

## Monitoring Windows Systems with PowerShell

SL1 version 8.14.0

## Table of Contents

Introduction	. 4
Monitoring Windows Devices in the ScienceLogic Platform	5
What is SNMP?	
What is PowerShell?	. 5
PowerPacks	
Configuring Windows Systems for Monitoring with SNMP	7
Configuring SNMP for Windows Server 2016 and Windows Server 2012	
Configuring Ping Responses	. 8
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 Windows Servers for Monitoring with PowerShell	
Prerequisites	
Configuring PowerShell	
Step 1: Configuring the User Account for the ScienceLogic Platform	
Option 1: Creating an Active Directory Account with Administrator Access	
Option 2: Creating a Local User Account with Administrator Access	
Option 3: Creating a Non-Administrator User Account	
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	
Creating a User Group and Adding a User in Active Directory	
Setting the Session Configuration Parameters and Group Permissions	
Creating a PowerShell Credential	
Optional: Configuring the User Account for Access to Windows Failover Cluster	38
Step 2: Configuring a Server Authentication Certificate	
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	
Step 3: Configuring Windows Remote Management	
Option 2: Manually Configuring Windows Remote Management	
Option 3: Using a Group Policy to Configure Windows Remote Management Step 4: Configuring a Windows Management Proxy	
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	
SNMP and PowerShell Dynamic Applications for Windows Devices	
SNMP Dynamic Applications for Windows Devices	
PowerShell Dynamic Applications	
Microsoft: Active Directory Server	
Microsoft: DHCP Server	
Microsoft: DNS Server	
Microsoft: Exchange Server	
Microsoft: Exchange Server 2010	
U -	·· -

Microsoft: Hyper-V Server	74
Microsoft: IIS Server	
Microsoft: Lync Server 2010	75
Microsoft: SharePoint Server	76
Microsoft: Skype for Business	76
Microsoft: SQL Server	77
Microsoft: Windows Server	78
Microsoft: Windows Server Services	79
Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows	
Servers	79
Error Messages for PowerShell Collection	80
Relationships with Other Types of Component Devices	81
Creating SNMP and PowerShell Credentials for Windows Devices	82
Creating an SNMP Credential	82
Creating a PowerShell Credential	85
Testing Windows Credentials	88
SNMP Credential Test	88
PowerShell Credential Test	88
Running a Windows Credential Test	88
Discovering Component Devices on Hyper-V Systems	90
Viewing Component Devices	90
Manually Aligning the Microsoft: Print Server Dynamic Application	
Executing the SL1 Agent with Windows PowerShell	93
What is an SL1 Agent?	
Agent-Compatible PowerPacks	
The Credential for the SL1 Agent	
Configuring the SL1 Agent Device Template	
Windows Dashboards	96
Installing the Microsoft Server Dashboards	96
Microsoft: Active Directory Server Performance	98
Microsoft: DNS Server Performance	101
Microsoft: Exchange Server 2010 Performance	103
Microsoft: Exchange Server 2013 Performance	. 106
Microsoft: IIS Server Performance	109
Microsoft: Lync Server 2010 Dashboards	111
Microsoft: Lync Server 2010 Performance	111
Microsoft: Lync Server 2010 Utilization	114
Microsoft: Skype for Business Dashboards	117
Microsoft: Lync Server 2013 Performance	. 117
Microsoft: Lync Server 2013 Utilization	
Microsoft: SQL Server Performance	123
Troubleshooting	
Troubleshooting WinRM Error Messages	
Debugging Code 401 Errors	
Debugging Code 500 Errors	
Troubleshooting PowerShell Error Messages	130

## Chapter

## Introduction

#### Overview

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

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					
What is SNMP?	5				
What is PowerShell?	5				
PowerPacks	6				

**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 <a href="https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6">https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6</a>.

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 100
- 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 100
- Microsoft: IIS Server, version 101
- Microsoft: Lync Server 2010, version 1.0
- Microsoft: SharePoint Server, version 1.0
- Microsoft: Skype for Business, version 100
- Microsoft: SQL Server, version 100
- Microsoft: Windows Server, version 108
- Microsoft: Windows Server Cluster, version 101
- Microsoft: Windows Server Services, version 101

## Chapter

# 2

## Configuring Windows Systems for Monitoring with SNMP

### Overview

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

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	21
Installing the SNMP Service	
Configuring the SNMP Service	25
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*:

	wind	ows Firewall w	an Auvanceu a	recurry		
ile Action View Help						
• 🔿 🙎 🖬 🗟 🚺						
Windows Firewall with Advance	Inbound Rules					Actions
🔣 Inbound Rules	Name	Group	•	Profile	Enabled 🔨	Inbound Rules
🌇 Outbound Rules 🛼 Connection Security Rules	🕑 Core Networking - Multicast Listener C	u Core Netwo	rking	All	Yes	in New Rule
Security Rules	🕜 Core Networking - Multicast Listener R			All	Yes	
Monitoring	🔮 Core Networking - Multicast Listener R	ep Core Netwo	rking	All	Yes	Filter by Profile
	🔮 Core Networking - Neighbor Discovery		-	All	Yes	🛛 🐨 Filter by State
	🔮 Core Networking - Neighbor Discovery		-	All	Yes	🕎 Filter by Group
	🔮 Core Networking - Packet Too Big (ICN		2	All	Yes	View
	Ocre Networking - Parameter Problem		-	All	Yes	G Refresh
	Ocre Networking - Router Advertiseme		2	All	Yes	
	Ore Networking - Router Solicitation (		-	All All	Yes ≡	Export List
	Core Networking - Teredo (UDP-In)				Yes	🛛 Help
	Core Networking - Time Exceeded (ICN		2	All	Yes	File and Drinter Chariner (Eaks Descent
	Distributed Transaction Coordinator (R	·			No No	File and Printer Sharing (Echo Request.
	Distributed Transaction Coordinator (RP Distributed Transaction Coo     Distributed Transaction Coordinator (TC Distributed Transaction Coo     File and Printer Sharing (Echo R			No	O Enable Rule	
			Sharing	All	No	🖌 🔏 Cut
	File and Printer Sharing (Echo R	nable Rule	Sharing	All	Yes	🗈 Сору
		Cut	Sharing	All	No	X Delete
		Copy	Sharing	All	No	
	City and Deinter Charles - (ND No.		Sharing	All	No	Properties
	File and Printer Sharing (NB-Ses	Delete	Sharing	All	No	🛛 👔 Help
		Properties	Sharing	All	No	
		Help	Sharing	All	No	
	File and Printer Sharing (Spooler Servic		2	All	No	
	File and Printer Sharing over SMBDirect		-	All	No	
	iSCSI Service (TCP-In)	iSCSI Service	-	All	No	
	Key Management Service (TCP-In)	Key Manage	ment Service	All	No	
	Netlogon Service (NP-In)	Netlogon Se	rvice	All	No	
	💿 Netlogon Service Authz (RPC)	Netlogon Se	rvice	All	No	
	Network Discovery (LLMNR-UDP-In)	Network Dis	covery	All	No	
	Network Discovery (NB-Datagram-In)	Network Dis	covery	All	No	
	Network Discovery (NB-Name-In)	Network Dis	covery	All	No	
	Network Discovery (Pub-WSD-In)	Network Dis	covery	All	No 🗸	
III >	< III				>	
ies 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:

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

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

🚡 Add Roles and Features Wizard 🗕 🗖								
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:	he server pool	to install roles and features.					
Confirmation Results	Name WIN-3UGJKS2COLQ	IP Address 10.100.100.22	Operating System Microsoft Windows Server 2012	R2 Standard				
		Server Manager. Off	dows Server 2012, and that have be line servers and newly-added serve					
		< Pre	vious Next > In	stall 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:

🚡 Add Roles and Features Wizard 💶 🗖								
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	NET Framework 3.5 Features         Image: Second S	.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.						
	IIS Hostable Web Core       Ink and Handwriting Services       <	Install						

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

þ	Add Roles and Features Wizard	x
1	Add features that are required for SNMP Service? The following tools are required to manage this feature, but do not have to be installed on the same server.	
[	<ul> <li>Remote Server Administration Tools</li> </ul>	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:

🚡 Add Roles and Features Wizard 🔄 🗖 🗙									
Confirm installation	DESTINATION SERVER WIN-3UGJKS2COLQ								
Before You Begin	To install the following roles, role services, or features on selected server, click								
Installation Type	Restart the destination server automatically if required								
Server Selection	Optional features (such as administration tools) might be displayed on this page	, , , , , , , , , , , , , , , , , , ,							
Server Roles	been selected automatically. If you do not want to install these optional feature their check boxes.	25, CIICK Previous to clear							
Features									
<b>Confirmation</b> Results	Remote Server Administration Tools Feature Administration Tools SNMP Tools SNMP Service SNMP WMI Provider								
	Export configuration settings Specify an alternate source path								
	< Previous Next >	Install Cancel							

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

#### Configuring the SNMP Service

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

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

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

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

SNMP Service Properties (Local Computer)								
General Log On	Recovery	Agent	Traps	Security	Dependencies			
Service name:	SNMP							
Display name:	SNMP Serv	ice						
Description:	Enables Sin (SNMP) req				Protocol is computer	]		
Path to executable C:\Windows\Syst		exe						
Startup type:	Automatic				~			
Service status: Running								
Start	Stop		Pau	ise	Resume			
You can specify the start parameters that apply when you start the service from here.								
Start parameters:								
	[	OK		Cancel	Apply			

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

4.	Select the	[Security]	tab.	The	security	settings	are d	isplayed:	
----	------------	------------	------	-----	----------	----------	-------	-----------	--

	SNMP	Service P	ropert	ties (Lo	cal Con	nputer) 🛛 🗙
General	Log On	Recovery	Agent	Traps	Security	Dependencies
🖌 Se	nd authenti	cation trap				
Acc	epted com	munity name	s			
	ommunity			Rig	nts	
	Ad	ld	Edi	t	Remo	ve
0	Accept SN	MP packets	from any	y host		
		MP packets				
	ocalhost					
L						
	Ad	ld	Edi	t	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 Se	rvice Propert	ties (Lo	ocal Con	nputer) 🛛 🗙
General Log On Re	covery Agent	Traps	Security	Dependencies
Send authenticati	on trap			
-Accepted commun	ity names			
Community		Rig		
public		RE/	AD ONLY	
				<b>Y</b>
SN	IMP Service	Config	juration	×
				Add
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*:

P		Windows	Firewall with Ad	vanced Sec	urity					_ 0	x
File Action View Help											
Þ 🔶 🙇 📰 🗟 🖬											
P Windows Firewall with Advance	Inbound Rules								1	Actions	
🗱 Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address	~	Inbound Rules	
Cutbound Rules	Remote Event Log Management (RPC-EP	. Remote Event Log Manage.	. All	No	Allow	No	%System	Any		New Rule	
Connection Security Rules	Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System	Any	112	-	
Monitoring	Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System	Any		Filter by Profile	•
	Remote Scheduled Tasks Management (	Remote Scheduled Tasks M.	All	No	Allow	No	%System	Any	11	Filter by State	•
	Remote Scheduled Tasks Management (	Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	11	Filter by Group	,
	Remote Service Management (NP-In)	Remote Service Managemer	nt All	No	Allow	No	System	Any	11	View	
	Remote Service Management (RPC)	Remote Service Managemer	nt All	No	Allow	No	%System	Any			
	Remote Service Management (RPC-EPM	Remote Service Managemer	nt All	No	Allow	No	%System	Any		Refresh	
	Inbound Rule for Remote Shutdown (RP	Remote Shutdown	All	No	Allow	No	%system	Any		🔒 Export List	
	Inbound Rule for Remote Shutdown (TC	Remote Shutdown	All	No	Allow	No	%system	Any	111	? Help	
	Remote Volume Management - Virtual D	. Remote Volume Manageme	All	No	Allow	No	%System	Any	112	- Help	
	Remote Volume Management - Virtual D	. Remote Volume Manageme	All	No	Allow	No	%System	Any		SNMP Service (UDP In)	-
	Remote Volume Management (RPC-EPM	. Remote Volume Manageme	All	No	Allow	No	%System	Any	15	C Enable Rule	
	Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow	No	System	Any	- 11-2	-	
	Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No	System	Any		🦨 Cut	
	Routing and Remote Access (PPTP-In)	Routing and Remote Access	All	No	Allow	No	System	Any		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						Any			
	SNMP Trap Service (UDP In)	Enable Kule	Private, Public	No	Allow	No	%System	Any	111	P Help	
	SNMP Trap Service (UDP In)	Cut	Domain	No	Allow	No	%System	Any	-11		
	TPM Virtual Smart Card Managemen	Copy ard Ma.	Domain	No	Allow	No	%System	Any			
	TPM Virtual Smart Card Managemen	Delete ard Ma.	Private, Public	No	Allow	No	%System				
	TPM Virtual Smart Card Managemen	ard Ma.	Domain	No	Allow	No	%System	Any	=		
	TPM Virtual Smart Card Managemen	Properties and Ma.	Private, Public	No	Allow	No	%System	Any			
	Wirtual Machine Monitoring (DCOM-	Help itoring	All	No	Allow	No	%System	Any			
	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	- I		
< III >	<							. >			
nable 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*:

	Windov	vs Firewall wit	h Advanced S	ecurity		
ile Action View Help						
• 🔿 🙍 🖬 🔂 👘						
Windows Firewall with Advance	Inbound Rules					Actions
🇱 Inbound Rules	Name	Group	•	Profile	Enabled ^	Inbound Rules
Cutbound Rules	🖉 Core Networking - Multicast Listener Qu.	Core Network	ing	All	Yes	🚉 New Rule
🏂 Connection Security Rules	🖉 Core Networking - Multicast Listener Rep	Core Network	ting	All	Yes	
nonitoring	🖉 Core Networking - Multicast Listener Rep	Core Network	ing	All	Yes	Filter by Profile
	🖉 Core Networking - Neighbor Discovery A	Core Network	sing	All	Yes	🕎 Filter by State
	🕑 Core Networking - Neighbor Discovery S.	Core Network	ing	All	Yes	Filter by Group
	🖉 Core Networking - Packet Too Big (ICMP	Core Network	ing	All	Yes	View
	🖉 Core Networking - Parameter Problem (l.	Core Network	ting	All	Yes	View
	💿 Core Networking - Router Advertisement	Core Network	ing	All	Yes	🖪 Refresh
	🖉 Core Networking - Router Solicitation (IC	Core Network	ing	All	Yes =	🔜 🔜 Export List
	🕑 Core Networking - Teredo (UDP-In)	Core Network	ing	All	Yes	- Help
	🕑 Core Networking - Time Exceeded (ICMP	Core Network	ing	All	Yes	le nep
	🔘 Distributed Transaction Coordinator (RPC	C) Distributed Tr	ansaction Coo	All	No	File and Printer Sharing (Echo Request
	🜑 Distributed Transaction Coordinator (RP	Distributed Tr	ansaction Coo	All	No	O Enable Rule
	Distributed Transaction Coordinator (TC.	Distributed Tr	ansaction Coo	All	No	-
	File and Printer Sharing (Echo R	en insta	Sharing		No	🖌 Cut
	🖉 File and Printer Sharing (Echo R	able Rule	Sharing	All	Yes	Copy
	🔘 File and Printer Sharing (LLMNF Cu	t	Sharing	All	No	🔀 Delete
	🖤 File and Printer Sharing (NB-Dat Co	ру	Sharing	All	No	Properties
	Sile and Printer Sharing (NB-Na De	lete	Sharing	All	No	
	🔘 File and Printer Sharing (NB-Ses 🥂 👘		Sharing	All	No	<table-cell> Help</table-cell>
	File and Printer Sharing (SMB-Ir	operties	Sharing	All	No	
	🖤 File and Printer Sharing (Spoole 🛛 🛛 He	lp	Sharing	All	No	
	File and Printer Sharing (Spooler Service -	File and Printe	er Sharing	All	No	
	🔘 File and Printer Sharing over SMBDirect (i	File and Printe	er Sharing over	All	No	
	🚳 iSCSI Service (TCP-In)	iSCSI Service		All	No	
	🔘 Key Management Service (TCP-In)	Key Managen	nent Service	All	No	
	🔘 Netlogon Service (NP-In)	Netlogon Sen	vice	All	No	
	🔘 Netlogon Service Authz (RPC)	Netlogon Sen	vice	All	No	
	Network Discovery (LLMNR-UDP-In)	Network Disc	overy	All	No	
	Wetwork Discovery (NB-Datagram-In)	Network Disc	-	All	No	
	🔘 Network Discovery (NB-Name-In)	Network Disc	overy	All	No	
	Network Discovery (Pub-WSD-In)	Network Disc	overy	All	No 🗸	
III >	< III				>	

### Installing the SNMP Service

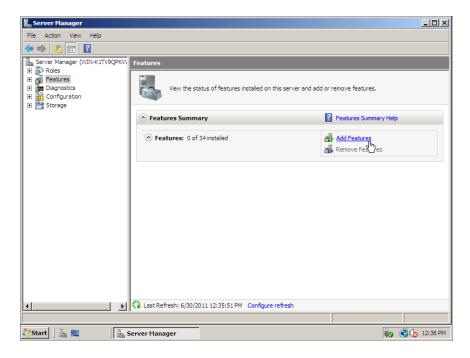
To install the SNMP service on a Windows 2008 Server, perform the following steps:

1. Open the Server Manager utility.

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

🗒 Server Manager			
File Action View Help			
🗢 🔿 🗾 🔜			
Server Manager (WIN-KITV9QPKVWS)  Roles R		ed on this server and add or remove features.	
	Last Refresh: 7/1/2011 12:49:38 PM Confi	igure refresh	
灯 Start 🛛 🚠 📰 👘 🗍 🛼 Server Ma	nager	to 🕄 🕼	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. Eeturies: 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 Manage	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         Image: Informational message below         Image: Ima	
	< Previous Mext > Instal 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: <ul> <li>I warning message below</li> <li>I warning message below</li> <li>Installation succeeded</li> <li>Installation succeeded</li> </ul> <li>Installation succeeded</li> <li>SIMP Service</li> <li>Installation succeeded</li>	
	< <u>Previous</u> <u>Next</u> > Close Cancel	

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

#### Configuring the SNMP Service

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

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

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

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

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

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

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

SNMP Service Properties (WI	N-K1TV9QPK	/WS)		×
General Log On Recovery	Agent Traps	Security [	Dependencies I	
	Agone   hope			
Send authentication trap				
- Accepted community names	,			
Community	Ri	ghts		
Add	Edit	Remov		
Add	E UII	Heimov	e	
C Accept SNMP packets	from any host			
- Accept SNMP packets	from these hos	ts	k	
localhost				
, Add	Edit	Remove		
Add	Ealt	Remove		
Leam more about <u>SNMP</u>				
r			1	
	ОК	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 (WIN-K1TV9QPKVWS)	×
General Log On Recovery Agent Traps Security Dependencies	
Send authentication trap	
Accepted community names	
Community Rights	
SNMP Service Configuration	
Community rights: Add	
READ ONLY	
Community Name:	
public	
Add Edit Remove	
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-2TVE5CDI76	2)	×
General Log On Recovery	Agent Traps	Security Dep	oendencies
Send authentication trap			
Accepted community name	es		
Community	Rig	hts	
cOsmOs	READ ONLY		
SNMP Service Configu	ration		×
Host name, IP or IPX a	ddress:	Car	ncel
	<u>danooo.</u>	_	
p p			
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*:

P		Wind	ows Firewall with Ac	vanced Se	urity				_ 0	×
File Action View Help										
Þ 🔿 🙍 🖬 🗟 🛛 🖬										
Windows Firewall with Advance	Inbound Rules	_		_		_		_	Actions	_
Inbound Rules	Name	a <b>A</b>	Profile	Enabled	L a vi	Override	_ n	L		
Cutbound Rules	Remote Event Log Management (RPC-EP.,	Group Remote Event Log Man		No	Action	No	Program	Local Address	Inbound Rules	
🌆 Connection Security Rules	Remote Event Log Management (RPC-EP	Remote Event Log Man	All		Allow		%System		🔯 New Rule	
🛛 戅 Monitoring	Remote Event Monitor (RPC)	Remote Event Monitor Remote Event Monitor	All	No		No No	%System		Filter by Profile	
	Remote Event Monitor (RPC-EPMAP)			No	Allow	No	%System %System	Any Any	Filter by State	
	Remote Scheduled Tasks Management (			No	Allow	No				
				No	Allow	No	%System	Any	Filter by Group	
	Remote Service Management (NP-In)	Remote Service Manage					System	Any	View	
	Remote Service Management (RPC)	Remote Service Manage		No	Allow	No	%System		Refresh	
	Remote Service Management (RPC-EPM			No	Allow	No	%System	Any		
	Inbound Rule for Remote Shutdown (RP	Remote Shutdown	All	No	Allow	No	%system	Any	Export List	
	Inbound Rule for Remote Shutdown (TC		All	No	Allow	No	%system	Any	🛛 🛛 Help	
	Remote Volume Management - Virtual D			No	Allow	No	%System			
	Remote Volume Management - Virtual D			No	Allow	No	%System		SNMP Service (UDP In)	
	Remote Volume Management (RPC-EPM	-		No	Allow	No	%System	Any	Enable Rule	
	Routing and Remote Access (GRE-In)	Routing and Remote Ac		No	Allow	No	System	Any	🔏 Cut	
	Routing and Remote Access (L2TP-In)	Routing and Remote Ac		No	Allow	No	System	Any		
	Routing and Remote Access (PPTP-In)	Routing and Remote Ac		No	Allow	No	System	Any	Сору	
SNMP Service (UD	Secure Socket Tunneling Protocol (SSTP		,	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	Help	
	SNMP Trap Service (UDP In)		Private, Public	No	Allow	No	%System	Any	И Нер	
	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	bre	Ma Domain	No	Allow	No	%System	Any		
TPM Virtual Smart Card Managemen     Virtual Machine Monitoring (DCOM-     Wirtual Machine Monitoring (Echo Requ	TPM Virtual Smart Card Managemen	Properties ard	Ma Private, Public	No	Allow	No	%System	Any		
	Wirtual Machine Monitoring (DCOM-	Help ito	ring All	No	Allow	No	%System	Any		
	Virtual Machine Monito	ring All	No	Allow	No	Any	Any			
<ul> <li>Virtual Machine Monitoring (Echo Reque</li> <li>Virtual Machine Monitoring (NB-Session</li> </ul>		Virtual Machine Monito	ring All	No	Allow	No	Any	Any		
		Virtual Machine Monito	ring All	No	Allow	No	Any	Any	-	
III >	<							>	1	
able Rule										

## Chapter



## Configuring Windows Servers for Monitoring with PowerShell

### Overview

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

Prerequisites	32
Configuring PowerShell	32
Step 1: Configuring the User Account for the ScienceLogic Platform	33
Option 1: Creating an Active Directory Account with Administrator Access	33
Option 2: Creating a Local User Account with Administrator Access	34
Option 3: Creating a Non-Administrator User Account	34
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	36
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	36
Creating a User Group and Adding a User in Active Directory	36
Setting the Session Configuration Parameters and Group Permissions	37
Creating a PowerShell Credential	
Optional: Configuring the User Account for Access to Windows Failover Cluster	
Step 2: Configuring a Server Authentication Certificate	38
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate .	
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	41
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	41
Step 3: Configuring Windows Remote Management	42

Option 1: Using a Script to Configure Windows Remote Management	.42
Option 2: Manually Configuring Windows Remote Management	.47
Option 3: Using a Group Policy to Configure Windows Remote Management	.50
Step 4: Configuring a Windows Management Proxy	.68
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	.69

#### Prerequisites

Before configuring PowerShell, ensure the following:

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

### Configuring PowerShell

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

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

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

- 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 Microsoff's documentation.

After creating your domain user account or local user account:

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

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

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

winrm configsddl default

- 2. On the **Permissions for Default** window, click the **[Add]** button, and then add the non-administrator user account.
- 3. Select the Allow checkbox for the **Read (Get, Enumerate, Subscribe)** and **Execute (Invoke)** permissions for the user, and then click **[OK]**.

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

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

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

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

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

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

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

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

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

If you use SL1 to monitor Microsoft Exchange Servers:

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

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

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

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

#### Creating a User Group and Adding a User in Active Directory

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

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

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

#### Setting the Session Configuration Parameters and Group Permissions

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

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

Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell

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

DOC	AD DCC	
PSSession Creators (MSTESTL Administrators (MSTESTLAB-H)	the second s	and the second se
Remote Management Users (M		141151
	Add	Bemove
emissions for PSSession eators	Allow	Deny
Full Control(All Operations)	~	
Read(Get,Enumerate,Subscribe)		
Write(Put,Delete,Create)		
Execute(Invoke)		
Special permissions		
or special permissions or advanced	eettinne .	
	ervan Get	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

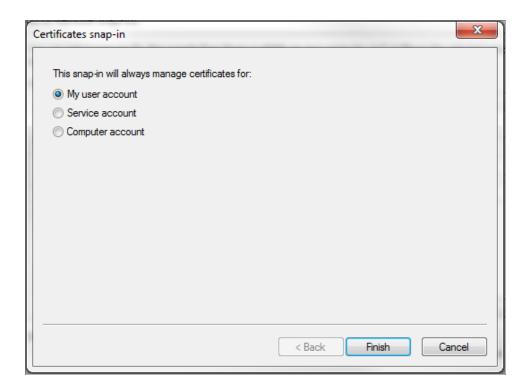
To use the Microsoft Management Console to create a self-signed certificate:

- 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 Management Event Viewer Folder Group Policy Object P Security Monitor	Microsoft Cor Microsoft Cor Microsoft Cor Microsoft Cor Microsoft and Microsoft Cor Microsoft Cor	E Add >		Remove Move Up Move Down
IP Security Policy M Link to Web Address escription:	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 on the ScienceLogic portal that automates configuration of Windows Remote Management and permissions required for the user account that will be used in the SL1 credential. The script configures all of the base Windows permissions required, except for opening up Windows Firewall ports for HTTP and/or HTTPS traffic. The configuration performed by the script is useful primarily for running collection with the Microsoft: Windows Server, Microsoft: Windows Server Services, Microsoft: Windows Server Event Logs, and Microsoft: SQL Server Enhanced PowerPacks. (Microsoft: SQL Server Enhanced requires further instance-specific permissions. See the Monitoring SQL Servers manual for more information.)

To use the PowerShell script, perform the following steps:

- Log in to the ScienceLogic portal, go to Downloads > Miscellaneous, and download the PowerShell script named WinRM Configuration Wizard Script (winrm\_configuration\_wizard.ps1). The link is : https://portal-cdn.sciencelogic.com/powerpackextras/5819/18486/winrm\_configuration\_wizard.zip
- 2. Unzip the downloaded file.
- 3. Using the credentials for an account that is a member of the Administrator's group, log in to the Windows server you want to monitor. You can log in directly or use Remote Desktop to log in.
- 4. Copy the PowerShell script named *winrm\_configuration\_wizard.ps1* to the Windows server that you want to monitor with SL1.
- 5. Right-click on the PowerShell icon and select Run As Administrator.
- 6. At the PowerShell prompt, navigate to the directory where you copied the PowerShell script named **winrm\_ configuration\_wizard.ps1**.
- 7. At the PowerShell prompt, enter the following to enable execution of the script:

Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process -Force

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

8. After the warning text, select Y.

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

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

.\winrm configuration wizard.ps1 -user <domain>\<username>

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

help .\winrm\_configuration\_wizard.ps1 -full

The most common way to run the script is silently:

.\winrm configuration wizard.ps1 -user <domain>\<username> -silent

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



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

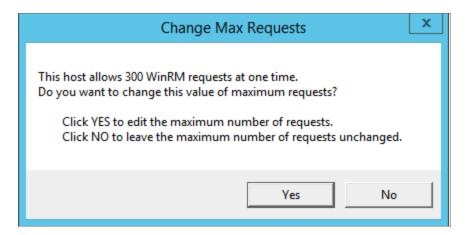


12. The Set Encryption Policy modal page appears. Select the appropriate choice for your environment.

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	-		x
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 thun	nbprin	ts:	
Get-ChildItem -Path Cert:\LocalMachine\My			
Then press OK to continue.			
Enter your certificate thumbprint here			< >
		OK	

**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 CANCEL to quit wizard (settings will not be updated).	
OK Cancel	

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

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

C:\Users\EM7Admin\Documents>certutil -ca.cert ca_name.cer CA cert[0]: 3 Valid CA cert[0]: BEGIN CERTIFICATE MIIDpTCCA02gAwIBAgIQHAmGt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ MRUwEwYKCZImi2PyLGQBGRYFbG9jYWwxGTAXBgoJkiaJk/IsZAEZFg]NU1RMMDEy UjIxJTAjBgNVBAMTHEITVEwwMTJSMilUTDAxMIIyLURDLTAxLUNBLTEwHhcNMTQw NDEIMTYINTQIWhcNMTkwNDEIMTcwNTQIWjBZMRUWEWYKCZImi2PyLGQBGRYFbG9j YWwxGTAXBgoJkiaJk/IsZAEZFg]NU1RMMDEyUjIxJTAjBgNVBAMTHEITVEwwMTJS MilUTDAxMIJyLURDLTAxLUNBLTEwggEiMA0GCSqGSID3DQEBAQUAA4IBDwAwggEK AoIBAQCmsP0N2QIJASpxq192rofUCZFaoBISpG0JyMiit+risfVAg1RgVFvc3mQK TKoOWqeiuNAuhIIfYFIhOsORNSOFHgUNgrasdruugSPL/oV23VDH2dqjHaDd6azY 7CcWfD6uu3oV0aZU9Sgt4HEymPU14QKGuZ1n4UTXIdepCAoN37oyNkoQg0ILUutp Q81i6YdkDyAUOwWyKnvSOosQpqAFSdFW7rgt80bIXf9F2n13yuwogEpfeQ+E8UH4 JGmt0pSZk7hsFDMxXkvRhdPugH7rIONGia0xyoVUUVqfiiK748LiE/Qve0X73wBo 7XLVsMSbWNo9SNxnf8/hiUTJOpOnAgMBAAGjaTBnMBMGCSsGAQBgJcUAgQGHgQA QwBBMA4GA1UdDwEB/wQEAwIBAjAPBgNVHRMBAF8EBTADAQH/MBOGA1UdDgQWBBR9 QjsBuyfqH2Prforx0g/z9102wDQQBgkrBgEAVI3FQEEAWIBADANBgkqhkiG9w0B
AQUFAAOCAQEATSkQpaWpO6i0IT+13980Is1HbTln6AyVGizU2MnRAWLKAxguEdha R/+1RL/qkNXJeqjpDAFsz22EIvei0KVCIbwEXeKePZnQGlujr2FLRbUWt+oA0/ES G4rxLIw//g4sOHK5JmRYCXJozDK8zrHOZADv/Trn6CEWxYaB6quQFzTQsm9WbUK trDogF27oDW29LGZ6z7TNn10XoKxEqUqCfR8EPFkctYrz/+bNFV8V3YJjdAm/42g 4hjdX04PG1hDj0Bg2srX+01tx8mAMjAvUdNg2kvU0m0dP6h17BqJJ08umJxPmfQI vWF1gNeTUNHTTYu1JdEeR7QhLhK6rkAnHw== END CERTIFICATE CertUti1: -ca.cert command completed successfully. C:\Users\EM7Admin\Documents>_

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

- 5. Exit the command prompt.
- 6. Log in to a domain controller in your Active Directory forest and navigate to the System Manager dashboard.

7. Click the **Tools** menu, then select Group Policy Management.

<b>a</b>	Server Manager	_ 0 ×
Server M  Dashboard  Local Server  Local Server  Local Server  AD CS  DNS  File and Storage Services	Server Manager Ianager	Active Directory Administrative Center Active Directory Administrative Center Active Directory Module for Windows PowerShell Active Directory Users and Services Active Directory Users and Computers Active Directory Users and Computers ADSI Edit Certification Authority Component Services Computer Management Defragment and Optimize Drives
ite IIS	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 (IIS) Manager ISCSI Initiator Local Security Policy ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor
	Image: AD CS         Image: AD DS         Image: AD DS<	Resource Monitor Security Configuration Wizard Services
	Image ability     Image ability     Image ability       Events     Events     Events       Services     Services     Services       Performance     Performance     Performance       RPA results     RPA results     RPA 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.

			Group Policy Ma	anagement		- 0 ×	
File Action View						_ 8 ×	
* * 2	a 🛛 🖬						
Group Policy Managem		Group Policy Objects in MSTL012R2.local					
Forest: MSTL012R2.I	ocal	Contents Delega	tion				
4 MSTL012R21	ocal	Name	•	GPO Status	WMI Filter	Modified	
🛒 Defa	Create a GPO in this domain, an	d Link it here	trollers Policy	Enabled	None None	3/19/201 2/4/2014	
⊨ Powe ≥ ⊆ Dom ⊳ ⊡ Grou	Link an Existing GPO		Cy Management Policy	All settings disabled	None	2/4/2014 4/17/201	
	Block Inheritance			All settings disabled	None	4/16/201	
Þ 🚔 WMI	Group Policy Modeling Wizard						
D Start	New Organizational Unit Search Change Domain Controller						
Sites							
👸 Group Polic							
	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	,					

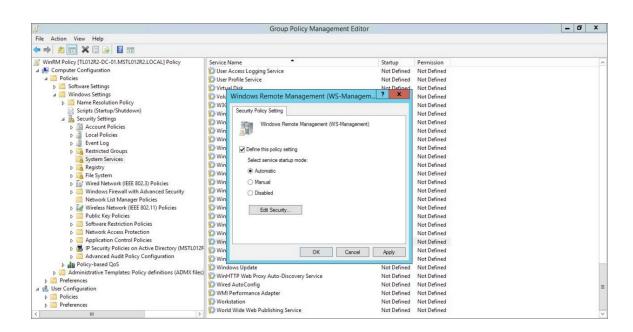
9. In the left panel, right-click the new group policy and select *Edit*. The **Group Policy Management Editor** page for the new Windows Remote Management group policy appears.

		Group Policy Ma	nagement		_ 0 ×	
File Action View					_ 8	
🔿 🖄 📰 📋 🤇						
Group Policy Management		Group Policy Objects in MSTL012R2.local				
↓ Winter Dom ↓ Com </th <th>omain Policy Il Remote Management Policy Edit Enforced</th> <th>Name Cefsul Domain Controllers Policy Cefsul Domain Policy CoverShell Remote Management Policy WinRM Policy WinRM Settings</th> <th>GPO Status Enabled Enabled All settings disabled Enabled All settings disabled</th> <th>WMI Filter None None None None</th> <th>Modfler 3/19/2 2/4/20 4/17/2 4/17/2 4/16/2</th>	omain Policy Il Remote Management Policy Edit Enforced	Name Cefsul Domain Controllers Policy Cefsul Domain Policy CoverShell Remote Management Policy WinRM Policy WinRM Settings	GPO Status Enabled Enabled All settings disabled Enabled All settings disabled	WMI Filter None None None None	Modfler 3/19/2 2/4/20 4/17/2 4/17/2 4/16/2	
		<	ш			
		J				

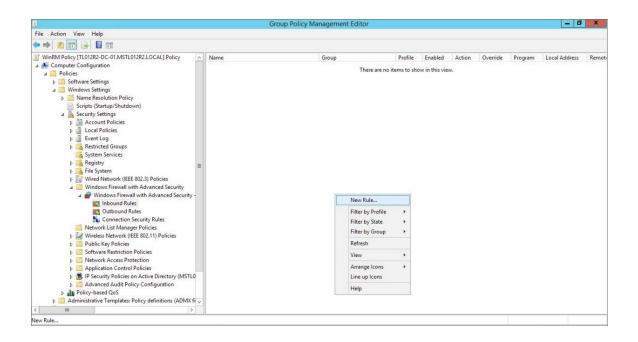
 In the left panel, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > System Services. In the right panel, locate the Windows Remote Management (WS-Management) service. Right-click the service, then select Properties.

	Group Policy Mar	nagement Editor		_ 0
ile Action View Help				
• 🔿 🙍 🗰 🔛 🗃 🖬 🖬				
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	Service Name	Startup	Permission	
Nonputer Configuration	🗱 User Access Logging Service	Not Defined	Not Defined	
a 📔 Policies	User Profile Service	Not Defined	Not Defined	
Software Settings	🗱 Virtual Disk	Not Defined	Not Defined	
Windows Settings	🗱 Volume Shadow Copy	Not Defined	Not Defined	
Name Resolution Policy	W3C Logging Service	Not Defined	Not Defined	
Scripts (Startup/Shutdown)	Windows Audio	Not Defined	Not Defined	
A Security Settings	Windows Audio Endpoint Builder	Not Defined	Not Defined	
Account Policies     Local Policies	Windows Color System	Not Defined	Not Defined	
Local Policies     Event Log	Windows Connection Manager	Not Defined	Not Defined	
	Windows Driver Foundation - User-mode Dr	iver Framework Not Defined	Not Defined	
A Restricted Groups System Services	Windows Encryption Provider Host Service	Not Defined	Not Defined	
> Registry	Windows Error Reporting Service	Not Defined	Not Defined	
File System	Windows Event Collector	Not Defined	Not Defined	
Wired Network (IEEE 802.3) Policies	Windows Event Log	Not Defined	Not Defined	
Windows Firewall with Advanced Security	Windows Firewall	Not Defined	Not Defined	
Network List Manager Policies	Windows Font Cache Service	Not Defined	Not Defined	
Wireless Network (IEEE 802.11) Policies	Windows Installer	Not Defined	Not Defined	
Public Key Policies	Windows Management Instrumentation	Not Defined	Not Defined	
Software Restriction Policies	Windows Modules Installer	Not Defined	Not Defined	
Network Access Protection	Windows Process Activation Service	Not Defined	Not Defined	
Application Control Policies	Windows Remote Management		Not Defined	
IP Security Policies on Active Directory (MSTL012F	Windows Store Service (WSServi Prop	erties Not Defined	Not Defined	
Advanced Audit Policy Configuration	Windows Time Help	Not Defined	Not Defined	
Policy-based QoS	Windows Update	Not Defined	Not Defined	
Administrative Templates: Policy definitions (ADMX files)	WinHTTP Web Proxy Auto-Discovery Service	Not Defined	Not Defined	
Preferences	Wired AutoConfig	Not Defined	Not Defined	
User Configuration Policies	WMI Performance Adapter	Not Defined	Not Defined	
Policies     Preferences	Workstation	Not Defined	Not Defined	
	World Wide Web Publishing Service	Not Defined	Not Defined	
ш >	-			

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]**.

J		Group Policy Managemer	t Editor							- 0	x
File Action	View Help										
수 🏟 🖄	🖬 🔒 🖪 🖬										
WinRM P	<b>2</b>	New Inbound Rule Wizard			Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ <u> </u>	Rule Type Select the type of firewall rule to	o create.		e	ms to shov	v in this view	N.				
Þ	Steps:										
⊿	Rule Type	What type of rule would you like to create?									
	Predefined Rules										
	<ul> <li>Action</li> </ul>	Program     Rule that controls connections for a program.     Port     Rule that controls connections for a TCP or UDP port.     Preddinged:									
		Windows Firewall Remote Management	~								
		Rule that controls connections for a Windows experience. Custom Custom rule.									
¢		< 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 Rules that are checked will be created. If a rule alrea	rements for the	selected predefin	ed group.								
	<ul> <li>Action</li> </ul>	Hules that are checked will be created. If a rule alreat the existing rule will be overwritten.	ady exists and is	checked, the co	ntents of								
		Name	Rule Exists	Profile	Desc								
		Windows Frewall Remote Management (RPC.,     Windows Frewall Remote Management (RPC)		All All	Inbou Inbou								
		< 10			>								
¢		E	< Back	Next >	Cancel						1		

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

5		Group Policy Management Editor							- 0	x
File Action	View Help									
	📅 🗟 🔽 📅									
WinRM Pe	2	New Inbound Rule Wizard	×	Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ № Comp ⊿ ₩ Po ↓ ₩ ↓ ↓	Action	when a connection matches the conditions specified in the rule.  What action should be taken when a connection matches the specified conditions?  What action should be taken when a connection matches the specified conditions?  Mow the connection This includes connections that are protected with IPsec as well as those are not.  Mow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be accured using the secured authenticated by using IPsec. Connections will be accured using the secured using the induces on the connection Security Rule node.		ems to sh	ow in this vie	w.				
		Block the connection  Cance  Cance Cance Cance  Cance  Cance  Cance  Cance Cance Cance Cance Cance Cance Cance Cance Cance Cance Cance Cance Cance Cance Cance Can								

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

	Group Policy	Management Edit	or		_ 0 ×
File Action View Help					
🖿 🔿 📶 🙆 🖬 🔟 📷					
4 🔛 Windows Settings	Automatic Certificate Request	•	-		
Name Resolution Policy     Scripts (Startup/Shutdown)     Scripts (Startup/Shutdown)		,	here are	no items to show in this view.	
Data Protection		New Refresh	•	Automatic Certificate Request	
BitLocker Drive Encryption BitLocker Drive Encryption Network Unlock		View			
Automatic Certificate Request Settings		Arrange Icons			
Trusted Root Certification Authorities Enterprise Trust		Line up Icons			
Intermediate Certification Authorities		Help			
Instee vulue Certificates     Untrusted Certificates     Trusted People     P   Software Restriction Policies     P   Peopleation Control Policies     P	X				

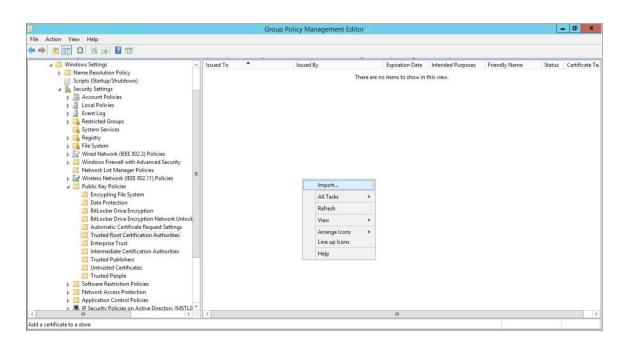
17. The Automatic Certificate Request Setup Wizard modal page appears. Click [Next].

Auton	natic Certificate Request Setup Wizard	Group Policy Managen	nent Editor		– 🖬 X
	Welcome to the Automatic Certificate Request Setup Jurant         with ward helps you set up automatic certificate requests         mageuty which you on one of the period of the perio	kquest •	There are no iter	ms to show in this view.	
▲ Au ■ Tr ■ Int ■ Int ■ Tr ■ Tr ■ Tr ■ Tr ■ Softwa > ■ Softwa > ■ Netwo > ■ Applic	Locker Drive Encryption Network Unlock tormatic Certificate Request Stitlings statel Root Certification Authorities terprise Trust errediate Certificates statel Publishens tuted Certificates statel People re Restriction Policies rk Access Protection ation Control Policies or Active Directory (MSTLO × )				

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

Automatic Certifi	cate Request Setup Wizard	Group Policy Ma	nagement Editor		- 0
Certificate Template The next time a computer logs on, a provided.	certificate based on the template you select	t is filequest			
A certificate template is a set of pred computers. Select a template from th Certificate templates:	efined properties for certificates issued to e following list.		There are no items to	o show in this view.	
Name Computer Domain Controller Errollment Agent (Computer) IPSec	Intended Purposes Client Authentication, Server Authen Client Authentication, Server Authen Certificate Request Agent IP security IKE intermediate				
< III		>			
BitLocker Drive B	< Back Next >	Cancel			
<ul> <li>Automatic Certii</li> <li>Trusted Root Ce</li> <li>Enterprise Trust</li> <li>Intermediate Certii</li> </ul>	icate Request Settings tification Authorities tification Authorities rs				
Trusted Publishe	cates				

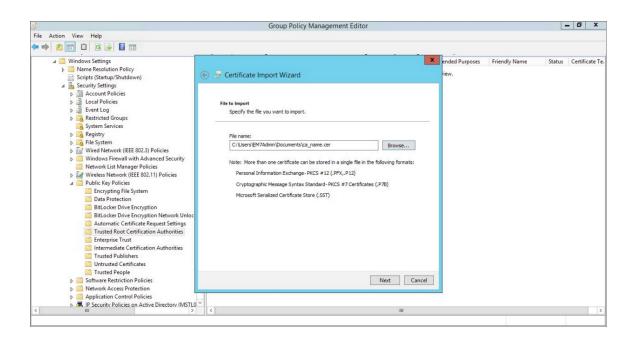
19. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration
 > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification
 Authorities. In the right panel, right-click and select Import.



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

	Group Policy Management Editor		- 0 X
File Action View Help			
Windows Settings     Diagonal Settings     Diagonal Settings     Setting (Startup/Shutdown)	🥏 Certificate Import Wizard	<ul> <li>ended Purposes Friendly Name</li> <li>riew.</li> </ul>	Status Certificate Te
Security Settings     Difference     Differenc	Welcome to the Certificate Import Wizard		
<ul> <li>System Services</li> <li>Registry</li> <li>File System</li> </ul>	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.		
<ul> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> </ul>	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.		
Vireless Network (IEEE 802.11) Policies Public Key Policies	Store Location		
🚞 Encrypting File System	O Current User		
Data Protection BitLocker Drive Encryption	Local Machine		
<ul> <li>BitLocker Drive Encryption Network Unloc</li> <li>BitLocker Drive Encryption Network Unloc</li> <li>Automatic Certificate Request Settings</li> <li>Trusted Root Certification Authorities</li> <li>Enterprise Trust</li> <li>Intermediate Certification Authorities</li> <li>Trusted Publishers</li> </ul>	To continue, click Next.		
Untrusted Certificates			
Trusted People			
Software Restriction Policies	Next Cancel		
Network Access Protection			
Application Control Policies           B         IP Security Policies on Active Directory (MSTL0)			
< III >	۲		>

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



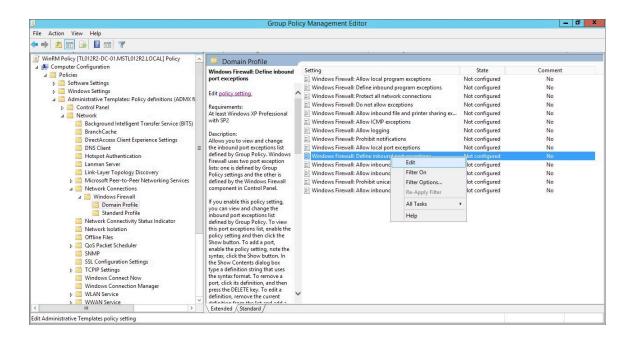
22. Select the **Place all certificates in the following store** radio button, then select the Trusted Root Certification Authorities certificate store and click [Next].

<u>u</u>	Group Policy Management Editor				- 0	x
File Action View Help						
<ul> <li>Image: Settings</li> <li>Image: Name Resolution Policy</li> <li>Scripts (Startup/Shutdown)</li> </ul>	😧 🦻 Certificate Import Wizard	ended Purposes riew.	Friendly Name	Status	Certific	.ate Te
	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.					
<ul> <li>P System</li> <li>Wird ov Krewall with Advanced Security</li> <li>Window Firewall with Advanced Security</li> <li>Network List Manager Policies</li> <li>Wireless Network (IEEE 802.1) Policies</li> <li>Public Key Policies</li> <li>Encrypting File System</li> <li>Data Protection</li> <li>BitLocker Drive Encryption</li> </ul>	Automatically select the certificate store based on the type of certificate Certificate atore: Trusted Root Certification Authorities Browse					
BitLocker Drive Encryption Network Unloc Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted People						
Software Restriction Policies     Metwork Access Protection     Application Control Policies	Next Cancel					
Application Control Policies     Application Control Policies     Application Control Policies     Application Control Policies						>

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

	Group Policy Management Editor		_ 0 ×
File Action View Help			
🗧 🔿 🙍 💼 🚨 🧟 👘			
▲ <sup>10</sup> Windows Settings	🛞 💆 Certificate Import Wizard	ended Purposes Friendly Name	Status Certificate T
Security Settings     Call Account Policies     Local Policies     Call Policies     Call Control Control     Call Contro     Call Control     Call Control     Call Contro     Call Control	Completing the Certificate Import Wizard		
ii System Services ▷ ii Registry ▷ ii System	The certificate will be imported after you click Finish. You have specified the following settings:		
<ul> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Security</li> <li>Network List Manager Policies</li> </ul>	Certificate Store Selected by User Content Certificate Content Certificate File Name C: Users EM7Admin Documents ka name.cer	]	
<ul> <li>Wireless Network (IEEE 802.11) Policies</li> <li>Public Key Policies</li> <li>Encrypting File System</li> </ul>	nie name c. poos privkumi podunons ka_mana.ce		
Data Protection BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc			
Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust			
Intermediate Certification Authorities Trusted Publishers Untrusted Certificates			
<ul> <li>Trusted People</li> <li>Software Restriction Policies</li> <li>Network Access Protection</li> </ul>	Finish Ca	ncel	
Application Control Policies     Application Control Policies     Application Control Policies on Active Directory (MSTL0     Application Control Policies on Active Directory (MSTL0     Application Control Policies	× <		

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.

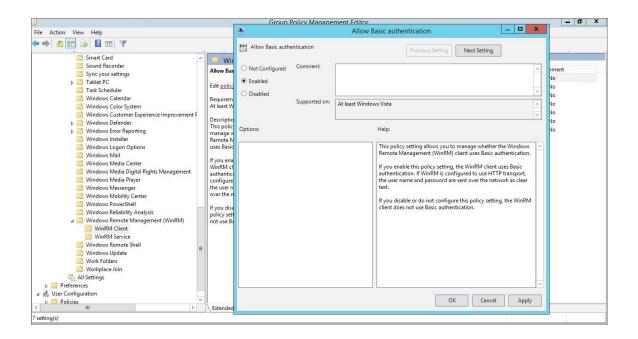


25. The Windows Firewall: Define inbound port exceptions modal page appears. Under Options, click [Show].

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:	^ kxceptions	State Comment
Software	Enabled	am exceptions	Not configured No
Administr	O Disabled	nnections	Not configured No
Control	Supported on: At Le	t Windows XP. Professional with SP2	Not configured No
⊿ 🚞 Netwo		Show Contents	Not configured No
🛄 Bai			Not configured No Not configured No
📫 Bra 🛅 Dir	Options:	Define port exceptions:	Not configured No Not configured No
		Value	Not configured No
Ho	Define port exceptions: Show	5985:TCP:*:enabled:WSMan	Not configured No
📔 Lar	Specify the port to open or block.	J 5986:TCP:*:enabled:WSMan tration exc	Not configured No
🛗 Lin	Syntax:	* exceptions	Not configured No
⊳ 🧾 Mi	and the second sec		Not configured No
⊿ 🧾 Ne	<port>:<transport>:<scope>:<status>:&lt;</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 🗂 SN	any number or combination of these:	OK Cancel	
SN SSI	IP addresses, such as 10.0.0.1	also enable the "Windows Firewall: Allow local port exceptions"	
⊳ 🛅 TC	Subnet descriptions, such as 10.2.3.0/24	policy setting.	
🚞 Wi			
🚞 Wi	< 111	Figure 1 If you disable this policy setting, the port exceptions list defined	
⊳ 🛄 WL ⊳ 🗂 WV		OK. Cancel Apply	
< W		OK Cancer Appry	

- 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]**.

	Group Policy Management Editor	- 0 X
File Action View Help	Trusted Hosts	
← ⇒ 2 🗊 🕞 🛛 🗊 🍸	Trusted Hosts Previous Setting Next Setting	
Sound Recorder Sound Recorder Sound Recorder Tablet PC Tablet PC Tablet PC Tablet PC Tablet PC Tablet PC Tatk Scheduler Windows Cale System Windows Color System Windows Color System Windows Defender Descrip Windows Defender Windows Media Player Windows Media Pl	adt       O Not Configured       Comment:	0 0 0 0
K III Steen	ded	
7 setting(s)		

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

<b>.</b>	Group	Policy Manage	ment Editor		- 0 ×
File Action View Help			Allow E	Basic authentication	
	Vir Allow Basic auth Not Configured ic. Enabled W Uisabled	Comment: Supported on:	Allow F	Previous Setting Next Setting	Iment         Iment           Ide         Ide           Ide
<ul> <li>Windows Error Reporting</li> <li>Windows Installer</li> <li>Windows Installer</li> <li>Windows Maia Conter</li> <li>Windows Media Clipital Rights Management</li> <li>Windows Media Player</li> <li>Windows Reliability Analysis</li> <li>Windows Remote Management (WinRM)</li> <li>Windows Update</li> <li>Windows Update</li> <li>Windows Update</li> <li>Windows Update</li> <li>Workplace Join</li> <li>Workplace Join</li> <li>Windows Uses</li> <li>Werkplace Join</li> <li>Windows Update</li> <li>Windows Update</li> </ul>	e w Options: acc ren RN RN tice se			Help: This policy setting allows you to manage whether the Windows 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. OK Cancel Apply	40 40 40 40 40
< III > \Extend	led			Carcer Apply	
10 setting(s)					

- 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	- 🗗 X
File Action View Help	Allow remote server management through WinRM -	
🗢 🔿 🙍 🔂 🔂 🗊 🍸	Allow remote server management through WinRM Previous Setting Next Setting	
Sound Recorder Sound Recorder Sync your settings Tablet PC Tablet PC Windows Calendar Windows Color System Mindows (Culor System) Kindows (Culor System) Kindow	O Not Configured Comment:     O Enabled     O Disabled     Supported on:     At least Windows Vista	
Windows Defender     Windows Error Reporting     Windows Isror Reporting     Windows Installer     Mindows Installer	D Options: Help: No	
Windows Logon Options     Remote service z       Windows Mail     Service z       Windows Media Center     HTP trib Windows Media Player       Windows Media Player     HTP trib Windows Media Player       Windows Media Player     HTP trib Windows Media Player       Windows Media Player     Hyou entitive and trib Windows Media Player       Windows Media Player     Hyou entitive and trib Windows Memote Management (WinRM)       Windows Remote Management (WinRM)     WinRM Service       Windows Remote Shell     On the H       Windows Remote Shell     Port 598       Workplace Join     Workplace Join       Workplace Join     Hy you dit       Workplace Join     Hy pould       Workplace Join     Hy pould <td>Pv4 filter:       *       This policy setting allows you to manage whether the Windows A Remote Management (WinRM) service automatically listens on the Work for requests on the HTTP transport over the default HTTP port.       Iso a constraint of the WinRM service automatically is the service automatically is the service automatically is the the service is the service</td> <td></td>	Pv4 filter:       *       This policy setting allows you to manage whether the Windows A Remote Management (WinRM) service automatically listens on the Work for requests on the HTTP transport over the default HTTP port.       Iso a constraint of the WinRM service automatically is the service automatically is the service automatically is the the service	
A (%) User Configuration     Vegardle	OK Cancel Apply	

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

	Group Pol	icy Management Editor		- 0	X
File Action View Help				in a sure of the second se	
🗢 🤿 🙍 🛅 🛱 🖷 🗟 🖶 📓 🖬 🔞 🛇 🔸					
<ul> <li>WinRM Policy [TL012R2-DC-01.MSTL012R2LOCAL] Policy</li> <li>Computer Configuration</li> <li>Policies</li> <li>Motive Settings</li> <li>Motive Settings</li> <li>Perferences</li> <li>Preferences</li> <li>Ini Files</li> <li>Files</li> <li>Files</li> <li>Network Shares</li> <li>Shortcuts</li> <li>Various Settings</li> <li>Ini Files</li> <li>Network Shares</li> <li>Shortcuts</li> <li>Deciries</li> <li>Preferences</li> <li>Perferences</li> </ul>	Processing (*) Processing (*)	A P, R, Vi A Li	Key Items to show in this view. Registry Item Collection Item Registry Wizard	Value Name	Тур
< III >	Preferences ⟨Extended ⟩ Standard	1			
Add a new registry item		a.			

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

<b>B</b>	Group Policy Management Editor	- 0 ×
File Action View Help		
🗢 🔿 🙍 🖬 📋 🗰 💁 🙀 👘		
<ul> <li>WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy</li> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Mindows Settings</li> <li>Preferences</li> <li>Finites</li> <li>Folders</li> <li>Init Files</li> <li>Folders</li> <li>Software Strings</li> <li>Network Shares</li> <li>Software Settings</li> <li>Software Settings</li> <li>Preferences</li> </ul>	New Registry Properties       Hive       Key         re are no items to show in this view.         General Common         Action:       Create         Hve:       HKEY_LOCAL_MACHINE         Value name         Default       LocalAccountTokenFlitterPolicy         Value type:       REG_DWORD         Value data:	Value Name Typ
	\Preferences / Extended \ Standard /	
Registry		

- Action. Select Create.
- Hive. Select HKEY\_LOCAL\_MACHINE.
- Key Path. Enter "SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system".
- Value name. Enter "LocalAccountTokenFilterPolicy".
- Value type. Enter "REG\_DWORD".
- Value data. Enter "1".
- Base. Select Decimal.
- 38. Click the [OK] button.
- 39. Repeat steps 36-38 to make an additional registry change to increase the maximum number of users who can access Windows Remote Management. In the New Registry Properties modal page, edit the following values:
  - Action. Select Create.
  - Hive. Select HKEY\_LOCAL\_MACHINE.
  - Key Path. Enter "SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\".
  - Value name. Enter "WinRS!MaxConcurrentUsers".
  - Value type. Enter "REG\_DWORD".
  - Value data. Enter "0x64 (100)".
  - Base. Select Decimal.

40. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration > Preferences > Control Panel Settings > Services. In the right panel, right-click and select New > Service.

VinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Computer Configuration Policies Policies Software Settings Software Settings Software Settings Computer Software Settings Policies Software Settings New + Service No policies selected No policies selected New + Service		Group Pol	cy Management	Editor				
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy Computer Configuration Policies Software Settings Mindows Settin	File Action View Help							
<ul> <li>Configuration         Policies         Software Settings         Mondows Settings         Mondows Settings         Mondows Settings         Porferences         Policies         Policies selected         New Options         Policies selected         Policies         Policie</li></ul>	= 🔿 🙍 💼 📋 📾 🗟 📓 🖬 🗟 😒 🕇							
№     Policies     Pate       ▶     Policies     Refresh       ▶     Preferences     View       Image Icons     Line up Icons	<ul> <li>WinRM Policy [TL012R2-DC-01.MSTL012R2LOCAL] Policy</li> <li>Computer Configuration</li> <li>Software Settings</li> <li>Software Settings</li> <li>Windows Settings</li> <li>Preferences</li> <li>Preferences</li> <li>Data Sources</li> <li>Data Sources</li> <li>Tokice Sources</li> <li>Devices</li> <li>Folder Options</li> <li>Local Users and Groups</li> <li>Network Options</li> <li>Soned Diators</li> <li>Power Options</li> <li>Scheduled Tasks</li> </ul>	Processing (*)	Name	Tr	iere are no item	is to show in this v	Recovery	
Preferences / Extended > Standard /	Preferences			Refresh View Arrange Icons Line up Icons	<b>F</b>			

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 [TL91282-DC-01.MSTL01282.LOCAL] Policy         WinRM Policy [TL91282-DC-01.MSTL01282.LOCAL] Policy         Policies         Preferences         Preferences         Policies         Policies         Policies         Preferences         Preferences         Preferences         Preferences         Policies     <	
Services	

• Startup. Select No change.

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

File Action View Help     Image: Computer Configuration     Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Im	₽	Group Policy Management Editor	- 0 ×
Compute Configuration     Policies     Software Settings     Software Settings			
(Therefore Administry	<ul> <li>Computer Configuration</li> <li>Policies</li> <li>Stotware Settings</li> <li>Windows Settings</li> <li>Ministrative Templates: Policy definitions (ADMX files)</li> <li>Preferences</li> <li>Windows Settings</li> <li>Control Panel Settings</li> <li>Devices</li> <li>Control Panel Settings</li> <li>Devices</li> <li>Local Users and Groups</li> <li>Network Options</li> <li>Power Options</li> <li>Scheduled Tasks</li> <li>Services</li> <li>Mer Configuration</li> <li>Devices</li> </ul>	New Service Properties       X       Startup       Account       Interactive       Recover         General       Recovery       Common       Select the computer's response if this service fails.       First failure:       Restart the Service       v         Second failure:       Restart the Service       v         Subsequent failures:       Restart the Service       v         Restart failures:       Restart the Service       v         Restart failures:       Restart the Service       v         Restart failures:       Restart failures:       Restart failures:         Program:	
	< III > \ Services	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.

<u>R</u>	Group Policy Management	- 0 X
🔜 File Action View Window Help		_ 8 ×
🗢 🔿 🙍 💽 🙆 🖬		
Group Policy Management     Group Policy Management     Group Policy Management     Group Policy Charles     Group Policy Charles     Group Policy Objects     Group Policy Objects     Group Policy Results	PowerShell Remote Management Policy         Scope Details Settings Delegation         Links         Display links in this location:         MSTL012R2.local         The following alex, domains, and OUs are linked to this GPO:         Location         Enforced         Vink Enabled         Delete Link(s)         Security Filtering         The settings in this GPO can only apply to the following groups, users, and computers:         Name         & Authenticated Users	· · · · · · · · · · · · · · · · · · ·
	Add     Remove     Properties       WMI Filtering     This GPD is linked to the following WMI filter:	

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 Mana	gement		- 0 ×
📓 File Action View Windo	w Help					_ # ×
🗢 🔿 🖄 🛅 🖏 🗂 🗙						
Group Policy Management		Links Display links	bilcy tails Settings Delegation Status in this location: MSTL012R2Jocal g sites, domains, and OUs are Inked to this GPO:			
Default Dom	ojects nain Controllers Policy nain Policy Remote Management Polic	Location		ink Enabled fes	Path MSTL012R2.local	
WinRM S	Edit					
👂 📑 WMI Filters	GPO Status	► ✓	Enabled			
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 <b>ing</b> s linked to the following WMI filter:			
		<none></none>	×	Open		
< 111	>					
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>
```

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

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

SNMP Dynamic Applications for Windows Devices	
PowerShell Dynamic Applications	
Microsoft: Active Directory Server	
Microsoft: DHCP Server	
Microsoft: DNS Server	72
Microsoft: Exchange Server	
Microsoft: Exchange Server 2010	
Microsoft: Hyper-V Server	
Microsoft: IIS Server	75
Microsoft: Lync Server 2010	
Microsoft: SharePoint Server	
Microsoft: Skype for Business	
Microsoft: SQL Server	77
Microsoft: Windows Server	
Microsoft: Windows Server Services	
Run Book Automations and Actions Associated with PowerShell Dynamic Application	ns for Windows Servers 79
Error Messages for PowerShell Collection	

## 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 Performance
- Microsoft: Windows Server Configuration Cache
- Microsoft: Windows Server BIOS Configuration
- 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 Performance Cache
- 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 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 Dynamic Applications use PowerShell to collect data as a supplement to SL1's internal collection capabilities:

- Microsoft: Windows Server IC Availability
- 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 Services

**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

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

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

Error Message	Possible Issue(s)
realm	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

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	82
Creating a PowerShell Credential	85
Testing Windows Credentials	
SNMP Credential Test	
PowerShell Credential Test	
Running a Windows Credential Test	88
Discovering Component Devices on Hyper-V Systems	90
Viewing Component Devices	90
Manually Aligning the Microsoft: Print Server Dynamic Application	91

## 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 **Credential Management** page (System > Manage > Credentials).

dential Management   Credentia	is Found (62)												Actions	Reset	Guid
													Create S	NMP Credent	
Profile Name *	Organization	RO Use	<u>RW</u> Use	DA Use	Type	Credential User		Host	Port	Timeout (m	<u>15) ID</u>	Last		atabase Cred	
						)	)					Al	Create S	OAP/XML Hos	t Crede
Amazon Web Services Credential	🚯 System				SOAP/XML Host	[ AWS Account Access	example.com		80	2000	1	2015-05-18	Create L	DAP/AD Cred	ential
Azure Credential - SOAP/XML	(all orgs)				SOAP/XML Host	<ad_user></ad_user>	login.windows.net		443	60000	60	2015-05-14	Create B	asic/Snippet (	Credent
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</td><td>Create S</td><td>SH/Key Crede</td><td>ntial</td></subscription_id_h<>	%D		22	180000	59	2015-05-14	Create S	SH/Key Crede	ntial
P Cisco SNMPv2 - Example	(all orgs)				SNMP				161	1500	3	2015-05-14		owerShell Cre	
P Cisco SNMPv3 - Example	(all orgs)				SNMP	[USER_GOES_HERE]			161	1500	2	2015-05-14	Greate P	owershell Cre	dentia
P Cisco: ACI	📸 [all orgs]			126	Basic/Snippet	admin	173.36.219.46		443	0	62	2015-05-14 1	5:05:24	em7admin	
P Cisco: ACI Credential	(all orgs)				Basic/Snippet	admin	198.18.133.200		443	0	61	2015-05-14 1	4:32:20	em7admin	
P Cloudkick - Example	(all orgs)				Basic/Snippet	[SECURITY KEY GOES	127.0.0.1		443	5000	9	2015-05-14 1	1:25:31	em7admin	
P CUCM PerfmonService 8.0 Example	(all orgs)				SOAP/XML Host		%D		8443	2000	4	2015-05-14 1	1:25:12	em7admin	
A EM7 Central Database	(all orgs)				Database	root	localhost		7706	0	51	2015-05-14 1	1:26:41	em7admin	
Je EM7 Collector Database	(all orgs)				Database	root	%D		7707	0	14	2015-05-14 1	1:25:43	em7admin	
A EM7 DB	[all orgs]				Database	root	%D		7706	0	35	2015-05-14 1	1:26:32	em7admin	
P EM7 DB - DB Info	(all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 1	1:26:32	em7admin	
PEM7 DB - My.cnf	👔 (all orgs)				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 1	1:26:32	em7admin	
PEM7 DB - Silo.conf	(all orgs)				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 1	1:26:32	em7admin	
A EM7 Default V2	(all orgs)				SNMP				161	1500	10	2015-05-14 1	1:25:42	em7admin	
P EM7 Default V3	(all orgs)				SNMP	em7defaultv3			161	500	11	2015-05-14 1	1:25:42	em7admin	
PEMC - Example	[all orgs]				Basic/Snippet	root	%D		443	10000	15	2015-05-14 1	1:25:47	em7admin	
A GoGrid - Example	(all orgs)				Basic/Snippet	[SECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 1	1:25:51	em7admin	
PIPSLA Example	👔 [all orgs]				SNMP				161	1500	5	2015-05-14 1	1:25:14	em7admin	
P LifeSize: Endpoint SNMP	(all orgs)				SNMP	control			161	3000	18	2015-05-14 1	1:25:58	em7admin	
P LifeSize: Endpoint SSH/CLI	(all orgs)				Basic/Snippet	auto	%D		22	3	17	2015-05-14 1	1:25:58	em7admin	
P Local API	(all orgs)				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 1	1:26:11	em7admin	
A NetApp 7-mode	(all orgs)				Basic/Snippet	root	%D		443	3000	24	2015-05-14 1	1:26:20	em7admin	
A NetApp w/SSL Option	(all orgs)				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 1	1:26:20	em7admin	
A NetApp w/SSL Option Off	all orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 1	1:26:20	em7admin	
P Nexus netconf	(all orgs)				Basic/Snippet		%D		22	10000	6	2015-05-14 1	1:25:16	em7admin	
A Nexus snmp	🚯 (all orgs)				SNMP				161	10000	7	2015-05-14 1	1:25:16	em7admin	
Polycom - Advanced	(all orgs)				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 1	1:26:24	em7admin	
Polycom - CDR	👔 [all orgs]				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 1	1:26:24	em7admin	
Polycom - Interface	all orgs]				SOAP/XML Host	admin	%D		80	20000	29	2015-05-14 1	1:26:24	em7admin	

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

Credential Editor		×
Create New SNMP Credential		Reset
Basic Settings Profile Name		SNMP Version
Port 161 1500	Timeout(ms)	Retries
SNMP Community (Read-Only)		SNMP Community (Read/Write)
Security Name	Secur	ity Passphrase
Authentication Protocol	Security Level entication Only ]	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. Choices are MD5 or SHA. The default value is MD5. This field is required.
- 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:

- 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.

edential Management   Credentia	iis Found (62)												ns Reset	Guid
												Creat	e SNMP Credential	
Profile Name *	Organization	RO Use	RW Use	DA Use	Type	Credential User		Host	Port	Timeout (n	ne) ID	Creat		
Tone Hune	Cirgeneauon	-				Credential Oser		1008					SOAP/XML Host Cr	
Amazon Web Services Credential	🚯 System				SOAP/XML Host	AWS Account Access	example.com		80	2000	1	2015-05-18 Creat	a LDAP/AD Credentia	al
Azure Credential - SOAP/XML	(all orgs)				SOAP/XML Host	<ad user=""></ad>	login.windows.net		443	60000	60	2015-05-14 Creat	Basic/Snippet Cred	enti
Azure Credential - SSH/Key	all orgs]				SSH/Key	<subscription h<="" id="" td=""><td>%D</td><td></td><td>22</td><td>180000</td><td>59</td><td></td><td>SSH/Key Credentia</td><td></td></subscription>	%D		22	180000	59		SSH/Key Credentia	
A Cisco SNMPv2 - Example	all orgs]				SNMP				161	1500	3	2015-05-		
A Cisco SNMPy3 - Example	(all orgs)				SNMP	IUSER GOES HEREI			161	1500	2	2015-05-4 Creat	e PowerShell Creden	
P Cisco: ACI	(all orgs)			126	Basic/Snippet	admin	173.36.219.46		443	0	62	2015-05-14 15:05:24	em7admin	_
A Cisco: ACI Credential	(all orgs)				Basic/Snippet	admin	198.18.133.200		443	0	61	2015-05-14 14:32:20		
Cloudkick - Example	(all orgs)				Basic/Snippet	ISECURITY KEY GOES			443	5000	9	2015-05-14 11:25:31	em7admin	
Q CUCM PerfmonService 8.0 Example	(all orgs)				SOAP/XML Host		%D		8443	2000	4	2015-05-14 11:25:12	em7admin	
EM7 Central Database	(all orgs)				Database	root	location		7706	0	51	2015-05-14 11:26:41	em7admin	
A EM7 Collector Database	(all orgs)				Database	root	%D		7707	0	14	2015-05-14 11:25:43	em7admin	
A EM7 DB	all orgs]				Database	root	%D		7706	0	35	2015-05-14 11:26:32	em7admin	
@ EM7 DB - DB Info	(all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 11:26:32	em7admin	
A EM7 DB - My.cnf	all orgs]				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 11:26:32	em7admin	
A EM7 DB - Silo.conf	a [all orgs]				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 11:26:32	em7admin	
EM7 Default V2	all orgs]				SNMP				161	1500	10	2015-05-14 11:25:42	em7admin	
A EM7 Default V3	(all orgs)				SNMP	em7defaultv3			161	500	11	2015-05-14 11:25:42	em7admin	
A EMC - Example	all orgs]				Basic/Snippet	root	%D		443	10000	15	2015-05-14 11:25:47	em7admin	
A GoGrid - Example	al orgs]				Basic/Snippet	ISECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 11:25:51	em7admin	
PIPSLA Example	(all orgs)				SNMP				161	1500	5	2015-05-14 11:25:14	em7admin	
A LifeSize: Endpoint SNMP	all orgs]				SNMP	control			161	3000	18	2015-05-14 11:25:58	em7admin	
2. A LifeSize: Endpoint SSH/CLI	all orgs]				Basic/Snippet	auto	%D		22	3	17	2015-05-14 11:25:58	em7admin	
A Local API	all orgs]				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 11:26:11	em7admin	
4. NetApp 7-mode	all orgs]				Basic/Snippet	root	%D		443	3000	24	2015-05-14 11:26:20	em7admin	
5. A NetApp w/SSL Option	(all orgs)				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 11:26:20	em7admin	
5. A NetApp w/SSL Option Off	al orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 11:26:20	em7admin	
. A Nexus netconf	all orgs]				Basic/Snippet		%D		22	10000	6	2015-05-14 11:25:16	em7admin	
Nexus snmp	(all orgs)				SNMP				161	10000	7	2015-05-14 11:25:16	em7admin	
Polycom - Advanced	all orgs]				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 11:26:24	em7admin	
). A Polycom - CDR	a [all orgs]				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 11:26:24	em7admin	
Polycom - Interface	(all orgs)				SOAP/XML Host	admin	%D		80	20000	29	2015-05-14 11:26:24	em7admin	
ewing Page: 1]												[Select Action]	•	G

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
	[Active Directory]
Hostname/IP	Timeout(ms)
	10000
Username	Password
Encrypted Port	PowerShell Proxy Hostname/IP
[yes] T 5986	
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

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]	×					
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

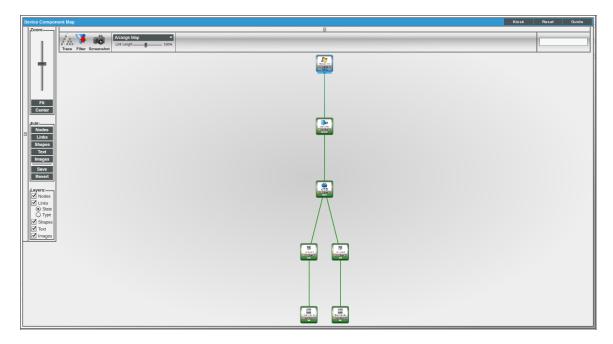
When SL1 performs collection for the "Microsoft Hyper-V Guest Configuration Cache" and "Microsoft Hyper-V Guest Discovery" Dynamic Applications, SL1 will create component devices for the virtual machines on the Hyper-V and align other Dynamic Applications to those component devices. All component devices 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 (Registry > Devices > Device Components) 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 (+):



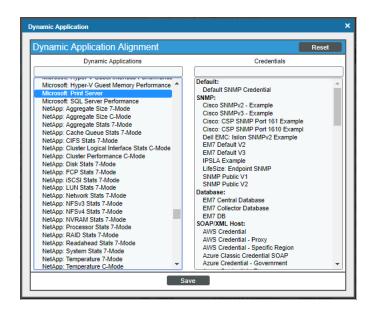
The Component Map page (Views > Device Maps > Components) allows you to view devices by root
node and view the relationships between root nodes, parent components, and child components in a map.
This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the
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 (<sup>J</sup>).
- 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



## Executing the SL1 Agent with Windows PowerShell

#### Overview

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

What is an SL1 Agent?	. 93
Agent-Compatible PowerPacks	.94
The Credential for the SL1 Agent	. 94
Configuring the SL1 Agent Device Template	. 95

## What is an SL1 Agent?

The *SL1 Agent* is a program that runs on a device or element monitored by SL1. The SL1 Agent collects data from the device, interface, or other element and pushes that data back to SL1. You can install and use multiple SL1 Agents, as needed.

Because an agent is always running on a device, the SL1 Agent can collect more granular data than can be collected by polling the device periodically with a Data Collector. You can collect data from devices using only the SL1 Agent or using a combination of the SL1 Agent and Data Collectors.

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 **Credential Management** page (System > Manage > Credentials):

Credential Editor [102]	>
Edit PowerShell Credential #102	New Reset
Basic Settings         Profile Name         SL1 Agent PowerShell Default         Hostname/IP         %D         Username         testLocalPowershell         Encrypted         Port         [no]         ▼	Account Type [[Local]  Timeout(ms) [10000 Password PowerShell Proxy Hostname/IP [
Active Directory Settings Active Directory Hostname/IP Save Save As	Domain

## 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 (Registry > Devices > Templates).
- 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:

Device Template Editor I Editing Dynamic A	pplication Subtemplates (Click field labels t	o enable/disable them)	New	Reset
Templat	e 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			
1. App: Microsoft: Windows Server B 🗬	All devices (all as any see Realized as a day	Align Dynamic Application With		•
2. App: Microsoft: Windows Server C 🚭	All devices (align new applications and up	date collection states)		•
App: Microsoft: Windows Server C     4. App: Microsoft: Windows Server C	Dynamic Application Settings			
5. App: Microsoft: Windows Server D		Dynamic Application		
6. App: Microsoft: Windows Server D	Microsoft: Windows Server BIOS Configu	Iration		•
<ol> <li>App: Microsoft: Windows Server D 8. App: Microsoft: Windows Server In </li> </ol>	Crea	dentials	Poll Rate	
9. App: Microsoft: Windows Server Ing	SL1 Agent PowerShell Default	•	Every 1 Minute	*
10. App: Microsoft: Windows Server IF		Dynamic Application Presentation Object(s)		
11. App: Microsoft: Windows Server M	BIOS Information	Enabled V		
12. App: Microsoft: Windows Server M	BIOS Information BIOS Details	Enabled V Enabled V		
13. App: Microsoft: Windows Server O	Hardware Make	Enabled V		
14. App: Microsoft: Windows Server P of 15. App: Microsoft: Windows Server S of	BIOS Version	Enabled V		
16. App: Microsoft: Windows Server 3	Discovery Object	Enabled V		
17. App: Microsoft: Windows Server U	Hardware Model	Enabled V		
🛉 Add New Dynamic App Sub-Template	Hardware Serial Number	Enabled T		
•	BIOS Manufacturer	Enabled T		
	Hardware Information	Enabled V		
	Dynamic Application Thresholds			
	Raw Data Retention		J days	
	Save	Save As		

- 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. select the SL1 Agent PowerShell credential in the Credentials field.
- 6. Click [Save].

## Chapter

# 7

## **Windows Dashboards**

#### Overview

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	98
Microsoft: DNS Server Performance	
Microsoft: Exchange Server 2010 Performance	103
Microsoft: Exchange Server 2013 Performance	
Microsoft: IIS Server Performance	109
Microsoft: Lync Server 2010 Dashboards	
Microsoft: Lync Server 2010 Performance	
Microsoft: Lync Server 2010 Utilization	114
Microsoft: Skype for Business Dashboards	117
Microsoft: Lync Server 2013 Performance	117
Microsoft: Lync Server 2013 Utilization	120
Microsoft: SQL Server Performance	123

## 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.

nported PowerPacks™   PowerPack Files Found [298]								Reset			
	PowerPack Name		Revisio	01115							_
	PowerPack Name	Version	<u>n</u>	GUID	All	Last E		All	Import	<u>ea</u> •	2
	Event Association Test	1	1	DED1884762194566B70BCD4DF3A742							
	Event Suppression Test	1	1	EC64565DCA55E155135F91F81F44D8-	_			_			
	SLPSD: Onboarding	0.20000		E121312B60972ED35BEDA19E88D195							
	SL_PS Cisco 3rd Party Device Support	1.39999		8B78EDB3A373B2D187ECEAE2545744				_			-
	NetApp Base Pack		6873	8014D5DAD2B8C9AC3E1DD84CC227E							
6.	Cisco: Contact Center Enterprise *BETA*		1119	7CC6AD933EFB4FF5D840EFEA40F85C	201	5-12-1	4 13:50:5	(201	5-10-2	9 14:56:54	/
7.	EM7 Standard Device Categories	7.7.0	255	7A7322AA30F189B42943C082EFD7121	201	5-06-0	2 18:30:5	E 201	5-10-2	9 14:56:54	1
8.	BL Test	1	2	74F7E816CF0FC9153700D2AF0982C2	201	5-10-2	9 10:56:1	1201	5-10-2	9 10:56:00	1
9.	BL Test	1	1	74F7E816CF0FC9153700D2AF0982C2	201	5-10-2	9 10:56:1	1201	5-10-2	9 10:54:18	1
10.	Microsoft: Office 365 *BETA*	0.5	138	8FA30F7D1FAC9162DD8C717D9EF778				201	5-10-20	0 16:44:37	1
11.	NetApp Base Pack	7.7.0	6838	8014D5DAD2B8C9AC3E1DD84CC227E	201	5-10-2	1 13:31:4	7201	5-10-20	0 16:44:37	1
12.	Cisco: Contact Center Enterprise *BETA*	0.5	1109	7CC6AD933EFB4FF5D840EFEA40F85C	201	5-12-1	4 13:50:5	(201	5-10-20	0 16:44:30	1
13.	EM7 Default Internal Events	7.7.0	316	BE1F363DB4BA9A10F5C6BC28931F0B	201	5-10-2	8 13:26:2	E 201	5-10-20	0 16:44:30	1
14.	F5 BIG-IP *BETA*	7.7.0	3242	BFA4E6B316FD2302D913EF38FE7FF82	201	5-10-2	8 13:26:2	7201	5-10-2	0 16:44:36	1
15.	Microsoft: Office 365 *BETA*	0.5	136	8FA30F7D1FAC9162DD8C717D9EF778				201	5-10-14	4 15:12:24	1
16.	Cisco: Contact Center Enterprise *BETA*	0.5	1022	7CC6AD933EFB4FF5D840EFEA40F85C	201	5-12-1	4 13:50:5	(201	5-10-14	4 15:12:2:	1
17.	Microsoft Base Pack	7.7.0	868	97469E96E98B5DAB516F3CCC8747CE	201	5-10-2	8 13:26:2	E 201	5-10-1:	3 12:47:54	1
18.	EM7 Default Internal Events	7.7.0	315	BE1F363DB4BA9A10F5C6BC28931F0B	201	5-10-2	8 13:26:2	201	5-10-1:	3 12:47:54	1
19.	NetApp Base Pack	7.7.0	6792	8014D5DAD2B8C9AC3E1DD84CC227E	201	5-10-2	1 13:31:4	7201	5-10-1:	3 12:47:54	1

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

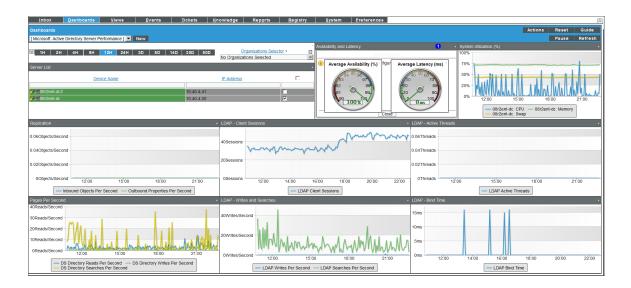
5. The Install PowerPack modal page appears. To install the PowerPack, click [Install].

nstall Power-Pack™   .kates_test_pp_3 \	/ersion 1			Reset			
Package Information GUID: 9F7EC Created: 2015-07-28 14:10:53	5CBC81D713AD94AF704FBA136C Updated: 2015-07-28 14:10:53	Revision: 2 Compil	Exported From: 7.6.0.beta ed: 2015-07-28 14:12:21				
Package Content							
	Theme Name		GUID	Action			
1. kates_test_theme_3			A6D9EA56C5FAE1F35E6F0411BD79AD0	update			
2. kates_test_theme_4			ADA02B6763C3CCA014FBB00A9A21A64	update			
Installation Key: hBGC6WETV3SH8Epeyp7cpySyuEak0FeBpD/IYENPd0oBScXOJmVT4Z12fQmolbNRR/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
월 1H 2H 4H 6H <mark>12H</mark> 24H	30 7D 14D 300 900	Crganizations Selector + 22 No Organizations Selected #
Several Ceda Jama PAddata C Ceda Jama PAddata C Paddata C Paddata C Paddata Paddata P Paddata P Paddata P Paddata P P	Available of and configured 202 This widget is not configured. Average Latency (ms) (1) (1) (1) (1) (1) (1) (1) (1	2010 1007
	Recursive Queries	Recursive Errors - 0.07Queries/Second
3Responses/Sec	0.08Queries/Second	0.06Queries/Second
2.5Responses/Sec	0.05Guerles/Second	0.05Queries/Second
2Responses/Sec	0.04Queries/Second	0.04Queries/Second
1.5Responses/Sec	0.03Queries/Second	0.03Queries/Second
1Responses/Sec	0.02Queries/Second	0.02Queries/Second
0.5Responses/Sec	0.01Queries/Second	0.01Queries/Second
OResponses/Sec 12'00 14'00 16'00 18'00 20'00 22'00	0Queries/Second 12'00 14'00 16'00 18'00 20'00 22'00	0Queries/Second 12'00 14'00 16'00 18'00 20'00 22'00
- Total Responses Sent/Sec - Total Queries Received/Sec	- Recursive Queries/Sec	- 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.

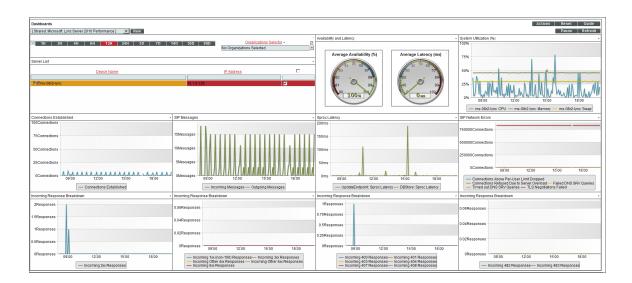
# Microsoft: Lync Server 2010 Dashboards

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 <a href="http://en.wikipedia.org/wiki/List\_of\_SIP">http://en.wikipedia.org/wiki/List\_of\_SIP</a> response codes.

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

**Incoming Response Breakdown**. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 482 Responses and Incoming 483 Responses. Each parameter is represented by a color-coded line. For a description of SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List of SIP response codes.

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

### Microsoft: Lync Server 2010 Utilization

The Microsoft: Lync 2010 Server Utilization dashboard provides an overview of how users are using a selected Lync 2010 server.

Dashboards		Actions Reset Guide
[ Shared: Microsoft: Lync Server 2010 Utilization ] 💽 New		Pause Refresh
		Connected AV Users ·
TH 2H 4H 6H 12H 24H 3D 7D 14D 30D 90D Creanizations Selector 2 2 Organizations Selected		0.06Users
Server List		
Device Name PAddress	0.04Conferences	0.04Users
[An]ms-08/2-lync 10.1.0.139	0.02Conferences	0.02Users
	0Conferences 80.00 10.00 12.00 14.00 16.00 18.00 20.0	0User88'00 10'00 12'00 14'00 16'00 18'00 20'0
	Number of Conferences	- Number of Users
Active Registered Endpoints	- Active IM Conferences -	Connected IM Users ·
2Endpoints	0.08Conferences	0.06Users
1Endpoints	0.04Conferences	0.04Users
0.5Endpoints		0.02Users
0Endpoints 08:00 10:00 12:00 14:00 16:00 18:00 20	0Conferences	0Usera
Endpoint Cache: Active Registered Endpoint	Active Conferences	- Connected Users
Number of Calls	Active AS Conferences -	Connected AS Users ·
1Calls	0.05Conferences	0.06Users
0.75Calls	0.04Conferences	0.04Users
0.25Calls		0.02Users
0C848	0 Conterence§800 10'00 12'00 14'00 16'00 18'00 20'0 — Adtwe Conterences	0User88-00 10'00 12'00 14'00 16'00 18'00 20'0 - 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.

Dashboards			Actions Reset Guide
[Microsoft: Lync Server 2013 Performance ]	w		Pause Refresh
	14D 30D 90D Organizations Selector •	2	System Utilization (%)     . 100%
	No Organizations Selected	Average Availability (%) Average Latency (ms)	75%
Server List Device Name	IP Address	2 94 95 96 97 50 50 60 70	50%
100000 Hearing	10.40.3.7	92 Q 98 (10 P 90)	25%
	10.00.0		0% 06:00 09:00 12:00 15:00
			- tt12r2-Is-01: CPU tt12r2-Is-01: Memory tt12r2-Is-01: Swap
Connections Established	SIP Messages	Sproc Latency	SIP Network Errors
	7500Messages	4ms	1Connections
75Connections	WWWWWWWWWWWWWWWWWW	4115	0.5Connections
50Connections	5000Messages	2ms 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
25Connections	2500Messages	AMMAR MARKEN MARKEN MARKEN AMARKEN AMA	0Connections 04:00 08:00 12:00
0Connections	0Messages 04'00 08'00 12'00	0ms 06:00 09:00 12:00 15	Connections Above Per-User Limit Dropped     Connections Refused Due to Server Overload
Connections Established	Incoming Messages — Outgoing Messages	UpdateEndpoint: Sproc Latency (msec)     DBStore: Sproc Latency	Failed DNS SRV Queries Timed out DNS SRV Queries     TLS Negotiations Failed
Incoming Response Breakdown	Incoming Response Breakdown	Incoming Response Breakdown	Incoming Response Breakdown     1
1000Responses A M. MAM MAN ALMAN		4Responses	0.05Responses
Mr. Mr. and M. and Mr. all Mar W	20Responses	2Responses	
500Responses	0Responses 04:00 08:00 12:00	0Responses 04'00 08'00 12'00	0.025Responses
0Responses 04:00 08:00 12:00	- Incoming 1xx (non-100) Responses	- Incoming 400 Responses - Incoming 401 Responses	0Responses 04:00 08:00 12:00
- Incoming 2xx Responses	Incoming 3xx Responses Incoming Other 4xx Responses     Incoming Other 5xx Responses Incoming 6xx Responses	<ul> <li>Incoming 403 Responses</li> <li>Incoming 404 Responses</li> <li>Incoming 407 Responses</li> <li>Incoming 408 Responses</li> </ul>	- Incoming 482 Responses - Incoming 483 Responses

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 <a href="http://en.wikipedia.org/wiki/List of SIP response codes">http://en.wikipedia.org/wiki/List of SIP response codes</a>.

- 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 <a href="http://en.wikipedia.org/wiki/List">http://en.wikipedia.org/wiki/List</a> 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.

Dashboards		Actions Reset Guide
[ Microsoft: Lync Server 2013 Utilization ]   New		Pause Refresh
		Connected AV Users ·
No Organizations Selected	20Conferences	20Users
Server List •	15Conferences	15Users M M A A A A A A A
	A. M. M. W. C. M. M. M. M. W.	10Users / have show which have show it
Device Name IP Address	10Conferences	loosers / / / / / / / /
P m 10.40.3.7 ♥	5Conferences	5Users
	0Conferences	OUsers
	06:00 09:00 12:00 15:00	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	
75Endpoints	MA MALAMAMA MAN	30Users 11/11/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/1/
		20Users WV WV VV WV -V VV VV VV
50Endpoints		
25Endpoints	5Conferences	10Users
		01/2017
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	15Users
0.04Calls		
	V V	
0.02Calls	5Conferences	5Users
0Calls 04!00 06!00 08!00 10!00 12!00 14!00	0Conferences 06:00 09:00 12:00 15:00	OUsers 04.00 06.00 08.00 10.00 12.00 14.00
UpdateEndpoint: Number of Calls	- Active Conferences	- Connected Users

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.

			Logged in as kgibson [Sign-out] Finder [Toolbox]
	owledge Reports Registry System Preferences Network Co	-Re Material Tallia	
Ousthourds			Actions Reset Guide
[ Shared: Microsoft: SQL Server Performance ]			Pause Refresh
		Availability and Latency -	
S 1H 2H 4H 6H 12H 24H 30 7D	140 300 900 Organizations Selector • D		80%
		Average Availabilit (%)	
Cuttom Device Table			62%
Device Name	IP. Address		
MIN-DEMO-MSSQL	192.168.41.105		40%
PerDemo_Lyno_2013	192.108.41.100		a diala dialahakaka, ala dialahakaka
ACME - DB-MSSQL - WebApp	192.168.32.112	1 95 1 95 90 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
ACME - DB MSSQL 2 - WebApp	192.100.32.113		
			0% 10.00 18.00 20.00 22.00 10.Jan 02.00
		$\sim$	
		Deadlocks	- CPU - Memory - Swap
Buffer Cache Hit Ratio	Average Walt Time     70µs	Deadlods     O.07Deadlods/Sec	0.07Waits/Second
	00.05	0.00Deadlooks/Sec	0.00WaitySecond
80%	0000	0.00Deadlooks/Sec	0.00 Warts Second
	50µs	0.05Deadlooks/Sec	0.05Walts/Second
80%	40µs	0.04Deadloda/Sec	0.04WaltySecond
	30µ5	0.03Deadlode/Sec	0.03Waits/Second
40%	30/15	0.03Deadloda/Sec	0.03Waits/Second
	20µs-	0.02Deadloda/Sec	0.02Waits/Second
20%	10µs	0.01Deadlook/Sec	0.01Waits/Second
		0Deadloda/Sec	0Waits/Second
0% teloo taloo 20/00 22/00 10.'Jan 02/00	0µs teloo 18/00 28/00 22/00 10. Jan 82/00	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%		12.5TransSecond	2.5%aib/Second
	3000000Sec	12.511818384410	
60%		10Trans/Second	2Wata/Second
	2000000Sec	7.5Trans/Second	1.5WaltySecond
40%			
	1000003sec	STrans'Second	1Walts/Second
20%		2.5Trans/Second	0.5Walts/Second
01	05ec 16/00 18/00 20/00 22/00 10.Jan 02/00		0Weits/Second
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
- 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

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

Troubleshooting WinRM Error Messages	
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 <b>Debugging Code 401</b> <i>Errors</i> .)
	Pre-authentication failed while getting initial credentials.
	Client not found in Kerberos database.

Error / Message	Cause / Resolution
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 <b>Debugging Code</b> 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.

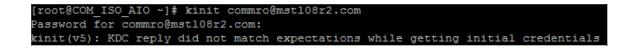
#### Debugging Code 401 Errors

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]
```

- 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:



- 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 - 2020, ScienceLogic, Inc.

#### All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC <sup>™</sup> 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<sup>™</sup> has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic<sup>™</sup> assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic<sup>™</sup> 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<sup>™</sup>
- EM7<sup>™</sup> and em7<sup>™</sup>
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management<sup>™</sup>

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