performance
- Microsoft: Exchange 2010 MBS Database Performance
- Microsoft: Exchange 2010 MBS Info Store RPC Processing Stats
- Microsoft: Exchange 2010 MBS Information Store Performance
- Microsoft: Exchange 2010 MBS Message Queuing Performance
- Microsoft: Exchange 2010 MBS Replay Log I/O Latency Requirements
- Microsoft: Exchange 2010 MBS RPC Client Throttling Performance
- Microsoft: Exchange 2010 MBS Store Client Request Performance
- Microsoft: Exchange 2010 TPS Disk Performance

- Microsoft: Exchange 2010 TPS Transport Database Performance
- Microsoft: Exchange 2010 TPS Transport Load Assessment Stats
- Microsoft: Exchange 2010 TPS Transport Queue Length Performance
- Microsoft: Exchange 2010 UMS General Performance

Microsoft: Hyper-V Server

NOTE: The Dynamic Applications in this PowerPack support Hyper-V Server 2012, 2012 R2, 2016, 2019, and 2022.

The following PowerShell Dynamic Applications can be used to collect performance data from Hyper-V servers:

- Microsoft: Hyper-V Component Count
- Microsoft: Hyper-V Logical Processor Performance
- Microsoft: Hyper-V Overall Guest CPU Performance
- Microsoft: Hyper-V Process Performance
- Microsoft: Hyper-V Root Virtual Processor Performance
- Microsoft: Hyper-V Virtual Processor Performance
- Microsoft: Hyper-V Virtual Storage Device Performance
- Microsoft: Hyper-V Virtual Switch Performance

The following PowerShell Dynamic Applications can be used to collect configuration data from Hyper-V servers:

- Microsoft: Hyper-V Component Count Configuration
- Microsoft: Hyper-V Host Configuration

This PowerPack also includes Snippet Dynamic Applications that discover virtual machines managed by the Hyper-V host. Although the Dynamic Applications are of type "Snippet", the snippets themselves perform PowerShell requests to collect data and use PowerShell credentials. See the *Discovering Component Devices* on Hyper-V Systems section for more information.

- Microsoft: Hyper-V Guest Configuration
- Microsoft: Hyper-V Guest Configuration Cache
- Microsoft: Hyper-V Guest Discovery

This PowerPack also includes Snippet Dynamic Applications that retrieve performance data from virtual machines managed by the Hyper-V host. Although the Dynamic Applications are of type "Snippet", the snippets themselves perform PowerShell requests to collect data and use PowerShell credentials:

- Microsoft: Hyper-V Connected Clients
- Microsoft: Hyper-V Guest CPU Performance
- Microsoft: Hyper-V Guest IDE Controller Performance

- Microsoft: Hyper-V Guest Interface Performance
- Microsoft: Hyper-V Guest Memory Performance

Microsoft: IIS Server

NOTE: The Dynamic Applications in this PowerPack support Internet Information Services (ISS) versions 7.5, 8.0, 8.5, and 10.0.

The following PowerShell Dynamic Applications can be used to collect performance data from IIS servers:

- Microsoft: IIS Active Server Pages Performance
- Microsoft: IIS Core Performance
- Microsoft: IIS Web Service Performance

The following PowerShell Dynamic Applications can be used to collect configuration data from IIS servers:

• Microsoft: IIS Server Configuration

Microsoft: Lync Server 2010

The following PowerShell Dynamic Applications can be used to collect performance data from Lync 2010 servers:

- Microsoft: Lync 2010 Announcement Service Performance
- Microsoft: Lync 2010 AS MCU Performance
- Microsoft: Lync 2010 Auto Attendant Performance
- Microsoft: Lync 2010 AV MCU Performance
- Microsoft: Lync 2010 AV SIP/MRAS/QOE Performance
- Microsoft: Lync 2010 Call Park Service Performance
- Microsoft: Lync 2010 Conferencing Compatibility Performance
- Microsoft: Lync 2010 Data Conferencing Performance
- Microsoft: Lync 2010 IM MCU Performance
- Microsoft: Lync 2010 Response Group Performance
- Microsoft: Lync 2010 SIP Load Management Performance
- Microsoft: Lync 2010 SIP Networking Performance
- Microsoft: Lync 2010 SIP Peers Performance
- Microsoft: Lync 2010 SIP Protocol Performance
- Microsoft: Lync 2010 SIP Response Performance
- Microsoft: Lync 2010 SipEps Incoming Message Performance
- Microsoft: Lync 2010 User Services Performance
- Microsoft: Lync 2010 Web Services Performance

The following PowerShell Dynamic Applications can be used to collect configuration data from Lync 2010 servers:

- Microsoft: Lync 2010 AS MCU Configuration
- Microsoft: Lync 2010 AV MCU Configuration
- Microsoft: Lync 2010 Conferencing Compatibility Configuration
- Microsoft: Lync 2010 Data Conferencing Configuration
- Microsoft: Lync 2010 Service Health Configuration
- Microsoft: Lync 2010 User Services Configuration

Microsoft: SharePoint Server

NOTE: The Dynamic Applications in this PowerPack support SharePoint Server 2010 SE.

The following PowerShell Dynamic Applications can be used to collect performance data from SharePoint servers:

- Microsoft: SharePoint Core Performance
- Microsoft: SharePoint Indexer Performance
- Microsoft: SharePoint Query Performance

Microsoft: Skype for Business

NOTE: This PowerPack was previously named Microsoft: Lync Server 2013.

The following PowerShell Dynamic Applications can be used to collect performance data from Lync 2013 servers:

- Microsoft: Lync 2013 AS MCU Performance
- Microsoft: Lync 2013 AV MCU Performance
- Microsoft: Lync 2013 AV SIP/MRAS/QOE Performance
- Microsoft: Lync 2013 Bandwidth Services Performance
- Microsoft: Lync 2013 Call Park Service Performance
- Microsoft: Lync 2013 Data Conferencing Performance
- Microsoft: Lync 2013 IM MCU Performance
- Microsoft: Lync 2013 Mediation Server Performance
- Microsoft: Lync 2013 Response Group Performance
- Microsoft: Lync 2013 SIP Load Management Performance
- Microsoft: Lync 2013 SIP Networking Performance
- Microsoft: Lync 2013 SIP Peers Performance

- Microsoft: Lync 2013 SIP Protocol Performance
- Microsoft: Lync 2013 SIP Response Performance
- Microsoft: Lync 2013 SipEps Incoming Message Performance
- Microsoft: Lync 2013 User Services Performance
- Microsoft: Lync 2013 Web Services Performance

The following PowerShell Dynamic Applications can be used to collect configuration data from Lync 2013 servers:

- x Microsoft: Lync 2013 AS MCU Configuration
- x Microsoft: Lync 2013 AV MCU Configuration
- x Microsoft: Lync 2013 Data Conferencing Configuration
- x Microsoft: Lync 2013 Service Health Configuration
- x Microsoft: Lync 2013 User Services Configuration

Microsoft: SQL Server

NOTE: The Dynamic Applications in this PowerPack support SQL Server 2012, 2014, 2016, 2017, 2019, and 2022.

The following PowerShell Dynamic Applications can be used to collect performance data from SQL servers:

- Microsoft: SQL Buffer Performance
- Microsoft: SQL Database Performance
- Microsoft: SQL Memory Performance
- Microsoft: SQL Plan Cache Performance
- Microsoft: SQL Query Performance
- Microsoft: SQL Session Performance
- Microsoft: SQL Table Lock/Latch Performance

Microsoft: Windows Server

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2012, 2012 R2, 2016, 2019, and 2022, as well as Windows 10.

The following PowerShell Dynamic Applications can be used to collect configuration data from Windows servers:

- Microsoft: Print Server
- Microsoft: Windows Server BIOS Configuration
- Microsoft: Windows Server Configuration Cache

- Microsoft: Windows Server CPU Configuration
- Microsoft: Windows Server Device Discovery
- Microsoft: Windows Server Disk Configuration
- Microsoft: Windows Server Interface Configuration
- Microsoft: Windows Server Memory Configuration
- Microsoft: Windows Server OS Configuration
- Microsoft: Windows Server Software Configuration

NOTE: The "Microsoft: Windows Server Configuration Cache" Dynamic Application caches data that is consumed by all of the other configuration Dynamic Applications in the list.

NOTE: When the "Microsoft: Windows Server OS Configuration" or "Microsoft: Windows Server Device Discovery" Dynamic Applications automatically align to Windows servers, they trigger events and Run Book Actions that classify the server.

The following PowerShell Dynamic Applications can be used to collect performance data from Windows servers:

- Microsoft: Windows Server CPU Performance
- Microsoft: Windows Server Disk Performance
- Microsoft: Windows Server Interface Performance
- Microsoft: Windows Server IPStats Performance
- Microsoft: Windows Server Memory Performance
- Microsoft: Windows Server Performance Cache
- Microsoft: Windows Server TCPStats Performance
- Microsoft: Windows Server UDPStats Performance

NOTE: The "Microsoft: Windows Server Performance Cache" Dynamic Application caches data that is consumed by all of the other performance Dynamic Applications in the list.

The following Snippet Dynamic Application creates a DCM+R relationship for AppDynamics, Dynatrace, New Relic, and virtual machine component devices with the physical Windows server device:

• Microsoft: Windows Server DCM+R Relationship

The following Snippet Dynamic Application monitors Windows services, displaying the status of all services in a configuration report:

• Microsoft: Windows Server Service Configuration

The following Dynamic Applications use PowerShell to collect data as a supplement to SL1's internal collection capabilities:

- Microsoft: Windows Server IC Cache Trigger
- Microsoft: Windows Server IC Detail
- Microsoft: Windows Server IC Filesystem Inventory
- Microsoft: Windows Server IC Filesystem Performance
- Microsoft: Windows Server IC Interface Inventory
- Microsoft: Windows Server IC Interface Performance
- Microsoft: Windows Server IC Port Performance
- Microsoft: Windows Server IC Process Inventory
- Microsoft: Windows Server IC Process Performance
- Microsoft: Windows Server IC Process Service Cache
- Microsoft: Windows Server IC Service Inventory
- Microsoft: Windows Server IC Service Performance

NOTE: The "Microsoft: Windows Server IC Cache Trigger" Dynamic Application needs to be enabled for both legacy and concurrent PowerShell collection.

Microsoft: Windows Server Event Logs

The following Snippet Dynamic Applications can be used to collect data from system, application, and security event logs on Microsoft Windows servers:

- Microsoft: Windows Server Application Events
- Microsoft: Windows Server Security Events
- Microsoft: Windows Server System Events

To customize how the *Microsoft*: *Windows Server Event Logs* Dynamic Applications filter event logs, perform the following steps for each Dynamic Application:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications) and search for the Dynamic Application you want to customize in the **Dynamic Application Name** column.
- 2. Click the wrench icon (🎤) for the Dynamic Application you want to edit.

- 3. In the [Snippets] tab, click the wrench icon (*P*) next to the item in the Snippet Registry pane.
- 4. In the Snippet Editor, you can edit the following fields:
 - EVENT_ID_FILTER_INCLUDE_LIST. Enter a list of Event IDs to include in your event logs.
 - EVENT_TYPE_FILTER_INCLUDE_LIST. Enter a list of Event Types to include in your event logs.
 - **EVENT_MSG_FILTER_INCLUDE_LIST**. Enter a list of Event Descriptions to include in your event logs. This field supports the use of the * wildcard character.
 - **EVENT_SRC_FILTER_INCLUDE_LIST**. Enter a list of Event Provider names to include in your event logs. This field supports the use of the * wildcard character.
- 5. Click the **[Save]** button.

Close <u>P</u> ropert	es <u>C</u> ollections	Presentati <u>o</u> ns	<u>S</u> nippets	<u>T</u> hresholds	Alerts	Subscribers	
Dynamic Applications [1662] I Snip	pet Editor & Registry Edi	ing Snippet [2025]				Gu	ide Reset
Snippet Get Security Event Log Ent		[Enabled]	Active State Snippet Code	¥	[Required -	Required Stop Collection]	T
EVENT_ID_FILTER_INCL # Add the list of Ev. # Example: the list of # return ev. # EVENT_ID_FILTER_IN	ent IDs you wish t of codes below wil ents where those E	o filter on to thi l cause the filte vent IDs are a mai	r to only				^
EVENT_TYPE_FILTER_IN # Add the list of Ev # following values a # - "Security Audit # - "Security Audit # Examples: # EVENT_TYPE_FILTER # CVENT_TYPE_FILTER	ent Types you wish e supported: success" ailure" SNCLUDE_LIST = ["S	to filter on to t ecurity Audit Fail	this list. The lure"]		13		
<pre># EVENT_TYPE_FILTER_ EVENT_MSG_FILTER_INC # Add the list of Ev # Use entire descrip # Examples: # EVENT_MSG_FILTER_I # EVENT_MSG_FILTER_I # EVENT_MSG_FILTER_I # ["An account was 1."</pre>	UDE_LIST = ["An a nt Descriptions y ion in filter or ICLUDE_LIST = ["An ICLUDE_LIST =	ccount was logged ou wish to filter use the * wildcard account was logge	off."] on to this li d character fo ed off."]	st. r partial descrip	-	5.	
EVENT_SRC_FILTER_INC # Add the list of Ev. # Supports the use o # Evamples:	ent Provider Names	you wish to filte haracter.					
			Save Save	As			
Snippet Registry 1. P Get Security Event Log Er	tries	Snippet Name				quired ID quired snip_2025 20	Date Edit 20-01-31 12:39:57 💣

Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows Servers

You can use the following Run Book Automation Policy and Run Book Action Policy to assign a device class to each Windows device that does not support SNMP:

- Microsoft: Windows Server Device Class Alignment (Run Book Automation Policy)
- Microsoft: Windows Server Device Class Alignment (Run Book Action Policy)

Devices that do not support SNMP are assigned a device class of type "pingable".

The automation policy is configured to trigger when the "Microsoft: Windows Server OS Configuration" or "Microsoft: Windows Server Device Discovery" Dynamic Applications are aligned with a device during discovery. These Dynamic Applications collect the name of the Windows operating system and store the name in a collection object named "Edition". The Run Book Automation policy and Run Book Action policy use the value of the collection object named "Edition" to assign a device class to each Windows device that does not support SNMP.

For example, if the collection object named "Edition" contains the value "Microsoft Windows Server 2012 R2 Datacenter", the Run Book Automation policy and the Run Book Action policy will assign the device to the device class "Microsoft Windows Server 2012 R2".

Error Messages for PowerShell Collection

Error Message	Possible Issue(s)
Preauthentication failed while getting initial credentials	Incorrect Password (Active Directory Accounts only)
Client not found in Kerberos database	Username does not exist in Active Directory (Active Directory Accounts only)
KRB5 error code 68 while getting initial credentials	Incorrect domain name (Active Directory Accounts only)
Bad HTTP response returned from server. Code 401, basic auth failed	Incorrect username/password or target server does not allow user account to perform WinRM operations.
ParseError	Incorrect port specified in credential
[Errno 111] Connection refused	Mismatch between server configuration and credential, e.g. encryption option selected but not enabled on server.
Hostname cannot be canonicalized	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance

The following table lists error messages that SL1 can generate during PowerShell collection.

Error Message	Possible Issue(s)
Cannot resolve network address for KDC in requested realm	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
Configuration file does not specify default realm	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
No credentials cache found	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
Server not found in Kerbers database	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance

Relationships with Other Types of Component Devices

Additionally, the Dynamic Applications in the *Microsoft: Windows Server* PowerPack can automatically build relationships between Windows servers and other associated devices:

- If you discover Dynatrace devices using the Dynamic Applications in the Dynatrace PowerPack, SL1 will automatically create relationships between Windows servers and Dynatrace hosts.
- If you discover Cisco AppDynamics devices using the Dynamic Applications in the Cisco: AppDynamics PowerPack, SL1 will automatically create relationships between Windows servers and AppDynamics nodes.
- If you discover New Relic devices using the Dynamic Applications in the New Relic APM Pro PowerPack, SL1 will automatically create relationships between Windows servers and New Relic servers.

Chapter

5

Creating Credentials and Discovering Windows Devices

Overview

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

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

The following sections describe how to create SNMP and PowerShell credentials for Windows devices that you want to monitor with SL1, general discovery steps, and how to discover Windows Server clusters and component devices on Hyper-V systems:

This chapter covers the following topics:

Creating an SNMP Credential	91
Creating a PowerShell Credential	95
Testing Windows Credentials	
Adding Devices Using Unguided Discovery	
Discovering Windows Server Clusters	
Discovering Devices with the Microsoft: Windows Server Discovery Template	
Discovering Component Devices on Hyper-V Systems	
Manually Aligning the Microsoft: Print Server Dynamic Application	

Creating an SNMP Credential

SNMP credentials allow SL1 to access SNMP data on a managed device. SL1 uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

- 1. Go to the **Credentials** page (Manage > Credentials).
- 2. Click the [Create New] button and then select Create SNMP Credential. The Create Credential modal page appears:

				Credential Tester
All Organizations	What organization manages this service?		 Timeout (m) 1500 	Select Credential Test
SNMP Version	SNMP Retries	Port*		Select Collector CUG1 AsimovSandboxCU1: 10.2.25.101
SNMP V2	~ 1	161		IP or Hostname to test "
SNMP Community (Read-Only)	SNMP Community (Read/Write)		Test Cre

- 3. Supply values in the following fields:
 - **Name**. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This is a required field.
 - All Organizations. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the What organization manages this service? drop-down field to align the credential with those specific organizations. This field is required.

NOTE: To learn more about credentials and organizations, see the section Aligning Organizations With a Credential.

- *Timeout (ms)*. Time, in milliseconds, after which SL1 will stop trying to communicate with the device. The default value is 1500.
- **SNMP Version**. SNMP version. Choices are SNMP V1, SNMP V2, and SNMP V3. The default value is SNMP V2.
- **Port**. The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.

• **SNMP Retries**. Number of times SL1 will try to authenticate and communicate with the external device. The default value is 1.

SNMP V1/V2 Settings

If you selected SNMP V1 or SNMP V2 in the **SNMP Version** field, complete these fields. These fields are inactive if you selected SNMP V3.

- SNMP Community (Read-Only). The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the SNMP Community (Read/Write) field.
- SNMP Community (Read/Write). The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the SNMP Community (Read Only) field.

SNMP V3 Settings

If you selected SNMP V3 in the **SNMP Version** field, complete these fields. These fields are inactive if you selected SNMP V1 or SNMP V2.

- Security Name. Name for SNMP authentication. This field is required.
- Security Passphrase. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a Security Level that includes authentication.

In addition to alphanumeric characters, you **can** also use the following special characters in an SNMP V3 security passphrase: ? - _ = , . : # + % \$ [] { } &! () | /

You cannot use the following special characters in an SNMP V3 security passphrase: "'\

- Authentication Protocol. Select an authentication algorithm for the credential. This field is required. Choices are:
 - ° MD5. This is the default value.
 - ° SHA
 - SHA-224
 - ° SHA-256
 - ° SHA-384
 - ° SHA-512

NOTE: The SHA option is SHA-128.

- **Security Level**. Specifies the combination of security features for the credentials. This field is required. Choices are:
 - No Authentication / No Encryption.
 - ° Authentication Only. This is the default value.
 - Authentication and Encryption.
- **Engine ID**. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- **Context**. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- **Privacy Protocol**. The privacy service encryption and decryption algorithm. This field is required. Choices are:
 - DES. This is the default value.
 - ° AES-128
 - ° AES-192
 - ° AES-256
 - AES-256-C. This option is for discovering Cisco devices only.
- Privacy Protocol Passphrase. Privacy password for the credential. This field is optional.
- 4. Click [Save & Close].

NOTE: If you would like to test your credential using the Credential Tester panel, click **[Save & Test]**. For detailed instructions on using the Credential Tester panel, see the *Using the Credential Tester Panel* section.

Creating an SNMP Credential in the SL1 Classic User Interface

SNMP Credentials allow SL1 to access SNMP data on a managed device. SL1 uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

- 1. Go to the Credential Management page (System > Manage > Credentials).
- 2. Click the **[Actions]** button and select Create SNMP Credential. The **Credential Editor** page appears.
- 3. Supply values in the following fields:
 - **Profile Name**. Name of the credential. Can be any combination of alphanumeric characters. This field is required.

- **SNMP Version**. SNMP version. Choices are SNMP V1, SNMP V2, and SNMP V3. The default value is SNMP V2.
- **Port**. The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.
- *Timeout (ms)*. Time, in milliseconds, after which SL1 will stop trying to communicate with the SNMP device. The default value is 1500.
- *Retries*. Number of times SL1 will try to authenticate and communicate with the external device. The default value is 1.

SNMP V1/V2 Settings

These fields appear if you selected SNMP V1 or SNMP V2 in the **SNMP Version** field. The fields are inactive if you selected SNMP V3.

- **SNMP Community (Read-Only)**. The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the **SNMP Community (Read/Write)** field.
- SNMP Community (Read/Write). The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the SNMP Community (Read Only) field.

SNMP V3 Settings

These fields appear if you selected SNMP V3 in the **SNMP Version** field. These fields are inactive if you selected SNMP V1 or SNMP V2.

- Security Name. Name for SNMP authentication. This field is required.
- Security Passphrase. Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a Security Level that includes authentication.
- Authentication Protocol. Select an authentication algorithm for the credential. This field is required. Choices are:
 - MD5. This is the default value.
 - ° SHA
 - ° SHA-224
 - ° SHA-256
 - ° SHA-384
 - ° SHA-512

NOTE: The SHA option is SHA-128.

- **Security Level**. Specifies the combination of security features for the credentials. This field is required. Choices are:
 - No Authentication / No Encryption.
 - ° Authentication Only. This is the default value.
 - Authentication and Encryption.
- **SNMP v3 Engine ID**. The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- **Context Name**. A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.
- **Privacy Protocol**. The privacy service encryption and decryption algorithm. This field is required. Choices are:
 - DES. This is the default value.
 - ° AES-128
 - ° AES-192
 - ° AES-256
 - AES-256-C. This option is for discovering Cisco devices only.
- Privacy Protocol Passphrase. Privacy password for the credential. This field is optional.
- 4. Click the [Save] button to save the new SNMP credential.
- 5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with SL1.

NOTE: When you define an SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

Creating a PowerShell Credential

If you configure your Windows system to respond to PowerShell requests from SL1, you can use PowerShell Dynamic Applications to collect information from your Windows system.

All of the PowerShell Dynamic Applications include a discovery object. If you include a credential for PowerShell Dynamic Applications in the discovery session that includes your Windows system, SL1 will automatically align the appropriate PowerShell Dynamic Applications to the Windows system. For more information about creating a discovery session, see the **Discovery & Credentials** manual.

To define a PowerShell credential in SL1, you will need the following information:

- 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.

To create a PowerShell credential:

- 1. Go to the **Credentials** page (Manage > Credentials).
- 2. Click the [Create New] button and then select Create Powershell Credential. The Create Credential modal page appears:

Name*				Credential Tester	
	ization manages this service?		Timeout (m) 1500	Select Credential Test	
Account Type Active Directory		Encrypted		Select Callector CUG1 AsimovSandboxCU1: 10.2.25.101	
Active Directory				IP or Hostname to test "	
Username "		Password *			Test Cred
Hostname/IP*		5985			
PowerShell Proxy Hostname/IP Active Directory Host/IP		Active Directory Domain			

- 3. Supply values in the following fields:
 - **Name**. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This field is required.
 - All Organizations. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the What organization manages this **service?** drop-down field to align the credential with those specific organizations. This field is required.

NOTE: To learn more about credentials and organizations, see the section Aligning Organizations With a Credential.

- *Timeout (ms)*. Time, in milliseconds, after which SL1 will stop trying to communicate with 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.
- 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.
- Hostname/IP. Hostname or IP address of the device from which you want to retrieve data. This field is required.
 - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
 - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the device that is currently using the credential. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
 - You can include the prefix HOST or WSMAN before the variable %D in this field if the device you want to monitor uses a service principal name (for example, "HOST://%D" or "WSMAN://%D").
 SL1 will use the WinRM service HOST or WSMan instead of HTTP and replace the variable with the IP address of the device that is currently using the credential.
- **Username**. Type the username for an account on the Windows device to be monitored or on the proxy server. This field is required.

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

- **Password**. Type the password for the account on the Windows device to be monitored or on the proxy server. This field is required.
- **Encrypted**. Select whether SL1 will communicate with the device using an encrypted HTTP or HTTPS connection:
 - Toggle on (blue) if SL1 will communicate with the device using an encrypted connection over HTTPS. If toggled on, 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.

NOTE: In SL1 versions 11.3.0 and later, a newer Kerberos library is used that allows for message encryption over HTTP. This feature is on by default and may eliminate the need for you to configure an HTTPS certificate depending on your security requirements.

- Toggle off (gray) . The credential is encrypted over HTTP rather than HTTPS.
- **Port**. Type the port number used by the WinRM service on the Windows device. This field is required and is automatically populated with the default port based on the value you selected in the

Encrypted field.

- **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 Host/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.
- Active Directory Domain. If you selected Active Directory in the Account Type field, type the domain where the monitored Windows device resides.
- 4. Click [Save & Close].

NOTE: If you would like to test your credential using the Credential Tester panel, click [Save & Test]. For detailed instructions on using the Credential Tester panel, see the Using the Credential Tester Panel section.

NOTE: If you update the credential after your initial discovery session, you will need to run a new discovery session to update the etc/krb5.conf file and to re-align Dynamic Applications.

Creating a PowerShell Credential in the SL1 Classic User Interface

To define a PowerShell credential in SL1:

- 1. Collect the information you need to create the credential:
 - The username and password for a user on the Windows device.
 - If the user is an Active Directory account, the hostname or IP address of the Active Directory server and the domain.
 - Determine if an encrypted connection should be used.
 - If you are using a Windows Management Proxy, the hostname or IP address of the proxy server.
- 2. Go to the **Credential Management** page (System > Manage > Credentials).
- 3. In the Credential Management page, click the [Actions] menu. Select Create PowerShell Credential.
- 4. The **Credential Editor** page appears, where you can define the following fields:
 - **Profile Name**. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
 - Hostname/IP. Hostname or IP address of the device from which you want to retrieve data. This field is required.
 - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.

- You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the device that is currently using the credential. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
- You can include the prefix HOST or WSMAN before the variable %D in this field if the device you want to monitor uses a service principal name (for example, "HOST://%D" or "WSMAN://%D").
 SL1 will use the WinRM service HOST or WSMan instead of HTTP and replace the variable with the IP address of the device that is currently using the credential.
- **Username**. Type the username for an account on the Windows device to be monitored or on the proxy server. This field is required.

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

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

- Active Directory Hostname/IP. If you selected Active Directory in the Account Type field, type the hostname or IP address of the Active Directory server that will authenticate the credential.
- **Domain**. If you selected Active Directory in the **Account Type** field, type the domain where the monitored Windows device resides.
- 5. To save the credential, click the **[Save]** button. To clear the values you set, click the **[Reset]** button.

NOTE: If you update the credential after your initial discovery session, you will need to run a new discovery session to update the etc/krb5.conf file and to re-align Dynamic Applications.

Testing Windows Credentials

Credential Tests define a series of steps that SL1 can execute on-demand to validate whether a credential works as expected. This section describes the SNMP and PowerShell Credential Tests that are included in the default installation of SL1.

SNMP Credential Test

The SNMP Credential Test can be used to test an SNMP credential for connectivity. The SNMP Credential Test performs the following steps:

- Test Reachability. Performs an ICMP ping request to the host specified in the credential.
- Test Port Availability. Performs an NMAP request to the UDP port specified in the credential on the host specified in the credential.
- Test SNMP Availability. Attempts an SNMP getnext request to .1.3.6.1 using the credential.

PowerShell Credential Test

The PowerShell Credential Test can be used to test a PowerShell credential for connectivity. The PowerShell Credential Test performs the following steps:

- Test Reachability. Performs an ICMP ping request to the host specified in the credential.
- Test Port Availability. Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential.
- Test Name Resolution. Performs an nslookup request on the host specified in the credential.
- **Test Kerberos**. If the credential does not specify local authentication, attempts to acquire a kerberos ticket using the credential.
- Test WinRM Connection. Attempts a WinRM connection using the credential.
- **Execute PowerShell Cmdlet**. Attempts to execute the 'Get-WmiObject Win32_Process | Select Name' PowerShell Cmdlet using the credential.

Running a Windows Credential Test

You can test a credential from the Credentials page using a predefined credential test.

To run a credential test from the **Credentials** page:

- 1. Go to the **Credentials** page (Manage > Credentials).
- 2. Click the Actions button (--) of the credential that you want to test, and then select Test.
- 3. The **Credential Test Form** modal page appears. Fill out the following fields on this page:
 - **Credential**. Select the credential to test. This drop-down list includes only credentials that you have access to. (If you clicked the **Actions** button (--) and then selected *Test* for a specific credential, then this field is read-only.)
 - Select Credential Test. Select a credential test to run. This drop-down list includes the ScienceLogic Default Credential Tests, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
 - Collector. Select the All-In-One Appliance or Data Collector that will run the test.
 - *IP or Hostname to Test*. Type a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
- 4. Click [Run Test] button to run the credential test. The Testing Credential window appears:

esting Credential				×
¢ step	DESCRIPTION	LOG MESSAGE	STATUS	
Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 2	 Passed 	?
Test Port Availability	Check to see if the appropriate port is open	Port 443 is open	 Passed 	?
Test Name Resolution	Check to see if nslookup can resolve the IP and hostname	Name resolution failed: Reverse failed, Forward failed	! Failed	?
Make of IRI Request	Check to see if a cLIRL request succeeds	cl IRI request failed: HTTP 400	Epiled	2

The **Testing Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- Step. The name of the step.
- **Description**. A description of the action performed during the step.
- Log Message. The result of the step for this execution of the credential test.
- **Status**. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
- **Step Tip**. Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".

To run a Windows credential test using the Credential Tester panel:

- 1. While defining a credential, supply values in the required fields on the Create Credential page.
- 2. Click the [Save & Test] button. This activates the Credential Tester fields.
- 3. In the Credential Tester panel, supply values in the following fields:

- Select Credential Test. Select a credential test to run. This drop-down list includes the ScienceLogic Default Credential Tests, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
- Select Collector. Select the All-In-One Appliance or Data Collector that will run the test.
- *IP or Hostname to test*. Type a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
- 4. Click [Run Test] button to run the credential test. The Testing Credential window appears:

sting Credential				×
¢ step	DESCRIPTION	LOG MESSAGE	STATUS	
Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 2	 Passed 	?
Test Port Availability	Check to see if the appropriate port is open	Port 443 is open	 Passed 	?
Test Name Resolution	Check to see if nslookup can resolve the IP and hostname	Name resolution failed: Reverse failed, Forward failed	! Failed	?
Make of IRL Request	Check to see if a cLIRL request succeeds	cLIRL request failed: HTTP 400	Failed	2

The **Testing Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- Step. The name of the step.
- **Description**. A description of the action performed during the step.
- Log Message. The result of the step for this execution of the credential test.
- **Status**. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
- **Step Tip**. Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".

Running a Windows Credential Test in the SL1 Classic User Interface

To run a Windows credential test from the **Credential Management** page:

- 1. Go to the Credential Management page (System > Manage > Credentials).
- 2. Click the [Actions] menu, and then select Test Credential. The Credential Tester modal page appears.
- 3. Supply values in the following fields:
 - Test Type. Select a credential test to run.
 - **Credential**. Select the credential you want to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.

- Hostname/IP. Enter a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
- Collector. Select the All-In-One Appliance or Data Collector that will run the test.
- 4. Click the [Run Test] button to run the credential test. The Test Credential window appears.

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- Step. The name of the step.
- **Description**. A description of the action performed during the step.
- Log Message. The result of the step for this execution of the credential test.
- **Status**. Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
- Step Tip. Mouse over the question mark icon (2) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".
- 5. Optionally, you can click the **[Execute Discovery Session]** button to run a discovery session using the **Credential**, **Hostname/IP**, and **Collector** you selected in the **Credential Tester** modal page.

Adding Devices Using Unguided Discovery

To run an unguided discovery:

- On the Devices page (I) or the Discovery Sessions page (Devices > Discovery Sessions), click the [Add Devices] button. The Select page appears.
- 2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
- 3. Click [Select]. The Add Devices page appears.
- 4. Complete the following fields:
 - **Discovery Session Name**. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
 - **Description**. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab. Optional.
 - Select the organization to add discovered devices to. Select the name of the organization to which you want to add the discovered devices.
- 5. Click [Next]. The Credentials page of the Add Devices wizard appears.
- 6. On the Credentials page, you can optionally do one of the following:

- If the credential you need is not in the list, click the [Create New] button to open the Create Credential window, where you can specify the name and organization for the credential, the thirdparty username and password, and other data such as Cloud Type and Proxy information. You can also test the credential before you save using the Credential Tester panel. Click [Save & Close] to save the credential and return to the Credential Selection page of the guided discovery session.
- To edit a credential on the **Credential Selection** page, click the name of the credential you would like to edit from the **Name** column and edit that credential as needed. You can also test the credential before you save using the **Credential Tester** panel. Click the **[Save & Close]** button on the **Edit Credential** window to save your updates.
- 7. On the **Credentials** page of the **Add Devices** wizard, select one or more credentials to allow SL1 to access a device's SNMP data and click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears.
- 8. Complete the following fields:
 - List of IPs/Hostnames. Provide a list of IP addresses, hostnames, or fully-qualified domain names for SL1 to scan during discovery. This field is required. In this field, you can enter a combination of one or more of the following:
 - One or more single IPv4 addresses separated by commas and a new line. Each IP address must be in standard IP notation and cannot exceed 15 characters. For example, "10.20.30.1, 10.20.30.2, 10.20."
 - One or more ranges of IPv4 addresses with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "10.20.30.1 10.20.30.254".
 - One or more IP address ranges in *IPv4 CIDR notation*. Separate each item in the list with a comma. For example, "192.168.168.0/24".
 - One or more ranges of IPv6 addresses with "-" (dash) characters between the beginning of the range and the end of the range. Separate each range with a comma. For example, "2001:DB8:0:0:0:0:0:0:001:DB8:0:0:0:0:0:0:003".
 - One or more IP address ranges in *IPv6 CIDR notation*. Separate each item in the list with a comma. For example, "2001:DB8:0:0:0:0:0:0/117".
 - One or more hostnames (fully-qualified domain names). Separate each item in the list with a comma.

TIP: You can also click the [Upload File] button to upload a comma-separated list of IPs.

• Which collector will monitor these devices?. Select an existing collector group to monitor the discovered devices. Required.

- **NOTE:** When assigning devices to a collector group, SL1's multi-tenancy rules will validate that the collector group you select belongs to the organization you selected in the previous field. If you attempt to run a discovery session where the devices, collector group, and credentials do not all belong to the same organization, you will receive an error message and will not be able to save or execute the discovery session.
 - *Run after save*. Select this option to run this discovery session as soon as you click [Save and Close].
 - Advanced options. Click the down arrow icon (\checkmark) to access additional discovery options.

In the Advanced options section, complete the following fields as needed:

- Initial Scan Level. For this discovery session only, specifies the data to be gathered during the initial discovery session. The options are:
 - System Default (recommended). Use the value defined in the Behavior Settings page (System > Settings > Behavior) in the classic user interface of SL1.
 - 1. Model Device Only. Discovery will discover if the device is up and running and if so, collect the make and model of the device. SL1 will then generate a device ID for the device so it can be managed by SL1.
 - 2. Initial Population of Apps. Discovery will search for Dynamic Applications to associate with the device. The discovery tool will attempt to collect data for the aligned Dynamic Applications. Discovery will later retrieve full sets of data from each Dynamic Application. Discovery will also perform 1. Model Device Only discovery.
 - 3. Discover SSL Certificates. Discovery will search for SSL certificates and retrieve SSL data. Discovery will also perform 2. Initial Population of Apps and 1. Model Device Only.
 - 4. Discover Open Ports. Discovery will search for open ports. Discovery will also perform 3. Discover SSL Certificates, 2. Initial Population of Apps, and 1. Model Device Only.

NOTE: If your system includes a firewall and you select *4*. *Discover Open Ports*, discovery might be blocked and/or might be taxing to your network.

5. Advanced Port Discovery. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform 3. Discover SSL Certificates, 2. Initial Population of Apps, and 1. Model Device Only.

NOTE: If your system includes a firewall and you select 5. Advanced Port Discovery, some devices might remain in a pending state (purple icon) for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

6. Deep Discovery. Discovery will use nmap to retrieve the operating system name and version. Discovery will also scan for services running on each open port and can use this information to match devices to device classes. Discovery will search for open ports, using a faster TCP/IP connection method. Discovery will also perform 3. Discover SSL Certificates, 2. Initial Population of Apps, and 1. Model Device Only.

NOTE: For devices that don't support SNMP, option 6. Deep Discovery allows you to discover devices that don't support SNMP and then align those devices with a device class other than "pingable". Note that option 6. Deep Discovery is compute-intensive.

NOTE: If SL1 cannot determine the appropriate Device Class, it will assign the device to the Generic SNMP Device Class.

- Scan Throttle. Specifies the amount of time a discovery process should pause between each specified IP address (specified in the IP Address/Hostname Discovery List field). Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
 - System Default (recommended). Use the value defined in the Behavior Settings page (System > Settings > Behavior) in the classic user interface for SL1.
 - Disabled. Discovery processes will not pause.
 - 1000 Msec to 10000 Msec. A discovery process will pause for a random amount of time between half the selected value and the selected value.
- **Port Scan All IPs**. For the initial discovery session only, specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
 - System Default (recommended). Use the value defined in the Behavior Settings page (System > Settings > Behavior) in the classic user interface for SL1.
 - Enabled. SL1 will scan all discovered IP addresses for open ports.
 - Disabled. SL1 will scan only the primary IP address (the one used to communicate with SL1) for open ports.
- **Port Scan Timeout**. For the initial discovery session only, specifies the length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are:
 - System Default (recommended). Use the value defined in the Behavior Settings page (System > Settings > Behavior).
 - Choices between 60 to 1,800 seconds.
- **Scan Ports**. Specify a list of ports to scan, separated by colons (:). The default is 21:22:25:80:136.

- Interface Inventory Timeout (ms). Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
 - During the execution of this discovery session, SL1 uses the value in this field first. If you delete
 the default values and do not specify another value in this field, SL1 uses the value in the
 Global Threshold Settings page (System > Settings > Thresholds).
 - If you specify a value in this field and do not apply a device template to this discovery session, the *Interface Inventory Timeout* setting in the *Device Thresholds* page (Registry > Devices > Device Manager > wrench icon > Thresholds) is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the *Global Threshold Settings* page (System > Settings > Thresholds).
- **Maximum Allowed Interfaces**. Specifies the maximum number of interfaces per devices. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
 - During the execution of this discovery session, SL1 uses the value in this field first. If you delete
 the default values and do not specify another value in this field, SL1 uses the value in the
 Global Threshold Settings page.
 - If you specify a value in this field and do not apply a device template to this discovery session, the Maximum Allowed Interfaces setting in the Device Thresholds page is set to this value for each discovered device. If there is no device template applied to the discovery session and no value is supplied in this field, SL1 uses the value in the Global Threshold Settings page.
- **Bypass Interface Inventory**. Specifies whether or not the discovery session should discover network interfaces.
 - Selected. SL1 will not attempt to discover interfaces for each device in the discovery session.
 For each discovered device, the *Bypass Interface Inventory* checkbox on the *Device* Investigator [Settings] tab will be selected.
 - Not Selected. SL1 will attempt to discover network interfaces, using the Interface Inventory Timeout value and Maximum Allowed Interfaces value.
- **Discover Non-SNMP**. Specifies whether or not SL1 should discover devices that don't respond to SNMP requests.
 - Selected. SL1 will discover devices that don't respond to the SNMP credentials selected in the SNMP Credentials field. These devices will be discovered as "pingable" devices.
 - Not Selected. SL1 will not discover devices that don't respond to the SNMP credentials selected in the SNMP Credentials fields.

NOTE: You must either select a credential for the discovery session or select the **Discover Non-SNMP** option. SL1 will prevent you from proceeding with discovery if you have not met those conditions.

- **Model Devices**. Determines whether or not the devices that are discovered with this discovery session can be managed through SL1. Choices are:
 - *Enabled*. When a device is modeled, SL1 creates a device ID for the device; you can then access the device through the **Device Manager** page and manage the device in SL1.
 - Disabled. If a device is not modeled, you cannot access the device through the Device Manager page, and you cannot manage the device in SL1. However, each discovered device will still appear in the Discovery Session logs. For each discovered device, the discovery logs will display the IP address and device class for the device. This option is useful when performing an initial discovery of your network, to determine which devices you want to monitor and manage with SL1. For the amount of time specified in the Device Model Cache TTL (h) field, a user can manually model the device from the Discovery Session window.
- Enable DHCP. Specifies whether or not the specified range of IPs and hostnames use DHCP.
 - Selected. SL1 will perform a DNS lookup for the device during discovery and each time SL1 retrieves information from the device.
 - Not Selected. SL1 will perform normal discovery.
- Device Model Cache TTL (h). Amount of time, in hours, that SL1 stores information about devices that are discovered but not modeled, either because the Model Devices option is not enabled or because SL1 cannot determine whether a duplicate device already exists. The cached data can be used to manually model the device from the Discovery Session window.
- Log All. Specifies whether or not the discovery session should use verbose logging. When you select verbose logging, SL1 logs details about each IP address or hostname specified in the IP Address/Hostname Discovery List field, even if the results are "No device found at this address."
 - Selected. This discovery session will use verbose logging.
 - Not Selected. This discovery session will not use verbose logging.
- Apply Device Template. As SL1 discovers a device in the IP discovery list, that device is configured with the selected device template. You can select from a list of all device templates in SL1. For more information on device templates, see the manual on Device Groups and Device Templates.
- 9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
- If you selected the Run after save option on this page, the discovery session runs, and the Discovery Logs page displays any relevant log messages. If the discovery session locates and adds any devices, the Discovery Logs page includes a link to the Device Investigator page for the discovered device.

Discovering Windows Server Clusters

To discover a Windows Server cluster with the *Microsoft*: Windows Server PowerPack, you must align the discovery Dynamic Application to one or more of the cluster node physical devices. To align the Dynamic Application:

- 1. On the [Collections] tab of the Device Investigator, click [Edit] and then click [Align Dynamic App]. The Align Dynamic Application window appears.
- 2. Click Choose Dynamic Application. The Choose Dynamic Application window appears:

Choose Dynamic Application		× ESC
Q. Type to search dynamicApplications	=	0
NAME N	TYPE Sitting Configuration	^
Avocent: Serial Port Performance	SNMP Performance	
Avocent: Serial Port Performance: ACS	SNMP Performance	
AWS Account Discovery	Snippet Configuration	- 1
AWS API Gateway Service Configuration	Snippet Configuration	
AWS API Gateway Service Discovery	Snippet Configuration	
AWS API Gateway Service Health	Snippet Journal	
AWS API Instance Configuration	Bulk Snippet Configuration	Ŷ

- 3. Select the "Microsoft: Windows Server Discovery" Dynamic Application and click **[Select]**. The name of the Dynamic Application appears in the **Align Dynamic Application** window.
- 4. If a default credential is listed below the Dynamic Application and you do not want to use that credential, uncheck the box next to the credential name.
- 5. Click Choose Credential. The Choose Credential window appears.
- 6. Select the credential you created for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
- 7. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

TIP: To *unalign* a Dynamic Application from a device, click the **[Actions]** button (---) for that Dynamic Application and select *Unalign Dynamic App*. However, be advised that when you unalign a Dynamic Application, you also delete the data it has collected.

Once you have aligned the "Microsoft: Windows Server Discovery" Dynamic Application, an event will be generated with the network name of the cluster. The "Microsoft: Windows Server Create Windows Cluster Virtual Device" Run Book action will execute and create a virtual device with the name of the cluster. The necessary Dynamic Applications will automatically align to the virtual device, and the cluster DCM tree will then be created over the next few polling cycles.

Discovering Windows Server Clusters in the SL1 Classic User Interface

To discover a Windows Server cluster with the *Microsoft: Windows Server* PowerPack, you must align the discovery Dynamic Application to one or more of the cluster node physical devices. To align the Dynamic Application:

- 1. Go to the **Device Manager** page (Devices > Device Manager).
- 2. In the **Device Manager** page, find a cluster node device and click its wrench icon (*P*).
- 3. In the **Device Administration** panel, click the **[Collections]** tab.
- 4. In the **Dynamic Application Collections** page, click the **[Actions]** menu and select Add Dynamic Application.
- 5. The **Dynamic Application Alignment** modal page appears. Locate the "Microsoft: Windows Server Discovery" Dynamic Application and select it.
- 6. After selecting a Dynamic Application, select the credential you created in the **Credentials** field.
- 7. Click the **[Save]** button in the **Dynamic Application Alignment** modal page to align the Dynamic Application and the credential to the device.

Once you have aligned the "Microsoft: Windows Server Discovery" Dynamic Application, an event will be generated with the network name of the cluster. The "Microsoft: Windows Server Create Windows Cluster Virtual Device" Run Book action will execute and create a virtual device with the name of the cluster. The necessary Dynamic Applications will automatically align to the virtual device, and the cluster DCM tree will then be created over the next few polling cycles.

Discovering Devices with the Microsoft: Windows Server Discovery Template

A *device template* allows you to save a device configuration and apply it to multiple devices. The Microsoft: Windows Server PowerPack includes a device template for discovering Microsoft devices.

The template will work as-is, unless you would like to remove a Dynamic Application from the template. To remove any Dynamic Applications you may not need:

- 1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
- 2. Locate the "Microsoft: Windows Server Discovery Template" and click its wrench icon (*P*). The **Device Template Editor** page appears.
- 3. Modify the **Template Name** field, as you will not want to overwrite the sample template.
- 4. Click the [Dyn Apps] tab. The Editing Dynamic Application Subtemplates page appears.
- 5. Click each Dynamic Application and replace the example credential with the credential created for the Windows server(s) being discovered.
- 6. To remove a Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page, click it's bomb icon () and then click **[OK]** when asked to confirm.
- 7. Click [Save As].

To discover the Windows Server devices that you want to monitor:

On the Devices page (I) or the Discovery Sessions page (Devices > Discovery Sessions), click the [Add Devices] button. The Select page appears:

Select the type of devices you want to monitor	;
C.J. Albaba Cloud Image: Microsoft Azure Citricity: Image: Microsoft Azure	Ceneral Information The workflow will allow you to discover and begin monitoring devices using core credentials such as SNMR Database, SOAPXML, Basic/Snipet. SNVRey, or Powershell credentials. Before you begin determine that you have these prerequisites in place: • A Origanization for the new device. If you need to create an Organization goto Reginy - Accounts - Organizations • A Collector Group that can reach the target device using a valid network bath for the need gorocol. The example, thin mame UDP 161 for SNNP and general ICMP traffic for Ping. If you don't know vhat Collector Group to use consult an SL Architecture degran or asky your SL System Administrator: • A Credentia for the device(a) being discovered. You can test any credential that you create as credential problems are the most common cause for discover y failure. Got to System - Manage - Credentials to create a credential. Use the Select button below to continue the Discovery workflow.

- 2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
- 3. Click [Select]. The Add Devices page appears.
- 4. Complete the following fields:
 - Name. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the [Discovery Sessions] tab.
 - **Description**. Optional. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the **[Discovery Sessions]** tab.
 - Select the organization to add discovered devices to. Select the name of the organization to which you want to add the discovered devices.
- 5. Click [Next]. The Credentials page of the Add Devices wizard appears.
- 6. On the **Credentials** page, click **[Next]**.
- 7. The Discovery Session Details page of the Add Devices wizard appears:

Step 1 Basic Information		Step 2 Credential Selection	3	Step 3 Discovery Session Details	×
	Ente	er basic discovery session details			
	List of IPs/Hostnames		File Upload		
	1 10.0.0.55				
	Which collector will discover these devices?				
	CUG em7aio17: 10.64.68.17		~	6	
	Run after save				
	•				
	Advanced Options 🗸				
				- Const	
< Back				Save A	nd Ruh

- 8. Complete the following fields:
 - List of IPs/Hostnames. Type the IP address or addresses for the Windows Server devices that you want to discover.
 - Which collector will monitor these devices?. Select an existing collector to monitor the discovered devices. Required.
 - *Run after save*. Select this option to run this discovery session as soon as you click [Save and Close].

In the Advanced options section, click the down arrow icon (\sim) to complete the following fields:

- Discover Non-SNMP.Enable this setting.
- Select Device Template. Select the device template that you configured.
- 9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
- 10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

To discover Windows Server devices in the SL1 classic user interface:

- 1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
- 2. In the Discovery Control Panel, click the [Create] button.
- 3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, complete the following fields:
 - Name. Type in a name for your discovery session.
 - IP Address/Hostname Discovery List. Type the IP address or addresses for the Windows Server devices that you want to discover.

- Discover Non-SNMP. Select this checkbox.
- Apply Device Template. Select the template you configured.
- 4. Click the [Save] button to save the discovery session, and then close the Discovery Session Editor window.
- 5. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning-bolt icon (\mathscr{I}) to run the discovery session.
- 6. The **Discovery Session** window appears. When the device(s) are discovered, click the device icon (\blacksquare) to view the **Device Properties** page for each device.

Discovering Component Devices on Hyper-V Systems

The *Microsoft: Hyper-V Server* PowerPack includes two Dynamic Applications that allow SL1 to collect information about the virtual machines running on a Hyper-V system.

To discover the virtual machines on a Hyper-V system as component devices, align the following two Dynamic Applications with a Hyper-V system:

- Microsoft: Hyper-V Guest Configuration Cache
- Microsoft: Hyper-V Gust Discovery

When these Dynamic Applications are aligned to a Hyper-V system, the platform will automatically create a device record for each virtual machine. The platform will also automatically align other Dynamic Applications from the *Microsoft: Hyper-V Server* PowerPack to each virtual machine.

Viewing Component Devices

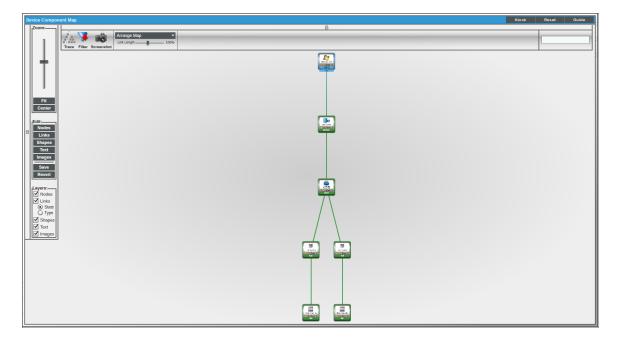
When SL1 performs collection for the "Microsoft Hyper-V Guest Configuration Cache" and "Microsoft Hyper-V Guest Discovery" Dynamic Applications, SL1 will create component devices for the virtual machines on the Hyper-V and align other Dynamic Applications to those component devices. All component devices appear in the **Device Manager** page just like devices discovered using the ScienceLogic discovery process.

In addition to the **Device Manager** page, you can view the Hyper-V system and all associated component devices in the following places in the user interface:

 The Device Components page (Devices > Device Components or Registry > Devices > Device Components in the SL1 classic user interface) displays a list of all root devices and component devices discovered by the platform. The Device Components page displays all root devices and component devices in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a Hyper-V system, find the Hyper-V system and select its plus icon (+):

Device Components Devices Found [2]									Actions Rese	Guid	e
Device Name •	IP Address	Device Category	Device Class Sub-class	DID		Organization	Current State	Collection Group	Collection State		
1. + P. mem7_ao	9 10.0.9.79	Infrastructure	.Content VirtualMachine	219	System		A Major C	CUG1	Active	📾 🏹 🚲	
 Part TL008-HQ-AP-01.msti008.MSTestLab.local 	9 10.40.1.15	Servers	Microsoft Windows Server 2008 R2	1031	System		ANotice C	CUG1	Active	📾 🎝 🚲	
Device Name *	IP Address	Device Category	Device Class Sub-class	DID		Organization	Current State	Collection Group	beta Collection		Ø
1. + Matacenter1		Infrastructure	.Content Datacenter	1032	System		A Healthy	CUG1	Unavailable	₩ ₩ <u>8</u>	
							-32			1.00.	

The Component Map page (Classic Maps > Device Maps > Components or Views > Device Maps > Components in the SL1 classic user interface) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the Component Map as new component devices are discovered. SL1 also updates each map with the latest status and event information. To view the map for a Hyper-V system, select the Hyper-V system from the left NavBar. To learn more about the Component Map page, see the Views manual.



Manually Aligning the Microsoft: Print Server Dynamic Application

The Microsoft: Print Server Dynamic Application must be manually aligned. To do so, perform the following steps:

- Find your Windows device in the **Device Manager** page (Registry > Devices > Device Manager and click its wrench icon (²).
- 2. From the **Device Properties** page for the Windows system, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
- 3. Click the **[Action]** button and then select Add Dynamic Application. The **Dynamic Application Alignment** page appears.
- 4. In the **Dynamic Applications** field, select the "Microsoft: Print Server" Dynamic Application.
- 5. In the **Credentials** field, select the credential you created for your Windows system.
- 6. Click the **[Save]** button.

Chapter



Using Microsoft PowerPacks

Overview

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

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

The following sections describe how to configure Microsoft servers or monitor Windows Services using specific PowerPacks:

This chapter covers the following topics:

Microsoft: DHCP Server PowerPack	115
Microsoft: Windows Server PowerPack	116

Microsoft: DHCP Server PowerPack

The following section describes how to monitor Windows DHCP services using the *Microsoft: DHCP Server* PowerPack.

Add User to DHCP Users Group

To monitor DHCP services, the monitoring user must be placed into the DHCP Users group in Active Directory. If that group does not already exist, run the following command as a Domain Administrator to create it:

netsh dhcp add securitygroups

Microsoft: Windows Server PowerPack

The following sections describe how to monitor Windows Services using the *Microsoft: Windows Server* PowerPack.

Prerequisites

To use the Microsoft: Windows Server PowerPack to monitor Windows services, you must first uninstall the deprecated Microsoft: Windows Server Services PowerPack if it is still installed on your SL1 system.

Monitoring Windows Services and Processes with PowerShell

Windows services can be monitored with internal collections and/or Dynamic Applications.

Monitoring services with **internal collection (IC)** processes integrate Windows services data into SL1, and Windows service monitoring policies can be created to alert on a selected service.

Monitoring services with a **Dynamic Application** will automatically alert when services set to Automatic without a triggered start aren't running. If a corresponding Run Book automation policy is enabled it will attempt to restart the service automatically.

Process monitoring is available using Internal Collection Dynamic Applications for processes.

Both types of service monitoring (IC and Dynamic Application) and process monitoring require the following:

- The "Microsoft: Windows Server IC Process Service Cache" Dynamic Application must be enabled and aligned to your device.
- In version 114 or later of the *Microsoft: Windows Server* PowerPack the "Microsoft: Windows Server IC Cache Trigger" Dynamic Application must be enabled and aligned to your device only if you are using concurrent PowerShell for collections. This Dynamic Application will keep the cache full to be read by cache consumers.
- Versions 112 and 113 of the Microsoft: Windows Server PowerPack require the :"Microsoft: Windows Server IC Cache Trigger" Dynamic Application to be enabled and aligned for both concurrent and legacy PowerShell collections.

Monitoring Windows Processes

To monitor Windows processes:

- The "Microsoft: Windows Server IC Process Inventory" Dynamic Application must be enabled and aligned to your device.
- The "Microsoft: Windows Server IC Process Performance" Dynamic Application must be enabled and aligned to your device.
- Once enabled, it can take up to two hours for the **[Processes]** tab to be enabled and display listed processes.

Monitoring Individual Windows Services via Internal Collections

To monitor individual services with internal collections:

- The "Microsoft: Windows Server IC Service Inventory" Dynamic Application must be enabled and aligned to the device.
- The "Microsoft: Windows Server IC Service Performance" Dynamic Application must be enabled and aligned to the device.

Monitoring Automatic Services with the Microsoft: Windows Server Service Configuration Dynamic Application

NOTE: You can monitor Windows services with the "Microsoft: Windows Server Service Configuration" Dynamic Application using both legacy and concurrent PowerShell collection.

You can monitor Windows services with the "Microsoft: Windows Server Service Configuration" Dynamic Application. This Dynamic Application requires that the "Microsoft: Windows Server IC Cache Trigger" Dynamic Application be enabled for concurrent PowerShell collection. Legacy PowerShell collection collects data without this Dynamic Application enabled. See the Concurrent PowerShell Collection section for more information.

The "Microsoft Windows Server Service Configuration" Dynamic Application will automatically create an event on any Windows device to which it is aligned when a Windows service set to "Automatic" is **not** in a running state and not excluded.

Restarting Automatic Windows Services Using the Run Book Automation Policy

If you want to restart Windows server services automatically when the service is not in a running state, you must enable the "Microsoft: Windows Server Start Automatic Service" Run Book automation policy as it is disabled by default. This will restart only services set to "Automatic". You must also align the "Microsoft: Windows Server Service Configuration" Dynamic Application to your device.

Excluding Automatic Services

The master.definitions_service_autostart_exclude database table specifies service with a type of "Automatic" that should not be monitored by the "Microsoft: Windows Server Service Configuration" Dynamic Application, either for a single device or all devices. The following services are defined as excluded for all devices by default:

- Distributed Transaction Coordinator
- Forefront Identity Manager Synchronization Service
- Google Update Service (gupdate)
- Microsoft .NET Framework NGEN v4.0.30319 X64
- Microsoft .NET Framework NGEN v4.0.30319_X86
- Performance Logs & Alerts
- Remote Registry
- Removable Storage
- Shell Hardware Detection

- Software Protection
- TPM Base Services
- Volume Shadow Copy
- Windows Service Pack Installer Update service
- Windows Modules Installer

Viewing the List of Excluded Services

You can view the list of excluded services by performing the following steps:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. In the **SQL Query** field, type the following query:

SELECT * FROM master.definitions_service_autostart_exclude;

- 3. Click [Go].
- 4. The output includes the following fields:
 - **service_name**. The name of the excluded service.
 - **did**. The ID for the device for which the service is excluded. If this value is 0, the exclusion applies to all devices.

Adding an Excluded Service for All Devices

You can exclude a service for all devices by performing the following steps:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. In the **SQL Query** field, type the following query, supplying the service name where indicated:

```
INSERT INTO master.definitions_service_autostart_exclude VALUES
("<service name>",0);
```

3. Click **[Go]**.

Adding an Excluded Service for a Single Device

You can exclude a service for a single device by performing the following steps:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. In the **SQL Query** field, type the following query:
 - Replace "X" with the device ID for which you want to exclude the service.
 - Supply the service name where indicated.

```
INSERT INTO master.definitions_service_autostart_exclude VALUES
("<service name>",X);
```

3. Click [Go].

Removing an Excluded Service

You can remove an entry from the list of exclusions by performing the following steps:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. In the **SQL Query** field, type the following query:
 - Replace "X" with the device ID associated with the entry that you want to delete.
 - Supply the service name where indicated.

```
DELETE FROM master.definitions_service_autostart_exclude WHERE
service name="<service name>" AND did=X;
```

3. Click [Go].

NOTE: For more information, see the **Restarting Automatic Windows Services Using the Run Book Automation Policy** section.

In version 115 of the PowerPack, functionality was added to allow the use of RegEx in the service name field to provide more functionality when selecting services to exclude. The RegEx will be applied to both the service name and the display name.

RegEx String	Excludes
.*Devices.*	Excludes any service with "Devices" in the service or display name.
^Clip	Excludes any service that has a service or display name staring with "Clip".
Service\$	Excludes any service that has a service or display name starting or ending with "Service".

Monitoring Windows Server Services with Monitoring Policies

You can also monitor your Windows services using monitoring policies. For information on how to create monitoring policies, see the *Monitoring Device Infrastructure Health* manual.

NOTE: You can monitor Windows services with monitoring policies using both legacy and concurrent PowerShell collection.

The **[Services]** tab for a device will display Yes in the **Monitored** column once a policy is created for a Windows service. The **[Performance]** tab will also display data for the monitored policies.

The following Dynamic Applications will need to be manually enabled to monitor Windows services using monitoring policies:

- Microsoft: Windows Server IC Cache Trigger. Needed for concurrent PowerShell collection.
- Microsoft: Windows Server IC Process Service Cache. Runs PowerShell requests and collects results.
- Microsoft: Windows Server IC Service Inventory. Cache Consumer.
- Microsoft: Windows Server IC Service Performance. Cache Consumer.

Granting Access To Services

In certain environments, you may not have access to read the service list or to certain services in the list. If you do not have access to the full list of services, an "Access Denied" error will appear in the logs when running the "Microsoft: Windows Server IC Process Service Cache" Dynamic Application in debug mode. If you do not have access to a particular service, that service will not appear in the list. This situation most commonly occurs on Microsoft SQL Servers where the service is run on a custom account.

In this situation it may be necessary to grant the user explicit access on the service manager and services themselves. There is no default UI for granting this access in a Windows Server. A PowerShell onboarding script is included in the *Microsoft: Windows Server* PowerPack that can be run with the <u>-services_only</u> argument, which will configure service monitoring. An example of that command is:

```
.\winrm_configuration_wizard_v3.3.ps1 -user <DOMAIN>\<USER> -silent -
services only
```

If a system was onboarded with the script using the default configuration, service monitoring will be automatically configured. If a service is added later, it may be necessary to re-run the script with the <u>-services_only</u> argument to enable permissions for the new service.

Chapter

7

Concurrent PowerShell Collection

Overview

This chapter describes how to configure and use concurrent PowerShell collection. Concurrent PowerShell collection allows multiple collection tasks to run at the same time with a reduced load on Data Collectors.

Concurrent PowerShell collection also prevents missed polls and data gaps because collection will execute more quickly. As a result, Data Collectors can collect more data using fewer system resources. The PowerShell Collector is an independent service running as a container on a Data Collector.

CAUTION: Do not use concurrent PowerShell collection if you are not using shared credentials, like Active Directory, on multiple servers. For example, concurrent PowerShell collection is not recommended for secure environments with unique credentials for each server, because concurrent PowerShell collection will use up a large amount of memory for processing the collections.

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

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

This chapter covers the following topics:

Prerequisites	
Scope	122
Enabling and Disabling Concurrent PowerShell for Collector Groups	123
The SL1: Concurrent PowerShell Monitoring PowerPack	124
Configuring the SL1: Concurrent PowerShell Monitoring PowerPack for Military Unique	124

Deployment (MUD) Environments	•••
Aligning the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application	125
Aligning the "ScienceLogic: PowerShell Collector Performance" Dynamic Application	. 128
Enabling HTTPS Between SL1 and the PowerShell Data Collector	129
Enabling and Disabling the Python PowerShell Remoting Protocol Client	. 130
Optional PowerShell CLI Parameters	130
Users with Windows 2008 R2 Servers or Windows 2012 Servers	. 131
Scale Recommendations	. 132

Prerequisites

The following prerequisites are required to use concurrent PowerShell collection:

- SL1 version 10.1.4 or greater
- "Microsoft: Windows Server" PowerPack version 110 or greater
- "SL1: Concurrent PowerShell Monitoring" PowerPack version 100 or greater (for SL1 versions prior to 11.3.0).

NOTE: As of SL1 version 11.3.0, the "SL1: Concurrent PowerShell Monitoring" PowerPack is no longer a requirement for concurrent PowerShell monitoring.

Scope

When the concurrent PowerShell collection service is enabled, PowerShell Configuration and PowerShell Performance Dynamic Applications are sent to the service.

The following PowerPacks can use the concurrent PowerShell collection service:

- Microsoft: Active Directory Server
- Microsoft: DHCP Server
- Microsoft: DNS Server
- Microsoft: Exchange Server
- Microsoft: IIS Server
- Microsoft: Lync Server 2013
- Microsoft: SharePoint Server
- Microsoft: SQL Server
- Microsoft: Hyper-V Server (partially)
- Microsoft: Windows Server (partially)

Enabling and Disabling Concurrent PowerShell for Collector Groups

To improve the process of collecting data via PowerShell and to collect metrics, you can enable concurrent PowerShell collection. You can enable one or more collector groups to use concurrent PowerShell collection.

- **CAUTION:** If you have enabled concurrent collection and you have used it to discover a very large number of devices or interfaces, disabling concurrent collection could have unintended consequences. After disabling concurrent collection, your Data Collector might become overburdened when it attempts to collect data for the same number of devices or interfaces but without the added processing capacity of concurrent collection.
- CAUTION: By default, a loopback to 127.0.0.1 is configured on the collector with the line localhost localhost.localdomain localhost4 localhost4.localdomain4 in the /etc/hosts file. If this line is removed, concurrent PowerShell collection will not function properly.

NOTE: Concurrent PowerShell collection is for PowerShell Performance and Performance Configuration Dynamic Application types and does not include Snippet Dynamic Applications that happen to run PowerShell commands.

Enabling and Disabling Concurrent PowerShell on All Collector Groups

To enable and disable concurrent PowerShell collection for all collector groups:

- 1. Go to the **Behavior Settings** page (System > Settings > Behavior).
- 2. Select the Enable Concurrent PowerShell Collection checkbox and click [Save].
- 3. To disable concurrent PowerShell collection, deselect the *Enable Concurrent PowerShell Collection* checkbox and click [Save].

Enabling and Disabling Concurrent PowerShell on a Specific Collector Group

To enable and disable concurrent PowerShell collection for a specific collector group:

- 1. Go to the Collector Group Management page (System > Settings > Collector Groups).
- Locate the collector group for which you want to enable concurrent PowerShell, and click its wrench icon (
 (*).
- 3. In the Enable Concurrent PowerShell Collection dropdown menu, select Yes and click [Save].

4. To disable concurrent PowerShell collection, select No in the **Enable Concurrent PowerShell Collection** dropdown and click **[Save]**.

The SL1: Concurrent PowerShell Monitoring PowerPack

The "SL1: Concurrent PowerShell Monitoring" PowerPack includes a device template, two Dynamic Applications that use SSH to monitor collectors with concurrent PowerShell enabled, and a number of event policies.

- The "ScienceLogic: PowerShell Collector Performance" Dynamic Application is an optional Dynamic Application used for troubleshooting.
- The "ScienceLogic: PowerShell Service Log Parser" Dynamic Application parses the log file from the PowerShell servers and converts errors into events aligned to the related device.
- The "SL1: Concurrent PowerShell Monitoring" device template can be used to align multiple Data Collectors to the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application.
- Event policies and corresponding alerts that are triggered when devices meet certain status criteria.

Configuring the SL1: Concurrent PowerShell Monitoring PowerPack for Military Unique Deployment (MUD) Environments

To use the "SL1: Concurrent PowerShell Monitoring" PowerPack on Military Unique Deployment (MUD) environments, you must create a new user on each MUD collector. After you have created a new user on each MUD collector, you must edit the sudo config file and the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application.

Configuring the Sudo Config File

CAUTION: ScienceLogic recommends that you use the command sudo visudo. This command verifies changes to the sudoers file before you save it.

After you create a new user on each MUD collector, you must add the following permission to the sudo config file (/etc/sudoers) to allow the new user to use sudo without a password:

User Alias SL1PARSER = "sl1monitor"

```
Cmnd_Alias PARSER = /opt/em7/bin/silo_mysql, /usr/bin/grep, /usr/bin/tail,
/usr/bin/awk
```

SL1PARSER ALL = NOPASSWD: PARSER

Configuring the ScienceLogic: PowerShell Service Log Parser Dynamic Application

To edit the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application snippet for a MUD environment:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Find the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application and click its wrench icon (🥍).
- 3. In the **Dynamic Applications Properties Editor**, click the **[Snippets]** tab.
- 4. In the **Dynamic Applications Snippet Editor & Registry** page, click the wrench icon (*P*) of the "ScienceLogic: PowerShell Service Log Parser" snippet.
- 5. The content of the snippet will appear. Edit the "False" value in the following snippet text to "True":

```
mud system = False
```

NOTE: The only valid values for "mud_system" are "True" or "False". "True" or "False" must be capitalized, as using all lowercase or uppercase letters will result in a snippet exception.

6. Click [Save].

Aligning the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application

To align the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application, first you must create an SSH/Key credential:

- 1. Go to the Credential Management page (System > Manage > Credentials).
- 2. In the Credential Management page, click the [Actions] menu. Select Create SSH/Key Credential.
- 3. The **Credential Editor** modal page appears. In this page, define the new SSH/Key credential using a valid username and password or SSH key for SL1 collectors:
 - Credential 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 current device (device that is currently using the credential).
 - You can include the variable %N in this field. SL1 will replace the variable with hostname of the current device (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.
 - **Port**. Port number associated with the data you want to retrieve.

NOTE: The default TCP port for SSH servers is 22.

- *Timeout (ms)*. Time, in milliseconds, after which SL1 will stop trying to communicate with the authenticating server.
- Username. Username for the Data Collector to be monitored.
- Password. Password for the Data Collector to be monitored.
- Private Key (PEM Format). Enter an SSH private key for the SL1 Data Collector, in PEM format.
- 4. Click the [Save] button to save the new SSH/Key credential.

Next, you can align the Dynamic Application manually or configure the device template. Using the device template is recommended when you want to align the Dynamic Application to multiple Data Collectors.

Manually Aligning the Dynamic Application

After creating the SSH/Key credential, you will manually align the Dynamic Application.

- 1. Go to the **Devices** page and find the device you want to manually align the Dynamic Application to. Click on it to go to the **Device Investigator**.
- 2. In the **Device Investigator**, click the **[Collections]** tab. Click **[Edit]** and then click **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
- 3. Click Choose Dynamic Application. The Choose Dynamic Application window appears.
- Select the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application and click [Select]. The "ScienceLogic: PowerShell Service Log Parser" Dynamic Application appears in the Align Dynamic Application window.
- 5. If a default credential is listed below the Dynamic Application and you want to use that credential, skip ahead to step 8. Otherwise, uncheck the box next to the credential name.
- 6. Click Choose Credential. The Choose Credential window appears.
- 7. Select the credential for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
- 8. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

To manually align the Dynamic Application using the SL1 classic user interface:

- 1. Go to the **Device Manager** page (Devices > Device Manager)
- 2. In the **Device Manager** page, find the device for which you want to view Dynamic Applications. Select its wrench icon (*P*)
- 3. In the Device Administration panel, select the [Collections] tab.
- 4. Click the **[Actions]** button and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears
- 5. In the **Dynamic Applications** field, select the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application.
- 6. In the *Credentials* field, select the proper credential.
- 7. Click the **[Save]** button.

Configuring the Device Template

After creating the SSH/Key credential, you will need to configure the device template included in the PowerPack.

NOTE: If you have already manually aligned the Dynamic Application, you do not need to perform the steps in this section.

To configure the device template:

- 1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
- Locate the "SL1: Concurrent PowerShell Monitoring" sample template and click its wrench icon (*P*). The Device Template Editor modal page appears.
- 3. Type a new name for the device template in the **Template Name** field so the sample template is not overwritten.
- 4. Click the [Dyn Apps] tab. The Editing Dynamic Application Subtemplates page appears.
- 5. In the **Subtemplate Selection** pane, select the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application.
- 6. In the Credentials drop-down list, select the SSH/Key credential that you created.
- 7. Click [Save As].

Applying the Device Template

If your Data Collector devices already exist on your SL1 system, perform the following steps to apply the device template:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager) and select the checkbox for each of your Data Collector devices.
- 2. In the Select Action menu, select MODIFY By Template and then click [Go].
- 3. In the Device Template Editor, select the template you created in the Template field.
- 4. Click [Apply].

If your devices have not yet been discovered, perform the following steps to discover the devices and apply the device template:

- 1. Go to the Discovery Control Panel page (System > Manage > Classic Discovery) and click [Create].
- 2. Supply values in the following fields:
 - Name. Type a name for the discovery session.
 - **Description**. Optionally, type a description of the discovery session.
 - IP Address/Hostname Discovery List. Provide a list of IP addresses for your Data Collectors.
 - SNMP Credentials. Select EM7 Default V2.
 - Model Devices. Select this checkbox.
 - Apply Device Template. Select the device template that you created.

- Log All. Select this checkbox.
- 3. Click the [Save] button to save the discovery session. Close the Discovery Session Editor page.
- 4. In the **Discovery Control Panel** page, click the **[Reset]** button. The new discovery session will appear in the **Session Register** pane.
- 5. To launch the new discovery session, click its Queue this Session icon (🖉).
- 6. If no other discovery sessions are currently running, the session will be executed immediately. If another discovery session is currently running, your discovery session will be queued for execution.

Aligning the "ScienceLogic: PowerShell Collector Performance" Dynamic Application

If you want to monitor your Data Collectors with the "ScienceLogic: PowerShell Collector Performance" Dynamic Application, you must manually align it to your Data Collectors using the SSH/Key credential. To do this:

- 1. Go to the **Devices** page and find the device you want to manually align the Dynamic Application to and click on it to go to the Device Investigator.
- 2. In the Device Investigator, click the **[Collections]** tab. Click **[Edit]** and then click **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
- 3. Click Choose Dynamic Application. The Choose Dynamic Application window appears.
- Select the "ScienceLogic: PowerShell Collector Performance" Dynamic Application and click [Select]. The "ScienceLogic: PowerShell Collector Performance" Dynamic Application appears in the Align Dynamic Application window.
- 5. If a default credential is listed below the Dynamic Application and you want to use that credential, skip ahead to step 8. Otherwise, uncheck the box next to the credential name.
- 6. Click Choose Credential. The Choose Credential window appears.
- 7. Select the credential for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
- 8. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **Collections** tab, and a confirmation message appears at the bottom of the tab.

To manually align the Dynamic Application using the SL1 classic user interface:

- 1. Go to the **Device Manager** page (Devices > Device Manager)
- 2. In the **Device Manager** page, find the device for which you want to view Dynamic Applications. Select its wrench icon (*P*)
- 3. In the Device Administration panel, select the [Collections] tab.
- 4. Click the **[Actions]** button and then select Add Dynamic Application. The **Dynamic Application Alignment** page appears
- 5. In the **Dynamic Applications** field, select the "ScienceLogic: PowerShell Collector Performance" Dynamic Application.

- 6. In the **Credentials** field, select the proper credential.
- 7. Click the **[Save]** button.

Enabling HTTPS Between SL1 and the PowerShell Data Collector

You can enable or disable HTTPS as the mode of transport for communication between SL1 and the PowerShell Data Collector. The PowerShell Data Collector is a service that runs on the Collector Group. The Data Collection service on the Collector Group can optionally communicate with the PowerShell Service to queue jobs and check for results using HTTPS. You would enable HTTPS if you must meet federal requirements to encrypt all network traffic, even if it never leaves the host.

To enable or disable HTTPS as the mode of transport for communication between SL1 and the PowerShell Data Collector, you must make some changes to the /opt/em7/services/powershell_ collector/powershell_collector.env configuration file. This file can also be used to configure the certificates used by the container when running on HTTPS.

Кеу	Value
USE_HTTPS	Default value is True .
	If set to False , HTTPS is disabled and the remaining SSL-related keys have no effect.
SSL_PRIVATE_KEY	These keys are used to specify the full path and filename of the certificate to be
SSL_SERVER_CERT	used by the PowerShell Data Collector when HTTPS is enabled. If these keys are not set, a self-signed certificate will be generated when the container is started.
SSL_CA_CERT	When specifying the file name and path, they must be accessible to the PowerShell Data Collector. For example, the directory /etc/ssl/certs is mapped to the PowerShell Data Collector, meaning any files within this directory are accessible to the PowerShell Data Collector, subject to the files' permissions. Any certificates placed in the directory on the PowerShell Data Collector must have the keys set as follows:
	SSL_PRIVATE_KEY=/etc/ssl/certs/my_cert.key Once the key is set, the Data Collector will pick up the files in the directory on startup.
	NOTE: USE_HTTPS must be set to <i>True</i> for these keys to work.
SSL_VERIFY	When USE_HTTPS is set to <i>True</i> , this key is used by SL1 when communicating with the PowerShell Data Collector.
	By default, the value is False .
	If set to True , the HTTPS connection will fail if the Data Collector is using a self- signed certificate.

The keys used are:

Enabling and Disabling the Python PowerShell Remoting Protocol Client

If you have concurrent PowerShell enabled in SL1, the default Python module used for transport to monitor Windows Devices is "pyWinRm". However, the "pypsrp" Python module can provide more efficient processing of PowerShell commands, particularly when virus detection software is enabled. To use the "pypsrp" module instead, run the following SQL query on the **Database Tool** page (System > Tools > DB Tool):

- 1. Select your database from the Select Database list.
- 2. Enter the following in the SQL Query field.

```
INSERT master.system_custom_config (field, field_value) VALUES ('enable_
pypsrp lib', 1)
```

A value of 1 will enable the "pypsrp" module. A value of 0 (or not having any setting for 'enable_pypsrp_lib') will revert to using "pyWinRM".

3. Click [Go].

To disable "pypsrp", use the following SQL query:

```
UPDATE master.system_custom_config set field_value = 0 WHERE field =
'enable_pypsrp_lib'
```

NOTE: Currently, you can only use the "pypsrp" module with concurrent PowerShell. Classic PowerShell monitoring will continue to use the "pyWinRM" module regardless of this database setting.

Optional PowerShell CLI Parameters

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

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

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

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

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

where:

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

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

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

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

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

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

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

Users with Windows 2008 R2 Servers or Windows 2012 Servers

Concurrent PowerShell collection will not work for Windows 2008 R2 servers or Windows 2012 servers when the *Encyrpted* field is set to Yes in the PowerShell credential. Windows 2008 R2 servers and Windows 2012 servers are no longer covered by Microsoft's Extended Support, but if you are still using those servers you have the following options:

- Use PowerShell credentials that have *Encryption* set to No.
- Disable the Concurrent PowerShell service on the Data Collector groups that include Windows 2008 R2 servers or Windows 2012 servers. This will reduce the number of servers that Data Collector group can support.
- Use the Microsoft Base Pack (WMI-based) PowerPack for the Windows 2008 R2 servers or the Windows

2012 servers.

• Use SNMP for the Windows 2008 R2 servers or the Windows 2012 servers.

Scale Recommendations

The following recommendations increase the number of Windows Servers the concurrent PowerShell collector can support:

- In the Device Properties page for all Windows Server devices (Registry > Devices > wrench icon), unselect the Dynamic Discovery checkbox. Alternatively, this can be set in bulk using a device template and device group. This prevents nightly discovery from attempting to align Dynamic Applications with a discovery object to all the devices on the collector, which does not use the concurrent PowerShell collector and will dramatically limit the number of Windows Server devices that can be monitored.
- Do not select any credentials in the discovery session used to discover new Windows Servers. Instead, use a template that includes unselecting the **Dynamic Discovery** checkbox and includes the desired Dynamic Applications with the appropriate credential aligned. When a credential is selected in the Discovery Session, it will attempt to align Dynamic Applications that include a discovery object, which does not use the concurrent PowerShell collector and will dramatically limit the number of Windows Server devices that can be monitored. The *Microsoft: Windows Server* PowerPack includes the "Microsoft: Windows Server Discovery Template" that you can use be used to create your template.

For information on creating and using device templates, see the **Device Groups and Device Templates** manual.

Additional Scale Tips

- The "Microsoft: Windows Server Services" PowerPack has been deprecated. To monitor services, use version 113 or later of the "Microsoft: Windows Server" PowerPack.
- Limit the use of the "Microsoft: Windows Server Event Logs" PowerPack as it does not work with the concurrent PowerShell collector.
- Use the "Microsoft: SQL Server" PowerPack instead of the "Microsoft: SQL Server Enhanced" PowerPack. The "Microsoft: SQL Server Enhanced" PowerPack does not work with the concurrent PowerShell collector.
- Disable Dynamic Applications that are not providing information required to meet your Service Level Agreements. There is an enhancement in caching included with concurrent PowerShell collection that will not send a PowerShell request from a cache-producing Dynamic Application unless at least one Dynamic Application is asking for that data. Disabling a cache-consuming Dynamic Application will also disable the cache producer from collecting that data. For example, the following Dynamic Applications are now disabled by default, as they are more diagnostic in nature and may not be required for routine monitoring:
 - Microsoft: Windows Server IPStats Performance
 - Microsoft: Windows Server TCPStats Performance
 - Microsoft: Windows Server UDPStats Performance
- Slow down the **Poll Frequency** for Dynamic Applications that do not include events. For example, the "Microsoft: Windows Server" PowerPack's Configuration Dynamic Applications used to be set to run every two hours and are now set to run every 12 hours.

Chapter



Executing the SL1 Agent with Windows PowerShell

Overview

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

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

NOTE: Monitoring with the SL1 Agent is available only on SL1 Extended.

The following sections provide an overview of local Agent execution on Windows devices with PowerShell:

This chapter covers the following topics:

What is an SL1 Agent?	. 133
Agent-Compatible PowerPacks	134
The Credential for the SL1 Agent	. 134
Configuring the SL1 Agent Device Templates	. 135

What is an SL1 Agent?

The **SL1 agent** is a program that you can install on a device monitored by SL1. There is a Windows agent, an AIX agent, a Solaris agent, and a Linux agent. The agent collects data from the device and pushes that data back to SL1.

Similar to a Data Collector or Message Collector, the agent collects data about infrastructure and applications.

You can configure an agent to communicate with either the Message Collector or the Compute Cluster.

NOTE: The following minimum agent versions are required for SL1 12.1.1: **Windows** version 131; **Linux** version 174; **AIX** version 180; and **Solaris** version 180.

For more information, see the Monitoring with the SL1 Agent manual .

Agent-Compatible PowerPacks

The following PowerPacks include the SL1 Agent PowerShell Default credential and SL1 Agent device template, which you can use to execute the SL1 Agent on Windows devices with PowerShell:

- Microsoft: Windows Server
- SL1 Agent Templates for Microsoft PowerPacks, which includes templates for the following:
 - Microsoft: DHCP Server
 - Microsoft: DNS Server
 - Microsoft: Exchange Server

NOTE: The Microsoft: Exchange Server PowerPack has two device templates. If the Exchange server monitored contains all Exchange roles, use the "SL1 Agent for Microsoft: Exchange Server Template." If your Exchange server has an Exchange Transport role, use the "SL1 Agent for Microsoft: Exchange Transport Server Template."

- Microsoft: IIS Server
- Microsoft: Lync Server
- Microsoft: SharePoint Server
- Microsoft: SQL Server
- Microsoft: Windows Server

The Credential for the SL1 Agent

The "SL1 Agent PowerShell Default" credential does not need to be configured and can be used as-is. You can find the credential in the **Credentials** page (Manage > Credentials):

Name* SL1 Agent PowerShell Default			Credential Tester
All Organizations What organization manages this service?	~	Timeout (ms) 10000	Select Credential Test
			Select Collector
Account Type Local			CUG em7aio17: 10.64.68.17
Hostname/IP*			IP or Hostname to test*
%D Username*			- Test 0
default Password*			-
Encrypted			- > }
Port* 5985			64
PowerShell Proxy Hostname/IP			
Active Directory Host/IP			
Active Directory Domain			
		Save & Test	

You can also find the credential on the **Credential Management** page (System > Manage > Credentials) in the SL1 classic user interface.

Configuring the SL1 Agent Device Templates

A *device template* allows you to save a device configuration and apply it to multiple devices. Windows PowerPacks include a device template for executing the SL1 Agent with PowerShell. If you apply this device template during discovery, SL1 aligns the appropriate Dynamic Applications to the discovered PowerShell device.

This device template does not need to be edited and will work as-is, unless you would like to remove a Dynamic Application from the template. To remove any Dynamic Applications you may not need:

- 1. Go to the **Configuration Templates** page (Devices > Templates, or Registry > Devices > Templates in the SL1 classic user interface).
- 2. Locate the SL1 Agent template (for example, "SL1 Agent for Microsoft: Windows Server Template") and click its wrench icon (
- 3. Click the [Dyn Apps] tab. The Editing Dynamic Application Subtemplates page appears.
- 4. Modify the Template Name field, as you will not want to overwrite the sample template.
- 5. To remove a Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page, click its bomb icon (), and then click **[OK]** when asked to confirm.
- 6. Click [Save As].

NOTE: Any time a cache-producing Dynamic Application aligned to the SL1 agent runs, all cacheconsuming Dynamic Applications will run as well. The cache-consuming Dynamic Application with the shortest **Polling Frequency** will control when all the other cache-consuming Dynamic Applications for the same cache producer will run.

Chapter

9

Windows Dashboards

Overview

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

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

The following sections describe how to install the dashboards included in SL1 for Microsoft servers and a description of each:

This chapter covers the following topics:

Installing the Microsoft Server Dashboards	137
Microsoft: Active Directory Server Performance	137
Microsoft: DNS Server Performance	139
Microsoft: Exchange Server 2010 Performance	141
Microsoft: Exchange Server 2013 Performance	143
Microsoft: IIS Server Performance	146
Microsoft: Lync Server 2010 Dashboards	148
Microsoft: Skype for Business Dashboards	153
Microsoft: SQL Server Performance	158

Installing the Microsoft Server Dashboards

The following PowerPacks contain dashboards for Microsoft servers:

- Microsoft: Active Directory Server Dashboards
- Microsoft: DNS Server Dashboards
- Microsoft: Exchange Server 2010 Dashboards
- Microsoft: Exchange Server 2013 Dashboards
- Microsoft: IIS Server Dashboards
- Microsoft: Lync Server 2010 Dashboards
- Microsoft: Skype for Business Dashboards
- Microsoft: SQL Server Dashboards

To view these dashboards in SL1, you must first install the corresponding PowerPack. To do so:

- 1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
- 2. Click the [Actions] button, then select Install PowerPack. The Imported PowerPacks modal page appears.
- Use the search filter in the *PowerPack Name* column heading to locate the PowerPack you want to install. To do so, enter text to match, including special characters, and the *Imported PowerPacks* modal page displays only PowerPacks that have a matching name.
- 4. Click the lightning-bolt icon (\swarrow) for the PowerPack that you want to install.
- 5. The Install PowerPack modal page appears. To install the PowerPack, click [Install].
- 6. The PowerPack now appears in the **PowerPack Manager** page. The contents of the PowerPack are automatically installed in your SL1 System.

Microsoft: Active Directory Server Performance

The Microsoft: Active Directory Server Performance dashboard provides an overview of the health and performance of a selected Active Directory server.

Context Quick Selector. This widget contains buttons for time span preset and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Active Directory servers that appear in the **Server List** widget.

Server List. This widget displays a list of Active Directory servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Active Directory server, in percent.
- The latency of the selected Active Directory server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Active Directory server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector**widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

Replication. Replication is the process by which the changes that are made on one domain controller are synchronized with and written to all other domain controllers in the domain or forest. The Replication widget displays a line graph. The line graph displays information about data that is replicated from the current Active Directory server to other Active Directory servers (the Outbound Properties Per Second) and information about data that is replicated from other Active Directory server to the current Active Directory server (Inbound Objects Per Second).

- The y axis displays objects per second.
- The x axis displays time. The increments vary, depending upon the date ranges selected in the **Context Quick Selector**widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

LDAP - Client Sessions. This widget displays the number of connected LDAP client sessions over time.

- The y axis displays number of sessions .
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

LDAP - Active Threads. This widget displays the number of threads in use by the LDAP subsystem of the local directory service.

- The y axis displays number of threads.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.

• Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

Pages Per Second. This widget displays a line graph. The line graph displays DS (domain server) directory reads per second, DS directory writes per second, and DS directory searches per second. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

LDAP - Writes and Searches. This widget displays a line graph. The line graph displays LDAP writes per second and LDAP searches per second. Each parameter is represented by a color-coded line.

- The y axis displays writers per second and searches per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

LDAP - Bind Time. This widget displays a line graph. The line graph displays the time required for completion of each successful LDAP binding.

- The y axis displays duration in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Active Directory server.

Microsoft: DNS Server Performance

The Microsoft: DNS Server Performance dashboard provides an overview of the health and performance of a selected DNS server.

Context Quick Selector. This widget contains buttons for time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of DNS servers that appear in the **Server List** widget.

Server List. This widget displays a list of DNS servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected DNS server, in percent.
- The latency of the selected DNS server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected DNS server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected DNS server.

Overall Performance. This widget displays a line graph. The line graph displays Total Responses Sent per Second and Total Queries Received per Second. Each parameter is represented by a color-coded line.

- The y axis displays responses per second and queries per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected DNS server.

Recursive Queries. This widget displays a line graph. The line graph displays Recursive Queries per Second.

- The y axis displays number of queries per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected DNS server.

Recursive Errors. This widget displays a line graph. The line graph displays Recursive Query Failures per Second and Recursive Time-Outs per Second. Each parameter is represented by a color-coded line..

- The y axis displays number of queries per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.

• Clicking on a data point displays the Device Performance graph for the selected parameter on the selected DNS server.

Microsoft: Exchange Server 2010 Performance

The Microsoft: Exchange Server 2010 Performance dashboard provides an overview of the health and performance of a selected Exchange 2010 server.

Context Quick Selector. This widget contains buttons for time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Exchange 2010 servers that appear in the **Server List** widget.

Server List. This widget displays a list of Exchange 2010 servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Exchange 2010 server, in percent.
- The latency of the selected Exchange 2010 server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, swap memory usage, and CPU usage for the selected Exchange 2010 server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

User Active Connections. This widget displays a line graph. The line graph displays the number of active user connections for the selected Exchange 2010 server during the selected duration.

- The y axis displays the number of users.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in the line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

OWA Requests. This widget displays a line graph. The line graph displays two lines: One for the frequency of Outlook Web Access requests for the selected Exchange 2010 server during the selected duration and another for the frequency of Web Services requests for the selected Exchange 2010 server during the selected duration.

- The y axis displays the number of requests per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

RPC Averaged Latency. This widget displays a line graph. The line graph displays the average latency of remote procedure calls (RPCs) for the selected Exchange 2010 server during the selected duration.

- The y axis displays the average RPC latency, in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

MBS Databases. This widget displays a line graph. The line graph displays two lines: One for I/O write latency for the mailbox server database for the selected Exchange 2010 and one for I/O read latency to the mailbox server for the selected Exchange 2010 server during the selected duration.

- The y axis displays the write and read latency statistics in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

Mailbox Messages. This widget displays a line graph. The line graph displays two lines: One for the number of mailbox messages sent to the selected Exchange 2010 server and one for the number of mailbox message sent from the selected Exchange 2010 server during the selected duration.

- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

Total Queue Messages. This widget displays a line graph. The line graph includes three lines: One for the number of messages in the submission queue, one for the number of messages in the delivery queue, and one for the number of queued message that were delivered for the selected Exchange 2010 server during the selected duration.

- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

SMTP Messages. This widget displays a line graph. The line graphs includes two lines: One for the number of SMTP messages sent from the selected Exchange 2010 server and one for the number of SMTP messages received by the selected Exchange 2010 server during the selected duration.

- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

Buckets Allocated. This widget displays a line graph. The line graph displays the number of buckets of version store memory used by the selected Exchange 2010 server during the selected duration.

- The y axis displays the number of allocated buckets.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

Microsoft: Exchange Server 2013 Performance

The Microsoft: Exchange Server 2013 Performance dashboard provides an overview of the health and performance of a selected Exchange 2013 server.

Context Quick Selector. This widget contains buttons for time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Exchange 2013 servers that appear in the **Server List**widget.

Server List. This widget displays a list of Exchange 2013 servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Exchange 2013 server, in percent.
- The latency of the selected Exchange 2013 server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays three lines: One for memory usage, one for swap memory usage, and one for CPU usage for the selected Exchange 2013 server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

User Active Connections. This widget displays a line graph. The line graph displays the number of active user connections for the selected Exchange 2013 server during the selected duration.

- The y axis displays the number of users.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in the line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

OWA Requests. This widget displays a line graph. The line graph displays two lines: One for the frequency of Outlook Web Access requests and one for the frequency of Web Services requests for the selected Exchange 2013 server during the selected duration.

- The y axis displays the number of requests per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

RPC Averaged Latency. This widget displays a line graph. The line graph displays the average latency for remote procedure calls (RPCs) for the selected Exchange 2013 server during the selected duration.

- The y axis displays the average RPC latency, in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.

• Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

MBS Databases. This widget displays a line graph. The line graph displays two lines: One for I/O write latency to the mailbox server database and one for I/O read latency to the mailbox server database for the selected Exchange 2013 server during the selected duration.

- The y axis displays the average write and read latency in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

Mailbox Messages. This widget displays a line graph. The line graph displays two lines: One for the number of mailbox messages sent from the selected Exchange 2013 and one for the number of mailbox messages delivered to the selected Exchange 2013 server during the selected duration.

- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

Total Queue Messages. This widget displays a line graph. The line graph displays three lines: One for the the number of messages in the submission queue, one for the number of messages in the delivery queue, and one for the number of queued message that were delivered for the selected Exchange 2013 server during the selected duration.

- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

SMTP Messages. This widget displays a line graph. The line graph displays two lines: One for the number of SMTP messages sent from the selected Exchange 2013 server and one for the number of SMTP messages received by the selected Exchange 2013 server during the selected duration.

- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.

• Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

Buckets Allocated. This widget displays a line graph. The line graph displays the number of buckets of version store memory used by the selected Exchange 2013 server during the selected duration.

- The y axis displays the number of allocated buckets.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2013 server.

Microsoft: IIS Server Performance

The Microsoft: IIS Server Performance dashboard provides an overview of the health and performance of a selected IIS server.

Context Quick Selector. This widget contains buttons for time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of IIS servers that appear in the **Server List** widget.

Server List. This widget displays a list of IIS servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected IIS server, in percent.
- The latency of the selected IIS server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected IIS server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

Current Users. This widget displays a line graph. The line graph displays Current Anonymous Users and Current Non Anonymous Users. Each parameter is represented by a color-coded line.

• The y axis displays number of users.

- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

Bytes Sent and Received. This widget displays a line graph. The line graph displays Bytes Sent Per Second and Bytes Received Per Second. Each parameter is represented by a color-coded line.

- The y axis displays kB of data per second..
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

Connections. This widget displays a line graph. The line graph displays the number of Active HTTP Connections.

- The y axis displays number of connections.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

Pages Per Second. This widget displays a line graph. The line graph displays the number of Pages (served) Per Second.

- The y axis displays number of pages per second..
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

Cache Hit %. The IIS server caches (in memory) frequently requested files. This widget displays a line graph. The line graph displays the ratio of kernel URI cache hits to total cache requests.

- The y axis displays percent of URI cache hits.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

404 *Errors Per Second*. This widget displays a line graph. The line graph displays the number of errors due to requests that couldn't be satisfied by the server because the requested document couldn't be found, per second.

- The y axis displays number of errors per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

Microsoft: Lync Server 2010 Dashboards

The Microsoft: Lync Server 2010 Dashboards PowerPack includes the following dashboards:

- Microsoft: Lync Server 2010 Performance
- Microsoft: Lync Server 2010 Utilization

Microsoft: Lync Server 2010 Performance

The Microsoft: Lync 2010 Server Performance dashboard provides an overview of the health and performance of a selected Lync 2010 server.

Context Quick Selector. This widget contains buttons for time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Lync 2010 servers that appear in the **Server List** widget.

Server List. This widget displays a list of Lync 2010 servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Lync 2010 server, in percent.
- The latency of the selected Lync 2010 server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Lync 2010 server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Connections Established. This widget displays a line graph. The line graph displays Connections Established.

- The y axis displays number of connections.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

SIP Message. SIP is a protocol for instant messaging and VOIP. This widget displays a line graph. The line graph displays Incoming Message and Outgoing Messages. Each parameter is represented by a color-coded line.

- The y axis displays number of messages.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Sproc Latency. Stored Procedure Call (sproc) latency is the time it takes for the Lync database to process the stored procedure call.

- The y axis displays the duration, in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

SIP Network Errors. This widget displays information about errors during instant messaging or VOIP. This widget displays a line graph. The line graph displays Connections Above Per-User Limit Dropped, Connections Refused Due to Server Overload, Failed DNS SRV Queries, Time Out DNS SRV Queries, and TLS Negotiations Failed. Each parameter is represented by a color-coded line.

- The y axis displays the number of connections that resulted in errors.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 2xx Responses. A 2xx Response means that a connection has been established.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 1xx (non-100) Responses, Incoming 3xx Responses, Incoming Other 4xx Responses, Incoming Other 5xx Responses, and Incoming 6xx Responses. Each parameter is represented by a color-coded line. For a description of SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List_of_SIP response codes.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 400 Responses, Incoming 401 Responses, Incoming Other 403 Responses, Incoming 404 Responses, Incoming 407 Responses, and Incoming 408 Responses. Each parameter is represented by a color-coded line. For a description of SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List of SIP response codes.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 482 Responses and Incoming 483 Responses. Each parameter is represented by a color-coded line. For a description of SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List of SIP response codes.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Microsoft: Lync Server 2010 Utilization

The Microsoft: Lync 2010 Server Utilization dashboard provides an overview of how users are using a selected Lync 2010 server.

Context Quick Selector. This widget contains the time span preset buttons and Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Lync 2010 servers that appear in the **Server List** widget.

Server List. This widget displays a list of Lync 2010 servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Lync 2010 server, in percent.
- The latency of the selected Lync 2010 server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Lync 2010 server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent t.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Active Registered Endpoints. Endpoints are devices that are connected to the Lync front-end server. This widget displays a line graph. The line graph displays Endpoint Cache: Active Registered Endpoints.

- The y axis displays numbered of registered endpoints.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Active IM Conferences. This widget displays the current number of IM conversations on the Lync server. Conferences usually include more than two users. This widget displays a line graph. The line graph displays Active Conferences.

- The y axis displays numbered of IM conferences.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Connected IM Users. This widget displays the current number of connected IM users. This widget displays a line graph. The line graph displays Connected Users.

- The y axis displays numbered of IM users.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Number of Calls. This widget displays the current number of voice calls on the Lync server. This widget displays a line graph. The line graph displays UpdateEndpoint: Number of Calls.

- The y axis displays numbered of calls.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Active AS Conferences. This widget displays the number of active conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Active Conferences.

- The y axis displays numbered of AS conferences.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Connected AS Users. This widget displays the number of users connected to conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Connected Users.

- The y axis displays numbered of AS users.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

Microsoft: Skype for Business Dashboards

The Microsoft: Skype for Business Dashboards PowerPack includes the following dashboards:

- Microsoft: Lync Server 2013 Performance
- Microsoft: Lync Server 2013 Utilization

Microsoft: Lync Server 2013 Performance

The Microsoft: Lync 2013 Server Performance dashboard provides an overview of the health and performance of a selected Lync 2013 server.

Context Quick Selector. This widget contains the time span preset buttons and Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Lync 2013 servers that appear in the **Server List** widget.

Server List. This widget displays a list of Lync 2013 servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Lync 2013 server, in percent.
- The latency of the selected Lync 2013 server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Lync 2013 server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Connections Established. This widget displays a line graph. The line graph displays Connections Established.

- The y axis displays number of connections.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2010 server.

SIP Message. SIP is a protocol for instant messaging and VOIP. This widget displays a line graph. The line graph displays Incoming Message and Outgoing Messages. Each parameter is represented by a color-coded line.

- The y axis displays number of messages.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Sproc Latency. Stored Procedure Call (sproc) latency is the time it takes for the Lync database to process the stored procedure call.

- The y axis displays the duration, in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

SIP Network Errors. This widget displays information about errors during instant messaging or VOIP. This widget displays a line graph. The line graph displays Connections Above Per-User Limit Dropped, Connections Refused Due to Server Overload, Failed DNS SRV Queries, Time Out DNS SRV Queries, and TLS Negotiations Failed. Each parameter is represented by a color-coded line.

• The y axis displays the number of connections that resulted in errors.

- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Incoming Response Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 2xx Responses. A 2xx Response means that a connection has been established.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Incoming Respond Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 1xx (non-100) Responses, Incoming 3xx Responses, Incoming Other 4xx Responses, Incoming Other 5xx Responses, and Incoming 6xx Responses. Each parameter is represented by a color-coded line. For a description of all SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List of SIP response codes.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Incoming Response Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 400 Responses, Incoming 401 Responses, Incoming Other 403 Responses, Incoming 404 Responses, Incoming 407 Responses, and Incoming 408Responses. Each parameter is represented by a color-coded line. For a description of all SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List of SIP response codes.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Incoming Response Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 482 Responses and Incoming 483 Responses. Each parameter is represented by a color-coded line. For a description of all SIP responses codes, see the Wikipedia page http://en.wikipedia.org/wiki/List_of_SIP response codes.

- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Microsoft: Lync Server 2013 Utilization

The Microsoft: Lync 2013 Server Utilization dashboard provides an overview of how users are using a selected Lync 2013 server.

Context Quick Selector. This widget contains buttons for time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of Lync 2013 servers that appear in the **Server List** widget.

Server List. This widget displays a list of Lync 2013 servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected Lync 2013 server, in percent.
- The latency of the selected Lync 2013 server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Lync 2013 server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Active Registered Endpoints. Endpoints are devices that are connected to the Lync front-end server. This widget displays a line graph. The line graph displays Endpoint Cache: Active Registered Endpoints.

- The y axis displays the number of registered endpoints.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Active IM Conferences. This widget displays the number of IM conversations on the Lync server. Conferences usually include more than two users. This widget displays a line graph. The line graph displays Active Conferences.

- The y axis displays the number of IM conferences.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Connected IM Users. This widget displays the current number of connected IM users. This widget displays a line graph. The line graph displays Connected Users.

- The y axis displays the number of IM users.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Number of Calls. This widget displays the current number of voice calls on the Lync server. This widget displays a line graph. The line graph displays UpdateEndpoint: Number of Calls.

- The y axis displays the number of calls.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Active AS Conferences. This widget displays the number of active conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Active Conferences.

- The y axis displays the number of AS conferences.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Connected AS Users. This widget displays the number of users connected to conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Connected Users.

- The y axis displays the number of AS users.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Lync 2013 server.

Microsoft: SQL Server Performance

The Microsoft: SQL Server Performance dashboard provides an overview of the health and performance of a selected SQL server.

Context Quick Selector. This widget contains buttons for the time span presets and the Organizations Selector.

- *Time span presets*. Users select the time span over which they want to view data. Selections range from one hour to 90 days.
- Organizations Selector. This drop-down list allows a user to select specific organizations for which they want to view data. This field filters the list of SQL servers that appear in the **Server List** widget.

Server List. This widget displays a list of SQL servers. Selecting a server drives the context for the other widgets in the dashboard.

Availability and Latency. This widget displays two gauges:

- The availability of the selected SQL server, in percent.
- The latency of the selected SQL server, in milliseconds.

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected SQL server during the selected duration. Each parameter is represented by a color-coded line.

- The y axis displays usage, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Buffer Cache Hit Ratio. This widget displays information about the percentage of page requests that are satisfied by data pages from the buffer cache without having to read from disk. The ratio is the total number of pages found in the buffer divided by the total number of requests. This widget displays a line graph. The line graph displays Buffer Cache Hit Ratio.

- The y axis displays the ratio, in percent.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Average Wait Time. This widget displays information about the average wait time to acquire a lock. This widget displays a line graph. The line graph displays Average Wait Time.

- The y axis displays the wait time, in milliseconds.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Deadlocks. This widget displays information about deadlocks. A deadlock occurs when two or more tasks permanently block each other because each task tries to lock a resource which the other tasks are also trying to lock. This widget displays a line graph. The line graph displays Number of Deadlocks Per Second.

- The y axis displays the number of deadlocks per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Lock Waits. This widget displays information about the number of lock requests per second that require the requester to wait. This widget displays a line graph. The line graph displays Lock Waits Per Second.

- The y axis displays the number of waits per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Catalog Cache Hit Ratio. This widget displays information about the ratio between catalog metadata cache hits and lookups. The ratio is the total number of pages found in the catalog metadata cache divided by the total number of lookups. This widget displays a line graph. The line graph displays Catalog Cache Hit Ratio.

- The y axis displays the ratio.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Page Life Expectancy. This widget displays information about the number of seconds a page will stay in the buffer pool (memory cache) without references. This widget displays a line graph. The line graph displays Page Life Expectancy.

- The y axis displays the number of seconds a page will stay in the buffer pool.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Transactions. A transaction is a sequence of operations that make up a single logical unit of work, usually a change to the database. This widget displays information about the number of transactions per second to the SQL server. This widget displays a line graph. The line graph displays Transactions Per Second.

- The y axis displays the number of transactions per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Latch Waits. A latch is an object that ensures data integrity for objects in the buffer pool (memory cache). This widget displays a line graph. The line graph displays Latch Waits Per Second.

- The y axis displays the number of waits per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected SQL server.

Chapter **10**

Troubleshooting

Overview

The following sections describe some of the error messages that you might see when configuring SL1 to monitor Windows devices.

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

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

For additional troubleshooting tips for PowerShell Monitoring, see the following video: https://www.youtube.com/watch?v=4RDSpdrU-sw.

This chapter covers the following topics:

Troubleshooting WinRM Error Messages	162
Troubleshooting PowerShell Error Messages	166

Troubleshooting WinRM Error Messages

SL1 can generate the following error messages when problems occur in Windows Remote Management (WinRM). For each error message, the top-most cause listed is the most likely reason for the error message.

Error / Message	Cause / Resolution
Incorrect username and/or password provided in the PowerShell Credential.	Bad HTTP response returned from server. Basic authentication failed. Code 401. (For more information, see the section Debugging Code 401 <u>Errors</u> .)
	Pre-authentication failed while getting initial credentials.
	Client not found in Kerberos database.
The device cannot respond to WinRM requests or the PowerShell credential settings do not match the device's WinRM configuration.	Kerberos-based authentication failed. Code 500. (For more information, see the section Debugging Code 500 Errors.)
	[Errno 111] Connection refused.
	ParseError.
Server is offline.	Increase the Timeout value on your ScienceLogic credential.

NOTE: If you receive an error message that is a combination of the first two error messages, then you must run debugging steps for both Code 401 and Code 500.

Debugging Code 401 Errors

If you encounter a Code 401 error, perform the following troubleshooting steps to debug the error:

- Determine if the error is caused by an issue with the Kerberos ticket:
 - $^\circ$ Ensure forward and reverse DNS are configured correctly when using Active Directory authentication:

nslookup [IP address]

nslookup [hostname]

° Ensure you are able to run the following command without error from the collector:

kinit [username@DOMAINNAME]

° If you see the following error, change the domain name to all capital letters:

[root@COM_ISO_AIO ~]# kinit commro@mstl08r2.com Password for commro@mstl08r2.com: kinit(v5): KDC reply did not match expectations while getting initial credentials

- Ensure that your WinRM settings match your ScienceLogic credential.
 - To print out current WinRM settings:
 - # winrm get winrm/config
 - If your ScienceLogic credential says no encryption, AllowUnencrypted should be set to True for both the Client and the Service:

winrm set winrm/config/client `@{AllowUnencrypted="\$true"}'

- # winrm set winrm/config/service `@{AllowUnencrypted="\$true"}'
- If you are using local type credentials, basic Authentication should be set to True for both Client and Service:

winrm set winrm/config/client/Auth `@{Basic="\$true"}'

- # winrm set winrm/config/service/Auth `@{Basic="\$true"}'
- If you are using AD type credentials, Kerberos Authentication should be set to True for both Client and Service:

winrm set winrm/config/client/Auth `@{Kerberos="\$true"}'

```
# winrm set winrm/config/service/Auth `@{Kerberos="$true"}'
```

- In the ScienceLogic credential, ensure the Active Directory *Hostname/IP* field contains the FQDN and the *LDAP Domain* field includes the domain.
- In the ScienceLogic credential, the value in the *LDAP Domain* field might need to be entered in all capital letters.
- Ensure your ScienceLogic credentials are correct:
 - SSH to your Data Collector and try running the following command:

wmic -U 'user%password' //IP "select * from Win32 ComputerSystem"

NOTE: If you choose to copy and paste the above command from this document into a shell session, you might have to replace the single and double quotation marks.

- If you are using Windows Servers 2012 and above, make sure that the user you are using belongs to the group: WinRMRemoteWMIUsers
- If multiple domains are in use, ensure that they are mapped in the [domain_realm] section of the Kerberos krb5.conf file.
 - The [domain_realm] section provides a translation from a domain name or hostname to a Kerberos realm name.
- Ensure that the username and password are correct and that you can log on to the system.
- Ensure your credential cache is up-to-date:
 - ° SSH to your Data Collector and cd to the /tmp/ directory.
 - ° Do an 'ls' to list all the contents of the /tmp/ directory.
 - ° If you see any files that being with "krb5cc ", delete those files.

Debugging Code 500 Errors

If you encounter a Code 500 error, perform the following troubleshooting steps to debug the error:

- In the ScienceLogic credential, increase the value in the Timeout field (e.g., 180000 ms.).
- Increase the timeout in the WinRM settings:

winrm set winrm/config `@{MaxTimeoutms="30000"}'

• Increase the maximum number of concurrent operations per user:

```
winrm set winrm/config/service `@{MaxConcurrentOperationsPerUser="100"}'
```

• Increase the maximum number of connections:

```
winrm set winrm/config/service `@{MaxConnections="100"}'
```

• Increase the maximum number of concurrent operations:

• Ensure that the Windows device being monitored is not exceeding its resource thresholds. You can do this by opening Resource Monitor on the Windows Device and monitoring the CPU usage.

Troubleshooting PowerShell Error Messages

SL1 can generate the following error message when monitoring Windows devices using PowerShell. This error message usually indicates that an issue with WinRM is not causing the error.

Error / Message	Cause / Resolution
Get-Counter The specified object was not found on the computer.	The PowerShell object was not found on the device that is being monitored. To test this, copy the PowerShell request from the Dynamic Application and run it on the Windows device in a PowerShell shell as Administrator. If you get a similar error message, then the counter does not exist on your Windows device. This means that the user must install the necessary service on the Windows device.

© 2003 - 2024, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010