

Monitoring Windows Systems with PowerShell

SL1 version 10.1.4, rev. 2

Table of Contents

Introduction	5
Monitoring Windows Devices in the ScienceLogic Platform	6
What is SNMP?	6
What is PowerShell?	6
PowerPacks	7
Configuring Windows Systems for Monitoring with SNMP	8
Configuring SNMP for Windows Server 2016 and Windows Server 2012	9
Configuring Ping Responses	9
Installing the SNMP Service	.10
Configuring the SNMP Service	15
Configuring the Firewall to Allow SNMP Requests	20
Contiguring Device Classes tor Windows Server 2016 and Windows 10	20
Manually Align the Device Class	21
Edit the Registry Key	21
Configuring SNMP for Windows Server 2008	22
	22
Installing the SNMP Service	. 23
Configuring the SINMP Service	26
Configuring the Firewall to Allow SINMP Requests	JI
	32
	33
Configuring PowerShell	33 24
Option 1: Configuring the User Account for the ScienceLogic Planorm	
Option 1: Creating all Active Directory Account with Administrator Access	25
Option 2: Creating a Local User Account with Administrator Access	25
Option 5: Creding d Non-Administration Oser Account	27
Optional: Configuring the User Account for Remote PowerShell Access to Huper V Server	
Creating a User Group and Adding a User in Active Directory	38
Setting the Session Configuration Parameters and Group Permissions	
Creating a PowerShell Credential	
Optional: Configuring the User Account for Access to Windows Failover Cluster	39
Step 2: Configuring a Server Authentication Certificate	39
Option 1. Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	- 40
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	42
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	. 42
Step 3: Configuring Windows Remote Management	.43
Option 1: Using a Script to Configure Windows Remote Management	43
Option 2: Manually Configuring Windows Remote Management	48
Option 3: Using a Group Policy to Configure Windows Remote Management	51
Step 4: Configuring a Windows Management Proxy	. 69
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	70
SNMP and PowerShell Dynamic Applications for Windows Devices	71
SNMP Dynamic Applications for Windows Devices	72
PowerShell Dynamic Applications	72
Microsoft: Active Directory Server	72
Microsoft: DHCP Server	. 73
Microsoft: DNS Server	73
Microsoft: Exchange Server	74
Microsott: Exchange Server 2010	74

Microsoft: Hyper-V Server	75
Microsoft: IIS Server	.76
Microsoft: Lync Server 2010	.76
Microsoft: SharePoint Server	.77
Microsoft: Skype for Business	.77
Microsoft: SQL Server	. 78
Microsoft: Windows Server	
Microsoft: Windows Server Event Logs	.80
Microsoft: Windows Server Services	.82
Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows	•
Servers	82
Error Messages for PowerShell Collection	82
Relationships with Other Types of Component Devices	.02
Creating SNMP and PowerShell Credentials for Windows Devices	85
Creating on SNMP Credential	86
Creating an SNMP Credential in the SL1 Classic Liser Interface	88
Creating a PowerShell Credential	91
Creating a PowerShell Credential in the SL1 Classic User Interface	94
Testing Windows Credentials	- / - 96
SNMP Credential Test	96
PowerShell Credential Test	96
Running a Windows Crodential Test	.70
Running a Windows Credential Test in the SL1 Classic Liser Interface	00
Discovaring Component Devices on Hyper V Systems	100
Viewing Component Devices	100
Manually Alianing the Microsoft: Print Sonver Dynamic Application	107
Concurrent PowerShell Collection	102
Prerequisites	103
Scope	100
Engling and Disabling Concurrent PowerShell for Collector Groups	104
Enabling Concurrent PowerShell on All Collector Groups	104
Disabling Concurrent PowerShell on All Collector Groups	105
Engling Concurrent PowerShell on a Specific Collector Group	105
Disabling Concurrent PowerShell on a Specific Collector Group	105
The SL1: Concurrent PowerShell Menitoring PowerPack	105
Aligning the "Sciencel egic: PowerShell Service Leg Parrer" Dynamic Application	100
Configuring the Device Template	100
Applying the Device Template	107
Scale Recommandations	107
Additional Scale Tins	100
Executing the SL1 Agent with Windows PowerShell	110
What is an SL1 Agent?	110
Agent-Compatible PowerPacks	111
The Credential for the SL1 Agent	111
Configuring the SL1 Agent Device Template	112
Windows Dashboards	114
Installing the Microsoft Server Dashboards	115
Microsoft Active Directory Server Performance	116
Microsoft DNS Server Performance	110
Microsoft Exchange Server 2010 Performance	121
Microsoft Exchange Server 2013 Performance	124
Microsoft IIS Server Performance	127
	· - /

Microsoft: Lync Server 2010 Dashboards	
Microsoft: Lync Server 2010 Performance	
Microsoft: Lync Server 2010 Utilization	132
Microsoft: Skype for Business Dashboards	135
Microsoft: Lync Server 2013 Performance	
Microsoft: Lync Server 2013 Utilization	138
Microsoft: SQL Server Performance	141
Troubleshooting	
Troubleshooting WinRM Error Messages	145
Debugging Code 401 Errors	
Debugging Code 500 Errors	
Troubleshooting PowerShell Error Messages	148

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).

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

Monitoring Windows Devices in the ScienceLogic Platform	. 6
What is SNMP?	6
What is PowerShell?	. 6
PowerPacks	7

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://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6.

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 1.0
- Microsoft: DNS Server, version 100
- Microsoft: Exchange Server, version 100
- Microsoft: Exchange Server 2010, version 1.2
- Microsoft: Hyper-V Server, version 101
- Microsoft: IIS Server, version 102
- Microsoft: Lync Server 2010, version 1.0
- Microsoft: SharePoint Server, version 1.0
- Microsoft: SQL Server, version 100
- Microsoft: Windows Event Logs, version 100
- Microsoft: Windows Server, version 109
- Microsoft: Windows Server Cluster, version 101
- Microsoft: Windows Server Services, version 101
- ScienceLogic: Concurrent PowerShell Monitoring, version 100

Chapter

2

Configuring Windows Systems for Monitoring with SNMP

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).

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

Configuring SNMP for Windows Server 2016 and Windows Server 2012	
Configuring Ping Responses	
Installing the SNMP Service	
Configuring the SNMP Service	
Configuring the Firewall to Allow SNMP Requests	
Configuring Device Classes for Windows Server 2016 and Windows 10	
Manually Align the Device Class	
Edit the Registry Key	
Configuring SNMP for Windows Server 2008	
Configuring Ping Responses	
Installing the SNMP Service	
Configuring the SNMP Service	
Configuring the Firewall to Allow SNMP Requests	

Configuring SNMP for Windows Server 2016 and Windows Server 2012

To configure SNMP on a Windows 2016 Server or a Windows 2012 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:

#	Windows	Firewall with Advanced S	ecurity		_ _ ×
File 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 Networking	All	Yes	Mary Rule
Connection Security Rules	🕜 Core Networking - Multicast Listener Rep	Core Networking	All	Yes	
p 🔩 Wonitoring	🖉 Core Networking - Multicast Listener Rep	Core Networking	All	Yes	Y Filter by Profile
	🕜 Core Networking - Neighbor Discovery A	Core Networking	All	Yes	🐨 Filter by State 🕨 🕨
	🔇 Core Networking - Neighbor Discovery S	Core Networking	All	Yes	🐨 Filter by Group 🕨 🕨
	🔮 Core Networking - Packet Too Big (ICMP	Core Networking	All	Yes	View
	🔮 Core Networking - Parameter Problem (I	Core Networking	All	Yes	
	🛛 🕑 Core Networking - Router Advertisement	Core Networking	All	Yes	Q Refresh
	Ore Networking - Router Solicitation (IC	Core Networking	All	Yes =	📑 Export List
	Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	🕐 Help
	Core Networking - Time Exceeded (ICMP	Core Networking	All	Yes	File and Drinter Charles a (Ealer Demost
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo	All	NO No	File and Printer Sharing (Ecno Request •
	Distributed Transaction Coordinator (RP	Distributed Transaction Cool	AU	No	O Enable Rule
	File and Printer Sharing (Echo R	Sharing	All	No	🔏 Cut
	File and Printer Sharing (Echo R	le Rule Sharing	All	Yes	🗈 Copy
	File and Printer Sharing (LLMNF Cut	Sharing	All	No	🗙 Delete
	File and Printer Sharing (NB-Dat Copy	, Sharing	All	No	Dremarties
	File and Printer Sharing (NB-Na Delet	Sharing	All	No	Propercies
	File and Printer Sharing (NB-Ses	Sharing	All	No	👔 Help
	File and Printer Sharing (SMB-Ir Prop	erties Sharing	All	No	
	🖤 File and Printer Sharing (Spoole Help	Sharing	All	No	
	File and Printer Sharing (Spooler Service	File and Printer Sharing	All	No	
	🔮 File and Printer Sharing over SMBDirect (i	File and Printer Sharing over	All	No	
	SCSI Service (TCP-In)	iSCSI Service	All	No	
	Key Management Service (TCP-In)	Key Management Service	All	No	
	WNetlogon Service (NP-In)	Netlogon Service	All	No	
	Whetlogon Service Authz (RPC)	Netlogon Service	All	No	
	Wetwork Discovery (LLMNR-UDP-In)	Network Discovery	All	No	
	Whetwork Discovery (NB-Datagram-In)	Network Discovery	All	No	
	Network Discovery (NB-Name-In)	Network Discovery	All All	NO No	
	TREGROTE DISCOVERY (PUB-WSD-IN)	Network Discovery	All	NU V	
				>	
Copies the current selection.					

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:

à	Add Roles and Features Wizard
Select installation	type Destination server win-bugks2colo
Before You Begin Installation Type	Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Server Selection	Role-based or feature-based installation Configure a single server by adding roles, role services, and features.
Features	 Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based
Results	or session-based desktop deployment.
	< Previous Next > Install Cancel

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

B	Add Role	es and Features V	√izard	_ D X
Select destination	n server			DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a virtua Select a server from th Select a virtual hard d Server Pool Filter:	l hard disk on which he server pool isk	to install roles and features.	
Confirmation Results	Name WIN-3UGJKS2COLQ	IP Address 10.100.100.22	Operating System Microsoft Windows Server 2012	R2 Standard
	1 Computer(s) found This page shows servers t Add Servers command in collection is still incomple	that are running Wind Server Manager. Off tte are not shown.	dows Server 2012, and that have be line servers and newly-added serve	een added by using the ers from which data
		< Pre	vious Next > In	Istall 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	_ _ X
Select features		DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection Server Roles Features Confirmation Results	INET Framework 3.5 Features Image: Interpretent of the state of the st	.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.
	< Previous Next >	Install
	< Previous Next >	Install Cancel

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

þ	Add Roles and Features Wizard	x
T	Add features that are required for SNMP Service? The following tools are required to manage this feature, but do not have to be installed on the same server.	
[Remote Server Administration Tools 	7
	▲ Feature Administration Tools	
	[Tools] SNMP Tools	
	✓ 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:

L	Add Roles and Features Wizard	_ D X
Confirm installation	ON selections	DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin		
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be displayed on this page	e because they have
Server Roles	their check boxes.	25, CIICK 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 Pr	ropert	ies (Lo	cal Con	nputer)	x
General Log On	Recovery	Agent	Traps	Security	Dependencies	
Service name:	SNMP					
Display name:	SNMP Serv	ice				
Description:	Enables Sin (SNMP) req	nple Net juests to	work Ma be proce	nagement essed by tł	Protocol is computer]
Path to executable C:\Windows\Syst	e: em32\snmp.e	exe				
Startup type:	Automatic				~	
Service status:	Running					
Start	Stop		Pau	ise	Resume	
You can specify th from here.	ne start paran	neters th	at apply	when you :	start the service	
Start parameters:						
	[OK		Cancel	Apply	

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

4.	Select the	[Security] t	tab. The	security setting	s are displayed:
----	------------	--------------	----------	------------------	------------------

SNMP Service P	operties (Local Com	nputer) 🛛 🗙
General Log On Recovery	Agent Traps Security	Dependencies
Send authentication trap		
Accepted community names		
Community	Rights	
	E dit Domo	
Add Add Accept SNMP packets	rom any host	
Accept SNMP packets	rom these hosts	
localhost		
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)	x
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 2008 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:

SNMP Service Properties (Local Computer)							
General Log On Re	covery Agent	Traps	Security	Dependencies			
Send authenticati	on trap						
-Accepted commun	ity names						
Community		Rig	hts				
public		RE/	AD ONLY				
				Y			
SN	IMP Service	Config	juration	^			
				bdd			
				A00			
Host name, IP	or IPX address:			Cancel			
Add	Edi	t	Remo	ive			
	01	<	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*:

🔐 Windows Firewall with Advanced Security 📃 🗖						_ 0 X				
File Action View Help										
									_	
Windows Firewall with Advance Inbo	ound Rules								Actions	
Inbound Rules Nam	ne	Group 📩	Profile	Enabled	Action	Override	Program	Local Address	Inbound Rules	
Connection Security Puler	emote Event Log Management (RPC-EP	Remote Event Log Manage.	. All	No	Allow	No	%System	Any	New Rule	
Monitoring	emote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System	Any	Charles DesCla	
W Re Montering	emote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System	Any	Plitter by Profile	,
C Re	emote Scheduled Tasks Management (Remote Scheduled Tasks M.	All	No	Allow	No	%System	Any	Filter by State	•
C Re	emote Scheduled Tasks Management (Remote Scheduled Tasks M.	All	No	Allow	No	%System	Any	Filter by Group	+
C Re	emote Service Management (NP-In)	Remote Service Managemer	it All	No	Allow	No	System	Any	View	•
O Re	emote Service Management (RPC)	Remote Service Managemer	it All	No	Allow	No	%System	Any	Defeat	
COR COR	emote Service Management (RPC-EPM	Remote Service Managemer	it All	No	Allow	No	%System	Any	Ca Kerresh	
l la	bound Rule for Remote Shutdown (RP	Remote Shutdown	All	No	Allow	No	%system	Any	Export List	
l In	bound Rule for Remote Shutdown (TC	Remote Shutdown	All	No	Allow	No	%system	Any	🛛 Help	
C R	emote Volume Management - Virtual D	Remote Volume Manageme	All	No	Allow	No	%System	Any	CNIN 10 C	1.5
C RI	emote Volume Management - Virtual D	Remote Volume Manageme	All	No	Allow	No	%System	Any	SINMP Service (UDP	In) 🔺
C C C C C C C C C C C C C C C C C C C	emote volume Management (RPC-EPM	Remote volume Manageme	All	NO	Allow	NO	%System	Any	Enable Rule	
	outing and Remote Access (GRE-In)	Routing and Remote Access	All	NO No	Allow	NO No	System	Any	🔏 Cut	
	outing and Remote Access (L2TP-In)	Routing and Remote Access	All	NO No	Allow	No	System	Any	Ra Conv	
	outing and Kemote Access (PPTP-In)	Secure Socket Tuppeling Br	All	No	Allow	No	System	Any	Selete	
	NMD Service (LDD In)	SNMD Service	Domain Public	Ver	Allow	No	%Suctore	Any	∧ Delete	
	NMP Service (UDP In)		Drivate Dublic	No	Allow	No	%System	Any	Properties	
	NMP Tran Service (UDP In)	Enable Rule	Private Public	No	Allow	No	%System	Δηγ	🛛 Help	
0 SI	NMP Trap Service (UDP In)	Cut	Domain	No	Allow	No	%System	Δηγ		
OT OT	PM Virtual Smart Card Managemen	Conv. ard Ma	Domain	No	Allow	No	%System	Δηγ		
ØT.	PM Virtual Smart Card Managemen	ard Ma.	Private Public	No	Allow	No	%System	Any		
ØT.	PM Virtual Smart Card Managemen	Jelete ard Ma.	. Domain	No	Allow	No	%System	Any	=	
	PM Virtual Smart Card Managemen	Properties ard Ma.	. Private, Public	No	Allow	No	%System	Any		
Ø vi	irtual Machine Monitoring (DCOM-	Help	All	No	Allow	No	%System	Any		
Øvi	irtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any		
Ø Vi	irtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any		
Ø Vi	irtual Machine Monitoring (NB-Session	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	-	

Enable Rule										

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*:

@	Winc	lows Firewall with	Advanced S	ecurity		_ D X
File Action View Help						
🗢 🄿 🙇 🖬 🗟 🖬						
🔗 Windows Firewall with Advance	Inbound Rules					Actions
🔣 Inbound Rules	Name	Group	•	Profile	Enabled 🔨	Inhound Rules
Cutbound Rules	🕜 Core Networking - Multicast Listener	Qu Core Networki	ng	All	Yes	Mara Rula
Connection Security Rules	🖉 Core Networking - Multicast Listener I	Rep Core Networki	ng	All	Yes	
p 📷 Monitoring	🕜 Core Networking - Multicast Listener I	Rep Core Networki	ng	All	Yes	Y Filter by Profile
	🕜 Core Networking - Neighbor Discover	y A Core Networki	ng	All	Yes	🕎 Filter by State 🕨 🕨
	🕑 Core Networking - Neighbor Discover	y S Core Networki	ng	All	Yes	🕎 Filter by Group 🕨 🕨
	🕜 Core Networking - Packet Too Big (IC	MP Core Networki	ng	All	Yes	View
	🔮 Core Networking - Parameter Problen	n (I Core Networki	ng	All	Yes	
	🔮 Core Networking - Router Advertisem	ent Core Networki	ng	All	Yes	🖸 Refresh
	Ore Networking - Router Solicitation	(IC Core Networki	ng	All	Yes ≡	Export List
	🔮 Core Networking - Teredo (UDP-In)	Core Networki	ng	All	Yes	🛛 Help
	Core Networking - Time Exceeded (IC	MP Core Networki	ng	All	Yes	
	Distributed Transaction Coordinator (RPC) Distributed Tra	nsaction Coo	All	No	File and Printer Sharing (Echo Request 🔺
	Distributed Transaction Coordinator (RP Distributed Transaction		nsaction Coo	o All No	No	🗿 Enable Rule
	Distributed Transaction Coordinator (IC Distributed Ira	uted Transaction Coo All	No	🔏 Cut	
	File and Printer Sharing (Echo R	Enable Rule	snaring	All	NO	Conv.
	File and Printer Sharing (Echo R	0.4	Sharing	All	res No	
	File and Printer Sharing (LLWINF	Cut	Sharing	All	No	
	File and Printer Sharing (NB-Na	Сору	Sharing	All	No	Properties
	File and Printer Sharing (NB-Sec	Delete	Sharing Sharing	All	No	🕐 Help
	File and Printer Sharing (SMB-Ir	Properties	Sharing		No	
	File and Printer Sharing (Snoole	Help	Sharing	All	No	
	File and Printer Sharing (Spooler Serve	e File and Printer	Sharing	All	No	
	File and Printer Sharing over SMBDire	t (i File and Printer	Sharing over	All	No	
	iSCSI Service (TCP-In)	iSCSI Service		All	No	
	Key Management Service (TCP-In)	Key Managem	ent Service	All	No	
	Netlogon Service (NP-In)	Netlogon Servi	ce	All	No	
	Netlogon Service Authz (RPC)	Netlogon Servi	ce	All	No	
	Network Discovery (LLMNR-UDP-In)	Network Disco	very	All	No	
	Network Discovery (NB-Datagram-In)	Network Disco	very	All	No	
	💿 Network Discovery (NB-Name-In)	Network Disco	very	All	No	
	🔘 Network Discovery (Pub-WSD-In)	Network Disco	very	All	No 🗸	
< III >	<				>	
Copies the current selection.						

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:

Server Manager			<u>- ×</u>
File Action View Help			
🗢 🔿 🔁 🚾 🛛 🖬			
Server Mancol La Control Cont	Features View the status of features installe	ed on this server and add or remove features.	
	Last Refresh: 7/1/2011 12:49:38 PM Confi	igure refresh	
]			
💐 Start 🛛 🚠 💻 🛛 🕌 Server Ma	inager	💀 🗟 🕼	1:04 PM

3. 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:

Add Features Wizard		X
Select Features		
Features Confirmation Progress Results	Select one or more features to install on this server. Eetures: Quality Windows Audio Video Experience Remote Assistance Remote Server Administration Tools Removable Storage Manager PC Over HTTP Proxy Simple TCP/IP Services Storage Manager HSSANs Storage Manager HSSANs Subsystem for UNIX-based Applications Telef Client Telnet Server PC Olimit Windows Process Activation Service Windows Process Activation Service Windows System Resource Manager Windows System Resource Manager	Description: Simple Network Management Protocol (SMMP) Services includes the SMMP Service and SMMP WMI Provider.
	< <u>Previous</u> <u>N</u> ext	> Install Cancel

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	ion 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.	
	< Previous Lext > Linstal Cancel	

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

Add Features Wizard		×
Installation Res	ılts	
Features Confirmation Progress Results	The following roles, role services, or features were installed successfully: I warning message below I warning message below I windows automatic updating is not enabled. To install the latest updates, use Windows Update in Control Panel to check for updates. I suffy Service Installation succeeded I suffy Service I suffy Service I suffy Service I s	
	< <u>Previous</u> <u>N</u> ext > Close Gancel	

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)	×
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	e: em32\snmp.exe	
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-K1TV9QPK\	WS)	×
General Lee On Bergaran		Security I r)anandanaian Ì
General Log On Necovery	Agent Traps		/ependencies
Send authentication trap			
- Assessed assessment			
Accepted community name	es .	1.	
Community	Ri	ghts	
Add	E dit	Remove	e
C Accept SNMP packet	s from any host		N
- Accept SNMP packet	s from these host	s	k
localhost			
Add	Edit	Remove	•
Leam more about SNMP			
	ОК	Cancel	Apply
	U.V.		7460

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	
SNMP Service Configuration	
Community rights: Add	
READ ONLY	
Community Name:	
public	
Add Edit Remove	
Learn 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 (W	IN-2TVE5CD176	2)	×
General Log On Recovery	Agent Traps	Security Dep	oendencies
Send authentication trap			
Accepted community name	es es		
Community	Rig	hts	
cOsmOs	REA	AD ONLY	
SNMP Service Configu	ration		×
		A	
Heat name ID or IDV a	ddraaa:	Car	ncel
	daless.		
Add	E dit	Remove	
Learn more about <u>SNMP</u>			
	ОК	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*:

Windows Firewall with Advanced Security					_ 0 ×				
File Action View Help									
ka 🔿 🙍 📰 🗟 🛛 🖬									
A Mindaux Convelle Advector				_		_	_		1
Windows Firewall with Advance	Inbound Rules								Actions
Cuthound Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address ^	Inbound Rules 🔺
Connection Security Rules	Remote Event Log Management (RPC-EP	Remote Event Log Manage	All	No	Allow	No	%System	Any	🐹 New Rule
Monitoring	Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System	Any	Filter by Profile
	Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System	Any	
	Remote Scheduled Tasks Management (Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	Y Filter by State
	Remote Scheduled Tasks Management (Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	Filter by Group
	Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	No	System	Any	View •
	Remote Service Management (RPC)	Remote Service Management	All	No	Allow	No	%System	Any	Refrech
	Remote Service Management (RPC-EPM	Remote Service Management	All	No	Allow	No	%System	Any	i keiresii
	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 Manageme	All	No	Allow	No	%System	Any	
	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	🔏 Cut
	Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No	System	Any	B. Com
	Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No	System	Any	Les copy
	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	No	Allow	No	%System	Any	
	SNMP Trap Service (UDP In)	choore more	Private, Public	No	Allow	No	%System	Any	1 riep
	SNMP Trap Service (UDP In)	Cut	Domain	No	Allow	No	%System	Any	
	TPM Virtual Smart Card Managemen	Copy ard Ma	Domain	No	Allow	No	%System	Any	
	TPM Virtual Smart Card Managemen	Delete ard Ma	Private, Public	No	Allow	No	%System	Any _	
	TPM Virtual Smart Card Managemen	Propertier and Ma	Domain	No	Allow	No	%System	Any =	
	TPM Virtual Smart Card Managemen	ard Ma	Private, Public	No	Allow	No	%System	Any	
	Wirtual Machine Monitoring (DCOM-	Help itoring	All	No	Allow	No	%System	Any	
	Wirtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	
	Wirtual Machine Monitoring (Echo Reque	Virtual Machine Monitoring	All	No	Allow	No	Any	Any	
	Wirtual Machine Monitoring (NB-Session	Virtual Machine Monitoring	All	No	Allow	No	Any	Any 🗸	
< III >	<							>	
Enable Rule									

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).

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

Prerequisites	33
Configuring PowerShell	33
Step 1: Configuring the User Account for the ScienceLogic Platform	34
Option 1: Creating an Active Directory Account with Administrator Access	34
Option 2: Creating a Local User Account with Administrator Access	35
Option 3: Creating a Non-Administrator User Account	35
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	37
Creating a User Group and Adding a User in Active Directory	38
Setting the Session Configuration Parameters and Group Permissions	38
Creating a PowerShell Credential	
Optional: Configuring the User Account for Access to Windows Failover Cluster	
Step 2: Configuring a Server Authentication Certificate	

Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	40
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	42
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	42
Step 3: Configuring Windows Remote Management	43
Option 1: Using a Script to Configure Windows Remote Management	43
Option 2: Manually Configuring Windows Remote Management	48
Option 3: Using a Group Policy to Configure Windows Remote Management	51
Step 4: Configuring a Windows Management Proxy	69
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	70

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

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

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

Step 1: Configuring the User Account for the ScienceLogic Platform

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

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

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

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

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

- Microsoft Exchange Server
- Hyper-V Servers

Option 1: Creating an Active Directory Account with Administrator Access

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

After creating your Active Directory account:

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

Option 2: Creating a Local User Account with Administrator Access

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

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

After creating your local user account with Local Administrator access:

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

Option 3: Creating a Non-Administrator User Account

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

After creating your domain user account or local user account:

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

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

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

winrm configsddl default

- 2. On the **Permissions for Default** window, click the **[Add]** button, and then add the non-administrator user account.
- 3. Select the Allow checkbox for the **Read (Get, Enumerate, Subscribe)** and **Execute (Invoke)** permissions for the user, and then click **[OK]**.
- 4. Access the Management console. To do this:
 - In Windows Server 2008, click [Start], right-click [Computer], click [Manager], and then expand [Configuration].
 - In Windows Server 2016 and 2012, right-click the Windows icon, click [Computer Management], and then expand [Services and Applications].
- 5. Right-click on [WMI Control] and then select Properties.
- 6. On the WMI Control Properties window, click the [Security] tab, and then click the [Security] button.
- 7. Click the **[Add]** button, and then add the non-administrator user or group in the **Select Users**, **Service Accounts**, or **Groups** dialog, then click **[OK]**.
- 8. On the **Security for Root** window, select the user o group just added, then in the **Permissions** section at the bottom of the window, select the **Allow** checkbox for the Execute Methods, Enable Account, and Remote Enable permissions.
- 9. Under the Permissions section of the Security for Root window, click the [Advanced] button.
- 10. In the Advanced Security Settings window, double-click on the user account or group you are modifying.
- 11. On the **Permission Entry** window, in the **Type** field, select Allow.
- 12. In the Applies to field, select This namespace and subnamespaces.
- Select the Execute Methods, Enable Account, and Remote Enable permission checkboxes, and then click [OK] several times to exit the windows opened for setting WMI permissions.
- 14. Restart the WMI Service from services.msc.

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

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

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

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

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

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

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

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

If you use SL1 to monitor Microsoft Exchange Servers:

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

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

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

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

Creating a User Group and Adding a User in Active Directory

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

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

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

Setting the Session Configuration Parameters and Group Permissions

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

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

Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell

- 3. When prompted, select **A**.
- 4. The **Permissions** dialog appears.

Administrators (MSTESTLAB-H	V01\Administrate	Creators) ors)
Remote Management Users (M	ISTESTLAB-HV	01\Remote
Г		
missions for PSSession	A@d	Hemove
eators	Allow	Deny
Full Control(All Operations)	~	
Read(Get,Enumerate,Subscribe)		
Write(Put, Delete, Create)		
Execute(Invoke)		
Special permissions		
r special permissions or advanced	i settings,	Advanced

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

Creating a PowerShell Credential

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

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

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

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

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

Step 2: Configuring a Server Authentication Certificate

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

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

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

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

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

- You have created an Active Directory user account on the Windows Server to allow communication between SL1 and the server. In this scenario, Active Directory will use Kerberos and AES-256 encryption to ensure secure data transfer and authentication, which means you do not need to configure a self-signed Server Authentication Certificate. You can skip this section and proceed to Step 3.
- You have created a *local account* on the Windows Server that uses Basic Auth to allow communication between SL1 and the server, and your network *includes a Microsoft Certificate server*. In this scenario, you should work with your Microsoft administrator to get a certificate for your Windows Server instead of configuring a self-signed Server Authentication Certificate. You can skip this section and proceed to Step 3.
- You have created a *local account* on the Windows Server that uses Basic Auth to allow communication between SL1 and the server, and your network *does not include a Microsoft Certificate server*. In this scenario, you must configure a self-signed Server Authentication Certificate on the Windows Server that you want to monitor with SL1 using one of the following methods:
 - Option 1: Use the Microsoft Management Console.
 - **Option 2**: If your Windows Server includes Windows Software Development Kit (SDK), you can use the makecert tool.
 - **Option 3:** If you are running PowerShell 4.0 or later, you can use the New-SelfSignedCertificate and Export-PfxCertificate commands.

NOTE: Self-signed certificates are appropriate for use on a trusted network, such as a LAN that includes both a ScienceLogic Data Collector and the Windows Server to be monitored.

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

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

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

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

Snap-in	Vendor	*	Console Root	Edit Extensions
ActiveX Control Authorization Manager Certificates Component Services Computer Managem Device Manager Mask Management Event Viewer Folder Folder Group Policy Object IP Security Monitor	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor	E Add >		Remove Move Up Move Down
IP Security Policy M	Microsoft Cor Microsoft Cor	•		Advanced

- 4. In the **Available snap-ins** list, select Certificates.
- 5. Click the **[Add >]** button. The **Certificates snap-in** window is displayed:



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

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

If your Windows system includes Windows Software Development Kit (SDK), you can use the MakeCert tool that is included in the kit to create a self-signed certificate.

• For information on the MakeCert tool, see:

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

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

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

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

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

• You can use the **New-SelfSignCertificate** command to create a self-signed certificate. For information on **New-SelfSignCertificate**, see:

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

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

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

Step 3: Configuring Windows Remote Management

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

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

There are three ways to configure Windows Remote Management:

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

Option 1: Using a Script to Configure Windows Remote Management

ScienceLogic provides a PowerShell script 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 Services, Microsoft: Windows Server Event Logs, and Microsoft: SQL Server Enhanced PowerPacks. (Microsoft: SQL Server Enhanced requires further instance-specific permissions. See the Monitoring SQL Servers manual for more information.)

To use the PowerShell script, perform the following steps:

- 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_wizardv3.0.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_wizardv3.0* to the Windows server that you want to monitor with SL1.
- 5. Right-click on the PowerShell icon and select Run As Administrator.
- At the PowerShell prompt, navigate to the directory where you copied the PowerShell script named winrm_ configuration_wizardv3.0.
- 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_wizardv3.0.ps1 -user <domain>\<username>

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

```
help .\winrm configuration wizardv3.0.ps1 -full
```

The most common way to run the script is silently:

```
.\winrm configuration wizardv3.0.ps1 -user <domain>\<username> -silent
```

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



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



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

Set Encryption Policy ×
Should your WinRM traffic from SL1 be encrypted? Click YES to use only encrypted data. Click NO to allow unencrypted data.
Yes No

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

13. The Change Max Requests modal page appears. Click [Yes].



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

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

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

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

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

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

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

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

Confirm Settings	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 OK to update WinRM settings.	
Click CANCEE to quit wizard (settings will not be updated).	
OK Cancel	

18. The **Complete** modal page 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
Basic Authentication = true Kerberos Authentication = true Allow Unencrypted WinRM Traffic = true Maximum WinRM Requests = 500 HTTP Port = 5985 HTTPS Port = 5986 Certificate Thumbprint = 4705BE1B838CDCA76BB1993BE3307C85DF61C93F The WinRM service will be restarted after this dialog is closed.
OK Cancel

19. Exit the PowerShell session.

Option 2: Manually Configuring Windows Remote Management

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

- 1. Log in to the server with an account that is a member of the local Administrators group, or a Domain Administrator's account if on a Windows server with the Domain Controller role installed.
- 2. Right-click on the PowerShell icon in the taskbar or the Start menu, and select Run as Administrator.
- 3. Execute the following command:

Get-ExecutionPolicy

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

Set-ExecutionPolicy RemoteSigned

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

winrm get winrm/config

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE: ScienceLogic recommends using an Active Directory account.

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

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

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

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

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

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

- 1. Log in to the server as an administrator.
- 2. Right-click on the PowerShell icon in the taskbar and select Run as Administrator.
- 3. At the PowerShell prompt, use the change directory (CD) command to navigate to a folder where you can create new files.

4. Save the root Certification Authority certificate to the local directory by executing the following command:

certutil.exe -ca.cert ca_name.cer

Cit.	Administrator: Command Prompt	- 0 ×
C:\Users CA cert CA cert CA cert MIIDpTCC MRUwEwYH UjIxJTA NDEIMTYJ YWwxGTA MilUTDAS AOIBAQCM 7CcWfD6d Q8li6Ydd JGmtOp52 7XLVsMSt QwBBMA4C QjSBuyFc AQUFAAOC R/+1RL/c G4rxLIw, trDogF27 4hjdX04F vWF1gNe1 ENU CertUtil C:\Users	<pre>\EM7Admin\Documents>certutil -ca.cert ca_name.cer 0]: 3 Valid 0]: IN CERTIFICATE Ao2gAwIBAgIQHAmGt7EAa4tGkBmjDbtA4DANBgkqhkiG9wOBAQUFADBZ CZImiZPyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/IsZAEZFg]NU1RMMDEy BQNVBAWTHEITVEwwMTJSWi1UTDAxMIJYLURDLTAxLUNBLTEwHhcNWTQw NTQ1WhcMTKwNDEJMTcwNTQ1WjBZMRUWEwYKCZImiZPyLGQBGRYFbG9j BgoJkiaJk/IsZAEZFg]NU1RMMDEyUjIXJTAjBgNVBAMTHEITVEwwMTJS MIJyLURDLTAxLUNBLTEwggEiMA0GC5qGSID3DQEBAQUAA4IBDwAwggEK sPONZQ1JA5pxq192rofUCZFa0BISpGOJyMiit+risfVAqIRgVFvc3mQK uNAuh11fYFIhOsORNSOFHgUNgrasdrvugSPL/oV23VDH2dq]HaDd6azY u3oVoaZU9Sgt4HEymPU14QkGuz1n4UTXIdepCAON370yNkoQg01LUutp bYaUOwWyKnvS0osQpqAFSdfW7rgt80bIXf9F2n13yuwqgEfeQ+E8UH4 k7hsFDMxXkvRhdPugH7rIONGiaOxyoVuUVqfiiK748LiE/QveOX73wBo wNo9SNxnf8/hiUJODONAgMBAAGjaTBnMBMGCSSGAQQBgjcUAQQGH9QA A1UdDwEE/wQEAwIBhjAPBgNVHRMBAF8EBTADAQH/MBOGALUdDgQWBBR9 H2PFforxOg/z9lo2wDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9wOB AQEATSkQpaWpO60IT+1398OIs1HbT1n6AyVGizU2MnRAWLKAxgudha kXXJeqjDAFsz2ZEIveiOKVCIbwEXekP2rQG1ujr2FLRbUWt+oA0/ES /g4sOHKSJmRYCXJozDK8zrH0ZADv/TTrn6CEWxYaB6quQFzTQsm9WbUK oDW29LGZ6z7TNn10XoKxEqUqCfR8EPFkctYrZ/+bNFV8X3YJjdAm/42g GlhDjOBgJsrx+01tx8mANjAvUdNg2kvU0m0dP6h17BqJJ08umJxPmfQI UNHfTYuJJdEeR7QhLhK6rkAnHw== CERTIFLCATE ; -ca.cert command completed successfully. \EM7Admin\Documents>_</pre>	
-		~

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.

la la	Server Manager	_ 0 ×
Server N Control Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Server Serve	Server Manager anager Dashboard WELCOME TO SERVER MANAGER OUICK START QUICK START 2 Add roles and features 3 Add other servers to manage	Construction of the second secon
NG IS	WHATS NEW 4 Create a server group LEARN MORE ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers total: 1	DNS Event Viewer Group Policy Management Internet Information Services (II5) Manager ISCSI Initiator Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor
	👫 AD CS 1 🗃 AD DS 1 🗟 DNS	Resource Monitor Security Configuration Wizard
	Manageability Manageability Events Events Services Services Performance Performance BPA results BPA results	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.

E.			Group Policy Ma	anagement		- 0 X	
📓 File Action View	Window Help					_ # ×	
🗢 🄿 🖄 📅 📋	a 🛛 🖬						
Group Policy Managem	ient	Group Policy Objects in MSTL012R2.local					
A Forest: MSTL012R2.	ocal	Contents Delega					
A MSTL012R2 In	ocal	Name	•	GPO Status	WMI Filter	Modified	
🛒 Defa	Create a GPO in this domain, and	d Link it here	trollers Policy	Enabled	None	3/19/201	
Powe	Link an Existing GPO		Management Policy	All settions disabled	None	2/4/2014	
þ 🖬 Dom	Block Inheritance			All settings disabled	None	4/16/201	
p 🎲 WMI	Group Policy Modeling Wizard	8					
Start	New Organizational Unit						
Sites	Search						
Group Polic	Change Domain Controller						
	Remove						
	Active Directory Users and Com	puters					
	New Window from Here						
	Refresh						
	Properties						
	Help						
		٢		ш		>	
Create a GPO in this domain	and link it to this container						

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

	Group Policy Ma	inagement		_ 0 ×	
ile Action View Window Help				- 8	
🔿 🙍 📋 🙆 🔯 📷					
Forest: MSTL012R2.local	Group Policy Objects in MSTL012R2.local Contents Delegation				
▲ ● MSTID1282.local ▲ ● MSTID1282.local ● DeverShell Remote Management Policy ● DeverShell Remote Management Policy ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	Name Pofeat Doman Controllers Policy PowerShell Renote Management Policy WinRM Polcy WinRM Polcy WinRM Settings	GPO Status Enabled Enabled All settings disabled Enabled All settings disabled	WMI Filter None None None None	Modified 3/19:20 2/4/201 4/17:20 4/17:20 4/16/20	
	c	W		13	

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

	Group Pol	icy Management Editor	• (1)		- 0 ×	
File Action View Help						
🗢 🏟 🖄 📷 🗶 🖼 🗟 🖬						
WIRMP Policy (T101282-DC-01.MSTL01282.L0CAL] Policy ▲ Computer Configuration ▲ Policies ▶ Software Resolution Policy ■ Scripts (Statup/Shutdown) ■ Security Settings ▶ Mame Resolution Policies ▶ Local Policies ▶ Local Policies ▶ Ecorthy Settings ▶ Advanced Security Settings ▶ Accurate Policies ▶ Ecorthy Settings ▶ Coal Policies ▶ Ecorthy Settings ▶ Restricted Groups ■ Security Settings ▶ Restricted Groups ■ System Services ▶ Restricted Groups ■ Windows Firewall with Advanced Security ■ Network (List Manager Policies ▶ Windows Firewall with Advanced Security ■ Network Access Protection ▶ Public (key Policies ▶ Window Advide Policics ▶ Public (key Policies ▶ Advanced Advide Policicy Configuration ▶ Advanced Advide Policy Configuration ▶ Policies ▶ Policies ▶ Policies ▶ Policies ▶ Policies ▶ Policies ▶ Policies	Service Name User Access Logging Service User Profile Service Virtual Disk Volume Shadow Copy	Startup Not Defined Not Defined Not Defined Not Defined	Permission Not Defined Not Defined Not Defined Not Defined		<	
	Walc Logging Service Windows Audio Windows Audio Endpoint Builder Windows Color System Windows Conection Marager Windows Enor Reporting Service Windows Inteller Windows Installer Windows Installer Windows Installer	-mode Driver Framework Service	Not Defined Not Defined	Not Defined Not Defined		
	Windows Modules Installer Windows Process Activation Servic Windows Remote Management Windows Store Service (WSServi Windows Update Windows Update Windows Update Window Update Window Config Winder AutoConfig Workstation Workstation Workstation Workstation	e Properties Help sry Service	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined 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].



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



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

<u>I</u>		Group Policy Management E	ditor						- 0	x
File Action	View Help									
WinRM P		New John and Bale Millioned	X	Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ 🌺 Comp ⊿ 🛄 Po ▷ 📫	Rule Type			ems to show	w in this vie	w.				
4 📫	Select the type of firewall rule t	to create.								
	Steps: Rule Type	What type of rule would you like to create?								
1	Predefined Rules									
	 Action 	Program Rule that controls connections for a program.								
		O Port Rule that controls connections for a TCP or UDP port.								
		Predefined: Windows Firewall Remote Management	~							
		Rule that controls connections for a Windows experience.								
		Custom rule.								
Þ										
<		< Back Next >	Cancel							

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

J		G	Froup Policy	Manageme	ent Editor							- 0	x
File Action	View Help												
WinRM P		New Inbound Rule Wizard				x	Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ 🚰 Comp ⊿ 🛄 Po ▷ 🚞 ⊿ 🚞	Predefined Rules Select the rules to be created for	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 requi	rements for the	selected predefin	ed group.								
	 Action 	ntents of											
		Name	Rule Exists	Profile	Desc								
	ream I III III III III III I III III III II	Windows Frewall Remote Management (RPC., Windows Frewall Remote Management (RPC)	No No	All All	Inbou Inbou)							
		< 10			>								
¢		E	< Back	Next >	Cancel						1		

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

J		Group Policy Management Editor							- 0	x
File Action	View Help									
	🖬 🔒 🔽 🖬									
WinRM Pe	#	New Inbound Rule Wizard	x	Profile	Enabled	Action	Override	Program	Local Address	Remot
▲ ₩ Comp	Action Speedy the action to be taken Steps: Predefined Rules Action	when a connection matches the conditions specified in the rule. What action should be taken when a connection matches the specified conditions? • Alow the connection This includes connections that are protected with IPsec as well as those are not. • Alow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections when eads. Customere. Block the connection		ems to shi	ow in this vie	w.				
4		< Back Finish Cance	4							

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 Polic	Management Edit	or		- 0 ×
File Action View Help					
🗢 🔿 🙍 🖬 🔒 📓 🖬					
⊿ 📋 Windows Settings 📃 ∧	Automatic Certificate Request	*	-		-
Name Resolution Policy Scripts (Startup/Shutdown) Security Settings Sucraty Startup/Shutdown) Sucraty Settings Sucraty Settings Sucraty Settings Sucraty Settings Sucraty Settings System Services Sucraty System S		,	here are	no items to show in this view.	
Encrypting File System Data Protection		New	•	Automatic Certificate Request	
BitLocker Drive Encryption		Refresh			
BitLocker Drive Encryption Network Unlock		View	•		
Trusted Root Certification Authorities		Arrange Icons Line up Icons	•		
Intermediate Certification Authorities		Help			
Intered Publishers Untrusted Certificates Trusted People Software Restriction Policies Network Access Protection Software Restriction Control Policies Network Access Protection Software Restriction Control Policies Network Access Protectory (MSTL0 With the Policies on Active Directory (MSTL0 With the Policies Withe Policies W					

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

Auton	natic Certificate Request Setup Wizard	Group Policy Manag	gement Editor		_ 0 ×
	Opencies Opencies This real helps you set up automatic certificate requests This real helps you set up automatic certificate requests This real helps you set up automatic certificate requests This request automatic certificate requests Statistic certificate requests This request automatic certificate requests To continue, click Nest This request automatic certificate requests	equest •	_ There are no	b items to show in this view.	
	Llocker Drive Encryption Llocker Drive Encryption Llocker Drive Encryption Network Unlock dromatic Certificate Request Settings uted Root Certification Authorities terprise Trust termediate Certificates usted Publicher er Restriction Policies ork Access Protection cation Control Policies on Active Directory (MSTLO ×)	-			

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

Automatic Certifi	cate Request Setup Wizard	K Group Pe	olicy Management Editor		- 0
Certificate Template The next time a computer logs on, a provided.	certificate based on the template you s	elect is fequest	•		4
A certificate template is a set of pred computers. Select a template from th Certificate templates:	efined properties for certificates issued e following list.	to	There a	re no items to show in this view.	
Name Computer Domain Controller Errollment Agent (Computer) IPSec	Intended Purposes Client Authentication, Server A Client Authentication, Server A Certificate Request Agent IP securty IKE intermediate	uthentication uthentication			
< ۱۱۱		>			
BitLocker Drive E	< Back Next >	Cancel			
BILLOCKET DIVE E Automatic Certii Trusted Root Ce Enterprise Trust Intermediate Ce	tification Authorities				
Trusted Publishe	cates				

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



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

	Group Policy Management Editor		- 0 X
File Action View Help			
Windows Settings Demonstration Policy Scripts (Startup/Shutdown) County Continuence	🤇 🥏 Certificate Import Wizard	 ended Purposes Friendly Name riew. 	Status Certificate Te
Security security Coord Policies Security Policies Security Event Log Restricted Groups	Welcome to the Certificate Import Wizard		
 System Services Registry File System 	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.		
 Wired Network (IEEE 802.3) Policies Windows Firewall with Advanced Security Network List Manager Policies Network List Manager Policies 	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.		
P Public Key Policies	Store Location		
Encrypting File System	O Current User		
Data Protection	Local Machine		
 BitLocker Drive Encryption Network Unloc BitLocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers 	To continue, click Next.		
Untrusted Certificates			
☐ Trusted People ▷ 11 Software Restriction Policies	Next Cancel]	
Network Access Protection			
Application Control Policies Application Control Policies Application Control Policies Application Control Policies			
< III >	< III		>

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



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

9	Group Policy Management Editor		- 0 X
File Action View Help Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settings Image: Security Settingsecurity Settingsecurity Settings	Group Policy Management Editor 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 the certificate. 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 riew.	Status Certificate Te
BitLocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authonities Enterprise Trust Intermediate Certification Authonities Trusted People D Software Restriction Policies D Network Access Protection D Application Control Policies D Application Control Policies D Strust Policies on Active Directory (MSTLO	V Cancel		د

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

J	Group Policy Management Editor			_ 0 X
File Action View Help				
🕨 🔿 📶 📋 🙆 🔂 📷				
▲ ▲ Windows Settings	🛞 🎐 Certificate Import Wizard	ended Pur	poses Friendly Name	Status Certificate 1
Security Settings B. Account Policies J. Local Policies J. Event Log Restricted Groups	Completing the Certificate Import Wizard			
iii Gystem Services ▷ ii Gegistry ▷ ii Gystem	The certificate will be imported after you click Finish.			
	Contract Store Selected by User Contract Store Selected by User Content Certificate File Name C: Users (EM7Admin/Documents)ca_name.cer			
Dista Protection BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authorities Entermose Trust				
 Intermediate Certification Authorities Trusted Publishers Unrusted Certificates Trusted People Sefavors Pactifician Delician 	Enit C	Concel		
Jortware Kestriction Policies Metwork Access Protection Manual Access Protection Manual Access Protection Manual Access Protection Manual Access Protection	rinish	Cancel		

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



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

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

		Group Policy Management Editor	– 0 ×
File Action View H	Se Windows F	ewall: Define inbound port exceptions – 🗖 🗙	
🔶 🐟 🙇 📷 🗟	Windows Firewall: Define inbound port es	eptions Previous Setting Next Setting	
⊿ 👰 Computer Config ⊿ 🦳 Policies	O Not Configured Comment:	A prentions	State Comment
Software 9 Windows	Enabled	am exceptions	Not configured No
A Administr	O Disabled	nnections	Not configured No
Contro	Supported on: At le	t Windows XP Professional with SP2	Not configured No
⊿ 🧮 Netwo		Show Contents	Not configured No
Bai	Ontions		Not configured No
Dir	options.	Define port exceptions:	Not configured No
DN I	Define and eventions.	Value	Not configured No
📔 Ho	Define port exceptions: Snow	5985:TCP:*tenabled:WSMan	Not configured No
🧾 Lar	Specify the port to open or block.	1 5986:TCP:*:enabled:WSMan tration exc	Not configured No
📔 Lin	Syntax:	* exceptions	Not configured No
D 🛄 Mi		ilticast or	Not configured No
4 Ne	<port>:<transport>:<scope>:<status>:<</status></scope></transport></port>	k exceptio	Not configured No
	<port> is a decimal port number</port>		
	<transport> is either "TCP" or "UDP"</transport>		
🗎 Ne	<scope> is either "*" (for all networks) o</scope>		
Off	a comma-separated list that contains		
▶ 🧰 Qo	any number or combination of these:	OK Cancel	
NIC	IP addresses, such as 10.0.0.1		
D TC	Subnet descriptions, such as 10.2.3.0/24	policy setting.	
🗎 Wi			
🚞 Wi	< 111	If you disable this policy setting, the port exceptions list defined	
▶ 🔛 WL		OK Cancel Apply	
<		Cancer Apply	

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



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

File Action View Help File Action View He		Group Policy Management Editor	- 0 X
	File Action View Help	🐣 Trusted Hosts 📃 🗕 🗖 🗙	
 Sind Read Sound Recorder Sound Recorder		Trusted Hosts Previous Setting Next Setting	
< III > Catended	Sound Recorder Sound Recorder Truste Difference Sound Recorder Sound Recorder Truste Difference	Will ed t ed t ed t ed t Not Configured Enabled Comment: Enabled Image: Supported on: At least Windows Vista Image: Supported on: Supported on: Supported on: Supported on: At least Windows Vista Image: Supported on: Supported on: Supported on: Supported on: Supported on: At least Windows Vista Image: Supported on: Supported on: Sup	ent
	Extension ()	nded	

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.

	Group F	olicy Manage	ment Editor		_ 0 ×
File Action View Help			Allow E	Basic authentication	
File Action View Help	Allow Basic auth Not Configured Enabled Disabled Options:	contraction Comment: Supported on:	Allow I	Basic authentication	
Windows Mail Hindows Mail Windows Media Center Windows Media Center Windows Media Player Windows Media Player Windows Remote Management (WinRM) WinRM Service Windows Remote Shell Windows Plate Plain Work Folders Work Folders Work Folders Work Service Work Service Work Folders Work Folders Estended Work Folders Ver Configuration Policies V				Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service accepts 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.	

- 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							
File Action View Help	Allow remote server management through WinRM -						
	Allow remote server management through WinRM Previous Satting Next Satting						
Smart Card Sound Recorder Syncy our settings b Tablet PC Task Scheduler Windows Calor System Windows Calor System Windows Customer Experience Improvement F b Windows Customer Experience Improvement F b Windows Intalier Windows Intalier Windows Mail Windows Mail Windows Mail Windows Media Digital Rights Management Windows Remote Management (WinRM) Windows Remote Shell Workplace Join Workplace Join Workplace Join Workplace Join Deploices Workplace Join Deploices Workplace Join Management (WinRM) Windows Remote Management (WinRM) Windows Remote Shell Windows Remote Shell Windows Remote Shell Window	Common relinde seven handsgeliet unough withow Previous Secting Next Setting Image: Common relinder seven handsgeliet unough withow ment Image: Common relinder seven handsgeliet unough withow Image: Common relinder seven handsgeliet unough withow ment Image: Common relinder seven handsgeliet unough withow Image: Common relinder seven handsgeliet unough withow Mext Setting Image: Common relinder seven handsgeliet unough withow Image: Common relinder seven handsgeliet unough withow Mext Setting allows you to manage whether the Windows Image: Common relinder seven handsgeliet unough withow Image: Common relinder seven handsgeliet unough withow Mext Setting allows you to manage whether the Windows Image: Common relinder seven handsgeliet unough with seven handsgeliet unough with the relinder severent and the relinder seven handsgeliet unout						
10 setting(s)							

36. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Preferences > Windows Settings > Registry. In the right panel, right-click and select New > Registry ltem.

	Group Poli	licy Management Editor			- 0	X
File Action View Help						
🗢 🧼 🙍 📰 📋 🗰 🗟 🗟 📷 🙆 🛇 🔸						
 WinRM Points (TL0128-2-OC-01.MSTL01282LOCAL) Policy Computer Configuration Policies Windows Settings Windows Settings Preferences Windows Settings Files Folders In Files Registry Network Shares Shortcuts Policies Sontcuts Policies Preferences 	Processing (*) Processing (*) Proces	Name Order	Action Hive There are no iter Tasks + te tesh w + up lcons p	Key ms to show in this view. Registry Item Collection Item Registry Wizard	Value Name	Тур
< III >	Preferences (Extended) Standard	1/				
Add a new registry item	111	·				

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

J.	Group Policy Management	Editor		- 0	x
File Action View Help					
🗢 🔿 🙍 🛅 🗎 🗰 🕢 🔂 🖬					
 WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Computer Configuration Software Settings Software Settings Software Settings Preferences Windows Settings Environment Fielders Init Files Registry Network Shares Sontrol Sanel Settings Sontrol Sanel Settings Sontrol Sanel Settings Policies Preferences 	Registry New Registry Properti General Common Action: Create Hive: HEEY_LOCAL_MACHINE Key Path: SOFTWARE/Microsoft/Window Value name Default LocalAccountTokenFilterPolicy Value type: REG_DWORD Value data: 1 OK Cancel A	S X Hive re are no items y y y CurrentVersio ↓ Base O Hexadecimal ● Decimal III	Key s to show in this view.	Value Name	Тур
< III >	eferences / Extended / Standard /				
registry					

- Action. Select Create.
- Hive. Select HKEY_LOCAL_MACHINE.
- Key Path. Enter "SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system".
- Value name. Enter "WinRS!MaxConcurrentUsers".
- Value type. Enter "REG DWORD".
- Value data. Enter "1".
- Base. Select Decimal.
- 38. Click the **[OK]** button.
- 39. Repeat steps 36-38 to make an additional registry change to the local account. In the **New Registry Properties** modal page, edit the following values:

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\Policies\Microsoft\Windows\WinRM\Service\".
- Value name. Enter "LocalAccountTokenFilterPolicy".
- Value type. Enter "REG_DWORD".

- Value data. Enter "1".
- **Base**. Select Decimal.
- 40. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Preferences > Control Panel Settings > Services. In the right panel, right-click and select New > Service.

	Group Pol	licy Management Editor				- 0 ×
ile Action View Help						
• 🔿 🚈 📋 👼 🍳 🔂 🖬 🙆 🛇 🕈						
 WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Windows Settings ■ Software Settings ■ Windows Settings ■ Windows Settings ■ Windows Settings ■ Outros Data Sources ■ Data Sources ■ Data Sources ■ Data Sources ■ Solutions ■ Control Panel Settings ■ Control Panel Settings ■ Sources ■ Data Sources ■ Data Sources ■ Data Sources ■ Data Sources ■ Data Sources ■ Polices ■ Sources ■ Sources ■ Policies 	Services Processing Original States No policies selected	Name Order New All Tasks Paste Refresh View Arange Ic. Line up Icc Help	Action There a	Startup Account re no items to show in th Service	Interactive his view.	Recovery

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

	Group Policy Management Editor	- 0 x
File Action View Help		
 WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Computer Configuration Policies Software Settings Software Settings Preferences Preferences Policies Policies Policies Software Settings Control Panel Settings Control Panel Settings Control Panel Settings Devices Policies Software Options Policies Policies Preferences 	Service Properties Startup Account Interactive Rec re are no items to show in this view. re are no items to show in this view.	overy
	Preferences / Extended / Standard /	
Jervices		

• Startup. Select No change.

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

File Action View Help	J.	Group Policy Management Editor	- 0 ×
WinRM Policy (TU012R2-DC-01.MSTL012R2.LOCAL) Policy Policies Postfundows Settings Postfundows Settings Postfundows Settings Power Options Policies Polici	File Action View Help		
< III > Preferences / Extended > Standard /	 WinRM Policy (TL012R2-DC-01.MSTL012R2L0CAL) Policy Computer Configuration Software Settings Software Settings Software Settings Preferences Windows Settings Control Panel Settings Control Panel Settings Data Sources Devices Incel Users and Groups Incel Users and Groups Scheduled Tasks Services Services Services Services Policies Preferences Preferences Preferences Preferences Retwork Options Retwork Options Network Options Scheduled Tasks Services Policies Preferences 	Pr New Service Properties Startup Account Interactive Recover General Recovery Common set the computer's response if this service fails. First failure: Restart the Service v Subsequent failure: Restart the Service v Subsequent failure: Restart the Service v Restart fail count after: 0 days Restart Service after: 1 minutes Program:	
	< III >	Preferences / Extended / Standard /	

- First failure. Select Restart the Service.
- Second failure. Select Restart the Service.
- Subsequent failures. Select Restart the Service.
- Restart fail count after. Select 0 days.
- **Restart service after**. Select 1 minute.
- 43. Click the **[OK]** button.

44. To enforce your group policy, in the left panel of the Group Policy Management Editor page, navigate to Forest > Domains > [your local domain] > PowerShell Remote Management Policy. In the PowerShell Remote Management Policy panel on the right, right-click the local domain name under The following sites, domains, and OUs are linked to this GPO and select Enforced.

Group Policy Management	_ 0 ×
	_ 8 ×
Down Shell Remote Management Policy Scope Datails Settings Delegation Links Display links in this location: MSTL012R2.local The following attes, domains, and OUs are linked to this GPO: Location Enforced MSTL012R2.local No Yes MSTL012R2.local Link Enabled Delete Link(s)	×)
Security Filtering The settings in this GPO can only apply to the following groupsusers, and computers: Name Add Remove Propeties WMI Filtering The Set To be linked to the following WMI filter: chones V Open	
	Group Policy Management PowerShell Remote Management Policy Score Details Setting: Delegation Unix Data Setting: Delegation Unix Data Setting: Delegation Unix Data Setting: Delegation Unix MSTED12R2/scal The following stea, domains, and OUs are linked to this GPO: Location Enforced Intering The settings in this GPO can only apply to the following groups, users, and computers: None Add Properties WIN Filtering The settings in this GPO can only apply to the following groups, users, and computers: None Add Properties V Open

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

			Group Policy Man	igement		- 0 ×
📓 File Action View Windo	w Help					_ # ×
🗢 🔿 🖄 🛅 🖏 🗂 🗙	G 🖬 🖬					
Group Policy Management ▲ A Forest: MSTU012R2.local ▲ ➡ ▲ ➡ MSTU012R2.local ↓ ➡ ↓ ➡ Default Domain Policy ↓ ➡ ↓ ➡		WinRM Person Scope Der Der Uinks Display links The following	bilcy talls Settings Delegation Status in this location: MSTL012R2.local g sites, domains, and OUs are linked to this GPO:			v]
 ₩inRM Policy Image: Domain Controllers Image: Oroup Policy Objects Image: Oroup Policy Objects Default Domain C Image: Default Domain P Image: PowerShell Remo 	lers ijects ain Controllers Policy ain Policy ermote Management Polic v	Location	Erforced 112R2.local No	ink Enabled /es	Path MSTL012R2.local	
WinRM S	Edit					
WMI Filters	GPO Status	► ✓	Enabled			
 Starter GPOs Sites Group Policy Mode Group Policy Result 	Back Up Restore from Backup Import Settings Save Report	-Juer	User Configuration Settings Disabled Computer Configuration Settings Disabled All Settings Disabled	computers:		
	View New Window from Here	٠				
	Copy Delete Rename Refresh	Add	d Properties			
	Help	lter O is	r ing s linked to the following WMI filter:			
		<none></none>	¥	Open		
<	>					
All settings enabled						

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.

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

- Configure a user account that SL1 will use to connect to the proxy server and the proxy server will use to connect to the target server. The user account can either be a local account or an Active Directory account; however, the user account must have the same credentials on the target and proxy servers and be in the Local Administrator's group on both servers.
- 2. If you have created a local user account on the Windows Server instead of an Active Directory account, you must configure encrypted communication between SL1 and the Windows server. To do this, you must configure a Server Authentication certificate.
- 3. Configure Windows Remote Management on the target server and the proxy server.
- 4. Log in to the proxy server as an administrator.
- 5. Open the PowerShell command window.
- 6. Right-click on the PowerShell icon in the taskbar and select Run as Administrator.
- 7. Execute one of the following commands on the proxy server to allow the proxy server to trust one or more target servers:
 - To allow the proxy server to trust all servers (not recommended), execute the following command: Set-Item WSMan:\Localhost\Client\TrustedHosts -value *
 - To allow the proxy server to trust only specific target servers, execute the following command, inserting a list that includes the IP address for each target server. Separate the list of IP addresses with commas.

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

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

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

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

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

Step 5: 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.

Chapter

4

SNMP and PowerShell 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).

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

SNMP Dynamic Applications for Windows Devices	72
PowerShell Dynamic Applications	72
Microsoft: Active Directory Server	72
Microsoft: DHCP Server	73
Microsoft: DNS Server	73
Microsoft: Exchange Server	74
Microsoft: Exchange Server 2010	74
Microsoft: Hyper-V Server	75
Microsoft: IIS Server	76
Microsoft: Lync Server 2010	76
Microsoft: SharePoint Server	77
Microsoft: Skype for Business	77
Microsoft: SQL Server	78

	Microsoft: Windows Server	. 79
	Microsoft: Windows Server Event Logs	. 80
	Microsoft: Windows Server Services	.82
	Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows Servers	82
	Error Messages for PowerShell Collection	.82
Re	lationships with Other Types of Component Devices	.84

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 Server Performance

Microsoft: DNS Server

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2008 R2, 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 2008 R2, 2012, and 2012 R2.

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 2008, 2012, 2014, and 2016.

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

- Microsoft: SQL 2008 Buffer Pages Performance
- 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 2008 R2, 2012, 2012 R2, and 2016, 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, which uses PowerShell requests to collect data, can be used to collect journal data from Windows servers:

• Microsoft: Windows Server Process List

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

• Microsoft: Windows Server DCM+R Relationship

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 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> roperties	<u>Collections</u> Presentations	<u>S</u> nippets <u>T</u>	hresholds <u>A</u> lerts	Subscribers	
Dynamic Applications [1662] I Snippet Edito	r & Registry Editing Snippet [2025]				Guide Reset
Snippet Name Get Security Event Log Entries	[Enabled]	Active State Snippet Code	▼ [Requ	Required uired - Stop Collection]	T
EVENT_ID_FILTER_INCLUDE_II # Add the list of Event ID # Example: the list of cod # return events w # EVENT_ID_FILTER_INCLUDE_I	<pre>ST = ["9003,1000,1004"] s you wish to filter on to th s below will cause the filte here those Event IDs are a ma .IST = [9003,1000,1004]</pre>	is list. r to only tch.			Î
EVENT TYPE FILTER INCLUDE _ # Add the list of Event Tyy # following values are sup # - "Security Audit Succes: # - "Security Audit Failurd # Examples: # EVENT TYPE FILTER INCLUDD # EVENT TYPE FILTER INCLUDD	<pre>LIST = ["Security Audit Failu tes you wish to filter on to onrted: " " " LIST = ["Security Audit Fai LIST = ["Security Audit Suc</pre>	re"] this list. The lure"] cess", "Security A	udit Failure"]		
EVENT MSG_FILTER_INCLUDE L: # Add the list of Event De: # Use entire description in # Examples: # EVENT_MSG_FILTER_INCLUDE # EVENT_MSG_FILTER_INCLUDE # ["An account was logged of	IST = ["An account was logged criptions you wish to filter i filter or use the * wildcar LIST = ["An account was logg LIST = "Shell Hardware Detec	off."] on to this list. d character for pa ed off."] tion service*"]	rtial description fi	lters.	
EVENT_SRC_FILTER_INCLUDE_L: # Add the list of Event Pro # Supports the use of the " # Evamples.	<pre>ST = ["WinLogin"] wider Names you wish to filt ' wildcard character.</pre>	er on to this list			÷
		Save Save As			
Snippet Registry	Snippet Name		State	Required ID	Date Edit
1. 🌽 Get Security Event Log Entries			Enable	d Required snip_2025 :	2020-01-31 12:39:57 💣

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2008 R2, 2012, and 2012 R2.

The following PowerShell Dynamic Applications can be used to collect configuration data from a Windows server about each Windows Service running on the Windows server:

• Microsoft: Windows Server Service Configuration

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)

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

Error Message	Possible Issue(s)
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
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 SNMP and PowerShell Credentials 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 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, as well as how to discover component devices on Hyper-V systems:

Creating an SNMP Credential	
Creating an SNMP Credential in the SL1 Classic User Interface	
Creating a PowerShell Credential	91
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	
Discovering Component Devices on Hyper-V Systems	
Viewing Component Devices	
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:

Name*				Credential Tester	
All Organizations	nization manages this service?	~	Timeout (ms) 1500	Select Credential Test	
CHIMMAN	Path Paradan			Select Collector CUG1 AsimovSandboxCU1: 10.2.25.101	
SNMP V2	× 1	161		IP or Mostourne to test "	
SNMP Community (Read-Only)		SNIMP Community (Read/Write)			Test Cre

- 3. Supply values in the following fields:
 - Name. Name of the credential. Can be any combination of alphanumeric characters.
 - 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.
 - *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.
 - **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
- 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).

Cree	dential Management Credentials	Found [62]											A	ctions	Reset	Guide
													C1	a ata SI	MP Credenti	al.
			RO	RW	DA								01			
	Profile Name *	Organization	Use	Use	Use	Type	Credential User		Host	Port	Timeout (ms)	ID	Last	eate Di	alabase credi	anuar
													AI Cr	eate S(DAP/XML Hos	t Credential
1.	Amazon Web Services Credential	🚯 System				SOAP/XML Host	[AWS Account Access	example.com		80	2000	1	2015-05-18 Cr	eate Ll	DAP/AD Crede	ential
2.	Azure Credential - SOAP/XML	🚯 [all orgs]				SOAP/XML Host	<ad_user></ad_user>	login.windows.net		443	60000	60	2015-05-14 Cr	eate Ba	asic/Snippet C	Credential
3.	Azure Credential - SSH/Key	👔 [all orgs]				SSH/Key	<subscription_id_h< td=""><td>%D</td><td></td><td>22</td><td>180000</td><td>59</td><td>2015-05-14 Or</td><td>eate S!</td><td>SH/Key Crede</td><td>ntial</td></subscription_id_h<>	%D		22	180000	59	2015-05-14 Or	eate S!	SH/Key Crede	ntial
4.	Cisco SNMPv2 - Example	🙀 [all orgs]				SNMP				161	1500	3	2015-05-14	a al a D	www.chall.Cra	
5.	Cisco SNMPv3 - Example	🙀 (all orgs)				SNMP	[USER_GOES_HERE]			161	1500	2	2015-05-14	eate Ft	owershell Cre	dential
6.	ACISCO: ACI	🙀 [all orgs]			126	Basic/Snippet	admin	173.36.219.46		443	0	62	2015-05-14 15:0	5:24	em7admin	
7.	A Cisco: ACI Credential	🙀 [all orgs]				Basic/Snippet	admin	198.18.133.200		443	0	61	2015-05-14 14:3	2:20	em7admin	
8.	A Cloudkick - Example	🙀 (all orgs)				Basic/Snippet	[SECURITY KEY GOES	127.0.0.1		443	5000	9	2015-05-14 11:2	5:31	em7admin	
9.	CUCM PerfmonService 8.0 Example	[all orgs]				SOAP/XML Host		%D		8443	2000	4	2015-05-14 11:2	5:12	em7admin	
10.	A EM7 Central Database	🙀 [all orgs]				Database	root	localhost		7706	0	51	2015-05-14 11:2	6:41	em7admin	
11.	A EM7 Collector Database	🙀 [all orgs]				Database	root	%D		7707	0	14	2015-05-14 11:2	5:43	em7admin	
12.	A EM7 DB	🙀 [all orgs]				Database	root	%D		7706	0	35	2015-05-14 11:2	6:32	em7admin	
13.	A EM7 DB - DB Info	🙀 (all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 11:2	6:32	em7admin	
14.	A EM7 DB - My.cnf	🙀 [all orgs]				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 11:2	6:32	em7admin	
15.	A EM7 DB - Silo.conf	🙀 [all orgs]				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 11:2	6:32	em7admin	
16.	A EM7 Default V2	🙀 [all orgs]				SNMP				161	1500	10	2015-05-14 11:2	5:42	em7admin	
17.	A EM7 Default V3	🙀 [all orgs]				SNMP	em7defaultv3			161	500	11	2015-05-14 11:2	5:42	em7admin	
18.	A EMC - Example	🙀 [all orgs]				Basic/Snippet	root	%D		443	10000	15	2015-05-14 11:2	5:47	em7admin	
19.	A GoGrid - Example	🙀 (all orgs)				Basic/Snippet	[SECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 11:2	5:51	em7admin	
20.	JPSLA Example	📸 [all orgs]				SNMP				161	1500	5	2015-05-14 11:2	5:14	em7admin	
21.	LifeSize: Endpoint SNMP	🙀 [all orgs]				SNMP	control			161	3000	18	2015-05-14 11:2	5:58	em7admin	
22.	A LifeSize: Endpoint SSH/CLI	🙀 [all orgs]				Basic/Snippet	auto	%D		22	3	17	2015-05-14 11:2	5:58	em7admin	
23.	🔑 Local API	🙀 [all orgs]				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 11:2	6:11	em7admin	
24.	A NetApp 7-mode	🙀 [all orgs]				Basic/Snippet	root	%D		443	3000	24	2015-05-14 11:2	6:20	em7admin	
25.	A NetApp w/SSL Option	🙀 (all orgs)				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 11:2	6:20	em7admin	
26.	NetApp w/SSL Option Off	🙀 [all orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 11:2	6:20	em7admin	
27.	A Nexus netconf	🙀 [all orgs]				Basic/Snippet		%D		22	10000	6	2015-05-14 11:2	5:16	em7admin	
28.	An Nexus snmp	🙀 [all orgs]				SNMP				161	10000	7	2015-05-14 11:2	5:16	em7admin	
29.	Advanced - Advanced	📸 [all orgs]				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 11:2	6:24	em7admin	
30.	A Polycom - CDR	🙀 [all orgs]				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 11:2	6:24	em7admin	
31.	A Polycom - Interface	👔 [all orgs]				SOAP/XML Host	admin	%D		80	20000	29	2015-05-14 11:2	6:24	em7admin	
[View	ing Page: 1]												[Select Action	1]		Go

2. Click the [Actions] button and select Create SNMP Credential. The Credential Editor page appears.

Credential Editor		×
Create New SNMP Credential		Reset
Basic Settings Profil	e Name	SNMP Version
Port 161	Timeout(ms)	Retries
SNMP V1/V2 Settings SNMP Community (Read	Only)	SNMP Community (Read/Write)
SNMP V3 Settings Security Name	Secu	rity Passphrase
Authentication Protocol	Security Level	SNMP v3 Engine ID
Context Name	Privacy Protocol	Privacy Protocol Pass Phrase
	Save	

- 3. Supply values in the following fields:
 - Profile Name. Name of the credential. Can be any combination of alphanumeric characters.
 - **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*.

- *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
- 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 an SSH/Key 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:

				Credential Tester	
All Organizations 💶 What organi	ization manages this service?		Timeout (ma) 1500	Select Credential Test	
				Select Collector CUG1 AsimovSandboxCU1: 10.2.25.101	
Account type Active Directory	v	Encrypted	-		
				IP or Hostname to test "	
Username "		Password *			Test Cred
		Port*			
riostname/ IP		3763			
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.
 - 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.
 - *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.
 - You can include the variable **%D** in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
 - You can include the variable **%N** in this field. SL1 will replace the variable with the hostname of the device that is currently using the credential. If SL1 cannot determine the hostname, SL1 will replace the variable with the primary, management IP address for the current device.
 - You can include the prefix HOST or WSMAN before the variable %D in this field if the device you want to monitor uses a service principal name (for example, "HOST://%D" or "WSMAN://%D").
 SL1 will use the WinRM service HOST or WSMan instead of HTTP and replace the variable with the IP address of the device that is currently using the credential.
- **Username**. Type the username for an account on the Windows device to be monitored or on the proxy server.

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

- **Password**. Type the password for the account on the Windows device to be monitored or on the proxy server.
- Encrypted. Select whether SL1 will communicate with the device using an encrypted connection:
 - Toggle on (blue) if SL1 will communicate with the device using an encrypted connection. If the connection is encrypted, 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.
 - Toggle off (gray) if the connection is not encrypted. If the connection is not encrypted, 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.
- **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.

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.

0																
Cle	benual management Credentials Fo	ouna (ozj												tions Rese	t Guide	
													Cre	ate SNMP Cred		
	Deefle Manue -	Orrentiation	RO	RW	DA		Constantial Users		March .	0	Times and (see)	10	Cre	ate Database C		
	Prome marrie	Organization	0.50	0.50	030	TAbe	Credendar Oser		109		Timeout (ms)	<u> </u>	Cre	ate SOAP/XML	Host Credentia	al
	O Amazara Web Caminas Candential	A Custom	_			COADIVAL Hand	FAIAN Assessed Assessed	an anna la anna		80	2000	4	2026.06.45	ate I DAP/AD C	redential	
	A Anna Credential SO ARIVAL	A [a] oran]				SOAP/ANE Host	AD LICEDS	look windows net		442	2000	60	2015-05-14 01-		- Condential	
2	A Azura Cradential SCHWay	(al orga)				COMP/INTE TIOST	CURSCRIPTION ID H	e n		22	120000	60	2010-00-14	rate basic/onipp	er Credential	
4	A Circo ShiMDy2 - Example	an (all orge)				SNMD	SODSCRIPTION_ID_I	10		161	1500	3	2015-05 Cre	rate SSH/Key Cr	edential	
ŝ	Q Cisco SNMPv3 - Example	(al orgs)				SNMP	IUSER GOES HEREI			161	1500	2	2015-05- Cre	ate PowerShell	Credential	
6	A Cisco: ACI	(al oros)			126	Basic/Spinnet	admin	173 36 219 46		443	0	- 62	2015-05-14 15:05	24 em7admin		
7	A Cisco: ACI Credential	a [all orgs]				Basic/Snippet	admin	198 18 133 200		443	0	61	2015-05-14 14:32	20 em7admin	- i	
8.	Cloudkick - Example	a [al orgs]				Basic/Snippet	ISECURITY KEY GOES	127.0.0.1		443	5000	9	2015-05-14 11:25	31 em7admin		
9.	Q CUCM PerfmonService 8.0 Example	at [all orgs]				SOAP/XML Host		%D		8443	2000	4	2015-05-14 11:25	:12 em7admin	- iii	
10.	P EM7 Central Database	a [all orgs]				Database	root	localhost		7706	0	51	2015-05-14 11:26	3:41 em7admin		
11.	A EM7 Collector Database	(all orgs)				Database	root	%D		7707	0	14	2015-05-14 11:25	3:43 em7admin	Ū	
12.	A EM7 DB	all orgs]				Database	root	%D		7706	0	35	2015-05-14 11:26	3:32 em7admin		
13.	PEM7 DB - DB Info	(all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 11:26	3:32 em7admin		
14.	PEM7 DB - My.cnf	🚯 [all orgs]				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 11:26	3:32 em7admin		
15.	A EM7 DB - Silo.conf	(all orgs)				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 11:26	3:32 em7admin		
16.	PEM7 Default V2	🙀 [all orgs]				SNMP				161	1500	10	2015-05-14 11:25	5:42 em7admin		
17.	PEM7 Default V3	(all orgs)				SNMP	em7defaultv3			161	500	11	2015-05-14 11:25	5:42 em7admin		
18.	A EMC - Example	🚯 [all orgs]				Basic/Snippet	root	%D		443	10000	15	2015-05-14 11:25	5:47 em7admin		
19.	A GoGrid - Example	[all orgs]				Basic/Snippet	[SECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 11:25	5:51 em7admin		
20.	A IPSLA Example	📸 (all orgs)				SNMP	-		-	161	1500	5	2015-05-14 11:25	5:14 em7admin		
21.	PLIfeSize: Endpoint SNMP	🚯 [all orgs]				SNMP	control			161	3000	18	2015-05-14 11:25	5:58 em7admin		
22.	A LifeSize: Endpoint SSH/CLI	🙀 [all orgs]				Basic/Snippet	auto	%D		22	3	17	2015-05-14 11:25	5:58 em7admin		
23.	A Local API	🙀 [all orgs]				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 11:26	8:11 em7admin		
24.	An NetApp 7-mode	🙀 [all orgs]				Basic/Snippet	root	%D		443	3000	24	2015-05-14 11:26	5:20 em7admin		
25.	A NetApp w/SSL Option	🚯 [all orgs]				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 11:26	5:20 em7admin		
26.	A NetApp w/SSL Option Off	🙀 [all orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 11:26	3:20 em7admin		
27.	A Nexus netconf	[all orgs]				Basic/Snippet		%D		22	10000	6	2015-05-14 11:25	5:16 em7admin		
28.	P Nexus snmp	🐞 [all orgs]				SNMP	-			161	10000	7	2015-05-14 11:25	5:16 em7admin		
29.	A Polycom - Advanced	[all orgs]				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 11:26	24 em7admin		1
30.	Polycom - CDR	(all orgs)				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 11:26	s:24 em7admin		1
31.	w Porycom - Interface	an orgsj				SUAPIXML Host	aomn	20		00	20000	29	2015-05-14 11:26	em7admin		1
[View	ing Page: 1] V												[Select Action]]	Go	

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

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

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

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

- **Encrypted**. Select whether SL1 will communicate with the device using an encrypted connection. Choices are:
 - yes. When communicating with the Windows server, SL1 will use a local user account with authentication of type "Basic Auth". You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate.
 - *n*o. When communicating with the Windows server, SL1 will not encrypt the connection.

- **Port**. Type the port number used by the WinRM service on the Windows device. This field is automatically populated with the default port based on the value you selected in the **Encrypted** field.
- Account Type. Type of authentication for the username and password in this credential. Choices are:
 - Active Directory. On the Windows device, Active Directory will authenticate the username and password in this credential.
 - Local. Local security on the Windows device will authenticate the username and password in this credential.
- *Timeout (ms)*. Type the time, in milliseconds, after which SL1 will stop trying to collect data from the authenticating server. For collection to be successful, SL1 must connect to the authenticating server, execute the PowerShell command, and receive a response within the amount of time specified in this field.
- **Password**. Type the password for the account on the Windows device to be monitored or on the proxy server.
- **PowerShell Proxy Hostname/IP**. If you use a proxy server in front of the Windows devices you want to communicate with, type the fully-qualified domain name or the IP address of the proxy server in this field.
- Active Directory Hostname/IP. If you selected Active Directory in the Account Type field, type the hostname or IP address of the Active Directory server that will authenticate the credential.
- **Domain**. If you selected Active Directory in the **Account Type** field, type the domain where the monitored Windows device resides.
- 5. To save the credential, click the **[Save]** button. To clear the values you set, click the **[Reset]** button.

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. Do one of the following:
 - Click the [Test Credentials] button, or
 - 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:

Т	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 d IRI Request	Check to see if a cl IRI request succeeds	cl IRI 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".

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:

Т	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 IRL Request	Check to see if a cl IRI request succeeds	cl IRI 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:

Credential Tester [BETA] X				
Test Type	[SNMP Credential Test]			
Credential	EM7 Default V2			
Hostname/IP				
Collector	em7ao ·			
Run Test				

- 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:

Test Credential Test execution complete							
	Step	Description	Log Message	Status			
1	Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 0.397ms	Passed 😯			
2	Test Port Availability	Check to see if the SNMP port is open	Port 161 is open	Passed 😯			
3	Test SNMP Availability	Check to see if a walk of SNMP will return results	The SNMP SysName is ScienceLogic EM7 G3 - All-In-One	Passed 😯			

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 (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.

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 (+):



• 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 (^J).
- 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



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 reduces 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.

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 the menu options, click the Advanced menu icon ($\overset{ astack{w}}{}$).

This chapter covers the following topics:

Prerequisites	103
Scope	104
Enabling and Disabling Concurrent PowerShell for Collector Groups	104
The SL1: Concurrent PowerShell Monitoring PowerPack	106
Scale Recommendations	108

Prerequisites

The following prerequisites are required to use concurrent PowerShell collection:

- SL1 version 10.2.0 or greater
- Microsoft: Windows Server PowerPack version 110 or greater
- SL1: Concurrent PowerShell Monitoring PowerPack version 100 or greater

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

NOTE: To enable and receive SL1 events related to concurrent PowerShell, you will need to install the *SL1*: Concurrent PowerShell Monitor PowerPack.

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: 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 which happen to run PowerShell commands.

Enabling Concurrent PowerShell on All Collector Groups

To enable concurrent PowerShell collection service for all collector groups:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. Enter the following in the **SQL Query** field:

```
INSERT INTO master.system_custom_config (`field`, `field_value`) VALUES ('enable_
powershell_service', '1');
```

Disabling Concurrent PowerShell on All Collector Groups

To disable concurrent PowerShell collection service for all collector groups:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. Enter the following in the **SQL Query** field:

```
UPDATE master.system_custom_config SET field_value=0 where field='enable_powershell_
service';
```

Enabling Concurrent PowerShell on a Specific Collector Group

To enable concurrent PowerShell collection for a specific collector group:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. Enter the following in the SQL Query field:

```
INSERT INTO master.system_custom_config (`field`, `field_value`, `cug_filter`)
VALUES ('enable powershell service CUGx', '1', 'collector group ID');
```

where:

collector_group_ID is the collector group ID. You can find this value in the **Collector Group Management** page (System > Settings > Collector Groups).

Disabling Concurrent PowerShell on a Specific Collector Group

To disable concurrent PowerShell collection for a specific collector group:

- 1. Go to the **Database Tool** page (System > Tools > DB Tool).
- 2. Enter the following in the **SQL Query** field:

```
UPDATE master.system_custom_config SET field_value=0 where field='enable_powershell_
service_CUGx';
```

where:

collector_group_ID is the collector group ID. You can find this value in the **Collector Group Management** page (System > Settings > Collector Groups).

The SL1: Concurrent PowerShell Monitoring PowerPack

The *SL1*: Concurrent PowerShell Monitoring PowerPack includes a device template and two Dynamic Applications that use SSH to monitor collectors with concurrent PowerShell enabled.

- 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 use to align multiple Data Collectors to the "ScienceLogic: PowerShell Service Log Parser" Dynamic Application.

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.

Credential Editor			×		
Create New SSH/Key Credential			Reset		
Basic Settings Credential Name					
Hostname/IP	Port	Timeout(ms)			
Username Password					
Private Key (PEM Format)					
		/			
	Save				

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.

Configuring the Device Template

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

To configure the device template:

- 1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
- 2. Locate the "SL1: Concurrent PowerShell Monitoring" sample template and click its wrench icon (***). 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. Selec the device template that you created.
 - Log All. Select this checkbox.
- 4. Click the [Save] button to save the discovery session. Close the Discovery Session Editor page.
- 5. In the **Discovery Control Panel** page, click the **[Reset]** button. The new discovery session will appear in the **Session Register** pane.



7. 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.

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

- Limit the use of the "Microsoft: Windows Server Services" PowerPack, as using this Dynamic Application can reduce the number of servers a collector can support by 40%. If you do use this PowerPack, consider slowing down the **Poll Frequency** of the "Microsoft: Windows Server Services" Dynamic Application.
- 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

7

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 (三).

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:

What is an SL1 Agent?	110
Agent-Compatible PowerPacks	111
The Credential for the SL1 Agent	111
Configuring the SL1 Agent Device Template	112

What is an SL1 Agent?

The *SL1 agent* is a program that you can install on a device monitored by SL1. The SL1 agent collects data from the device and pushes that data back to SL1.

Similar to a Data Collector or Message Collector, the SL1 Agent collects data about infrastructure and applications.

The agent can be configured to communicate with either the Message Collector or Compute Cluster.

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
 - 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), or the **Credential Management** page (System > Manage > Credentials) in the SL1 classic user interface:

Name" SL1 Agent PowerShell Default		Credential Tester	
All Organizations What organization manages this service?	V 10000	Select Credential Test	
		Select Collector	
Account Type		CUG em7aio17: 10.64.68.17	
Local	~		
Hostname/IP*		IP or Hostname to test*	
%D Username*			
default			
Password 1			
Encrypted			
Port*		L2	
5985			
PowerShell Proxy Hostname/IP			
Active Directory Host/IP			
Active Directory Domain			
	Save & Test		

Credential Editor [102]	
Edit PowerShell Credential #102	New Reset
Basic Settings	
Profile Name	Account Type
SL1 Agent PowerShell Default	[Local]
Hostname/IP	Timeout(ms)
%D	10000
Username	Password
testLocalPowershell	
Encrypted Port	PowerShell Proxy Hostname/IP
Active Directory Settings Active Directory Hostname/IP	Domain
Save Save As	

Configuring the SL1 Agent Device Template

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:

Template Name SL1 Agent for Microsoft: Windows Server Template	
Config Interface CV Policies Port Policies Svc Policies Proc Policies Dyn Apps	Logs
Subtemplate Selection Template Application Behavior Align Dynamic Application With 1. App: Microsoft: Windows Server B Image: Microsoft: Windows Server C App: Microsoft: Windows Server C 3. App: Microsoft: Windows Server D Image: Microsoft: Windows Server D Image: Microsoft: Windows Server D 6. App: Microsoft: Windows Server D Image: Microsoft: Windows Server D Image: Microsoft: Windows Server D 7. App: Microsoft: Windows Server D Image: Microsoft: Windows Server D Image: Microsoft: Windows Server D 8. App: Microsoft: Windows Server D Image: Microsoft: Windows Server D Image: Microsoft: Windows Server D 8. App: Microsoft: Windows Server D Image: Microsoft: Windows Server D Image: Microsoft: Windows Server D 9. App: Microsoft: Windows Server D Image: Microsoft: Windows Server M Image: Microsoft: Windows Server M 1. App: Microsoft: Windows Server M Image: Microsoft: Windows Server M Image: Microsoft: Windows Server M 1. App: Microsoft: Windows Server M Image: Microsoft: Windows Server M Image: Microsoft: Windows Server M 1. App: Microsoft: Windows Server M Image: Microsoft: Windows Server M Image: Microsoft: Windows Server M 1. App: Microsoft: Windows Server M Image: Microsoft: Windows Server M Imadware Make Imabled V	▼ ▼ ê ▼

- 5. 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.
- 6. Click [Save].

Chapter



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 the menu options, click the Advanced menu icon ($\overset{ astack{weightarrow}}{ astack{weightarrow}}$).

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

Installing the Microsoft Server Dashboards	
Microsoft: Active Directory Server Performance	
Microsoft: DNS Server Performance	
Microsoft: Exchange Server 2010 Performance	
Microsoft: Exchange Server 2013 Performance	
Microsoft: IIS Server Performance	
Microsoft: Lync Server 2010 Dashboards	
Microsoft: Lync Server 2010 Performance	
Microsoft: Lync Server 2010 Utilization	
Microsoft: Skype for Business Dashboards	
Microsoft: Lync Server 2013 Performance	
Microsoft: Lync Server 2013 Utilization	
Microsoft: SQL Server Performance	141

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.

ano	uted PowerPacks™ I PowerPack	Files I	Found	[208]				Reset
hþo		i neo i	ound	[200]				
	PowerPack Name	Version	Revisio n	GUID	Last Edite	d	Imported •	
					All	All	•	_
1.	Event Association Test	1	1	DED1884762194566B70BCD4DF3A7422	2015-12-16 09	:43:07 2015	5-12-16 09:43:00	1
2.	Event Suppression Test	1	1	EC64565DCA55E155135F91F81F44D8-2	2015-12-09 07	:44:17 2015	5-12-09 07:44:12	1
3.	SLPSD: Onboarding	0.20000	287	E121312B60972ED35BEDA19E88D195 2	2015-11-12 12	:14:05 2015	5-11-12 12:13:50	/ [
4.	SL_PS Cisco 3rd Party Device Support	1.39999	151	8B78EDB3A373B2D187ECEAE25457442	2015-11-05 12	:17:39 2015	5-11-05 12:16:54	/ 🗆
5.	NetApp Base Pack	7.7.0	6873	8014D5DAD2B8C9AC3E1DD84CC227E2	2015-10-21 13	31:47 2015	5-10-29 14:56:55	1
6.	Cisco: Contact Center Enterprise *BETA*	0.5	1119	7CC6AD933EFB4FF5D840EFEA40F85C2	2015-12-14 13	:50:50 2015	5-10-29 14:56:54	1
7.	EM7 Standard Device Categories	7.7.0	255	7A7322AA30F189B42943C082EFD71212	2015-06-02 18	30:56 2015	5-10-29 14:56:54	1
8.	BL Test	1	2	74F7E816CF0FC9153700D2AF0982C212	2015-10-29 10	:56:112015	5-10-29 10:56:06	1
9.	BL Test	1	1	74F7E816CF0FC9153700D2AF0982C212	2015-10-29 10):56:11 <mark>20</mark> 15	5-10-29 10:54:15	1
10.	Microsoft: Office 365 *BETA*	0.5	138	8FA30F7D1FAC9162DD8C717D9EF778		2015	5-10-20 16:44:37	1
11.	NetApp Base Pack	7.7.0	6838	8014D5DAD2B8C9AC3E1DD84CC227E2	2015-10-21 13	31:47 2015	5-10-20 16:44:37	1
12.	Cisco: Contact Center Enterprise *BETA*	0.5	1109	7CC6AD933EFB4FF5D840EFEA40F85C2	2015-12-14 13	:50:50 2015	5-10-20 16:44:36	1
13.	EM7 Default Internal Events	7.7.0	316	BE1F363DB4BA9A10F5C6BC28931F0B 2	2015-10-28 13	3:26:25 2015	5-10-20 16:44:36	1
14.	F5 BIG-IP *BETA*	7.7.0	3242	BFA4E6B316FD2302D913EF38FE7FF822	2015-10-28 13	:26:27 2015	5-10-20 16:44:36	1
15.	Microsoft: Office 365 *BETA*	0.5	136	8FA30F7D1FAC9162DD8C717D9EF778		2015	5-10-14 15:12:24	/ 🗌
16.	Cisco: Contact Center Enterprise *BETA*	0.5	1022	7CC6AD933EFB4FF5D840EFEA40F85C2	2015-12-14 13	:50:50 2015	5-10-14 15:12:23	1
17.	Microsoft Base Pack	7.7.0	868	97469E96E98B5DAB516F3CCC8747CE2	2015-10-28 13	3:26:26 2015	5-10-13 12:47:54	1
18.	EM7 Default Internal Events	7.7.0	315	BE1F363DB4BA9A10F5C6BC28931F0B 2	2015-10-28 13	:26:25 2015	5-10-13 12:47:54	1
19.	NetApp Base Pack	7.7.0	6792	8014D5DAD2B8C9AC3E1DD84CC227E2	2015-10-21 13	31:47 2015	5-10-13 12:47:54	1 🗌
~~		770	0011		ID ale at A ati	00.07.0047		

4. Click the lightning-bolt icon (🖉) for the PowerPack that you want to install.

5. The Install PowerPack modal page appears. To install the PowerPack, click [Install].

nstall Power-Pack™ .kates_test_	pp_3 Version 1			Reset	
Package Information GUID: 9 Created: 2015-07-28 14	F7ECF5CBC81D713AD94AF704FBA136C 10:53 Updated: 2015-07-28 14:10:53	Revision: 2 Compile	Exported From: 7.6.0.beta d: 2015-07-28 14:12:21		
Package Content					
	Theme Name		GUID	Action	
1. kates_test_theme_3			A6D9EA56C5FAE1F35E6F0411BD79AD0	update	
kates_test_theme_4			ADA02B6763C3CCA014FBB00A9A21A64	update	
Installation Key: hBGC6WETV3SH8Epeyp7cpySyuEak0FeBpD/IYENPd0oBScXOJmVT4Z1ZfQmolbNRR/6MJw6aZOvgFY() 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 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.

Dashboards [Microsoft DNS Server Performance] New		Actions Reset Guide Pause Refresh
ैं। 111 211 411 611 <mark>1211</mark> 241	i 30 70 140 300 900	<u>Organizations Selecter</u>
Sever List	Average Latency (m)	Solite 100% 1 100% 1 <t< th=""></t<>
Overall Performance -	Recursive Queries Op7QueriesSecond Op7QueriesSecond	OBr2ent-dc: CPU — OBr2ent-dc: Memory — OBr2ent-dc: Swap Recursive Errors C07Queries/Second
3Responses/Sec 2.5Responses/Sec	0.06Queries/Second	0.06Queries/Second
2ResponsedSec	0.04Queries/Becond	0.050uenessecond
1.SResponse.Slee	0.032.ur/H1896.com 0.052.ur/H1896.com 0.012.ur/H1896.com	0 0304mins/04cond 0 0204mins/04cond 0 0704mins/04cond
0Responses/Sec12'00 14'00 16'00 18'00 20'00 22'0022'00	0Queries/Second 12'00 14'00 16'00 18'00 20'00 22'00 - Recursive Queries/Sec	- 0Queries/Second 12'00 14'00 16'00 16'00 20'00 22'00 - Recursive Query Failure/Sec - Recursive Time-Outs/Sec

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.

- 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.

Dashboards		Actions Reset Guide
[Shared: Microsoft: Lync Server 2010 Utilization] 💽 New		Pause Refresh
	Active A/ Conferences .	Connected A/ Users ·
M 1H 2H 4H 6H 12H 24H 3D 7D 14D 30D 90D Organizations Selector -		
2 organizations serected	0.06Conferences	0.06Users
Server List		
Device Name IP Address	0.04Conferences	0.04Users
9.mlms-08r2-lync 10.1.0.139	0.02Conferences	0.02Users
	0Conferences 00 10'00 12'00 14'00 16'00 18'00 20'	0Users 00 10'00 12'00 14'00 16'00 18'00 20'0
	Number of Ocertowney	Number of Learn
	- Number of Comerences	- Nomber of Osers
Active Registered Endpoints .	Active IM Conferences .	Connected IM Users ·
2Endpoints		
	0.06Conterences	0.06Users
1.5Endpoints		
	0.04Conferences	0.04Users
1Endpoints		
0.5Fe desists	0.02Conferences	0.02Users
o denapoints		
0Endpoints	0Conferences	OUsers
08:00 10:00 12:00 14:00 16:00 18:00 20	08:00 10:00 12:00 14:00 16:00 18:00 20	08:00 10:00 12:00 14:00 16:00 18:00 20:
- Endpoint Cache: Active Registered Endpoint	- Active Conferences	- Connected Users
Number of Calls	Active AS Conferences .	Connected AS Users .
1Calls		
	0.06Conferences	0.06Users
0.75Calls		
	0.04Conferences	0.04Users
0.5Calls		
	0.02Conferences	0.021 (sers
0.25Calls	VAL GATHERET COM	UNE DAVIA
0C388 8:00 10:00 12:00 14:00 16:00 18:00 20	0Conterences 00 10:00 12:00 14:00 16:00 18:00 20:	0USer88:00 10:00 12:00 14:00 16:00 18:00 20:0
- UpdateEndpoint: Number of Calls	- Active Conferences	- Connected Users

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.

Dashboarde			Actions Reset Quide
[Microsoff: Lync Server 2013 Performance]	w		Pause Refresh
₩ 1H 2H 4H 6H 12H 24H 3D 7D	14D 30D 90D <u>Organizations Selector</u> E No Organizations Selected •	Availability and Latency	System Utilization (%)
Server Lot Device Name (24miltran2-s-01	10.40.37		005 205 05 0600 0000 1200 1500
Connections Established 100Connections 25Connections 25Connections 00Connections 0Connections	000 Messages 400 Messages 5000 Messages 400 00 00 1200 0 Messages 0400 00 00 1200		SP Helsonk Errors Connections Con
Incoming Response Breakdown			Incoming Response Breakdown
1000Responses 500Responses 0Responses 04:00 00:00 12:00 	20Responses 000 000 12.00 Incoming 100 (Responses) 1000 (Responses) 1000 (Responses) Incoming 100 (Responses) 1000 (Responses) 1000 (Responses) Incoming 100 (Responses) 1000 (Responses) 1000 (Responses)	4Responses 06 0.0 0.0 12.00 Incoming 400 Responses Incoming 400 Responses Incoming 404 Responses Incoming 404 Responses Incoming 407 Responses Incoming 404 Responses Incoming 404 Responses Incoming 404 Responses	0.05Responses 0.025Responses 0.025Responses 0.000 t2:00 (400 08:00 t2:00 (400 08:00 t2:00)

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.

Post local		Antiona Dennet Outlete
Dashboards		Actions Reset Guide
[microsoli: Lynic server 2013 oblization]	Asker N/ Oschermen	
V 1H 2H 4H 6H 12H 24H 3D 7D 14D 30D 90D Organizations Selector • O No Organizations Selector • O	Active AV conferences	20Users
Server List •	15Conferences W WWWWWWWWWW	
Device Name IP Address	10Conferences	10Users
³² m [®] ti12r2-is-01 10.40.3.7 ₽	5Conferences	5Users
	0Conferences 06:00 09:00 12:00 15:00	0Users 04:00 06:00 08:00 10:00 12:00 14:00
	Number of Conferences	- Number of Users
Active Registered Endpoints .	Active IM Conferences .	Connected IM Users 1 -
100Endpoints	15Conferences	30Users
75Endpoints	10Conferences	AND AND AN ANA ANA ANA
50Endpoints	1000millioneu	
25Endpoints	SConferences	10Users
0Endpoints 06:00 09:00 12:00 15:00	0Conferences 06'00 09'00 12'00 15'00	0Users 04:00 06:00 08:00 10:00 12:00 14:00
- Endpoint Cache: Active Registered Endpoint	- Active Conferences	- Connected Users
Number of Calls •	Active AS Conferences ·	Connected AS Users ·
0.06Calls	15Conferences	
0.04Calls		
0.02Calls	SConferences	5Users
0Calls	0Conferences	OUsers
04:00 06:00 08:00 10:00 12:00 14:00	06:00 09:00 12:00 15:00	04:00 06:00 08:00 10:00 12:00 14:00

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.

Lu Sciencel ogic			Logged in as ligitison (Sign-out)
Interest Constants Views Events Teleste Views	underden Benerate Benjahr Busham Bestammer Haburah Ca	-Re Material Tallia	
Dathoute			Actions Report Guide
[Shared: Microsoft: SQL Server Performance]			Pause Refresh
		Availability and Latency -	
S 1H 2H 4H 6H 12H 24H 30 7D	140 300 900 Openizations Selector • D		976
		Average Availabilit (%)	
Custom Device Table			62%
Device Name	IP Address		
2 Main DEMOLASSO	192 168 41 105		40%
PerDemo_Lyno_2013	192.168.41.100		, MALI ALANIKA, TATATA
ACME - DB-MSSQL - WebApp	192.168.32.112	1 95 95 10 90 90 90 90 90 90 90 90 90 90 90 90 90	
ACME - DB MSSQL 2 - WebApp	192.108.32.113		
		\sim	10.00 10.00 20.00 22.00 10.301 02.00
			- CPU - Memory - Swap
Buffer Cache Hit Rado	- Average Walt Time 70µs	Deadlods O.07Deadlods/Sec	0.07Waits/Second
80%	0049	0.00Deadlooks/Sec	0.00 Warts Second
	50µs-	0.05Deadlooks/Sec	0.05Walts/Second
80%	40µs	0.04Deadloda/Sec	0.04WaltySecond
40%	3048	0.03Deadloda/Sec	0.03Waits/Second
	20µs	0.02Deadloda/Sec	0.02Waits/Second
20%	10µs	0.01Deadlook/Sec	0.01Waits/Second
16/00 18/00 20/00 22/00 10. Jan 02/00	^{10/0} 16/00 18/00 20/00 22/00 10. Jan 02/00	18:00 21:00 10. Jan 03:00	18:00 21:00 10. Jan 03:00
Buffer Cache Hit Ratio	Average Wait Time	Number of Deadlocks Per Second	Lock Waits Per Second
Catalog Cache Hit Ratio	Page Life Expectance	Transactions	Latch Waits -
100%		16Trans/Second	3Walts/Second
80%		11 Frankrund	2 Ritabilitament
	3000000Sec	12.511818384410	
60%		10Trans/Second	2Wata/Second
	2000003ec	7.5Trans/Second	1.5WaltySecond
40%			
	10000005ec	STrans'Second	1Walts/Second
20%		2.6Trans/Second	0.5Walts/Second
01	0540		(Manager Street
16:00 18:00 20:00 22:00 10. Jan 02:00	16:00 18:00 20:00 22:00 10. Jan 02:00	18:00 21:00 10 Jan 03:00	18:00 21:00 10. Jan 03:00
- Catalog Cache Hit Ratio	- Page Life Expectancy	- Transactions Per Second	- Latch Waits Per Second

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



Troubleshooting

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).

The following sections describe some of the error messages that you might see when configuring SL1 to monitor Windows devices:

Troubleshooting WinRM Error Messages	145
Debugging Code 401 Errors	
Debugging Code 500 Errors	
Troubleshooting PowerShell Error Messages	

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 <i>Errors</i> .)
	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 <i>Timeout</i> 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:
 - Ensure forward and reverse DNS are configured correctly when using Active Directory authentication:
 - # nslookup [IP address]
 - # nslookup [hostname]
 - \circ $\,$ 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 you are using Windows Server 2008, 2008r2, or below, ensure that the user you are using is an administrator. This is a Windows requirement.
- 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:

winrm set winrm/config/service `@{MaxConcurrentOperations="500"}'

• 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 - 2021, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010