

Monitoring Windows Systems with WMI

ScienceLogic version 8.10.2

Table of Contents

Introduction	. 4
Monitoring Windows Devices in the ScienceLogic Platform	5
What is SNMP?	5
What is WMI?	. 5
PowerPacks	5
Configuring Windows Systems for Monitoring with SNMP	7
Configuring SNMP for Windows Server 2016 and Windows Server 2012	. 8
Configuring Ping Responses	. 8
Installing the SNMP Service	9
Configuring the SNMP Service	.14
Configuring the Firewall to Allow SNMP Requests	.19
Configuring Device Classes for Windows Server 2016 and Windows 10	.19
Manually Align the Device Class	20
Edit the Registry Key	.20
Configuring SNMP for Windows Server 2008	21
Configuring Ping Responses	21
Installing the SNMP Service	
Configuring the SNMP Service	.25
Configuring the Firewall to Allow SNMP Requests	
Configuring SNMP for Windows Desktop Systems	30
Enabling SNMP on Windows Desktop Systems	
Additional Steps for Configuring SNMP for Windows 10	
Configuring Windows Systems for Monitoring with WMI	
Configuring WMI on Windows 2008 and Later Servers	.40
Step 1: Configuring Services	
Step 2: Configuring the Windows Firewall	
Step 3: Configuring a User Account and Permissions	
Configuring Namespace and DCOM Security Permissions	
Configuring User Account Control to Allow Elevated Permissions	
Configuring WMI for Windows Desktop Systems	
Step 1: Configuring Services	
Step 2: Configuring Windows Firewall	
Step 3: Setting the Default Namespace Security	
Step 4: Setting the DCOM Security Level	
Step 5: Disabling User Account Control	
SNMP and WMI Dynamic Applications for Windows Devices	
SNMP Dynamic Applications	
WMI Dynamic Applications	
Microsoft Base Pack	
Relationships with Other Types of Component Devices	
Creating SNMP and WMI Credentials for Windows Devices	
Creating an SNMP Credential	
Creating a WMI Credential	
Testing Windows Credentials	
SNMP Credential Test	
Basic/Snippet Credential Test	
Running a Windows Credential Test	
Monitoring a Windows Cluster	.81
Monitoring Windows Clusters in the ScienceLogic Platform	
Discovering Cluster Nodes	.82

Aligning a Dynamic Application with a Cluster Node	
Disabling Collection of a Dynamic Application on a Device	
Discovering the Cluster IP Address	
Aligning Dynamic Applications with the Cluster Device	
Using a Device Template to Configure Dynamic Applications	
Automatically Restarting Windows Services	
What is the Windows Restart Automatic Services PowerPack?	
Configuring the Windows Restart Automatic Services PowerPack	
Excluding Automatic Services	
Viewing the List of Excluded Services	
Adding an Excluded Service for All Devices	
Adding an Excluded Service for a Single Device	
Removing an Excluded Service	
-	

Chapter

Introduction

Overview

This manual describes how to monitor Windows systems in SL1 using SNMP and Windows Management Instrumentation (WMI) credentials and Dynamic Applications.

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

Monitoring Windows Devices in the ScienceLogic Platform	5
What is SNMP?	5
What is WMI?	5
PowerPacks	5

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 WMI agent
- Requesting information using the SL1 agent

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

For more information about using the SL1 agent to monitor Windows devices, see the **Monitoring Using** *the ScienceLogic Agent* 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 WMI?

Windows Management Instrumentation, or WMI, is a Windows Service developed to access management information. WMI is a middle-layer technology that enables standardized management of Windows-based computers. It collects computer management data from a wide variety of sources and makes it accessible by using standard interfaces. WMI's specific query language is similar to SQL. For a comparison of WQL and SQL, see http://technet.microsoft.com/en-us/library/cc180454.aspx

PowerPacks

This manual describes content from the following PowerPacks:

- Microsoft Base Pack PowerPack, version 106.
- Windows Restart Automatic Services PowerPack, version 100.

1

Chapter

Configuring Windows Systems for Monitoring with SNMP

Overview

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

Configuring SNMP for Windows Server 2016 and Windows Server 2012	
Configuring Ping Responses	8
Installing the SNMP Service	9
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	20
Edit the Registry Key	
Configuring SNMP for Windows Server 2008	
Configuring Ping Responses	21
Installing the SNMP Service	
Configuring the SNMP Service	
Configuring the Firewall to Allow SNMP Requests	
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:

	Wildo	ws Firewall with Advanced S	county		
le Action View Help					
• 🔿 🙍 🖬 🗟 🚺					
Windows Firewall with Advance	Inbound Rules				Actions
🕵 Inbound Rules	Name	Group	Profile	Enabled 🔨	Inbound Rules
🌇 Outbound Rules	🕜 Core Networking - Multicast Listener Qu	Core Networking	All	Yes	🗱 New Rule
Source Connection Security Rules	🕜 Core Networking - Multicast Listener Rep	p Core Networking	All	Yes	Tilter by Profile
and monitoring	🔮 Core Networking - Multicast Listener Rep		All	Yes	1 '
	🖉 Core Networking - Neighbor Discovery A	-	All	Yes	🕎 Filter by State
	🔮 Core Networking - Neighbor Discovery S	~	All	Yes	🕎 Filter by Group
	🔮 Core Networking - Packet Too Big (ICMF		All	Yes	View
	🖉 Core Networking - Parameter Problem (I	~	All	Yes	Q Refresh
	Core Networking - Router Advertisemen		All	Yes	
	Core Networking - Router Solicitation (IC	-	All	Yes ≡	📑 Export List
	Core Networking - Teredo (UDP-In)	Core Networking	All All	Yes Yes	👔 Help
	Core Networking - Time Exceeded (ICMF Distributed Transaction Coordinator (RP			No	File and Printer Sharing (Echo Request
	Distributed Transaction Coordinator (RP)	1		No	
	Distributed Transaction Coordinator (TC			No	O Enable Rule
	File and Printer Sharing (Echo R	Sharing	All	No	🦂 Cut
	File and Printer Sharing (Echo R	able Rule Sharing	All	Yes	E Copy
	File and Printer Sharing (LLMNF Cu		All	No	🗶 Delete
		opy Sharing	All	No	
	Cile and Drinker Sharing /ND Na	elete Sharing	All	No	Properties
	File and Printer Sharing (NB-Ses	Sharing	All	No	👔 Help
	File and Printer Sharing (SMB-Ir	operties Sharing	All	No	
	File and Printer Sharing (Spoole He	elp Sharing	All	No	
	File and Printer Sharing (Spooler Service)	File and Printer Sharing	All	No	
	File and Printer Sharing over SMBDirect ((i File and Printer Sharing over	All	No	
	iSCSI Service (TCP-In)	iSCSI Service	All	No	
	🚳 Key Management Service (TCP-In)	Key Management Service	All	No	
	🚳 Netlogon Service (NP-In)	Netlogon Service	All	No	
	Netlogon Service Authz (RPC)	Netlogon Service	All	No	
	Network Discovery (LLMNR-UDP-In)	Network Discovery	All	No	
	Network Discovery (NB-Datagram-In)	Network Discovery	All	No	
	Network Discovery (NB-Name-In)	Network Discovery	All	No	
	Network Discovery (Pub-WSD-In)	Network Discovery	All	No 🗸	
III >	<			>	

Installing the SNMP Service

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

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

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

b	Add Roles and Features Wizard					
Select installation	type Destination server win-sug/ks2colq					
Before You Begin Installation Type	Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).					
Server Selection Server Roles	 Role-based or feature-based installation Configure a single server by adding roles, role services, and features. 					
Features O Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.						
Results						
< Previous Next > Install Cancel						

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

Add Roles and Features Wizard							
Select destination	n server			DESTINATION SERVER WIN-3UGJKS2COLQ			
Before You Begin Select a server or a virtual hard disk on which to install roles and features. Installation Type Select a server from the server pool Server Selection Select a virtual hard disk Server Roles Server Pool Features Filter:							
Confirmation Results	Name WIN-3UGJKS2COLQ	IP Address 10.100.100.22	Operating System Microsoft Windows Server 2012	2 R2 Standard			
		Server Manager. Off	dows Server 2012, and that have b line servers and newly-added serv				
		< Pre	vious Next >	nstall 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:

Select features DESTINATIO	
Before You Begin Select one or more features to install on the selected server.	
Installation Type Features Description	
Server Selection Server Roles Peatures Confirmation Results Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management IIS Hostable Web Core Ink and Handwriting Services NET Framework 3.5 Features NET Framework 3.5 combin power of the .NET Framework 3.5 combin power of the .NET Framework APIs with new technologies building applications that of appealing user interfaces, pi your customers' personal id information, enable seamles secure communication, and the ability to model a range business processes.	rk 2.0 for otect entity s and provide
< Previous Next > Install	Cancel

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

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

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

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

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

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

Configuring the SNMP Service

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

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

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

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

SNMP	Service Propert	ties (Lo	cal Con	nputer) 🛛 🗙		
General Log On	Recovery Agent	Traps	Security	Dependencies		
Service name:	SNMP					
Display name:	SNMP Service					
Description:	Enables Simple Net (SNMP) requests to					
	Path to executable: C:\Windows\System32\snmp.exe					
Startup type:	Startup type: Automatic 🗸					
Service status:	Running					
Start	Stop	Pau	ise	Resume		
You can specify t from here. Start parameters:	he start parameters th	nat apply	when you	start the service		
Start parameters.						
	10	< [Cancel	Apply		

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

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

SNMF	? Service P	Propert	ies (Lo	cal Con	nputer) 🛛 💌	
General Log On	Recovery	Agent	Traps	Security	Dependencies	
Send auther	tication trap					
- Accepted cor	nmunity name	s				
Community			Rig	nts		
A	.dd	Edi	t	Remo	ve	
		,				
	NMP packets NMP packets	-				
localhost	ми раскез		se nosis			
locariost						
				_		
	.dd	Edit		Remo	ve	
		OK	;	Cancel	Apply	1
		2.				1

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

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

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

		window	s Firewall with Adv	/anced Sec	urity					- 0	×
le Action View Help											
🔿 🔁 🖬 🗟 🖬											
Windows Firewall with Advance	Inbound Rules									Actions	_
K 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	-
La Connection Security Rules	Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System	Any	112	-	
. 🛃 Monitoring	Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System	Any	11	Filter by Profile	
	Remote Scheduled Tasks Management (Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	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 Manageme	nt All	No	Allow	No	System	Any	11		
	Remote Service Management (RPC)	Remote Service Manageme	nt All	No	Allow	No	%System	Any		View	
	Remote Service Management (RPC-EPM	Remote Service Manageme	nt All	No	Allow	No	%System	Anv		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	- 112		
	Remote Volume Management - Virtual D	Remote Volume Managem	a. All	No	Allow	No	%System		111	? Help	
	Remote Volume Management - Virtual D			No	Allow	No	%System			SNMP Service (UDP In)	
	Remote Volume Management (RPC-EPM			No	Allow	No	%System	Any		C Enable Rule	-
	Routing and Remote Access (GRE-In)	Routing and Remote Acces		No	Allow	No	System	Any	11	-	
	Routing and Remote Access (L2TP-In)	Routing and Remote Acces		No	Allow	No	System	Any		🦨 Cut	
	Routing and Remote Access (PPTP-In)	Routing and Remote Acces		No	Allow	No	System	Any		Сору	
	Secure Socket Tunneling Protocol (SSTP			No	Allow	No	System	Any		X Delete	
	SNMP Service (UDP In)	SNMP Service	Domain, Public	Yes	Allow	No	%System				
	SNMP Service (UDP In)		Private, Public	No	Allow	No	%System	Any		Properties	
	SNMP Trap Service (UDP In)	Enable Rule	Private, Public	No	Allow	No	%System		- 11	? Help	
		Cut	Domain	No	Allow	No	%System	Any	-11-		
		Copy ard Ma		No	Allow	No	%System	Any			
		Delete ard Ma		No	Allow	No	%System				
	TPM Virtual Smart Card Managemen	Delete ard Ma		No	Allow	No	%System		=		
	TPM Virtual Smart Card Managemen	Properties and Ma		No	Allow	No	%System				
	Wirtual Machine Monitoring (DCOM-	Help		No	Allow	No	%System	Any			
	Wirtual Machine Monitoring (Echo Reque			No	Allow	No	Any	Any	-11		
	Wirtual Machine Monitoring (Echo Reque			No	Allow	No	Any	Any			
	Wirtual Machine Monitoring (NB-Session			No	Allow	No	Any	Any			
	A.c. 114 12 14 15 1 (00.00)								~		
III >	< III							>			

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:

- 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.
- If you want SL1 to discover your Windows Server using an IPv4 address, locate the File and Printer Sharing (Echo Request - ICMPv4-In) rule.
- 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:

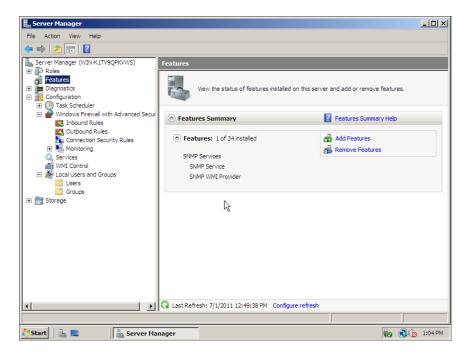
	Wind	lows Firewall wi	th Advanced S	ecurity		
le Action View Help						
• 🔿 🙇 🖬 🖬 🖬						
Windows Firewall with Advance	Inbound Rules					Actions
🔣 Inbound Rules	Name	Group	•	Profile	Enabled 🔨	Inbound Rules
🔀 Outbound Rules	🔇 Core Networking - Multicast Listener	Qu Core Networl	ding	All	Yes	🗱 New Rule
tonnection Security Rules	🔇 Core Networking - Multicast Listener I	Rep Core Networl	cing	All	Yes	
s wonitoring	🕑 Core Networking - Multicast Listener I	Rep Core Networl	king	All	Yes	Filter by Profile
	🔇 Core Networking - Neighbor Discover	y A Core Networl	ling	All	Yes	🕎 Filter by State
	🕑 Core Networking - Neighbor Discover	y S Core Networl	ling	All	Yes	Y Filter by Group
	🕑 Core Networking - Packet Too Big (IC	MP Core Networl	ling	All	Yes	View
	🔇 Core Networking - Parameter Problen	n (I Core Networl	cing	All	Yes	
	🔇 Core Networking - Router Advertisem	ent Core Networl	ding	All	Yes	🖸 Refresh
	🖉 Core Networking - Router Solicitation	(IC Core Networl	ang	All	Yes =	= Export List
	🔇 Core Networking - Teredo (UDP-In)	Core Networl		All	Yes	- Help
	🔇 Core Networking - Time Exceeded (IC	MP Core Networl	ang	All	Yes	
	🔘 Distributed Transaction Coordinator (RPC) Distributed T	ransaction Coo	All	No	File and Printer Sharing (Echo Reques
	🔘 Distributed Transaction Coordinator (RP Distributed T	ransaction Coo	All	No	Enable Rule
	Distributed Transaction Coordinator (TC Distributed T	ransaction Coo	All	No	🖉 🔏 Cut
	File and Printer Sharing (Echo R	Enable Rule	Sharing	All	No	
	🖉 File and Printer Sharing (Echo R		Sharing	All	Yes	Сору
		Cut	Sharing	All	No	🔀 Delete
	File and Printer Sharing (NB-Dat	Сору	Sharing	All	No	Properties
	File and Printer Sharing (NB-Na	Delete	Sharing	All	No	2 Help
	File and Printer Sharing (NB-Ses	Properties	Sharing	All	No	
	SMB-Ir 🔮 🖤 🖉	Propercies	Sharing	All	No	
		Help	Sharing	All	No	
	File and Printer Sharing (Spooler Servi		-	All	No	
	File and Printer Sharing over SMBDire		er Sharing over	All	No	
	SCSI Service (TCP-In)	iSCSI Service		All	No	
	WKey Management Service (TCP-In)	Key Manager		All	No	
	Whetlogon Service (NP-In)	Netlogon Ser		All	No	
	Netlogon Service Authz (RPC)	Netlogon Ser		All	No	
	Network Discovery (LLMNR-UDP-In)	Network Disc	2	All	No	
	Network Discovery (NB-Datagram-In)		-	All	No	
	Network Discovery (NB-Name-In)	Network Disc		All	No	
	Network Discovery (Pub-WSD-In)	Network Disc	overy	All	No 🗸	~
III >	<				>	

Installing the SNMP Service

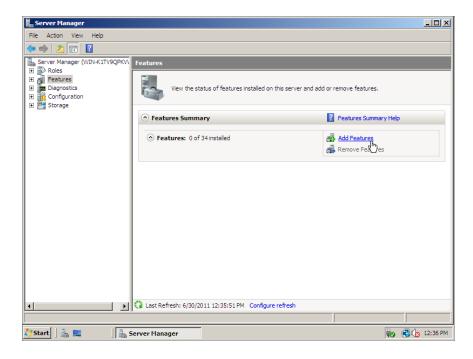
To install the SNMP service on a Windows 2008 Server, perform the following steps:

1. Open the Server Manager utility.

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



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 This server might need to be restarted after the installation completes.	
	< <u>Previous</u> <u>Next></u> <u>Instal</u> Cancel	

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

Add Features Wizard		X
Installation Res	sults	
Features Confirmation Progress Results	The following roles, role services, or features were installed successfully: Image: Antiperiod State of the services of the services of the services of the service of the	
	< <u>Previous</u> <u>Next</u> > <u>Close</u> 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-K1TV9QPKVWS)	x
General Log On	Recovery Agent Traps Security Dependencies	_
Service name:	SNMP	
Display name:	SNMP Service	
Description:	Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.	
Path to executable C:\Windows\Syste	·	
Startup type:	Automatic	
Help me configure	service startup options.	
Service status:	Started	
Start	Stop Pause Resume	
You can specify th from here.	e start parameters that apply when you start the service	
Start parameters:		
	OK Cancel Apply	

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

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

SNMP Service Properties (W	IN-K1TV9QP	KVWS)	×
General Log On Recovery	Agent Tra	ps Security	Dependencies
Send authentication trap			
- Accepted community name			
Community		Rights	
Add	Edit	Remo	ove
C Accept SNMP packets	s from any hos	st	
 Accept SNMP packets 	s from these h	osts	k
localhost			
Add	Edit	Remo	ve
Leam more about <u>SNMP</u>			
	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)	x
General Log On Recovery Agent Traps Security Dependencies	
Send authentication trap Accepted community names Community Rights	
SNMP Service Configuration	
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 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.
- Click the [Add] button to add the community string to list of community strings this Windows 2008 Server accepts.
- 8. In the Accept SNMP packets from these hosts panel, click the Add... button. The SNMP Service Configuration pop-up window is displayed:

SNMP Service Properties (WIN-2TVE5CDI762)
General Log On Recovery Agent Traps Security Dependencies
Cepted community names
Community Rights
cOsmOs READ ONLY
SNMP Service Configuration
Add
Host name, IP or IPX address:Cancel
Add Edit Remove
Learn more about <u>SNMP</u>
OK Cancel Apply

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

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

Configuring the Firewall to Allow SNMP Requests

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

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

🔗 Windows Firewall with Advanced Security 🗕 🗖 🌅									x	
File Action View Help										
🔶 🧆 📰 📑 🚺										
P Windows Firewall with Advance	Inbound Rules						Actions			
🔣 Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Inbound Rules	
🗱 Outbound Rules	Remote Event Log Management (RPC-EP	Remote Event Log Manage	All	No	Allow	No	%System	Any	Rew Rule	
Lonnection Security Rules	Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow N	No	%System	Any		
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	No	%System	Any	🕎 Filter by State	•
	Remote Scheduled Tasks Management (Remote Scheduled Tasks M	All	No	Allow	No	%System	Any	Filter by Group	•
	Remote Service Management (NP-In)	Remote Service Management	All	No	o Allow No System Any	Any	1 · · ·	· · ·		
	Remote Service Management (RPC)	Remote Service Management		No	Allow	No	%System	Any	View	•
	Remote Service Management (RPC-EPM	Remote Service Management	All	No	Allow	No	%System		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		
	Remote Volume Management - Virtual D Remote Volume Manageme Remote Volume Management - Virtual D Remote Volume Manageme Remote Volume Management (RPC-EPM Remote Volume Manageme		All		I Help					
				No	Allow	No	%System	Any	SNMP Service (UDP In)	-
				No	Allow	No	%System	Any	O Enable Rule	-
	Routing and Remote Access (GRE-In)	Routing and Remote Access	All	No	Allow	No	System	Any		
	Routing and Remote Access (L2TP-In)	Routing and Remote Access	All	No	Allow	No	System	Any	a Cut	
	Routing and Remote Access (PPTP-In) Routing and Remote Access Secure Socket Tunneling Protocol (SSTP SNUP Service (UDP In) SNUP Service		All	No	Allow	No	System	Any	В Сору	
			All	No	Allow	No	System	Any	🗙 Delete	
			Domain, Public	Yes	Allow	No	%System	Any		
	SNMP Service (UDP In)	C1 11 10 C 1	Private, Public	No	Allow	No	%System	Any	Properties	
	SNMP Trap Service (UDP In)	Enable Rule	Private, Public	No	Allow	No	%System		🕜 Help	
	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	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 Regue	All	No	Allow	No	Any	Any			
	Wirtual Machine Monitoring (Echo Regue	All	No	Allow	No	Any	Any			
	Wirtual Machine Monitoring (NB-Session	All	No	Allow	No	Any	Any	-		
	Z						· · · · · · · · · · · · · · · · · · ·	-		
								1	1	
nable Rule										

Configuring SNMP for Windows Desktop Systems

This section describes how to configure devices that are running a desktop version of the Windows operating system for monitoring by SL1 using SNMP.

Before performing the tasks described in this section, you must know the IP address of each SL1 appliance in your network. If you have not installed a SL1 appliance, you must know the future IP address that will be used by each SL1 appliance.

2

NOTE: To be monitored by SL1, a Windows device must be running the Windows 7 operating system or later.

NOTE: TCP/IP must be installed and configured before you can install SNMP on a Windows device.

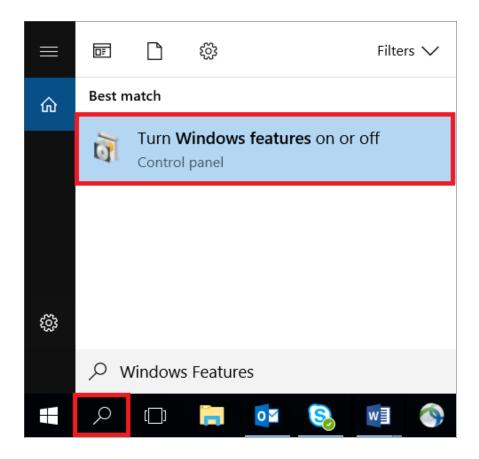
Enabling SNMP on Windows Desktop Systems

You must enable SNMP on each Windows device that you want to monitor with $\mathsf{SL1}$.

NOTE: The following instructions describe how to enable SNMP on devices running a desktop version of the Windows 10 operating system. For instructions on how to enable SNMP on earlier Windows versions, consult Microsoft's documentation.

To enable SNMP on a device running a desktop version of the Windows 10 operating system:

- 1. Click the magnifying glass icon in the bottom-left corner and type "Windows Features" in the **Search** *Windows* field.
- 2. Click Turn Windows features on or off.

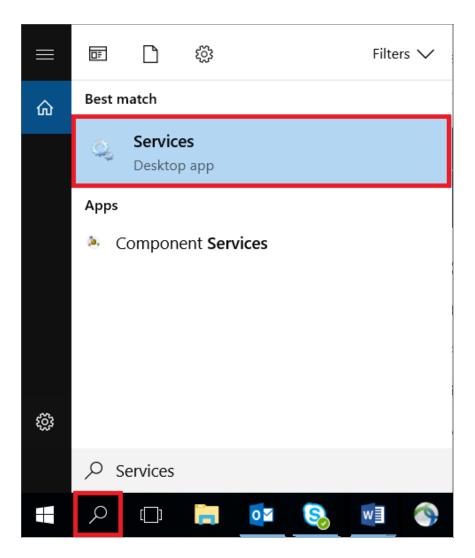


3. In the Turn Features on or off window, expand the Simple Network Management Protocol (SNMP) folder and then select the WMI SNMP Provider checkbox.

Windows Features —		\times
Turn Windows features on or off		?
To turn a feature on, select its check box. To turn a feature off, box. A filled box means that only part of the feature is turned		check
Microsoft XPS Document Writer		^
Hereit MultiPoint Connector		
Print and Document Services		
RAS Connection Manager Administration Kit (CMA	<)	
Remote Differential Compression API Support		
RIP Listener		
E Services for NFS		
Simple Network Management Protocol (SNMP)		
WMI SNMP Provider		
Simple TCPIP services (i.e. echo, daytime etc)		
🗄 🔳 📙 SMB 1.0/CIFS File Sharing Support		
SMB Direct		
Telnet Client		\sim
ОК	Cã	ancel

- 4. Click **[OK]**, and then click **[Close]** after the confirmation message appears.
- 5. Click the magnifying glass icon in the bottom-left corner and type "Services" in the Search Windows field.

6. Click the **Services** Desktop app.



e Action View	· · · ·					
Services (Local)						
Services (Local)	Services (Local)	^				
	SNMP Service	Name	Description	Status	Startup Type	Log On As
	Stop the service	Server	Supports file	Running	Automatic (Tri	Local System
	Restart the service	Shared PC Account Manager	Manages pr		Disabled	Local System
		Shell Hardware Detection	Provides not	Running	Automatic	Local System
		🎑 Smart Card	Manages ac	Running	Automatic (Tri	Local Service
	Description: Enables Simple Network	Smart Card Device Enumerat	Creates soft		Manual (Trigg	Local System
	Management Protocol (SNMP)	Smart Card Removal Policy	Allows the s		Manual	Local System
	requests to be processed by this	SNMP Service	Enables Sim	Running	Automatic	Local System
	computer. If this service is stopped,	🆏 SNMP Trap	Receives tra		Manual	Local Service
	the computer will be unable to process SNMP requests. If this service is disabled, any services that explicitly	🆏 Software Protection	Enables the		Automatic (De	Network Se
		🎑 Spatial Data Service	This service i		Manual	Local Service
	depend on it will fail to start.	🎑 Spot Verifier	Verifies pote		Manual (Trigg	Local System
		🎑 SSDP Discovery	Discovers ne	Running	Manual	Local Service
		🎑 State Repository Service	Provides req	Running	Manual	Local System
		Still Image Acquisition Events	Launches ap		Manual	Local System
		Storage Service	Provides ena	Running	Manual (Trigg	Local System
		Storage Tiers Management	Optimizes th	-	Manual	Local System
		Superfetch	Maintains a	Running	Automatic	Local System
		Symantec Endpoint Protecti	Provides mal	Running	Automatic	Local System
		Symantec Network Access C	Checks that	-	Manual	Local System
		Sync Host_1b4edb	This service	Running	Automatic (De	Local System
		System Event Notification S	Monitors sy	Running	Automatic	Local System
		System Events Broker	Coordinates	Running	Automatic (Tri	Local System
		A Task Scheduler	Enables a us	Running	Automatic	Local System
		CP/IP NetBIOS Helper	Provides sup	Running	Manual (Trigg	Local Service
		A Telephony	Provides Tel		Manual Manual	Network Se
		Chemes	Provides use	Running	Automatic	Local System

7. From the list of services in the right pane, double-click **SNMP Service**.

8. In the SNMP Service Properties dialog box, click the [General] tab and enter the following:

SNMP Ser	SNMP Service Properties (Local Computer)										
General	Log On	Recovery	Agent	Traps	Security	Dependencies					
Service	Service name:		SNMP								
Display	name:	SNMP Service									
Descript	Description:		Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.								
	Path to executable: C:\WINDOWS\System32\snmp.exe										
Startup	type:	Automatic	Automatic ~								
Service	Service status: Running										
S	Start		Stop Pause			Resume					
You can specify the start parameters that apply when you start the service from here.											
Start pa	rameters:										
			Oł	(Cancel	Apply					

• Startup type. Select Automatic.

- 9. In the SNMP Service Properties dialog box, click the [Security] tab.
- 10. In the Accepted community names pane, click [Add].

SNMP Service Properties (Local Computer)										
General	Log On	Recovery	Agent	Traps	Security	Dependencies				
Send authentication trap										
Accepted community names										
Community Rights										
	Add Edit Remove									
		IP packets fr IP packets fr	-							
lo	calhost									
	Ad	ld	Edit		Remo	ove				
			OK	(Cancel	Apply				

11. In the **SNMP Service Configuration** dialog box, complete the following fields:

SNMP Service Configuration		×
Community rights: READ ONLY	~	Add
Community Name:	•	Cancel

- Community rights. Select READ ONLY.
- Community Name. Type the SNMP Community String.
- 12. Click the **[Add]** button.
- 13. In the **SNMP Service Properties** dialog box, in the **[Security]** tab, select the Accept SNMP packets from these hosts checkbox and then click **[Add]**.
- 14. In the SNMP Service Configuration dialog box, complete the following field:

SNMP Service Configuration	×
	Add
Host name, IP or IPX address:	Cancel

- Host name, IP or IPX address. Type the IP address of your ScienceLogic Data Collector or All-In-One Appliance.
- 15. Click [Add].
- 16. In the SNMP Service Properties dialog box, click the [General] tab.

17. If the service is not running, click the **[Start]** button in the **Service status** pane.

SNMP Se	rvice Prop	perties (Loc	al Com	outer)				\times
0		_	-	_		_		
General	Log On	Recovery	Agent	Traps	Security	Depender	ncies	
Service	name:	SNMP						
Display	name:	SNMP Ser	vice					
Descript	tion:	Enables Si (SNMP) re				Protocol is computer		
	executabl DOWS\Sy	e: stem32∖snm	p.exe					
Startup	type:	Automatic					~	
Service	status:	Stopped						
s	Start	Stop)	Pau	ise	Resum	е	
from he		he start para	meters th	at apply	when you s	start the ser	vice]
			Oł	(Cancel	/	Apply	

18. Click [OK].

Additional Steps for Configuring SNMP for Windows 10

To configure SNMP for Windows 10 operating systems, you must also **Configure Device Classes for Windows** 10.

Chapter

with WMI

3

Overview

The following sections describe how to configure Windows Server 2008 and later and Windows desktop systems for monitoring by SL1 using SNMP:

Configuring Windows Systems for Monitoring

Configuring WMI on Windows 2008 and Later Servers	
Step 1: Configuring Services	
Step 2: Configuring the Windows Firewall	
Step 3: Configuring a User Account and Permissions	
Configuring Namespace and DCOM Security Permissions	43
Configuring User Account Control to Allow Elevated Permissions	
Configuring WMI for Windows Desktop Systems	
Step 1: Configuring Services	
Step 2: Configuring Windows Firewall	
Step 3: Setting the Default Namespace Security	
Step 4: Setting the DCOM Security Level	
Step 5: Disabling User Account Control	

Configuring WMI on Windows 2008 and Later Servers

Windows Management Instrumentation, or WMI, is the infrastructure that provides information about operations and management on Windows-based operating systems. WMI can be configured to respond to remote requests from SL1.

To configure a Windows device to respond to remote requests, you must perform the following steps:

- 1. Configure Services
- 2. Configure the Windows Firewall
- 3. Configure a user account and permissions

Most remote requests can be performed by a standard (non-administrator) user account that has been granted specific privileges. However, some requests can be performed only by a user with elevated permissions. For requests performed by SL1 to a Windows server, the following users have elevated permissions:

- The default "Administrator" user account.
- A user account in the Administrators group on a Windows server that has User Account Control disabled.
- A user account in the **Administrators** group on a Windows server where a registry entry has been added to disable remote User Account Control filtering.

For a list of WMI classes that require elevated permissions, see <u>http://msdn.microsoft.com/en-</u>us/library/windows/desktop/aa826699%28v=vs.85%29.aspx

For a list of default WMI Dynamic Applications that require elevated permissions, see the chapter on Dynamic Applications for Windows Devices.

Step 1: Configuring Services

The following services must be running for a Windows device to respond to remote WMI requests:

NOTE: ScienceLogic recommends you set all these services to automatically start.

- COM+ Event System
- DCOM Server Process Launcher
- Remote Procedure Call (RPC)
- Remote Registry
- Server
- Windows Management Instrumentation

To ensure a service is running, perform the following steps:

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

Server Manager						_ 🗆
File Action View Help						
🔄 🔿 🙍 📷 🗠 📾 🚺 🖬 🕨						
Server Manager (QA-DOM-CTRL-1)	Services					Actions
Roles Features	Ö. Services					Services
Diagnostics						More Actions
Configuration	Select an item to view its description.	Name A	Description Status	Startup Type	Log On As 🔺	
(D) Task Scheduler		Active Directory Domain Services	AD DS Dom Started	Automatic	Local System	11
🗄 💣 Windows Firewall with Advanced Secu		Active Directory Web Services	This servic Started	Automatic	Local System	
Services		Application Experience	Processes Started	Manual	Local System	
WMI Control		🔍 Application Identity	Determines	Manual	Local Service	
🗄 🔠 Storage		C Application Information	Facilitates Started	Manual	Local System	
	1	Application Layer Gateway Service	Provides s	Manual	Local Service	
		Application Management	Processes i	Manual	Local System	
		🚳 Background Intelligent Transfer Service	Transfers f Started	Manual	Local System	
		Base Filtering Engine	The Base F Started	Automatic	Local Service	
		Certificate Propagation	Copies use Started	Manual	Local System	
		🖾 CNG Key Isolation	The CNG k	Manual	Local System	
		🚳 COM+ Event System	Supports S Started	Automatic	Local Service	
		COM+ System Application	Manages t	Manual	Local System	
		Computer Browser	Maintains a	Disabled	Local System	
		🚳 Credential Manager	Provides s	Manual	Local System	
		Cryptographic Services	Provides fo Started	Automatic	Network S	
		COM Server Process Launcher	The DCOM Started	Automatic	Local System	
		🖾 Desktop Window Manager Session Manager	Provides D Started	Automatic	Local System	
		OFS Namespace	Enables vo Started	Automatic	Local System	
		OF5 Replication	Enables yo Started	Automatic	Local System	
		O DHCP Client	Registers a Started	Automatic	Local Service	
		Diagnostic Policy Service	The Diagno Started	Automatic (D	Local Service	
		Diagnostic Service Host	The Diagno	Manual	Local Service	
		Diagnostic System Host	The Diagno	Manual	Local System	
		Sisk Defragmenter	Provides Di	Manual	Local System	
		Distributed Link Tracking Client	Maintains I	Manual	Local System	
		Distributed Transaction Conrdinator	Coordinate Started	Automatic (D		
		DNS Client	The DNS Cl Started	Automatic	Network S	
	1	DNS Server	Enables DN Started	Automatic	Local System	
	1	Encrypting File System (EFS)	Provides th	Manual	Local System	
	1	Extensible Authentication Protocol	The Extens	Manual	Local System	
	1	S File Replication Service	Synchroniz Started	Automatic	Local System ·	1
()	Extended Standard	and the second se				-
	Centerious / Standard /					

2. For each required service, the **Startup Type** column should display Automatic. If a service does not have a **Startup Type** of Automatic, double-click on that service. The Properties window for that service is displayed:

COM+ Event Syste	m Properties (QA-	DOM-CTRL-1)	×
General Log On	Recovery Depende	encies	
Service name:	EventSystem		
Display name:	COM+ Eivent System	i	
Description:	Supports System Ev which provides auto	ent Notification S matic distribution	ervice (SENS), ▲ of events to ▼
Path to executable C:\Windows\syste	e: em32\svchost.exe -k l	LocalService	
Startup type:	Automatic		▼
Help me configure	service startup option	<u>18.</u>	
Service status:	Started		
Start	Stop	Pause	Resume
You can specify th from here.	ie start parameters tha	at apply when you	ı start the service
Start parameters:			
	OK	Canc	el Apply

- 3. In the **Startup Type** field, select Automatic.
- 4. Click the [Apply] button.
- 5. If the service has not already started, click the **[Start]** button.

Step 2: Configuring the Windows Firewall

To configure Windows Firewall to accept remote WMI requests:

- 1. Click the magnifying glass icon in the bottom-left corner and type "Command Prompt" in the **Search Windows** field.
- 2. Execute the following two commands in the Command Prompt window:

netsh advfirewall firewall set rule group="windows management instrumentation (wmi)"
new enable=yes
netsh advfirewall firewall set rule group="remote administration" new enable=yes

3. If the result of the second command is "No rules match the specified criteria", run the following two commands:

netsh firewall set service remoteadmin enable
netsh advfirewall firewall set rule group="remote administration" new enable=yes

Step 3: Configuring a User Account and Permissions

There are three ways to configure the user account that SL1 will use to perform WMI requests:

- To monitor the Windows server using WMI Dynamic Applications that require *standard permissions*, you can configure a standard user account for use by SL1. The user account for use by SL1 must be included in the Distributed COM Users and Performance Monitor Users groups. (For more information, consult Microsoft's documentation.)
- 2. To monitor the Windows server using WMI Dynamic Applications that require **elevated permissions**, you can use the default "Administrator" user account. If you use the "Administrator" user account, you do not need to make changes to the User Account Control settings.
- To monitor the Windows server using WMI Dynamic Applications that require *elevated permissions*, you can also use a user account that is included in the *Administrators* group. However, you must perform **one** of the following additional steps to use this type of user account:
 - Option 1: Make the user a member of the Distributed COM Users and Performance Monitor Users groups, in addition to the Administrator group. (For more information, consult Microsoft's documentation.)
 - Option 2: Configure User Access Control to allow elevated permissions.

Configuring Namespace and DCOM Security Permissions

For each of these methods, you must ensure that the configured Namespace and DCOM security permissions allow that user to perform remote requests.

To configure the Namespace and DCOM security permissions:

- 1. In the left pane of the Server Manager window, expand the Configuration section.
- 2. Right-click on the WMI Control entry and then select Properties.
- 3. In the WMI Control Properties window, click the [Security] tab:

WMI Con	trol Properties			?	х
General	Backup/Restore	Security	Advanced		
Namesp	ace navigation allo	ws you to s	et namespace spe	ecific security.	
±	Root				
				Security	
		OK	Cance	el App	ły

4. In the Security tab, select the Root entry from the navigation pane and then select the [Security] button. The Security for Root window appears.

5. In the **Security for Root** window, select the **[Advanced]** button. The **Advanced Security Settings for Root** window is displayed:

Security for Root	Х
Security	
Group or user names: Administrators (DESKTOP-SR36R55\Administr no_admin (DESKTOP-SR36R55\no_admin)	ators)
Add Permissions for no_admin Allow Execute Methods Image: Comparison of the second seco	Remove Deny
OK Cancel	Apply

6. In the Advanced Security Settings for Root window, click the [Add] button. The Select User, Computer, Service Account, or Group window appears.

Adv	vanced S	ecurity Settings for Root				_		
Dwn	ier:	Administrators (DESKTOP-SR36F	855\Administrators) C	hange				
ern	nissions	Auditing						
	additiona	al information, double-click a perm	nission entry. To modify	y a permission entry, select	the entry and clic	c Edit (if a	ivailable).	
	Туре	Principal	Access	Inherited from	Applies to			-
-	Allow	Administrators (DESKTOP-SR3		None	This names			
2	Allow	no_admin (DESKTOP-SR36R55	Enable Account	None	This names	pace only	, ,	
	Add	Remove View						
Di	isable inl	heritance						
					ОК С	ancel	Арр	ly

7. In the Select User, Computer, Service Account, or Group window :

Select Users or Groups	×
Select this object type: Users, Groups, or Built-in security principals	Object Types
From this location:	
DESKTOP-SR36R55	Locations
Enter the object names to select (<u>examples</u>):	
	Check Names
Advanced OK	Cancel

- In the *Enter the object name to select* field, enter the name of the user account that SL1 will use to perform WMI requests or the name of a group that includes that user account.
- Click the [Check Names] button to verify the name and then click the [OK] button.

8. The **Permission Entry for Root** window is displayed:

Permission	Entry for Root		-		×
Principal:	no_admin (DESKTOP-SR36R55\no_admin) Select a principal				
Type:	Allow				
Applies to:	This namespace and subnamespaces $\qquad \lor$				
Permissions	✓ Execute Methods ☐ Full Write ☐ Partial Write	Enable Account Remote Enable Read Security Edit Security		Clear a	Ш
			ОК	Can	cel

- Select This namespace and subnamespaces in the **Apply to** field and select the **Allow** checkbox for all permissions.
- Click the [OK] button.
- 9. In the Advanced Security Settings for Root window, click the [Apply] button.
- 10. Click the **[OK]** button in each open window to exit.
- 11. Go to the Start menu and select [Run].

12. In the **Run** window, enter "dcomcnfg" and click **[OK]**. The **Component Services** window is displayed:

Component Services	Help			_ D >
🗢 🔿 🗾 🔚 🖬 🖾	🛛 🕞 🗅 🗎 🗰 🧰	1)
Console Root Component Services Component Services Note: Services (Local) Services (Local) Services (Local)	Name COM+ Applications DCOM Config Running Processes Distributed Transaction Coordinator		Actions My Computer More Actions	,

13. In the left pane, expand **Component Services > Computers**. Right-click on **My Computer** and select *Properties*. The **My Computer Properties** window is displayed.

14. In the My Computer Properties window, select the [Default Properties] tab:

My Computer Properties ? 🗙					
Default Protocols COM Security MSDTC General Options Default Properties					
Enable Distributed COM on this computer					
Enable COM Internet Services on this computer					
Default Distributed COM Communication Properties					
The Authentication Level specifies security at the packet level.					
Default Authentication Level:					
Connect					
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity. Default Impersonation Level:					
Identify 🔽					
Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous. Provide additional security for reference tracking					
Learn more about <u>setting these properties</u> .					

- Ensure that the **Enable Distributed COM on this computer** checkbox is selected.
- Select Connect in the **Default Authentication Level** drop-down list.
- Select Identify in the **Default Impersonation Level** drop-down list.
- If you made changes in the [Default Properties] tab, click the [Apply] button.

15. Select the [COM Security] tab:

My Computer Properties	? ×				
General Options Default Properties Default Protocols COM Security MSDT0					
Access Permissions You may edit who is allowed default access to applications. You m also set limits on applications that determine their own permissions. Caution: Modifying access permissions can affect the abil of applications to start, connect, function and/or run securely.					
Edit Limits Edit Default	נ				
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.					
Edit Limits Edit Default					
Learn more about <u>setting these properties</u> .					
OK Cancel Ap	ply				

- 16. Select the [Edit Limits...] button in the Access Permissions pane.
- 17. In the window that appears, click the [Add...] button. The Select Users, Computers, Service Accounts, or Groups window is displayed.
 - Enter the name of the user account that SL1 will use to perform WMI requests or the name of a group that includes that user account.
 - Click the Check Names button to verify the name and then click the [OK] button.

- 18. Select the group or user you added in the **Group or user names** pane and then select the **Allow** checkbox for all permissions.
- 19. Click the **[OK]** button.
- 20. Click the [Edit Default...] button in the Access Permissions pane, then repeat steps 16 19.
- 21. Click the **[Edit Limits...]** button in the **Launch and Activation Permissions** pane, then repeat steps 16 19.
- 22. Click the **[Edit Default...]** button in the **Launch and Activation Permissions** pane, then repeat steps 16 19.
- 23. Click the **[Apply]** button.
- 24. Click **[Yes]** in the confirmation window.

Configuring User Account Control to Allow Elevated Permissions

If you want to use WMI Dynamic Applications that require elevated permissions to monitor a Windows server and you are using a user account other than the default "Administrator" user account, you must perform **one** of the following two tasks:

- Option 1: Disable User Account Control.
- Option 2: Add a registry entry that disables remote User Account Control filtering.

Option 1: Disabling User Account Control

To disable User Account Control:

- 1. Open the Control Panel in Large Icon or Small Icon view.
- 2. Select User Accounts.

3. Select Change User Account Control Settings. The User Account Control Settings window is displayed:

😌 User Account Control Settings		_	×
User Account Control he <u>Tell me more about User</u>	e notified about changes to your computer elps prevent potentially harmful programs from making changes to r Account Control settings	your computer.	
Always notify			
 	 Never notify me when: Apps try to install software or make changes to my computer I make changes to Windows settings 		
	i Not recommended.		
Never notify			
	ОК	Cancel	

- 4. Move the slider to **Never Notify**.
- 5. Click the **[OK]** button.
- 6. Restart the Windows server.

Option 2: Adding a Registry Entry that Disables Remote User Account Control Filtering

To add a registry entry that disables remote User Account Control filtering:

1. To disable the filter, open a text editor and add the following lines to a new file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001
```

- 2. Save the file with a ".reg" extension.
- 3. In Windows Explorer, double click on the .reg file.
- 4. Select [Yes] in the pop-up window.

Configuring WMI for Windows Desktop Systems

This section describes how to configure devices that are running a desktop version of the Windows operating system for monitoring by SL1 using WMI.

Before performing the tasks described in this section, you must know the IP address of each SL1 appliance in your network. If you have not installed a SL1 appliance, you must know the future IP address that will be used by each SL1 appliance.

NOTE: To be monitored by SL1, a Windows device must be running the Windows 7 operating system or later.

NOTE: TCP/IP must be installed and configured before you can install SNMP on a Windows device.

Windows Management Instrumentation (WMI) is the infrastructure that provides information about operations and management on Windows-based operating systems. WMI can be configured to respond to remote requests from SL1. To configure a device running a desktop version of the Windows operating system to respond to remote requests, you must perform the following steps:

- 1. Configure Services
- 2. Configure the Windows Firewall
- 3. Set Default Namespace Security
- 4. Set the DCOM Security Level
- 5. Disable User Account Control

NOTE: The following instructions describe how to configure WMI on devices running a desktop version of the Windows 10 operating system. For instructions on how to configure WMI on earlier Windows versions, consult Microsoft's documentation.

Step 1: Configuring Services

The following services must be running for a Windows device to respond to remote WMI requests:

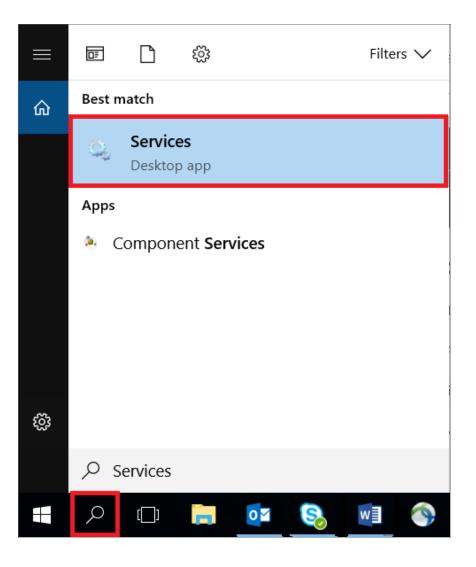
NOTE: ScienceLogic recommends you set all these services to start automatically.

- COM+ Event System
- Remote Access Auto Connection Manager
- Remote Access Connection Manager

- Remote Procedure Call (RPC)
- Remote Procedure Call (RPC) Locator
- Remote Registry
- Server
- Windows Management Instrumentation
- WMI Performance Adapter
- Workstation

To ensure a service is running, perform the following steps:

- 1. Click the magnifying glass icon in the bottom-left corner and type "Services" in the Search Windows field.
- 2. Click the **Services** Desktop app.



3. From the list of services in the right pane, perform the remaining steps for **each** of the services you want to check. This example uses **Workstation**. However, you should check each of the following services:

Services							_	×
le Action View	Help							
🔿 👘 🔝 🕼	à 🗟 🛛 🖬 🕨 🔳 🕪							
Services (Local)	O Services (Local)							
	Workstation	Name	Description	Status	Startup Type	Log On As		
	Stop the service Pause the service Restart the service Description: Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.	Windows Perception Service Windows Push Notifications System Service Windows Push Notifications User Service_1b4e Windows PushToInstall Service Windows Search Windows Store Install Service Windows Update WinHTTP Web Proxy Auto-Discovery Service Wird AutoConfig WINA VacConfig Wind Ferformance Adapter Work Folders Work Folders	Enables spat., This service r., This service ., Provides infr., Windows Re., Provides infr., Maintains d., Enables the ., WinHTTP im., The Wired A., The WLANS., Provides per., This service ., Creates and	Running Running Running Running Running	Manual (frigg_ Automatic Automatic Manual (frigg_ Manual Automatic (De. Manual Manual (frigg_ Manual Automatic Manual Manual Automatic Manual Automatic	Local System Local System		
		WWAN AutoConfig Xbox Accessory Management Service Xbox Game Monitoring Xbox Live Auth Manager Xbox Live Game Save Xbox Live Networking Service	This service This service This service Provides aut This service This service		Manual Manual (Trigg Manual (Trigg Manual Manual (Trigg Manual	Local Service Local System Local System Local System Local System Local System		

- COM+ Event System
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Procedure Call (RPC)
- Remote Procedure Call (RPC) Locator
- Remote Registry
- Server
- Windows Management Instrumentation
- WMI Performance Adapter
- Workstation

- 4. Double-click the name of the service. In this example, we double-clicked Workstation.
- 5. In the Workstation Properties dialog box, click the [General] tab and complete the following field:

Workstati	on Prope	erties (Local	Computer)		\times
General	Log On	Recovery	Dependencies		
Service	name:	LanmanWo	orkstation		
Display	name:	Workstation	1		
Descript	tion:		d maintains client network co vers using the SMB protocol. I		
	executabl DOWS\Sy		ost.exe -k NetworkService -p		
Startup	type:	Automatic		~	
Service	status:	Running			
S	Start	Stop	Pause	Resume	
You car from he		ne start para	meters that apply when you st	art the service	
Start pa	rameters:				
			OK Cancel	Apply	

- Startup Type. Select Automatic.
- 6. Click the **[Apply]** button.
- 7. If the service has not already started, click the **[Start]** button.
- 8. Repeat steps 4-7 for each service.

Step 2: Configuring Windows Firewall

To configure Windows Firewall to accept remote WMI requests:

- 1. Click the magnifying glass icon in the bottom-left corner and type "Command Prompt" in the **Search** *Windows* field.
- 2. Execute the following two commands in the Command Prompt window:

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)"
new enable=yes
netsh advfirewall firewall set rule group="remote administration" new enable=yes
```

3. If the result of the second command is "No rules match the specified criteria", run the following two commands:

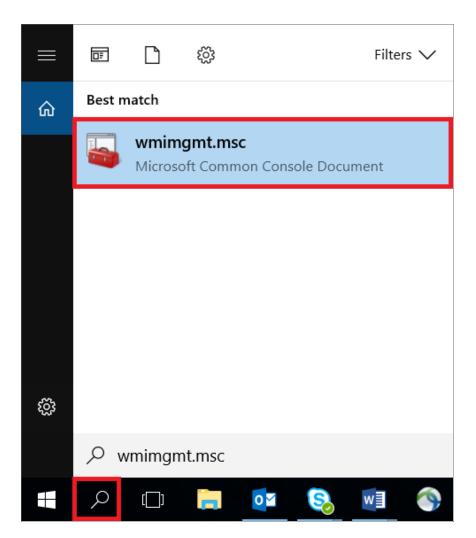
```
netsh firewall set service remoteadmin enable
netsh advfirewall firewall set rule group="remote administration" new enable=yes
```

Step 3: Setting the Default Namespace Security

To set the default namespace security, perform the following steps:

1. Click the magnifying glass icon in the bottom-left corner and type "Services" in the Search Windows field.

2. Click the **wmimgmt.msc** Microsoft Common Console Document.



3. In the WmiMgmt window, right click WMI Control (Local) and select Properties.

🔚 WmiMgmt - [Console	Root\WMI Control (Local)]			
	Favorites Window Help			_ 8 ×
	? 🖬			
🗀 Console Root			Actions	
i WMI Control (Local		nstrumentation (WMI)	WMI Control (Local)	^
Connect to another computer			More Actions	•
		ws Management Instrumentation (WMI)		
	New Window from Here			
	New Taskpad View			
	Properties			
	Help			
Opens the properties dialog	box for the current selection.		1	

4. In the WMI Control (Local) Properties window, click the [Security] tab, click Root, and then click the [Security] button.

WMI Con	trol (Local) Prope	erties			?	×
General	Backup/Restore	Security	Advanced			
	pace navigation allo	ws you to s	set namespa	ce specific se	ecurity.	
				Se	curity	
		Oł	<	Cancel	Ap	ply

5. In the Security for Root window, click Administrators, and then click the [Advanced] button.

Security for Root		×
Security Group or user names:		ators)
Permissions for no_admin Execute Methods Full Write Partial Write Provider Write Enable Account Remote Enable For special permissions or advance click Advanced.	Add Allow	Remove Deny
ОК	Cancel	Apply

6. In the Advanced Security Settings for Root window, click Administrators, and then click the [Edit...]button.

		Security Settings for Root			
Owr	ner:	Administrators (DESKTOP-SR36	R55\Administrators) Cha	inge	
Permissions Auditing					
or	addition	al information, double-click a peri	mission entry. To modify a	permission entry, select	the entry and click Edit (if available).
Perr	nission e	entries:			-
	Туре	Principal	Access	Inherited from	Applies to
	Allow	Administrators (DESKTOP-SR3	Special	None	This namespace and subname.
8	Allow	no_admin (DESKTOP-SR36R55	Enable Account	None	This namespace only
	Add	Remove Edit			

7. In the **Permission Entry for Root** window, enter the following:

Permission	n Entry for Root		- 0
Principal:	no_admin (DESKTOP-SR36R55\no_admin)	elect a principal	
Гуре:	Allow	~	
Applies to:	This namespace and subnamespaces	~	
Permission	s: Execute Methods	I Enable Account	
	Full Write	Remote Enable	
	Partial Write Provider Write	Etit Security	
] Only app	oly these permissions to objects and/or contain	ers within this container	Clear all
			OK Cance

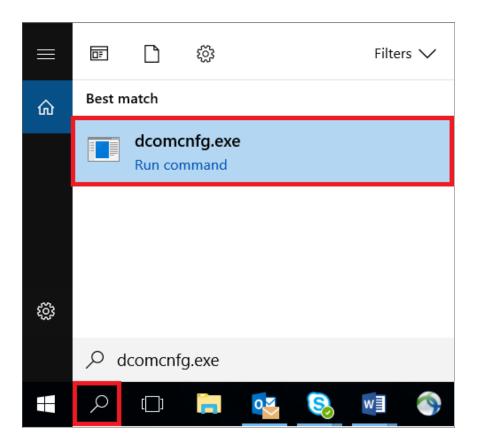
- Type. Select Allow.
- Applies to. Select This namespace and subnamespaces.
- **Permissions**. Select the Execute Methods, Full Write, Partial Write, Provider Write, Enable Account, Remote Enable, Read Security, and Edit Security checkboxes.
- 8. Click **OK** in this window and the following windows, and then close the **WmiMgmt** window.

Step 4: Setting the DCOM Security Level

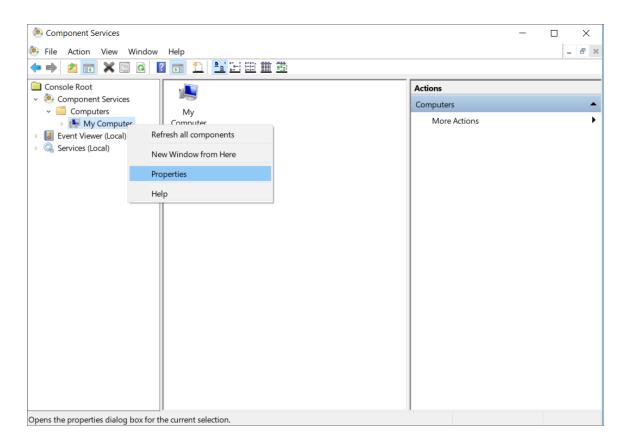
To set the DCOM Security Level, perform the following steps:

1. Click the magnifying glass icon in the bottom-left corner and type "dcomcnfg.exe" in the **Search Windows** field.

2. Click the **dcomcnfg.exe** command.



3. In the Component Services window, expand Component Services > Computers, right-click My Computer, and then select *Properties*.



4. In the **My Computer Properties** window, click the **[Default Properties]** tab and then complete the following fields:

My Computer Properties			?	\times
Default Protocols	COM Sec	urity	MSDTC	
General	Options	Default	Properties	
⊡ Enable Distributed COM	on this computer			
□ Enable COM Internet Se	rvices on this comp	outer		
Default Distributed COM	Communication Pr	operties		
The Authentication Level	specifies security a	t the packet le	vel.	
Default Authentication	_evel:			
Connect		~		
The impersonation level s who is calling them, and				
using the client's identity.				
Default Impersonation	Level:			
Identify		~		
Security for reference trac and that the default impe				
Provide additional se	curity for reference	tracking		
Learn more about <u>setting th</u>	iese properties.			
	ОК	Cancel	Арр	ly

- Enable Distributed COM on this computer. Select this checkbox.
- Default Authentication Level. Select Connect.
- Default Impersonation Level. Select Identify.

5. In the My Computer Properties window, click the [COM Security] tab. Under Launch and Activation Permissions, click the [Edit: Default...] button.

My Computer Propert	ies	? ×
General	Options	Default Properties
Default Protocols	COM Security	
Delduit i lotocols	,	MODIO
Access Permissions		
	o is allowed default access t s on applications that detem	
	Modifying access permissio ations to start, connect, func	
	Edit Limits	Edit Default
activate objects. determine their of Caution affect th	o is allowed by default to lau You may also set limits on a	pplications that ation permissions can
	Edit Limits	Edit Default
Learn more about <u>set</u>	ting these properties.	
	OK	Cancel Apply

6. In the Launch and Activation Permission window, select the following:

aunch and Activation Permission		? >	<				
Default Security							
Group or user names:							
SYSTEM							
Administrators (SILO2461\Administrators)							
SE INTERACTIVE							
	Add	Remove	í				
	7 101 01	110111010					
Permissions for Administrators	Allow	Deny					
Permissions for Administrators	Allow	Deny]				
Local Launch	⊻ ,						
Local Launch Remote Launch	y ,						
Local Launch Remote Launch Local Activation							
Local Launch Remote Launch Local Activation							
Local Launch Remote Launch Local Activation							
Local Launch Remote Launch Local Activation							
Local Launch Remote Launch Local Activation							

- Group or user names. Select Administrators.
- Permissions for Administrators. Set Local Launch, Remote Launch, Local Activation, and Remote Activation to Allow.
- 7. Click **[OK]**.

8. In the My Computer Properties window, in the Launch and Activation Permissions pane, click the [Edit Limits...] button.

My Computer Properti	es		?	×		
General	Options	Default Properties				
Default Protocols	COM Security	y	MSDTC			
Access Permissions						
You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions.						
	Modifying access permission tions to start, connect, fun					
	Edit Limits	Edit De	fault			
activate objects. Y determine their ov Caution: affect the	is allowed by default to la ou may also set limits on a	applications the	at ons can			
	Edit Limits	Edit De	fault			
Learn more about setting these properties.						
	OK	Cancel	Арр	oly		

9. In the Launch Permission window, select the following:

aunch and Activation Permission	l	? >	<				
Security Limits							
Group or user names:			_				
		^					
Image: ALL APPLICATION PACKAGES Image: S-1-15-3-1024-2405443489-874036122-4286035555-1823							
Administrators (SILO2461\Administrators)							
Reformance Log Users (SILO2461\Performance Log Users ~							
<		>					
	Add	Remove					
Permissions for Administrators	Allow	Deny	_				
Permissions for Administrators	Allow	Deny]				
]				
Local Launch							
Local Launch Remote Launch							
Local Launch Remote Launch Local Activation	y , y , y ,						
Local Launch Remote Launch Local Activation	y , y , y ,						
Local Launch Remote Launch Local Activation	y , y , y ,						
Local Launch Remote Launch Local Activation	y , y , y ,						
Local Launch Remote Launch Local Activation	y , y , y ,						

- Group or user names. Select Administrators.
- Permissions for Administrators. Set Local Launch, Remote Launch, Local Activation, and Remote Activation to Allow.
- 10. Click OK in this window and the following windows, and then close the Component Services window.
- 11. Restart the computer to save the settings.

Step 5: Disabling User Account Control

To monitor a device running Windows 7, 8, or 10, you must perform the following additional steps to disable the User Account Control (UAC) filter for remote logins:

1. Use a text editor such as Notepad to create a new file.

2. Include the following in the file .:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001
```

- 3. Save the file with a name of your choice, like disableUAC.reg, to the directory of your choice. Make sure to save the new file with the .reg suffix.
- 4. In Windows Explorer, double click on the .reg file to execute it.

Chapter

4

SNMP and WMI Dynamic Applications for Windows Devices

Overview

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

SNMP Dynamic Applications	71
WMI Dynamic Applications	72
Microsoft Base Pack	72
Relationships with Other Types of Component Devices	73

SNMP Dynamic Applications

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

WMI Dynamic Applications

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

NOTE: Although the SL1 supports WMI Dynamic Applications, ScienceLogic recommends that you use PowerShell Dynamic Applications where possible. PowerShell is the preferred management platform for Microsoft products.

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

The following PowerPack includes WMI Dynamic Applications for Microsoft systems.

Microsoft Base Pack

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2008, 2012, and 2016, as well as Windows XP, 7, 8, and 10 desktop systems.

The following WMI Dynamic Applications can be used to collect performance data from Windows Servers or Windows desktop systems as a user with standard permissions:

- Windows CPU
- Windows Disk
- Windows Interface
- Windows Memory

The following WMI Dynamic Applications can be used to collect configuration data from Windows Servers or Windows desktop systems as a user with standard permissions:

- Windows Asset
- Windows Process List
- Windows Service List
- Windows SMART Status

Relationships with Other Types of Component Devices

Additionally, the Dynamic Applications in the *Microsoft Base Pack* 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

Creating SNMP and WMI Credentials for Windows Devices

Overview

The following sections describe how to create SNMP and WMI credentials for Windows devices that you want to monitor with SL1:

Creating an SNMP Credential	74
Creating a WMI Credential	.77
Testing Windows Credentials	.78
SNMP Credential Test	78
Basic/Snippet Credential Test	79
Running a Windows Credential Test	.79

Creating an SNMP Credential

SNMP Credentials (called "community strings" in earlier versions of SNMP) 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	e Name	SNMP Version
Port 161	Timeout(ms)	Retries
SNMP V1/V2 Settings SNMP Community (Read-	Only) S	NMP Community (Read/Write)
SNMP V3 Settings Security Name	Securit	y Passphrase
Authentication Protocol	Security Level	SNMP v3 Engine ID
Context Name	Privacy Protocol	Privacy Protocol Pass Phrase
	Save	

- 3. Supply values in the following fields:
 - **Profile Name**. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
 - **SNMP Version**. SNMP version. Choices are SNMP V1, SNMP V2, and SNMP V3. The default value is SNMP V2. This field is required.

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

SNMP V1/V2 Settings

These fields appear if you selected SNMP V1 or SNMP V2 in the **SNMP Version** field. Otherwise, these fields are grayed out.

- 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. Otherwise, these fields are grayed out.

- 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. Choices are DES or AES. The default value is DES. This field is required.
- 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 a SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

Creating a WMI Credential

NOTE: Although the SL1 supports WMI Dynamic Applications, ScienceLogic reommends that you use PowerShell Dynamic Applications where possible. PowerShell is the preferred management platform for Microsoft products.

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

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

You can create a credential for WMI Dynamic Applications from the **Credential Management** page. To create a credential for a WMI Dynamic Application:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Select the [Create] button in the upper right of the page. Select Basic/Snippet Credential.

edential Management Credentials Found [I	0]												Create Reset	Guide
		BQ	BW	DA								S	NMP Credential	
Profile Name *	Organization	Use	Use	Use	Taxe	Credential User		Host	Eed	Timeout (ms)	2	Last D	stabase Credential	6
. / 99.160	(all orgs)			350	SOAP/XML Host	-	%D		443	20000	53	2013-03-12	DARXIIL Host Credentia	
2. 🤌 9.163	(all orgs)	-		449	SOAP/XML Host	-	%D		443	20000	54	2010-00-12		
3. Polan0a	(all orgs)	57		7	SNMP				161	2000	38		DAP/AD Credential	1
 Polsm0s (Longer Timeout) 	(all orgs)				SNMP	-		-	161	5000	39	2013-02-27	asic/Snippet Credential	1
Cloudkick - Example	(all orgs)			-	Basic/Snippet	[SECURITY KEY GOES HE			443	5000	12			
B PCUCM 7	(all orgs)	-		8	SOAP/ONL Host		%D		8443	10000	52	2013-03-11 11:2		
7. PCUCM 8	🙀 (all orgs)			8	SOAP/XML Host	em7app	%D		8443	10000	51	2013-03-11 11:2		
 PCUCM PerfmonService 8.0 Example 	🙀 (all orgs)	-		-	SOAP/XML Host	-	%D		8443	2000	13	2013-03-11 11:2		
9. PEM7 Collector Database	🙀 (all orgs)	-		-	Database	root	%D		7707	0	14	2013-03-29 17:		
0. PEM7 Default V2	🙀 (all orgs)	54			SNMP				161	1500	18	2013-02-27 16:		
PEM7 Default V3	🙀 (all orgs)	9			SNMP	em7defaultv3		-	161	500	19	2013-02-27 16:		
2. HEMC - Example	(all orgs)				Basic/Snippet	root	%D		443	10000	7	2013-03-29 17:		
3. PGLaDOS_Cred	(all orgs)				SNMP				161	1500	80	2013-03-29 11:		
4. 🤌GoGrid - Example	(all orgs)				Basic/Snippet	[SECURITY KEY GOES HE	127.0.0.1		443	5000	16	2013-02-27 16:		
PLIfeSize: Endpoint SNMP	🙀 (all orgs)				SNMP	control		-	161	3000	10	2013-02-27 16:		
 PLifeSize: Endpoint SSH/CLI 	(all orgs)				Basic/Snippet	auto	%D		22	3	9	2013-03-25 17:		
. Printest	(all orgs)			1	Database	postgres	10.168.44.220		5432	0	58	2013-03-21 16>	15:56 mhussain	
PMSSQL	(all orgs)	-		-	Database	58	10.0.9.241		1433	0	35	2013-02-27 16:	I5:00 em7admin	
Physics	(all orgs)				Database	root	%D		7706	0	38	2013-02-27 18:		
ANetApp	(all orgs)				Basic/Snippet	root	%D		443	3000	15	2013-03-29 17:	5:00 jfolk	
PNetApp w/SSL Option	(all orgs)				SOAP/XML Host	root	%D		443	3000	82	2013-03-29 17:	5:00 jfolk	
PNetApp w/SSL Option Off	(all orgs)	-		-	SOAP/XML Host	root	%D		443	3000	81	2013-03-29 17:	5:00 jfolk	
Pnew_cred_name	(none)				Database	usert	myhost		162	1600	65	2013-03-28 17:	11:56 em7admin	
Pnew cred name	(none)				Database	usert	myhost		162	1600	70	2013-03-26 17>	14:46 em7admin	
Pnew_cred_name	Silopoel	-			Database	userl	my.host		162	1600	75	2013-03-26 17:1	i3:15 em7admin	
POracle	alial grash	-		-	Detabase	EM7ADWIN	10.0.9.151		1521	0	32	2013-02-27 16:	14:41 em7admin	
Polycom - Advanced	(all orgs)				SOAP/ONL Host	admin	%0		80	20000	3	2013-03-22 18:	4:57 sseplowitz	
Polycom - Interface	al al orgs]				SOAP/XIL Host	admin	%D		80	20000	4	2013-02-27 16:	9.09 em7admin	
Provcom - Network	a la la cost	-			SOAP/XML Host	admin	%D		80	20000	5	2013-02-27 16:	9.09 em7admin	
Polycom - System	(all orgs)	-		-	SOAPOOL Host	admin	50		80	20000	2	2013-02-27 18	9.09 em7admin	
Preivcom CDR	(all orgs)				SOAP/OWL Host	admin	50		80	20000	6	2013-02-27 16:	9.09 em7admin	
2. Prostores	(Val cros)			-	Detabase		192.168.11.135		5432	0	33	2013-02-27 16:		
3. PPostgres	(all orgs)				Detabase		192.168.11.135		5412	0	50	2013-03-07 11:5		
A POALDAP	(multiple orgs)				LDAP/AD	uide%u ourPeople dorsci			389	1000	57	2013-03-15 16:		
PRackspace - Example	(all orgs)				Basio/Snippet	IUSERNAME GOES HEREI			443	5000	28	2013-02-27 16:		
5. PSio AD	(all orgs)				LDAP/AD	SuB%d	192,168,40,11		389	1000	40	2013-02-27 16:		
Snippet Cred Test	(all orgs)				BasicScippet	em7admin	10.0.9.52		22	3000	55	2013-03-13 151		
ASNINP Public V1	(all orgs)	309			SNMP				161	1500	20	2013-02-27 16		
PSNI/P Public V2	al orgal	7		4	SNMP				161	1500	21	2013-02-27 16		
ASvease	(all orgs)			·	Detabase	88	10.0.9.242		5010	0	24	2013-02-27 16:		
PTandberg Endpoint - Config	(all orgs)					USERNAME HERE	50		80	10000	24	2013-02-27 16:		
PTandberg Endpoint - History	(all orgs)					USERNAME HERE	10		50	10000	25	2013-02-27 16:		
Plandberg Endpoint - History	a (all orgs)					USERNAME HERE	SD SD		80	10000	23	2013-02-27 16:		
 Anderg Endpoint - Status ATandberg: HTTPS 	(all orgs)			-	SOAPOOL Host		50		443	10000	29	2013-02-27 18.		
A Tandberg: https://www.seconfiguration	(all orgs)				SOAPOOL Host		%D		443	5000	31	2013-03-13 14:		
 Provoucing: Amp contriguration 	Secon orga				OUMPHANE HOSE	Out int	80		443	0101	01	2010/03/13 143	N.21 meossan	-

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

Credential Editor		×
Create New Basic/Snippet Credential		Reset
Basic Settings		
	Credential Name	
Hostname/IP	Port	Timeout(ms)
Usern	ame	Password
	Save	

- Credential Name. Name of the credential. Can be any combination of alphanumeric characters.
- Hostname/IP. Hostname or IP address of the device from which you want to retrieve data. To use the same WMI default credential for multiple devices, enter %D in this field.
- **Port**. Port number associated with the data you want to retrieve. For WMI Dynamic Applications that perform WBEM requests, supply the port used by the WBEM service on the device. For WMI Dynamic Applications that perform WMI requests, which includes all default WMI Dynamic Applications in SL1, enter any valid port number in this field; the platform does not specify a port number when performing WMI requests.
- *Timeout (ms)*. Time, in milliseconds, after which the platform will stop trying to communicate with the authenticating server.
- Username. Username for a user account on the device.

NOTE: To specify a domain user, enter the username in the format DOMAIN\username. In most cases, you should use a domain user in the credential and use the format DOMAIN\username.

- Password. Password for a user account on the device.
- 4. To save the credential, select the [Save] button. To clear the values you set, select 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 Basic/Snippet 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.

Basic/Snippet Credential Test

The Basic/Snippet Credential Test can be used to test a Basic/Snippet credential for connectivity. The Basic/Snippet 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.

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						
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						
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						
	Step Test Reachability Test Port Availability	Step Description Test Reachability Check to see if the device is reachable using ICMP Test Port Availability Check to see if the SNMP port is open	Step Description Log Message 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 Test Port Availability Check to see if the SNMP port is open Port 161 is open	Step Description Log Message Status Test Reachability Check to see if the device is reachable using ICMP The device is reachable using ICMP. The average response time is 0.397ms Passed Test Port Availability Check to see if the SNMP port is open Port 161 is open 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 (b) 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.

Chapter

Monitoring a Windows Cluster

Overview

The following sections describe how to monitor a Windows Cluster using SL1:

Monitoring Windows Clusters in the ScienceLogic Platform	
Discovering Cluster Nodes	82
Aligning a Dynamic Application with a Cluster Node	
Disabling Collection of a Dynamic Application on a Device	
Discovering the Cluster IP Address	84
Aligning Dynamic Applications with the Cluster Device	
Using a Device Template to Configure Dynamic Applications	87

Monitoring Windows Clusters in the ScienceLogic Platform

The general approach for monitoring a Windows Cluster is to discover each cluster node and then discover the shared IP address as an additional, separate, device:

- For each cluster node, configure SL1 to monitor the non-cluster related aspects of the devices. For example, the CPU, memory, and interface utilization for each node. When you configure monitoring for each cluster node, you will ensure that the cluster services are not monitored on each cluster node.
- For the additional device that represents the cluster itself, configure SL1 to monitor the clustered services. For example, you would align the performance Dynamic Applications that collect data about a Windows device to this device record. When you configure monitoring for the device record that represents the clustered services, you will ensure that node-specific data, for example, CPU, memory, and interface utilization, is not monitored through the shared IP.

NOTE: Version 101 of the *Microsoft: SQL Server Enhanced* PowerPack does not support the ability to monitor SQL Server clusters. The SQL Servers that you monitor must not be using Windows Server Failover Clustering (WSFC) or SQL Server Failover Cluster Instances (FCI) for high-availability.

By monitoring the shared IP address separately, SL1 will always poll the active cluster node for information about the clustered service.

Discovering Cluster Nodes

The steps to discover the individual cluster nodes depend on the types of Dynamic Application you will use to monitor the cluster services, i.e. the Dynamic Applications that will be aligned with the device record for the shared IP address. When you discover each cluster node, you must configure SL1 to ensure that the Dynamic Applications for the clustered service are not aligned automatically.

There are several approaches to preventing the Dynamic Applications for the clustered service from being automatically aligned to each cluster node:

- In the discovery session for a cluster node, do not include any credentials that can be used to collect the Dynamic Applications for the clustered service. For example, if you will use WMI Dynamic Applications to monitor the clustered service, do not include a credential that can be used to successfully make WMI requests in the discovery session. By using this method, you might prevent the automatic alignment of Dynamic Applications that you would like to align with the cluster nodes; in this case, you would have to align those Dynamic Applications manually.
- In some cases, you might need or want to include credentials that can be used to collect Dynamic Applications for the clustered service in the discovery session for a cluster node. This typically occurs when the Dynamic Applications for the clustered service use the SNMP protocol. If you need to include any credential that can be used to collect Dynamic Applications for the clustered service in the discovery session for a cluster node, you can allow the Dynamic Applications for the clustered service to align with the device records for the cluster nodes, then manually disable collection for those Dynamic Applications on those devices. SL1 will not re-enable collection for those Dynamic Applications.

The following sub-sections describe how to manually align a Dynamic Application with a cluster node and how to disable collection of a Dynamic Application on a device. If you are configuring SL1 to monitor multiple clusters that provide the same service, you can speed up both of these tasks by creating and applying device templates.

Aligning a Dynamic Application with a Cluster Node

If you need to manually align a Dynamic Application to a cluster node, perform the following steps:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Select the wrench icon (*P*) for the cluster node. The **Device Properties** page is displayed.
- 3. Select the [Collections] tab. The Dynamic Application Collections page is displayed.
- 4. Select the **[Action]** button.
- 5. Select Add Dynamic Application. The Dynamic Application Alignment page appears:

ynamic Application Alignment		Reset
Dynamic Applications	Credentials	
	Select A Dynamic Application First	
Database Performance: LEM7: Event Count LEM7: High Frequency Data Pull Sinpet Configuration: LCloudkick: Overview LCloudkick: State LEMC Agent Information LEMC Cache Config LEMC Caching LEMC Caching LEMC Costomer Replaceable Unit Config LEMC Customer Replaceable Unit Config LEMC Caching LEMC Customer Replaceable Unit Config LEMC Cache Storage Processor Config LGoGrid: Dassword Lists LGoGrid: Status LHAST Resource: Memory Config Marcosoft HyperV Guest Configuration Marcosoft HyperV Guest Configuration	Select A Dynamic Application First	
LRackspace: Flavors Rackspace: Images	•	

- 6. In the **Dynamic Application Alignment** page, select the Dynamic Application you want to align in the **Dynamic Applications** field.
- 7. In the Credentials field, select the credential for the Dynamic Application.
- 8. Select the **[Save]** button.

Disabling Collection of a Dynamic Application on a Device

If you need to manually disable collection for a Dynamic Application on a device, perform the following steps:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Select the wrench icon (It is device record for the cluster. The **Device Properties** page is displayed.

3. Select the [Collections] tab. The Dynamic Application Collections page is displayed:

Close	Properties	T <u>h</u> resholds	Collections	Monitors				
<u>S</u> chedule	Logs	T <u>o</u> olbox	Interfaces	 <u>R</u> elationships	<u>T</u> ickets	Redirects	Notes	
Device Name	MSSQL-CLUSTER-1.0	A.LOCAL		Managed Ty	/pe Physical Device			_
IP Address / ID	10.168.44.206 38			Catego	ory Servers			
Class	Microsoft			Sub-Cla	Windows 2008	Server R2		
Organization	DC - Servers			Uptir	me 2 days, 17:24:26	5	Windov	vs 2008
Collection Mode	Active			Collection Tir	me 2012-03-19 18:4	5:00	🔺 🗢 🖬	1 🖶 🥜
Description	Hardware: Intel64 Far	mily 6 Model 46 Stepping	6 AT/AT COMPATIBLE	- S Group / Collec	tor CUG em7_ao		MSSQL-CLU	STER-1.QA
Applica	ation [™] Collections					Expar	nd Action Reset	Guide
Anamic Applica		Dynamic Application		ID	Poll Frequency	Type	Credential	
+ Informant: Mem		a priorition of apprior training			5 mins	SNMP Performance	Default SNMP Credential	1
+ Informant: Volu					5 mins	SNMP Performance	Default SNMP Credential	1
+ MSSQL: Gener	ral			84	10 mins	SNMP Performance	Default SNMP Credential	1
+ MSSQL: Memor	ry			83	10 mins	SNMP Performance	Default SNMP Credential	1
+ MSSQL: SQL S	Stats			82	10 mins	SNMP Performance	Default SNMP Credential	9
+ Host Resource	: CPU Config			12	1440 mins	SNMP Configuration	Default SNMP Credential	1
+ Host Resource				9	120 mins	SNMP Configuration	Default SNMP Credential	9
+ Host Resource					5 mins	Snippet Performance	Default SNMP Credential	1
+ Host Resource				8	5 mins	Snippet Performance	Default SNMP Credential	1
+ Host Resource	e: Memory Config			11	1440 mins	Snippet Configuration	Default SNMP Credential	1
						[Select	Action]	Go

- 4. Select the checkbox for each Dynamic Application you want to disable.
- 5. In the Select Action drop-down list, select Disable All Collection Objects.
- 6. Select the **[Go]** button.

Discovering the Cluster IP Address

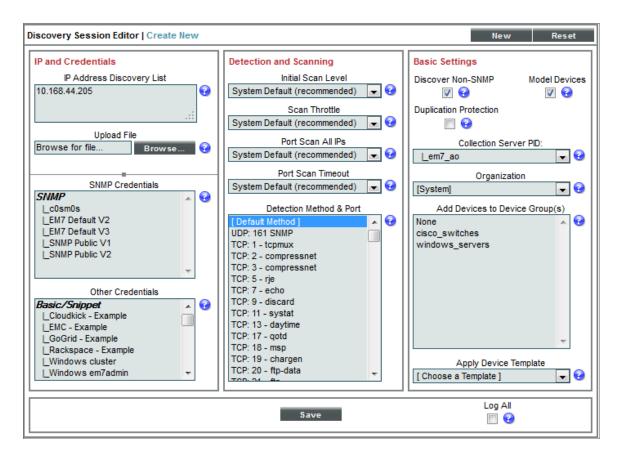
To discover the additional device that represents the cluster, you must run a discovery session to discover a shared IP address for the cluster as a pingable device. By discovering the shared IP address as a cluster, you will prevent SL1 from automatically collecting node-specific data using SNMP. After discovering the cluster as a pingable device, you can manually align the Dynamic Applications that will monitor the clustered service with the device record for the cluster.

If you are configuring SL1 to monitor multiple clusters that provide the same service, you can **create a device** *template* to speed up the manual configuration of Dynamic Applications.

To discover the virtual IP of the cluster as a pingable device:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).

2. Select the [Create] button. The Discovery Session Editor page appears:



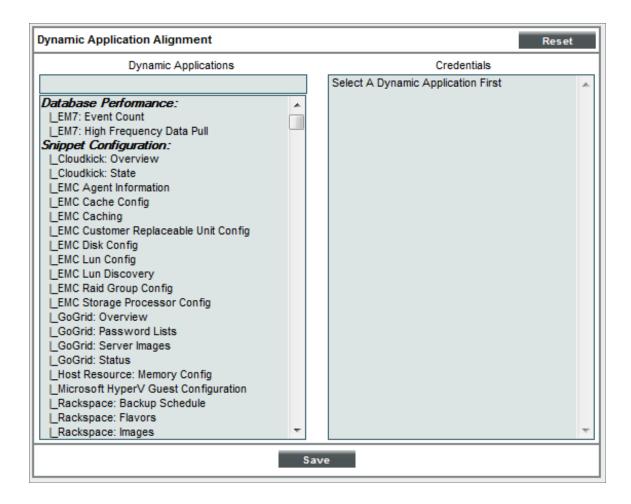
- 3. Supply values in the following fields:
 - IP Address Discovery List. Enter the shared IP address for the cluster.
 - SNMP Credentials. Do not select any credentials.
 - Other Credentials. Do not select any credentials.
 - Discover Non-SNMP. Select this checkbox.
 - **Duplication Protection**. Deselect this checkbox. If you discovered the cluster nodes as SNMP devices, SL1 will have associated the shared IP address for the cluster with one of those nodes. You must disable duplication protection for SL1 to discover the shared IP address as a new device.
 - Apply Device Template. If you are using a device template to configure Dynamic Applications, select the device template in this field.
- 4. For the other fields in this page, you can use the default values or select different values based on your operating procedures.
- 5. Select the **[Save]** button.
- 6. In the Discovery Control Panel page, select the lightning bolt icon (🖉) for the new discovery session.

6

Aligning Dynamic Applications with the Cluster Device

To manually align a Dynamic Application to the device record for the cluster, perform the following steps:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Select the wrench icon (*P*) for the device record for the cluster. The **Device Properties** page is displayed.
- 3. Select the [Collections] tab. The Dynamic Application Collections page is displayed.
- 4. Select the **[Action]** button.
- 5. Select Add Dynamic Application. The Dynamic Application Alignment page appears:



- 6. In the **Dynamic Application Alignment** page, select the Dynamic Application you want to align in the **Dynamic Applications** field.
- 7. In the Credentials field, select the credential for the Dynamic Application.
- 8. Select the **[Save]** button.

Using a Device Template to Configure Dynamic Applications

If you are configuring SL1 to monitor multiple clusters that provide the same service, you can create a device template to speed up the manual configuration of Dynamic Applications on the cluster nodes and/or the device record that represents the cluster.

To create a device template that configures a Dynamic Application on a device:

- 1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
- 2. Select the [Create] button. The Device Template Editor page is displayed.
- 3. Select the [Dyn Apps] tab. The Editing Dynamic Application Subtemplates page is displayed:

Device Template Editor Editing Dynam	ic Application Subtemplates (Click field labels	to enable/disable them)	New Reset
Ten	nplate Name		
Config Interface CV Policie	es Port Policies Svc Policies Proc Policie	s Dyn Apps	
Subtemplate Selection Add New Dynamic App Sub-Template	Template Application Behavior All devices (align new applications and update of	Align Dynamic Application With collection states)	
	Dynamic Application Settings		
	Alteon: Load Trending	Dynamic Application	_
	Crea	dentials	oll Rate
	Default SNMP credential ARP Entries Concurrent Connections Per Port Connection Rate Per Virtual Server Port Bindings Real Server Current Sessions	Enabled v Enabled v Enabled v Enabled v	 V
	Oynamic Application Thresholds No thresholds available for selected application.	m	Þ

- 4. Select Add New Dynamic App Sub-Template in the left pane.
- 5. Supply values in the following fields:
- Align Dynamic Application With. Select All devices.
- Dynamic Application. Select the Dynamic Application that you want to configure.
- **Credentials**. If you want to use the device template to align Dynamic Applications with a device, enable this field by clicking on the field name. Select the credential you want to align with the Dynamic Application on all devices to which this template is applied. If you want to use the device template to disable collection for this Dynamic Application, do not enable this field.

6

- 6. If you want to use the device template to disable collection for this Dynamic Application, select the name of each object that appears in the **Dynamic Application Settings** page. The object names appear below the **Credentials** field. In the drop-down list for each object, select Disabled.
- 7. If you want to configure multiple Dynamic Applications with this device template, repeat steps 4–6 for each additional Dynamic Application.
- 8. Select the [Save] button.

You can apply the device template to all devices in a discovery session by selecting the device template in the **Apply Device Template** field in the discovery session. To apply a device template to one or more devices after discovery:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Select the checkbox for each device to which you want to apply the device template.
- 3. In the Select Action drop-down list, select Modify By Template.
- 4. Select the [Go] button. The Device Template Editor page is displayed:

Device Template Editor	Applying Template to D	evices Config Template S	Gettings (Click field labels to enable/dis	able them)	Reset
Template New / One-off	Template 💌	Save When Applied & Cont	irmed Template Name		
Config Interface	CV Policies Port F	Policies Svc Policies Pro	c Policies Dyn Apps		
Access & Monitoring				Device Preferences	
Device Organization	Acme Corporation	-		Auto-Clear Events	Scan All IPs
SNMP Read	c0sm0s	🚽 SNMP Writ	None 👻		
Availability Protocol	TCP	🚽 🗸 Avail Po	rt ICMP 👻	Accept All Logs	Dynamic Discovery
Latency Protocol	TCP	- Latency Po	rt ICMP 🚽		_
Avail+Latency Alert	Disabled	.		Daily Port Scans	Preserve Hostname
Collection	Enabled	- Collector Gr	p CUG 👻		
Coll. Type	Standard	.		Auto-Update	Disable Asset Update
Critical Ping	Disabled	-			
Event Mask	Disabled	-			
Device Retention & Basi	ic Thresholds			1	
System Latenc	У <u>- </u>	500 ms	Bandwidth Data		30 days
			Normalized BW Data	1	30 days
Device Logs Ma	× ġ	5000 records	Performance Data		30 days ≡
Log Age Ma	× 4	30 days	Normalized Perf Data	1	30 days
Number of Availabilit Ping		1 pings	Ping Packet Size	1 8	100 %
			Арріу		

- 5. Select the device template that you want to apply in the *Template* field.
- 6. Select the [Apply] button. A summary of the changes you are about to make is displayed.
- 7. Select the [Confirm] button.

Chapter

7

Automatically Restarting Windows Services

Overview

The following sections describe how to use the Windows Restart Automatic Services PowerPack in SL1:

What is the Windows Restart Automatic Services PowerPack?	
Configuring the Windows Restart Automatic Services PowerPack	
Excluding Automatic Services	
Viewing the List of Excluded Services	
Adding an Excluded Service for All Devices	
Adding an Excluded Service for a Single Device	92
Removing an Excluded Service	

What is the Windows Restart Automatic Services PowerPack?

The Windows Restart Automatic Services PowerPack can be used to:

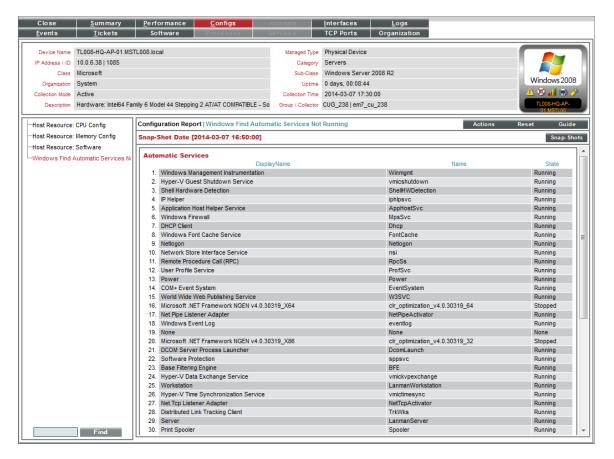
- Monitor the state of Windows services with a startup type of "Automatic" using WMI.
- Automatically start failed services by making an RPC over SMB request.

Configuring the Windows Restart Automatic Services PowerPack

To configure the content in the Windows Restart Automatic Services PowerPack:

- 1. Configure your Windows device to respond to remote WMI requests.
- 2. Create a WMI credential for your Windows device .
- 3. Align the "Windows Find Automatic Services Not Running" Dynamic Application to the device with the WMI credential. If you include the WMI credential you created in the discovery session for your Windows device, this Dynamic Application will be aligned automatically.

The Dynamic Application collects the status of all services with a startup type of "Automatic" that are not on the **exclusion list**:



If a service with a startup type of "Automatic" is in a non-running state, SL1 will generate a major event. By default, this event will trigger the "Start Required Windows Services" automation policy, which will execute an RPC over SMB request to start the failed service. No additional configuration is required to configure this automation.

Excluding Automatic Services

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

- ATI HotKey Poller
- Distributed Transaction Coordinator
- Performance Logs and Alerts
- Removable Storage
- TPM Base Services
- Windows Service Pack Installer update service
- VSS

Viewing the List of Excluded Services

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

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

SELECT * FROM master.definitions_service_autostart_exclude;

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

Adding an Excluded Service for All Devices

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

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

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

3. Click **[Go]**.

Adding an Excluded Service for a Single Device

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

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

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

3. Click [Go].

Removing an Excluded Service

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

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

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

3. Click [Go].

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010