



Monitoring Windows Systems with PowerShell

ScienceLogic version 8.9.0

Table of Contents

Introduction	4
Monitoring Windows Devices in the ScienceLogic Platform	5
What is SNMP?	5
What is PowerShell?	5
PowerPacks	6
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	22
Configuring the SNMP Service	25
Configuring the Firewall to Allow SNMP Requests	30
Configuring Windows Servers for Monitoring with PowerShell	31
Configuring PowerShell	32
Step 1: Configuring the User Account for the ScienceLogic Platform	32
Option 1: Creating an Active Directory Account	33
Option 2: Creating a Local User Account with Administrator Access	33
Option 3: Creating a Non-Administrator Local User Account	34
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server ...	35
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	36
Creating a User Group and Adding a User in Active Directory	36
Setting the Session Configuration Parameters and Group Permissions	36
Creating a PowerShell Credential	37
Step 2: Configuring a Server Authentication Certificate	37
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	38
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	40
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	40
Step 3: Configuring Windows Remote Management	41
Option 1: Using a Script to Configure Windows Remote Management	41
Option 2: Manually Configuring Windows Remote Management	47
Option 3: Using a Group Policy to Configure Windows Remote Management	49
Step 4: Configuring a Windows Management Proxy	67
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	68
SNMP and PowerShell Dynamic Applications for Windows Devices	69
SNMP Dynamic Applications for Windows Devices	70
PowerShell Dynamic Applications	70
Microsoft: Active Directory Server	70
Microsoft: DHCP Server	71
Microsoft: DNS Server	71
Microsoft: Exchange Server	72
Microsoft: Exchange Server 2010	72
Microsoft: Hyper-V Server	73
Microsoft: IIS Server	74

Microsoft: Lync Server 2010	74
Microsoft: SharePoint Server	75
Microsoft: Skype for Business	75
Microsoft: SQL Server	76
Microsoft: Windows Server	77
Microsoft: Windows Server Services	78
Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows Servers	78
Error Messages for PowerShell Collection	79
Creating SNMP and PowerShell Credentials for Windows Devices	81
Creating an SNMP Credential	81
Creating a PowerShell Credential	84
Testing Windows Credentials	86
SNMP Credential Test	87
PowerShell Credential Test	87
Running a Windows Credential Test	87
Discovering Component Devices on Hyper-V Systems	88
Viewing Component Devices	89
Monitoring a Windows Cluster	90
Monitoring Windows Clusters in the ScienceLogic Platform	90
Discovering Cluster Nodes	91
Aligning a Dynamic Application with a Cluster Node	91
Disabling Collection of a Dynamic Application on a Device	92
Discovering the Cluster IP Address	93
Aligning Dynamic Applications with the Cluster Device	95
Using a Device Template to Configure Dynamic Applications	96
Windows Dashboards	98
Installing the Microsoft Server Dashboards	98
Microsoft: Active Directory Server Performance	100
Microsoft: DNS Server Performance	103
Microsoft: Exchange Server 2010 Performance	105
Microsoft: Exchange Server 2013 Performance	108
Microsoft: IIS Server Performance	111
Microsoft: Lync Server 2010 Dashboards	113
Microsoft: Lync Server 2010 Performance	113
Microsoft: Lync Server 2010 Utilization	116
Microsoft: Skype for Business Dashboards	119
Microsoft: Lync Server 2013 Performance	119
Microsoft: Lync Server 2013 Utilization	122
Microsoft: SQL Server Performance	125
Troubleshooting	129
Troubleshooting WinRM Error Messages	129
Debugging Code 401 Errors	130
Debugging Code 500 Errors	131
Troubleshooting PowerShell Error Messages	132

Chapter 1

Introduction

Overview

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

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

- Monitoring Windows Devices in the ScienceLogic Platform* 5
- What is SNMP?* 5
- What is PowerShell?* 5
- PowerPacks* 6

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software, which is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

Monitoring Windows Devices in the ScienceLogic Platform

The ScienceLogic platform can monitor a Windows device using the following methods:

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

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

For more information about using the ScienceLogic 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. The ScienceLogic platform 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**. The ScienceLogic platform 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. The ScienceLogic platform can then query the device to retrieve the stored data.

What is PowerShell?

Windows PowerShell is a command-line shell and scripting language for administration of Windows systems. The ScienceLogic platform can execute PowerShell requests on target Windows devices via WinRM (Windows Remote Management). For an overview of Windows PowerShell, see <https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6>.

The ScienceLogic platform supports the following PowerShell versions for monitoring Windows devices:

- PowerShell 3.0
- PowerShell 4.0
- PowerShell 5.1

PowerPacks

This manual describes content from the following PowerPack versions:

- Microsoft: Active Directory Server, version 100
- Microsoft: DHCP Server, version 1.0
- Microsoft: DNS Server, version 100
- Microsoft: Exchange Server, version 100
- Microsoft: Exchange Server 2010, version 1.2
- Microsoft: Hyper-V Server, version 100
- Microsoft: IIS Server, version 100
- Microsoft: Lync Server 2010, version 1.0
- Microsoft: SharePoint Server, version 1.0
- Microsoft: Skype for Business, version 100
- Microsoft: SQL Server, version 100
- Microsoft: Windows Server, version 105
- Microsoft: Windows Server Services, version 1.1

Configuring Windows Systems for Monitoring with SNMP

Overview

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

Configuring SNMP for Windows Server 2016 and Windows Server 2012	8
<i>Configuring Ping Responses</i>	8
<i>Installing the SNMP Service</i>	9
<i>Configuring the SNMP Service</i>	14
<i>Configuring the Firewall to Allow SNMP Requests</i>	19
<i>Configuring Device Classes for Windows Server 2016 and Windows 10</i>	19
Manually Align the Device Class	20
Edit the Registry Key	20
Configuring SNMP for Windows Server 2008	21
<i>Configuring Ping Responses</i>	21
<i>Installing the SNMP Service</i>	22
<i>Configuring the SNMP Service</i>	25
<i>Configuring the Firewall to Allow SNMP Requests</i>	30

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 the ScienceLogic platform 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, the ScienceLogic platform scans TCP ports 21, 22, 23, 25, and 80.

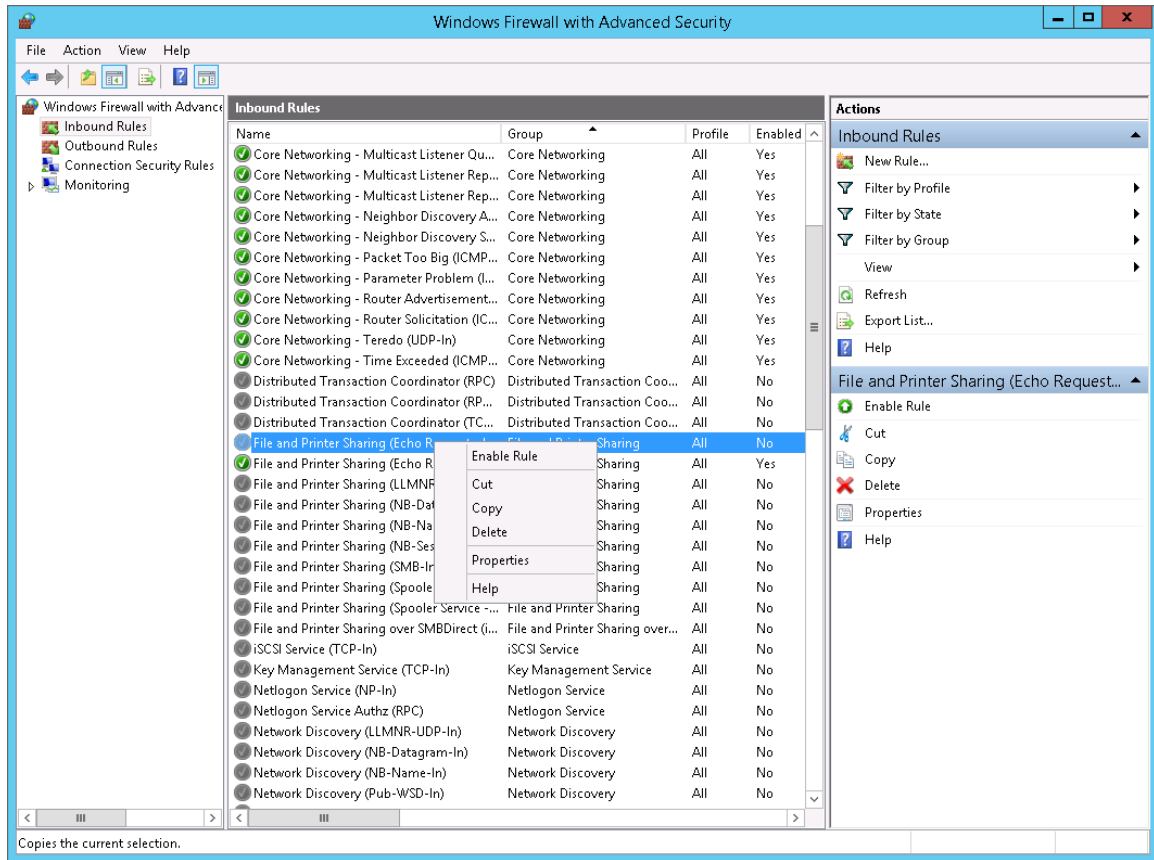
The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in the ScienceLogic platform, you must perform one of the following tasks:

- 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 the ScienceLogic platform to discover your Windows Server using an IPv4 address, locate the *File and Printer Sharing (Echo Request - ICMPv4-In)* rule.

4. If you want the ScienceLogic platform 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*:

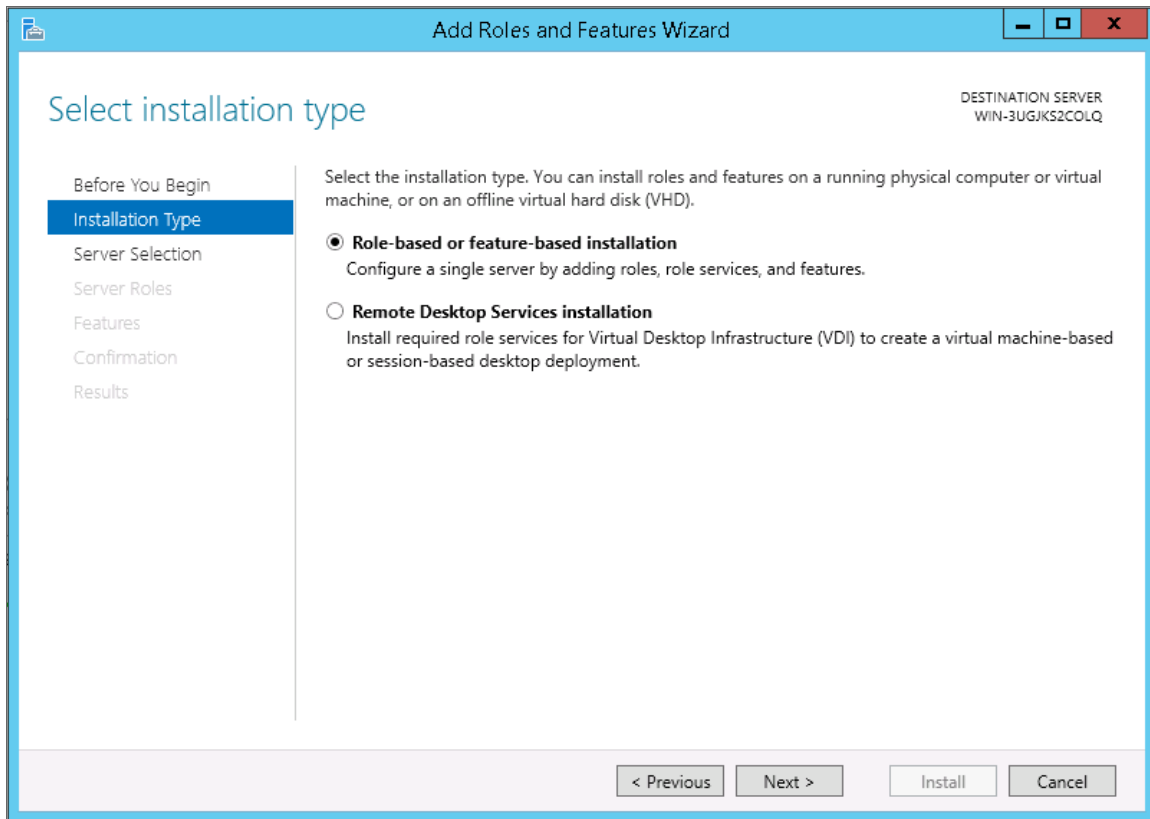


Installing the SNMP Service

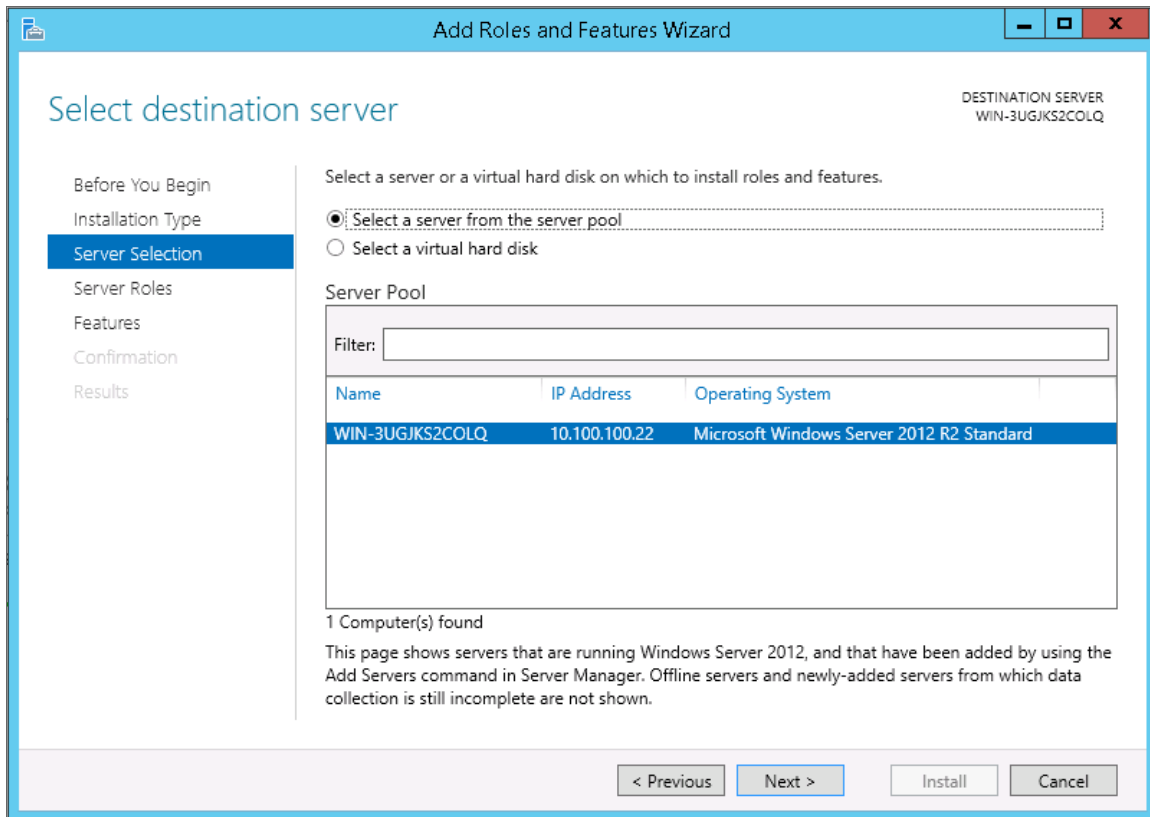
To install the SNMP service on a Windows 2012 Server or Windows 2016 Server, perform the following steps:

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.

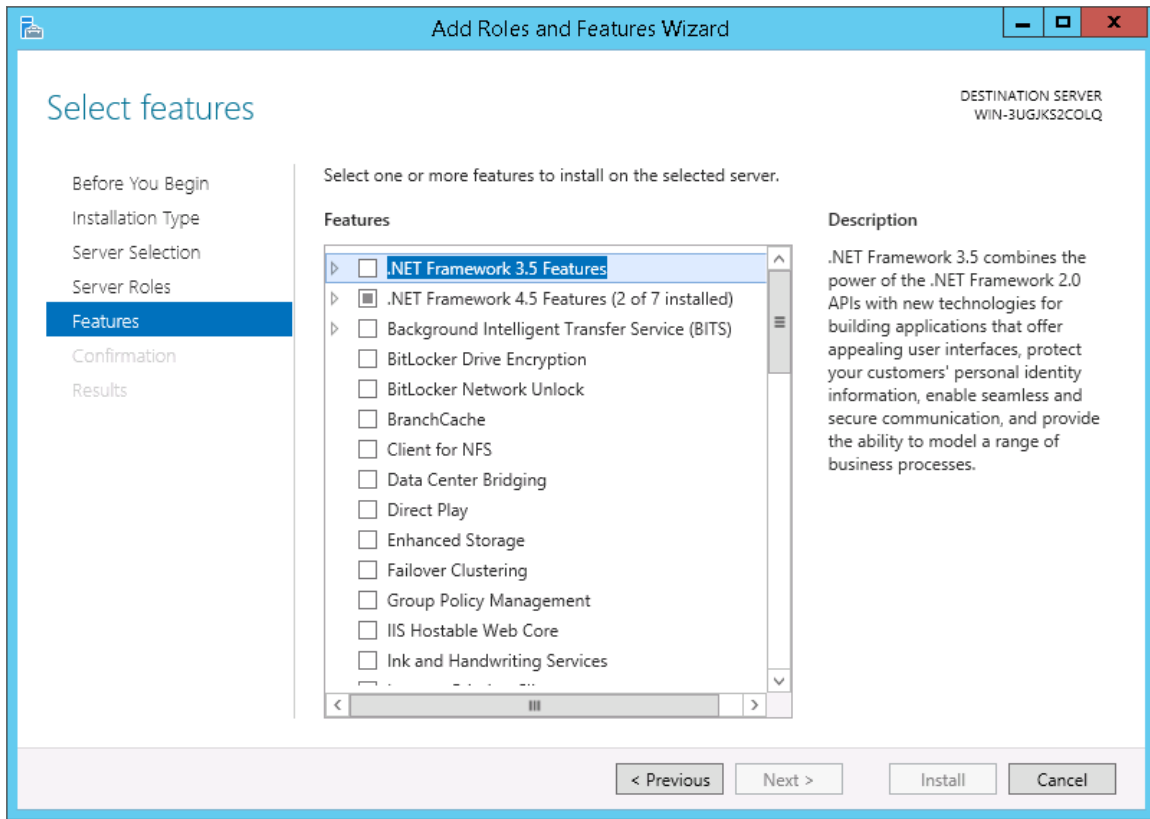
3. If the server does not skip the **Before you begin** page, click the **[Next >]** button to manually skip it. The **Select installation type** page is displayed:



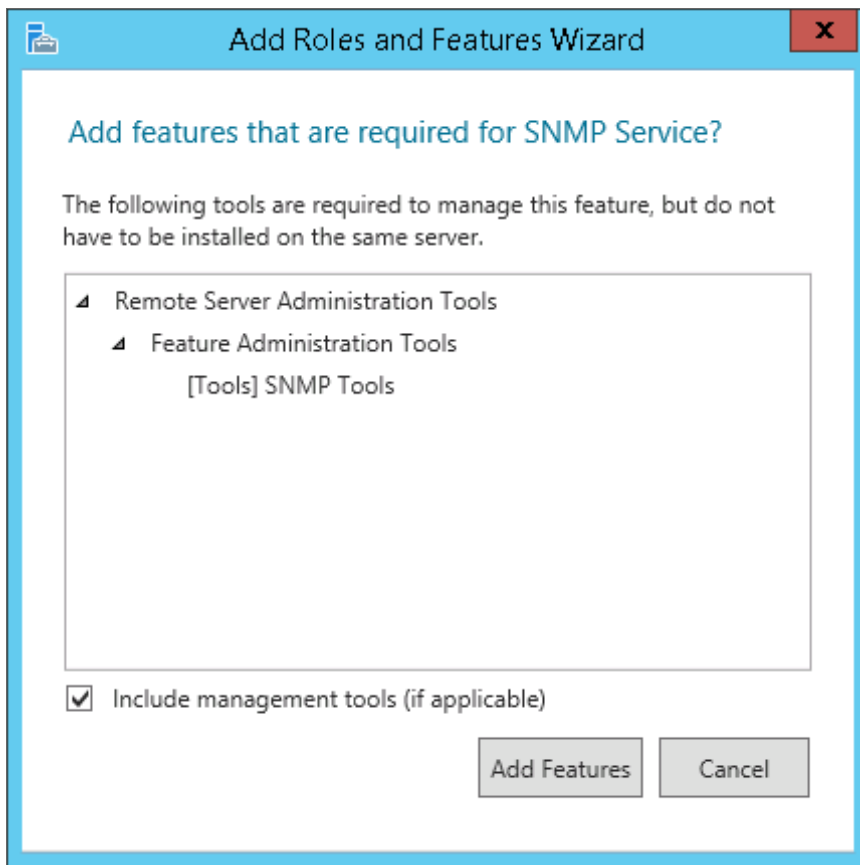
4. Click the **[Next >]** button to continue with *Role-based or feature-based installation*. The **Select destination server** page is displayed:



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:

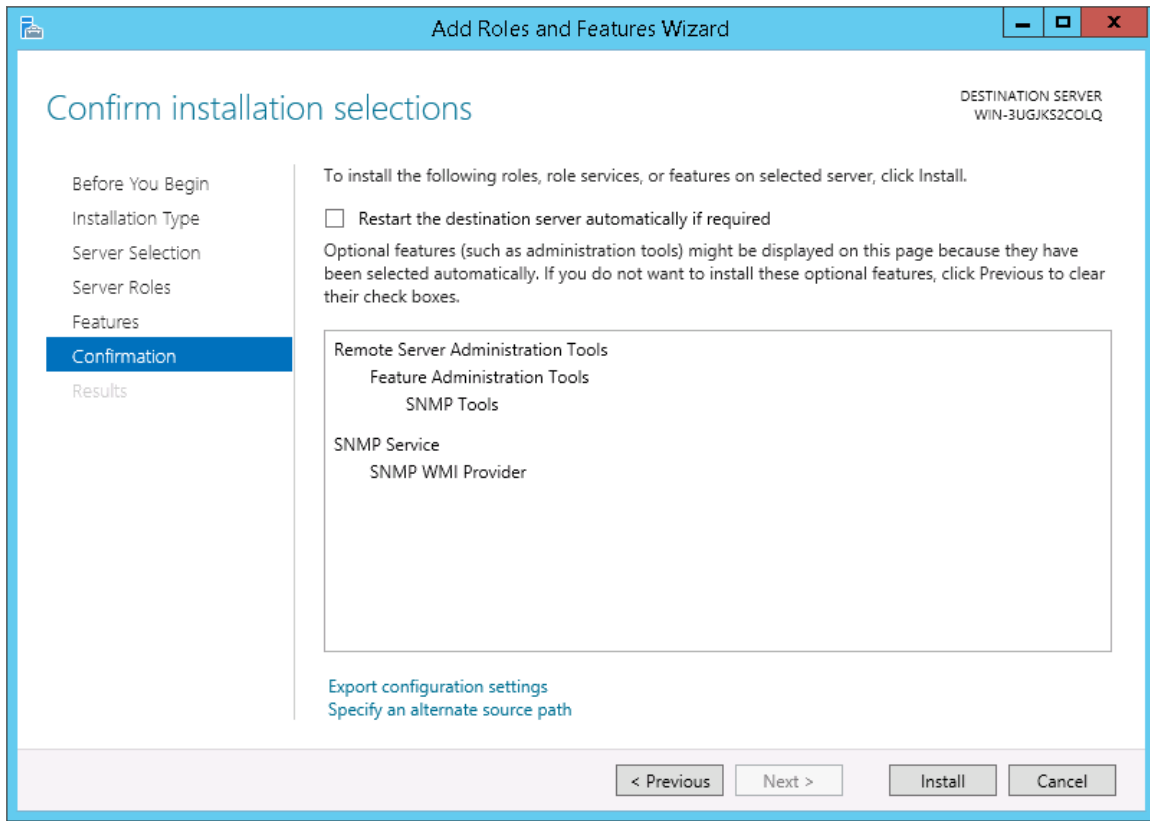


7. Select the *SNMP Service* checkbox. The following confirmation window is displayed:



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:



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

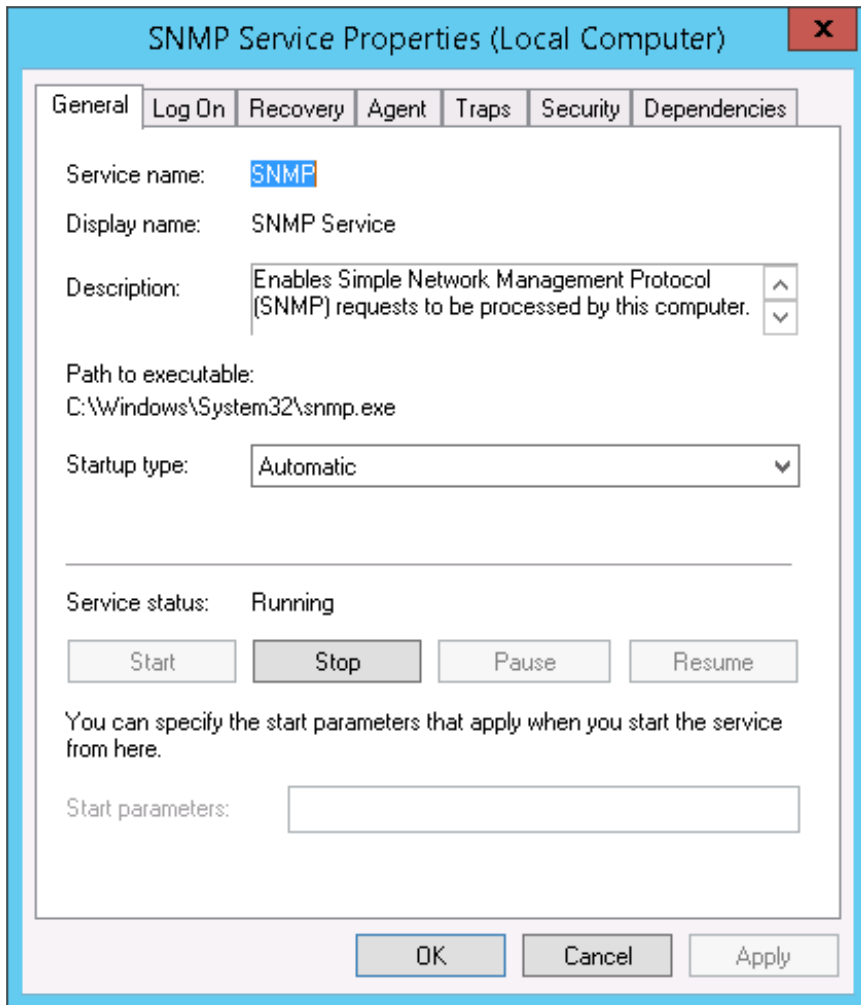
Configuring the SNMP Service

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**.

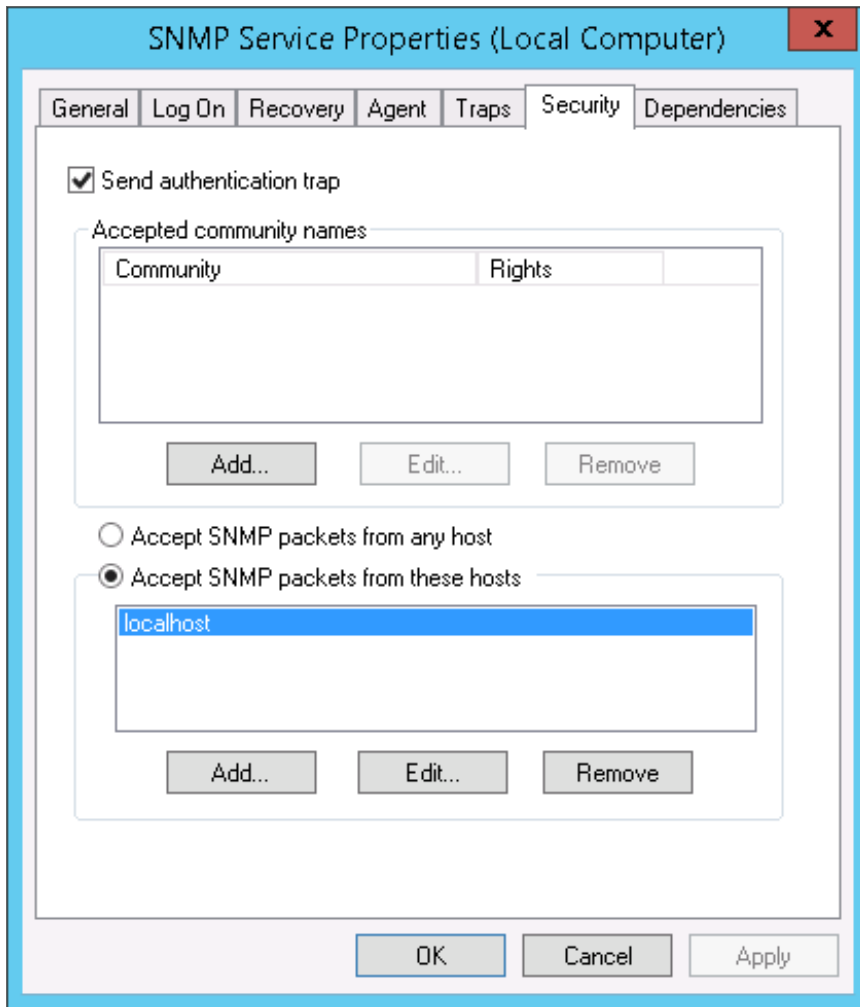
1. In the upper-right of the **Server Manager** window, select **[Tools] > Services**. The **Services** window is displayed.

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

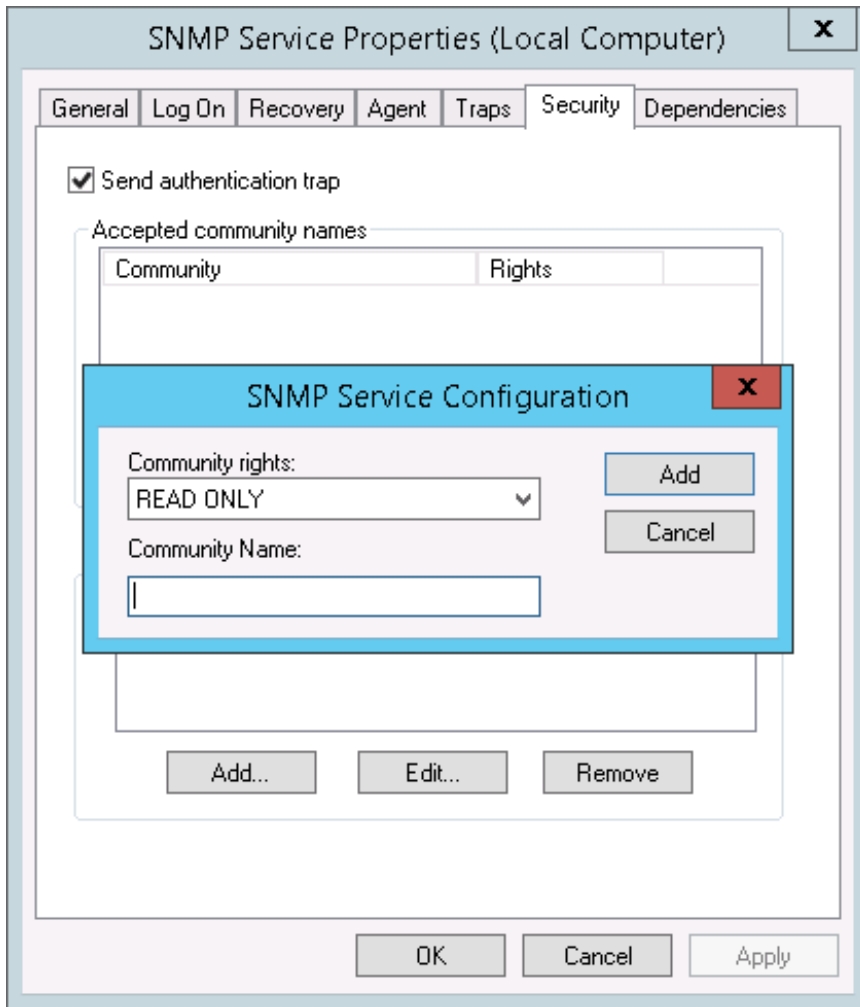


3. In the **Startup type:** field, select *Automatic*.

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



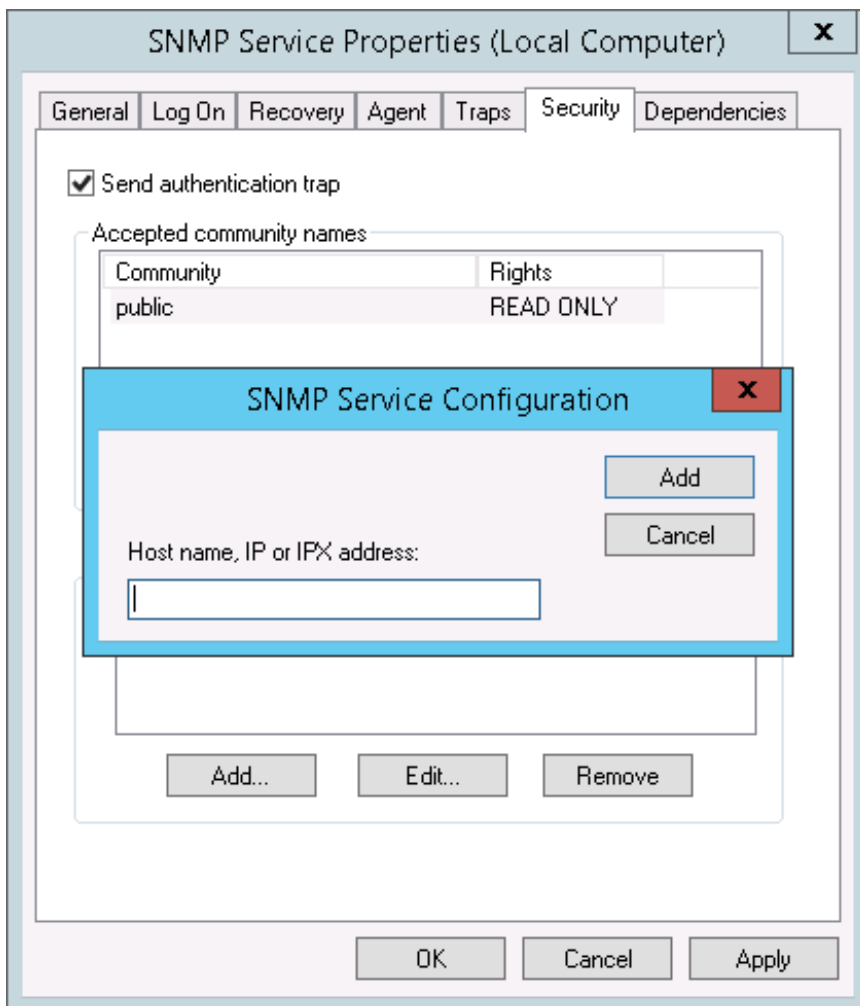
5. In the **Accepted community names** panel, click the **[Add...]** button. The **SNMP Service Configuration** pop-up window is displayed:



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 the ScienceLogic platform to request information from this Windows 2012 Server or Windows 2016 Server using this SNMP community string. This option does not allow the ScienceLogic platform 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 the ScienceLogic platform to request information from this Windows 2008 server and to perform write operations on this Windows 2012 Server or a Windows 2016 Server using this SNMP community string.

- **Community name.** Enter the SNMP community string that the ScienceLogic platform 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 the ScienceLogic platform, 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:



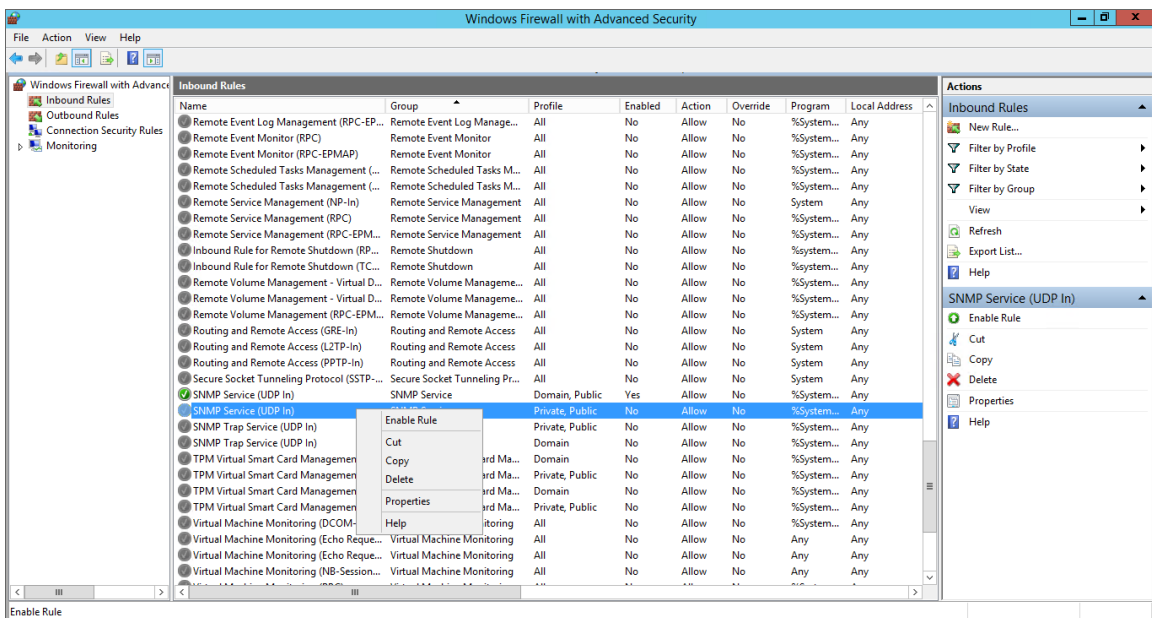
9. In the **Host name, IP or IPX address** field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.

10. Click the **[Add]** button to add the appliance to the list of authorized devices.
11. If you are using the ScienceLogic platform 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*:



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 the ScienceLogic platform 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 the ScienceLogic platform 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, the ScienceLogic platform scans TCP ports 21, 22, 23, 25, and 80.

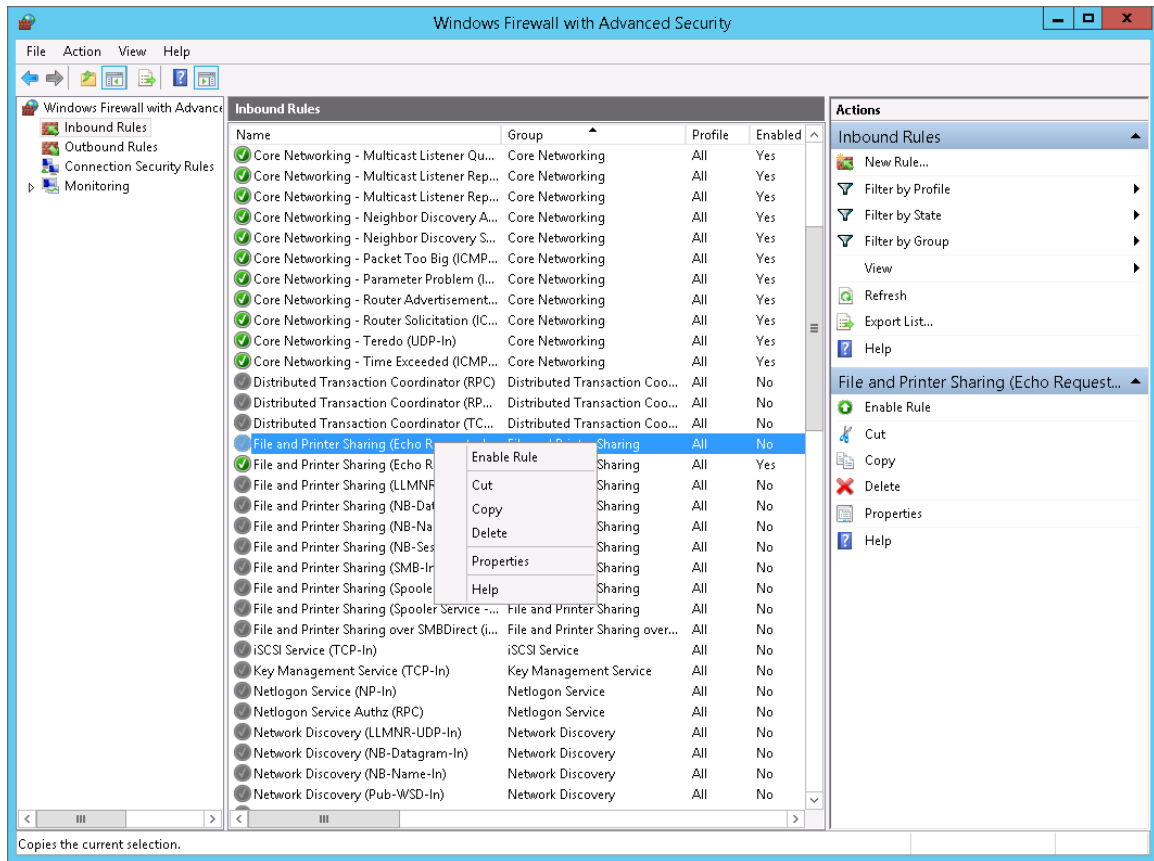
The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in the ScienceLogic platform, you must perform one of the following tasks:

- 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 the ScienceLogic platform to discover your Windows Server using an IPv4 address, locate the *File and Printer Sharing (Echo Request - ICMPv4-In)* rule.
4. If you want the ScienceLogic platform to discover your Windows Server using an IPv6 address, locate the *File and Printer Sharing (Echo Request - ICMPv6-In)* rule.

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

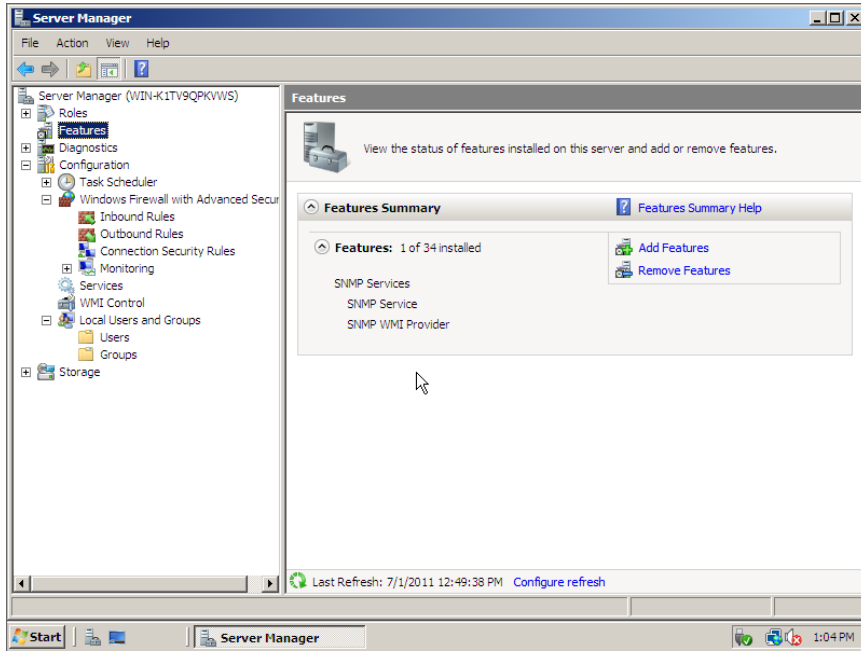


Installing the SNMP Service

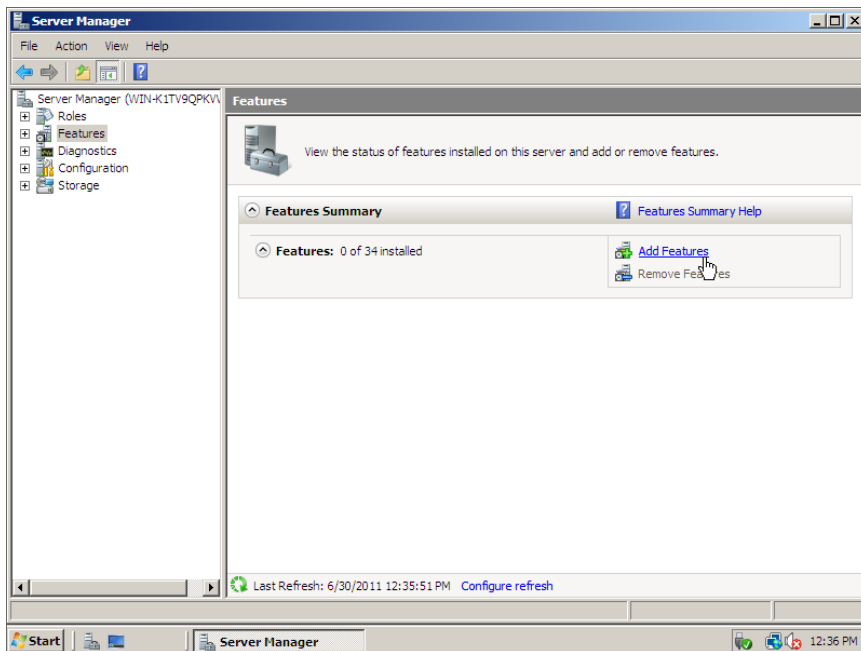
To install the SNMP service on a Windows 2008 Server, perform the following steps:

- Open the **Server Manager** utility.

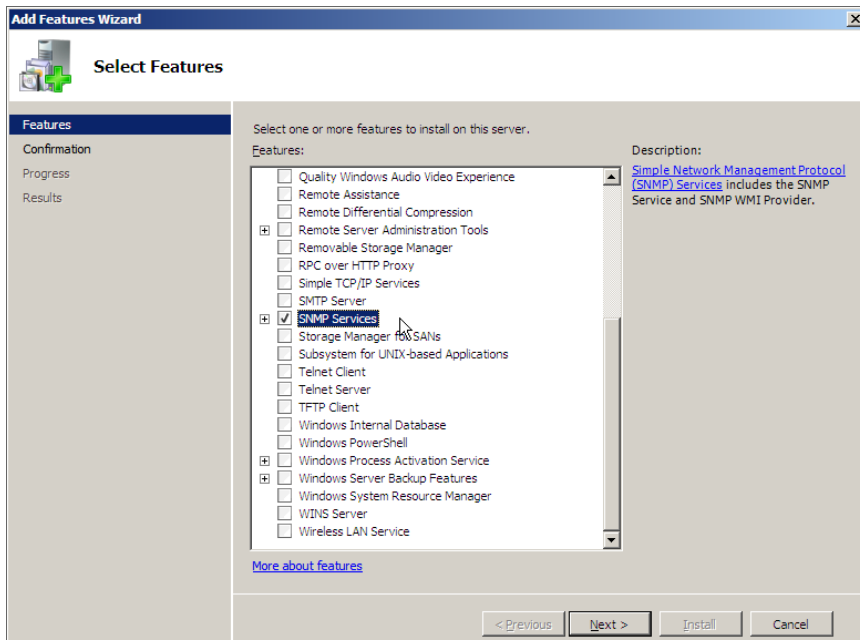
2. In the left pane of the **Server Manager** window, select *Features*. The **Features Summary** is displayed:



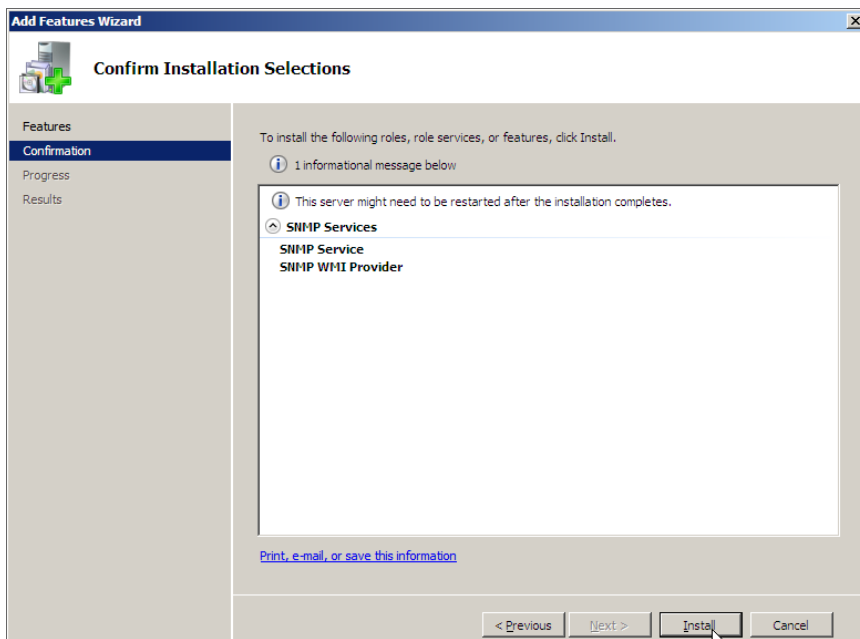
3. If the **Features Summary** displays "SNMP Service" and "SNMP WMI Provider" in the list of installed services (as shown above), you can skip to the section on configuring the SNMP service. If "SNMP Service" and "SNMP WMI Provider" are not included in the list of installed services, select **Add Features**:



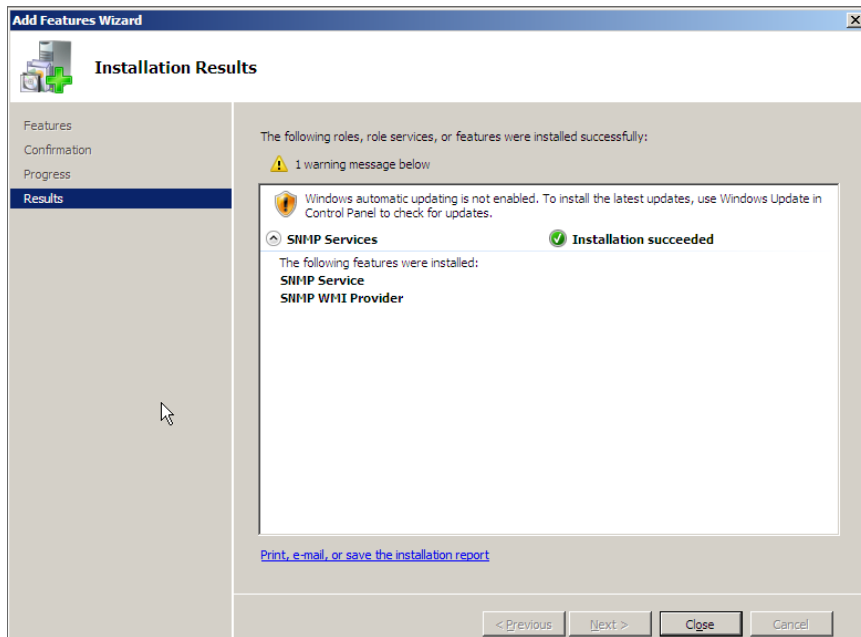
4. In the **Select Features** window, select **SNMP Services**:



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:



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



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

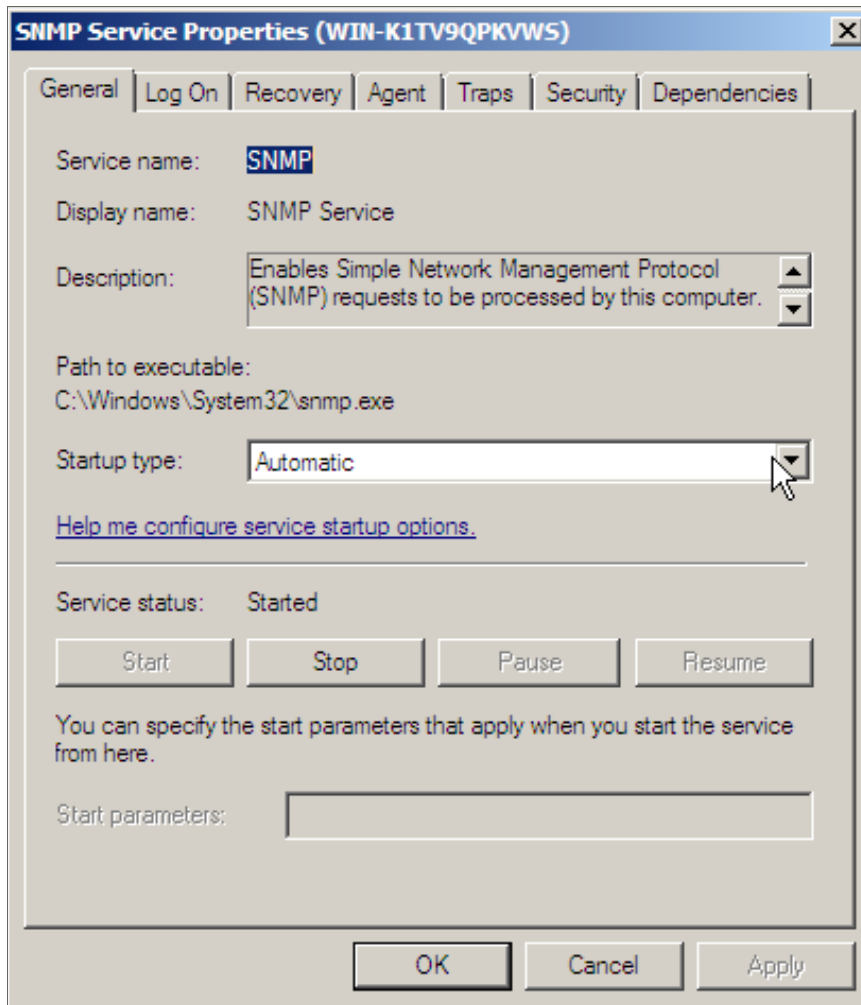
Configuring the SNMP Service

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**.

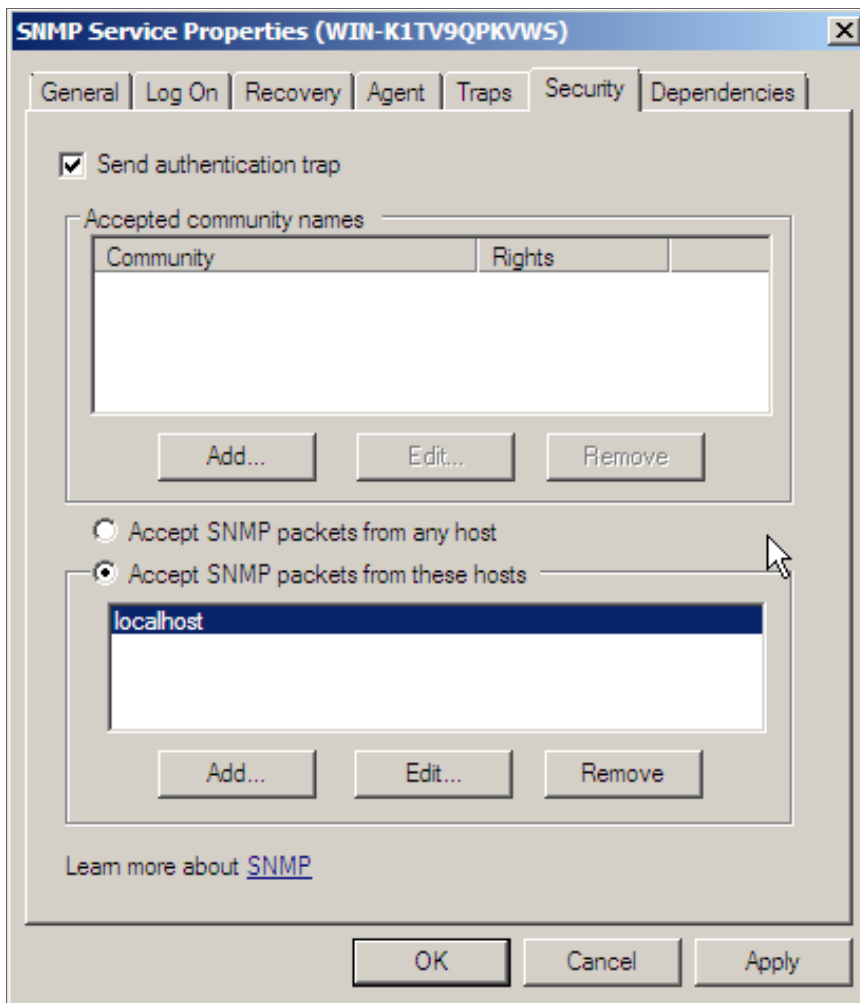
1. In the left pane of the **Server Manager** window, expand the *Configuration* section, and then select *Services*.

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

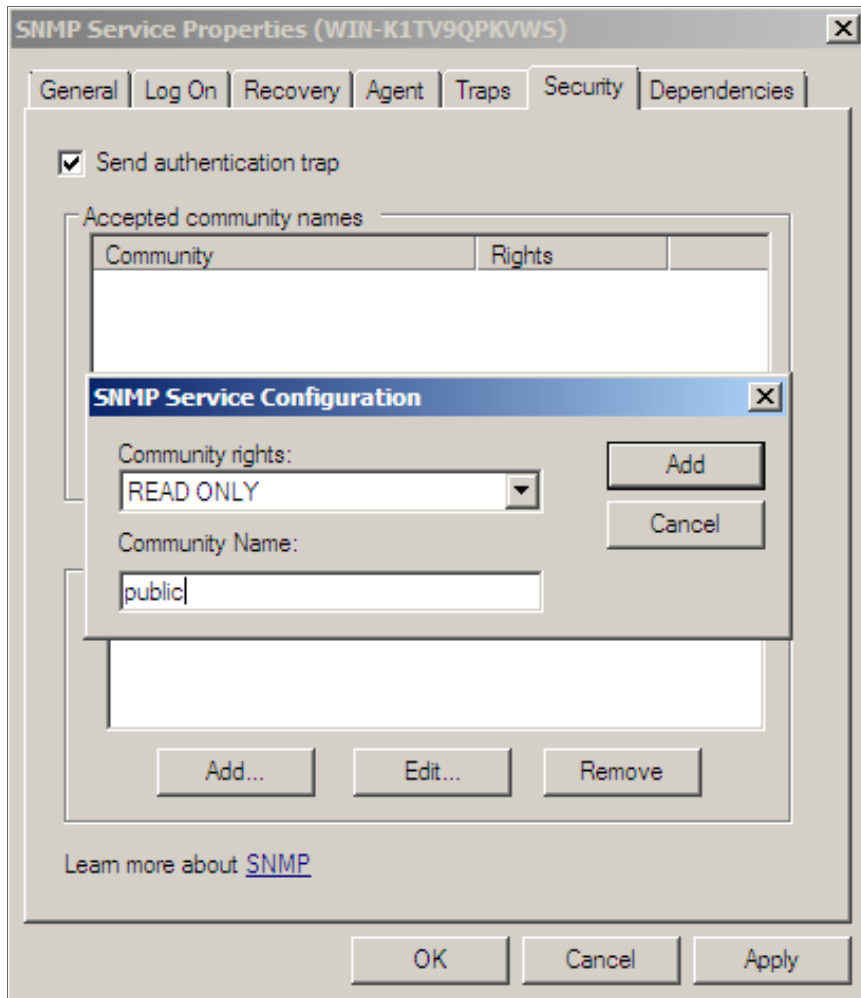


3. In the **Startup type:** field, select *Automatic*.

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



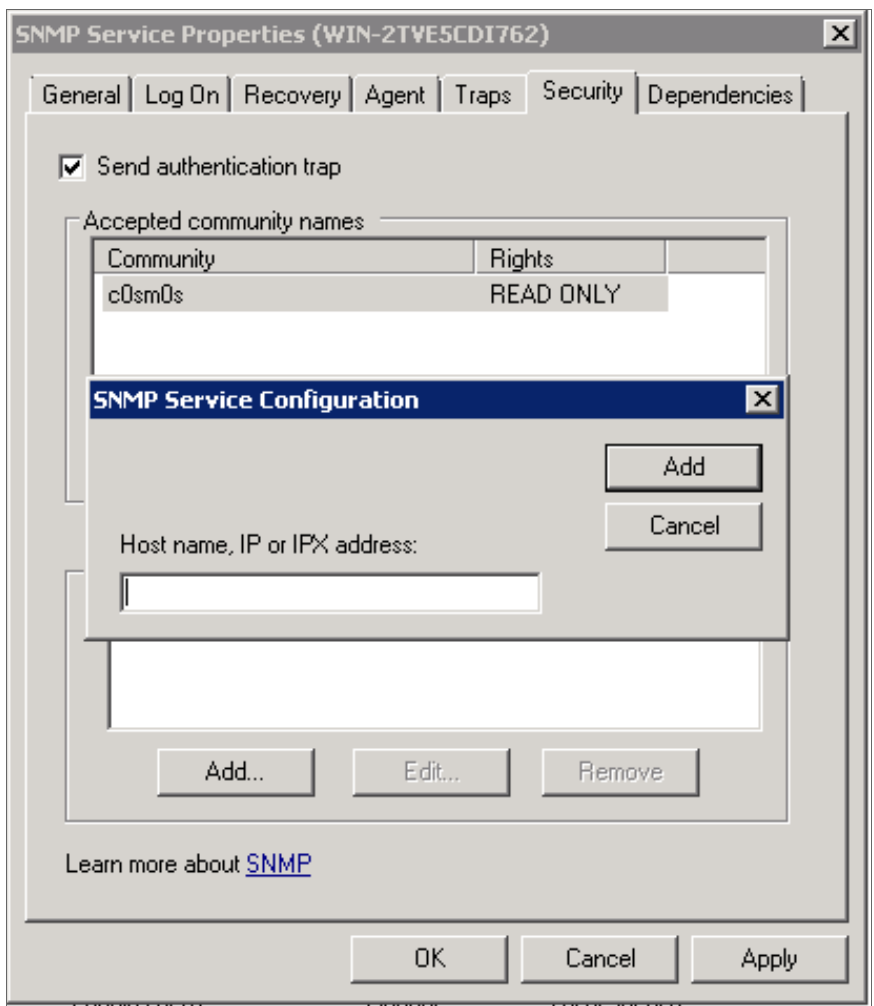
5. In the **Accepted community names** panel, click the **[Add...]** button. The **SNMP Service Configuration** pop-up window is displayed:



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 the ScienceLogic platform to request information from this Windows 2008 Server using this SNMP community string. This option does not allow the ScienceLogic platform to perform write operations on this Windows 2008 Server using this SNMP community string.
 - **READ WRITE.** Select this option to allow the ScienceLogic platform 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 the ScienceLogic platform will use to make SNMP requests to this Windows 2008 Server. When you create a credential for this Windows 2008 Server in the ScienceLogic platform, you will enter this community string in one the following fields in the **Credential Editor** modal page:
 - SNMP Community (Read-Only). Enter the SNMP community string in this field if you selected *READ ONLY* in the **Community rights** drop-down list.
 - SNMP Community (Read/Write). Enter the SNMP community string in this field if you selected *READ WRITE* in the **Community rights** drop-down list.
7. Click the **[Add]** button to add the community string to list of community strings this Windows 2008 Server accepts.
 8. In the **Accept SNMP packets from these hosts** panel, click the **Add...** button. The **SNMP Service Configuration** pop-up window is displayed:



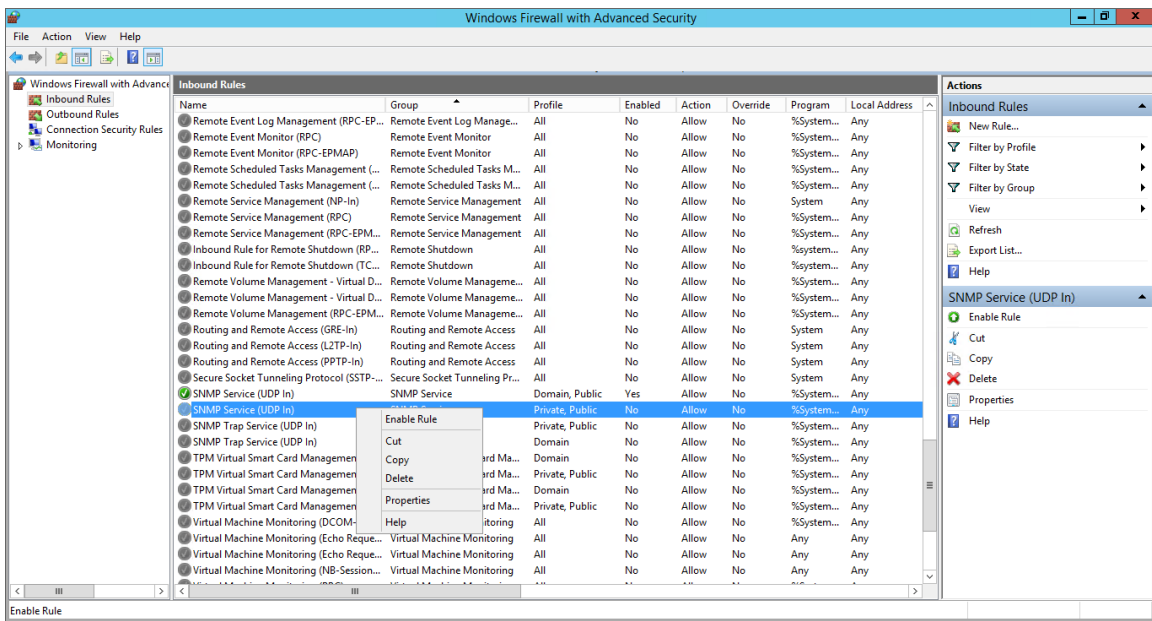
9. In the **Host name, IP or IPX address** field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.

10. Click the **[Add]** button to add the appliance to the list of authorized devices.
11. If you are using the ScienceLogic platform 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*:



Configuring Windows Servers for Monitoring with PowerShell

Overview

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

<i>Configuring PowerShell</i>	32
Step 1: Configuring the User Account for the ScienceLogic Platform	32
<i>Option 1: Creating an Active Directory Account</i>	33
<i>Option 2: Creating a Local User Account with Administrator Access</i>	33
<i>Option 3: Creating a Non-Administrator Local User Account</i>	34
<i>Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server</i>	35
<i>Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers</i>	36
<i>Creating a User Group and Adding a User in Active Directory</i>	36
<i>Setting the Session Configuration Parameters and Group Permissions</i>	36
<i>Creating a PowerShell Credential</i>	37
Step 2: Configuring a Server Authentication Certificate	37
<i>Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate</i>	38
<i>Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate</i>	40
<i>Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate</i>	40
Step 3: Configuring Windows Remote Management	41
<i>Option 1: Using a Script to Configure Windows Remote Management</i>	41
<i>Option 2: Manually Configuring Windows Remote Management</i>	47

Option 3: Using a Group Policy to Configure Windows Remote Management	49
Step 4: Configuring a Windows Management Proxy	67
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously ...	68

Configuring PowerShell

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

1. [Configure a user account](#) that the platform will use to connect to the Windows Server. The user account can either be a local account or an Active Directory account.

TIP: For ease-of-configuration, ScienceLogic recommends using an Active Directory account that is a member of the Local Administrator's group on the Windows Server.

2. [Configure a Server Authentication Certificate](#) to encrypt communication between the platform and the Windows Server.

NOTE: If you have created an Active Directory account on the Windows Server, or if your network includes a Microsoft Certificate server, you can skip this step. You must configure a Server Authentication Certificate **only** if you have created a local account on the Windows Server and your network **does not include** a Microsoft Certificate server.

3. [Configure Windows Remote Management](#).
4. Optionally, [configure a Windows server as a Windows Management Proxy](#).

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

5. Optionally, you can [increase the number of PowerShell Dynamic Applications that can run simultaneously](#) against a single Windows server.

Step 1: Configuring the User Account for the ScienceLogic Platform

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

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

- **Option 1:** [Create an Active Directory Account](#)
- **Option 2:** [Create a local user account with Local Administrator access](#)
- **Option 3:** [Create a non-administrator local user account](#)

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

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

- [Microsoft Exchange Server](#)
- [Hyper-V Servers](#)

Option 1: Creating an Active Directory Account

If you have Local Administrator access to the Windows servers that you want to monitor with PowerShell or WinRM, you can create an Active Directory account that is a member of the Local Administrator group on each server you want to monitor. For instructions, consult Microsoft's documentation.

TIP: For ease-of-configuration, ScienceLogic recommends this method, as it does not require you to configure a Server Authentication Certificate to ensure secure data transfer and authentication.

After creating your Active Directory account:

- If you use the ScienceLogic platform to monitor Microsoft Exchange Servers, you must [configure the user account for remote PowerShell access to Microsoft Exchange Server](#).
- If you use the ScienceLogic platform to monitor Hyper-V Servers, you must [configure the user account for remote PowerShell access to the Hyper-V Servers](#).
- Otherwise, *you can skip the remainder of this section and proceed to Step 3.*

Option 2: Creating a Local User Account with Administrator Access

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

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

After creating your local user account with Local Administrator access:

- If you use the ScienceLogic platform to monitor Microsoft Exchange Servers, you must [configure the user account for remote PowerShell access to Microsoft Exchange Server](#).
- If you use the ScienceLogic platform to monitor Hyper-V Servers, you must [configure the user account for remote PowerShell access to the Hyper-V Servers](#).
- Otherwise, *you can skip the remainder of this section and proceed to Step 2*.

Option 3: Creating a Non-Administrator Local User Account

If you do not have Local Administrator access to the servers that you want to monitor with PowerShell or WinRM, then you must first create a domain user account or create a non-administrator local user account on the Windows Server. For instructions, consult Microsoft's documentation.

After creating your local non-administrator user account:

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

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

1. Log in to Windows PowerShell as an administrator and execute the following command:

```
winrm configsddl default
```

2. On the **Permissions** window, click the **[Add]** button, and then add the non-administrator domain user or group.
3. Select the *Allow* checkbox for the **Read (Get, Enumerate, Subscribe)** and **Execute (Invoke)** permissions for the user, and then click **[OK]**.
4. Access the Management console. To do this:
 - In Windows Server 2008, click **[Start]**, right-click **[Computer]**, click **[Manager]**, and then expand **[Configuration]**.
 - In Windows Server 2016 and 2012, right-click the Windows icon, click **[Computer Management]**, and then expand **[Services and Applications]**.
5. Right-click on **[WMI Control]** and then select *Properties*.
6. On the **WMI Control Properties** window, click the **[Security]** tab, and then click the **[Security]** button.
7. Click the **[Add]** button, and then add the non-administrator domain user or group.
8. Select the *Allow* checkbox for the **Execute Methods**, **Enable Account**, and **Remote Enable** permissions, and then click **[OK]**.
9. On the **WMI Control Properties** window, click the **[Advanced]** tab.

10. Double-click on the user account (or group).
11. On the **Permission Entry** window, in the **Type** field, select *Allow*.
12. In the **Applies to** field, select *This namespace and subnamespaces*.
13. Select the **Execute Methods**, **Enable Account**, and **Remote Enable** permission checkboxes, and then click **[OK]**.
14. Restart the WMI Service from services.msc.

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

15. In the Management console, go to System Tools > Local Users and Groups > Groups.
16. Right-click **Performance Monitor Users**, and then select *Properties*.
17. On the **Performance Monitor Users Properties** window, click the **[Add]** button.
18. In the **Enter the object names to select** field, type the non-administrator domain user or group name, and then click **[Check Names]**.
19. Select the user or group name from the list and then click **[OK]**.
20. In the **Performance Monitor Users Properties** window, click **[OK]**.
21. Run cmd as an administrator and execute the following command:

```
sc sdset SCMANAGER D: (A;;CCLCRPRC;;;AU) (A;;CCLCRPWPRC;;;SY) (A;;KA;;;BA) S:
(AU;FA;KA;;;WD) (AU;OIIOFA;GA;;;WD)
```

22. Optionally, you can create a self-signed certificate for WinRM by executing the following command:

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

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

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

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

24. Ensure that your local firewall allows inbound TCP connections on port 5986. You may have to create a new rule on Windows Firewall if one does not already exist.

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

If you use the ScienceLogic platform to monitor Microsoft Exchange Servers:

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

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

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

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

Creating a User Group and Adding a User in Active Directory

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

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

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

Setting the Session Configuration Parameters and Group Permissions

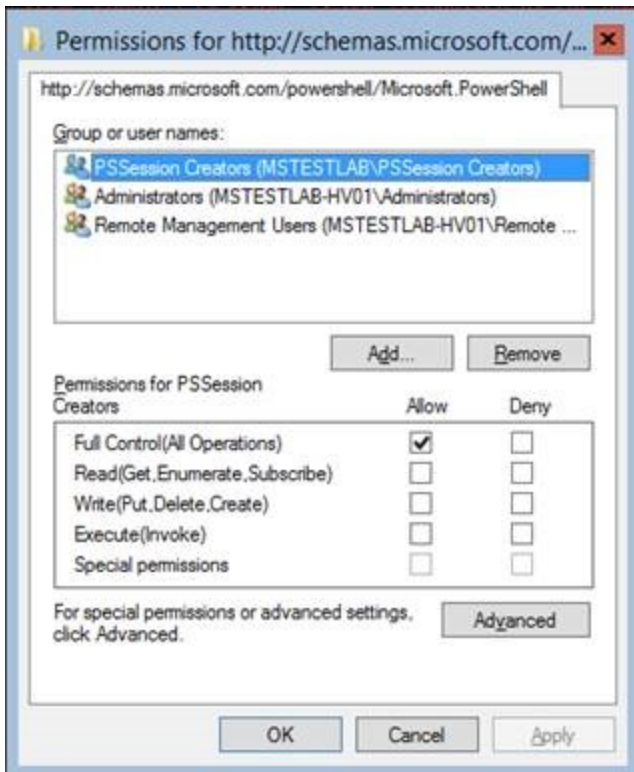
To set the Session Configuration and the Group Permissions on the Hyper-V Server:

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

```
Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell
```

3. When prompted, select **A**.

4. The **Permissions** dialog appears.



5. In the **Permissions** dialog, supply values in the following fields:

- **Group or user names.** Select the name of the group you created in Active Directory.
- **Permissions for group.** For **Full Control (All Operations)**, select the *Allow* checkbox.

6. Click the [OK] button.

Creating a PowerShell Credential

To create a PowerShell credential using the new user account, follow the instructions in the [Creating a PowerShell Credential](#) section.

Step 2: Configuring a Server Authentication Certificate

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

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

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

The sections below describe how to configure a Server Authentication Certificate on the Windows Server. This is only one task included in configuring an HTTPS listener. However, not all users need to configure a Server Authentication Certificate.

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

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

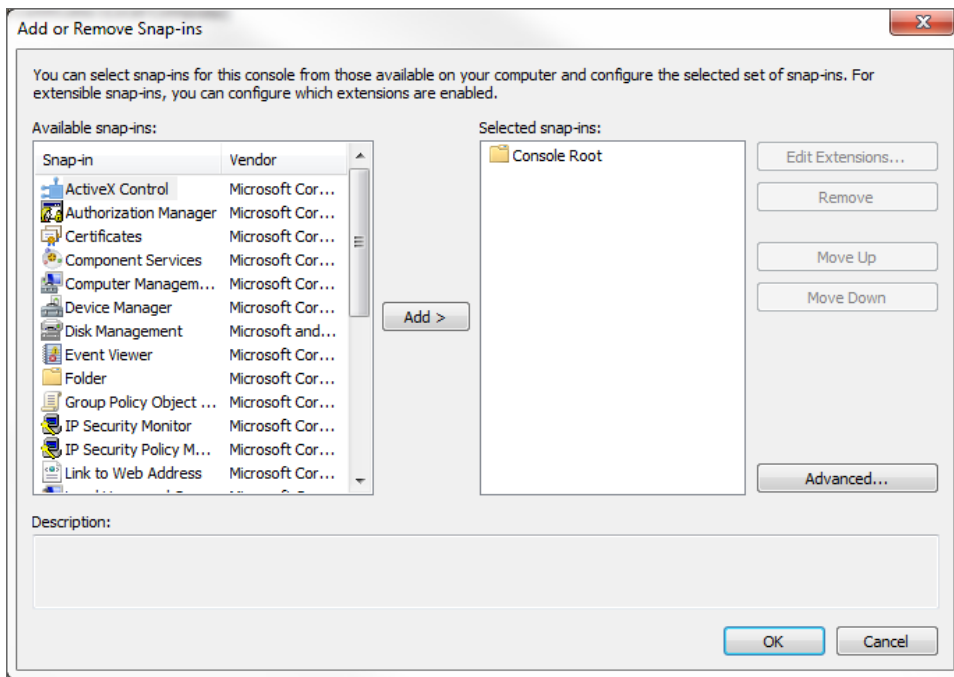
NOTE: Self-signed certificates are appropriate for use on a trusted network, such as a LAN that includes both a ScienceLogic Data Collector and the Windows Server to be monitored.

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

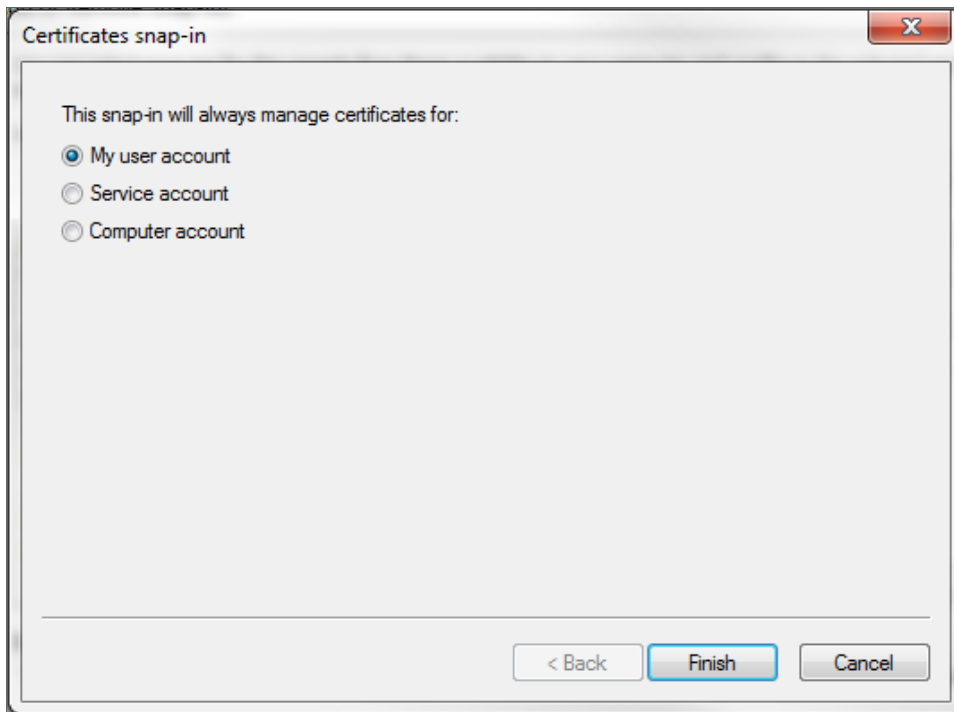
To use the **Microsoft Management Console** to create a self-signed certificate:

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

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



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



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

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

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

- For information on the MakeCert tool, see:
<https://msdn.microsoft.com/library/windows/desktop/aa386968.aspx>
- For details on creating a self-signed certificate with MakeCert and installing the certificate in the Trusted Root Certification Authorities store, see:
<https://msdn.microsoft.com/en-us/library/ms733813%28v=vs.110%29.aspx>

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

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

- You can use the **New-SelfSignCertificate** command to create a self-signed certificate. For information on **New-SelfSignCertificate**, see:
<https://technet.microsoft.com/en-us/library/hh848633%28v=wps.630%29.aspx>
- You can use the **Export-PfxCertificate** command to export the private certificate. For information on the **Export-PfxCertificate**, see:
<https://technet.microsoft.com/en-us/library/hh848635.aspx>

Step 3: Configuring Windows Remote Management

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

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

There are three ways to configure Windows Remote Management:

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

Option 1: Using a Script to Configure Windows Remote Management

ScienceLogic provides a PowerShell script on the ScienceLogic portal that automates the installation and configuration of Windows Remote Management.

To use the PowerShell script, perform the following steps:

1. Log in to the ScienceLogic portal, go to **Downloads > Miscellaneous**, and download the PowerShell script named **WinRM Configuration Wizard Script (winrm_configuration_wizard.ps1)**. The link is : <https://portal.sciencelogic.com/portal/miscellaneous/download/3943>
2. Unzip the downloaded file.
3. Log in as an administrator to the Windows server you want to monitor with the ScienceLogic platform. You can log in directly or use Remote Desktop to log in.

NOTE: During login, use the username and password that you will use later to allow the ScienceLogic platform to monitor the Windows server.

4. Copy the PowerShell script named **winrm_configuration_wizard.ps1** to the Windows server that you want to monitor with the ScienceLogic platform.
5. Right-click on the PowerShell icon and select **Run As Administrator**.
6. At the PowerShell prompt, navigate to the directory where you copied the PowerShell script named **winrm_configuration_wizard.ps1**.
7. At the PowerShell prompt, enter the following to enable execution of the script:

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

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

8. After the warning text, select Y.

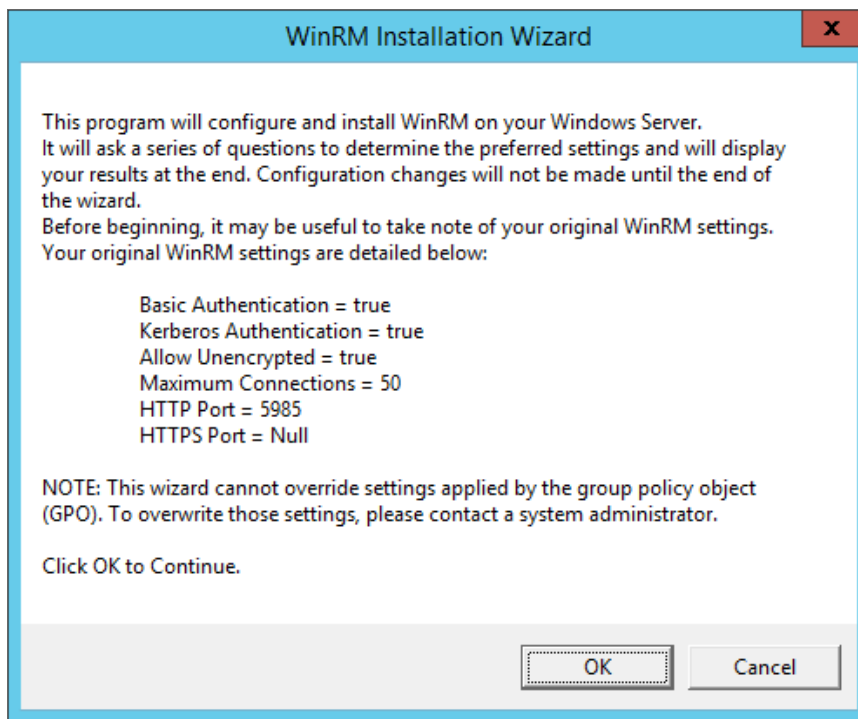
NOTE: If your Windows configuration requires further steps to allow execution of the script, PowerShell will display prompts. Follow the prompts.

9. At the PowerShell prompt, enter the following to execute the script:

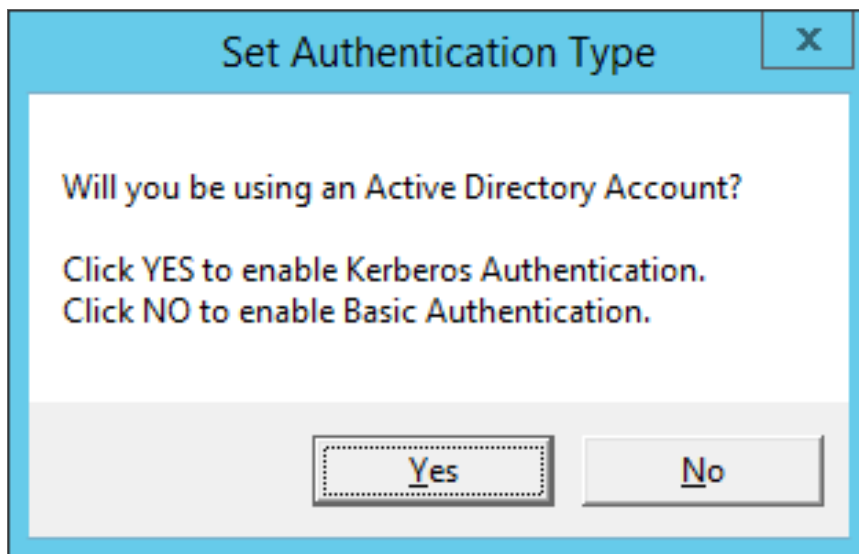
```
.\winrm_configuration_wizard.ps1
```

NOTE: To execute the script in debug mode, enter the following:
.\winrm_configuration_wizard.ps1 -debug

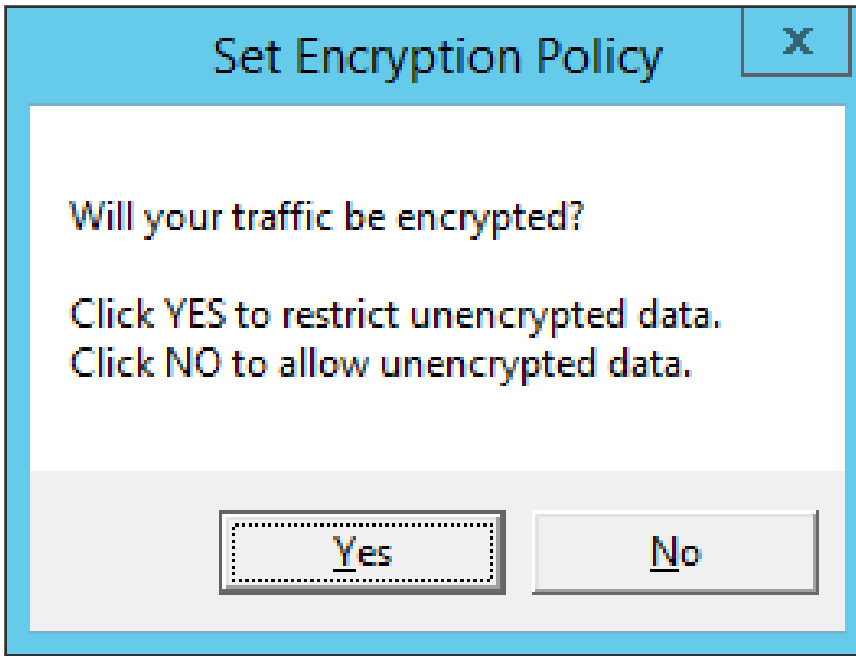
10. The **WinRM Installation Wizard** modal page appears. Click **[OK]**.



11. The **Set Authentication Type** modal page appears. Select the appropriate choice for your environment.

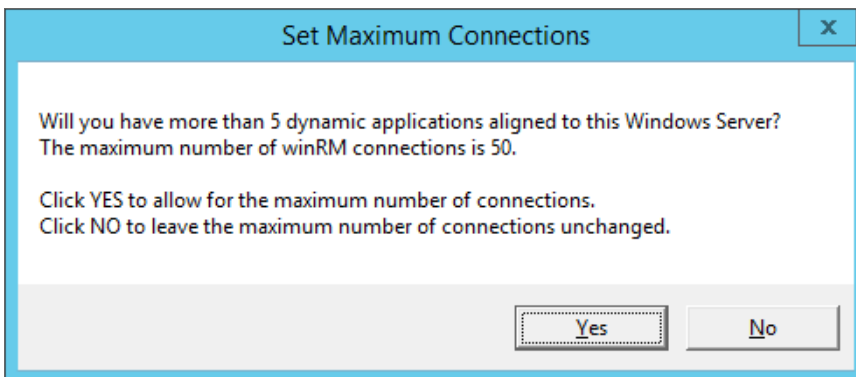


12. The **Set Encryption** modal page appears. Select the appropriate choice for your environment.

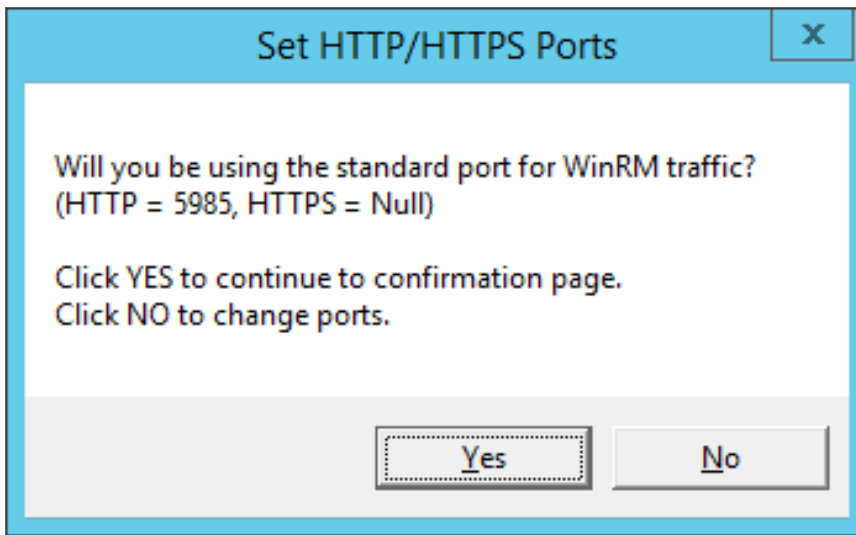


- **Click YES to restrict unencrypted data.** If when communicating with the Windows server, the ScienceLogic platform will use a local user account with authentication of type "Basic Auth", select this option. You must then use HTTPS and can use a Microsoft Certificate or a self-signed certificate. For information on creating a self-signed certificate, see [Configuring a Server Authentication Certificate](#).
- **Click NO to allow unencrypted data.** If when communicating with the Windows server, the ScienceLogic platform will use an AD account, all authentication information is encrypted via Kerberos. Additional encryption is unnecessary.

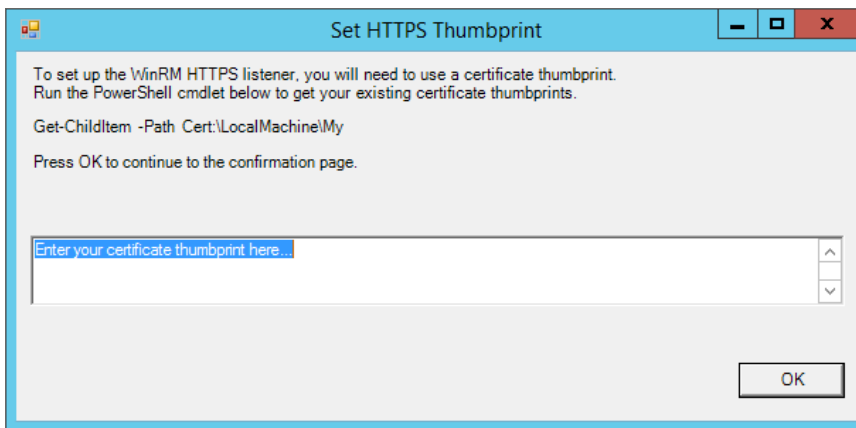
13. The **Set Maximum Connections** modal page appears. Click [Yes].



14. The **Set HTTP/HTTPS Ports** modal page appears. Select the appropriate choice for your environment.

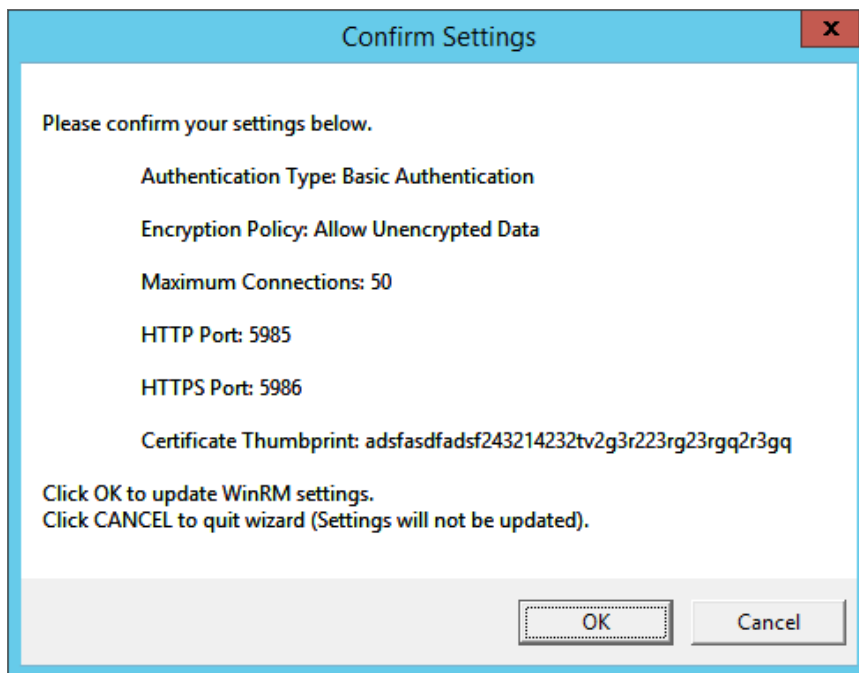


15. The **Set HTTPS Thumbprint** modal page appears. Enter the information for your certificate thumbprint, then click [OK].

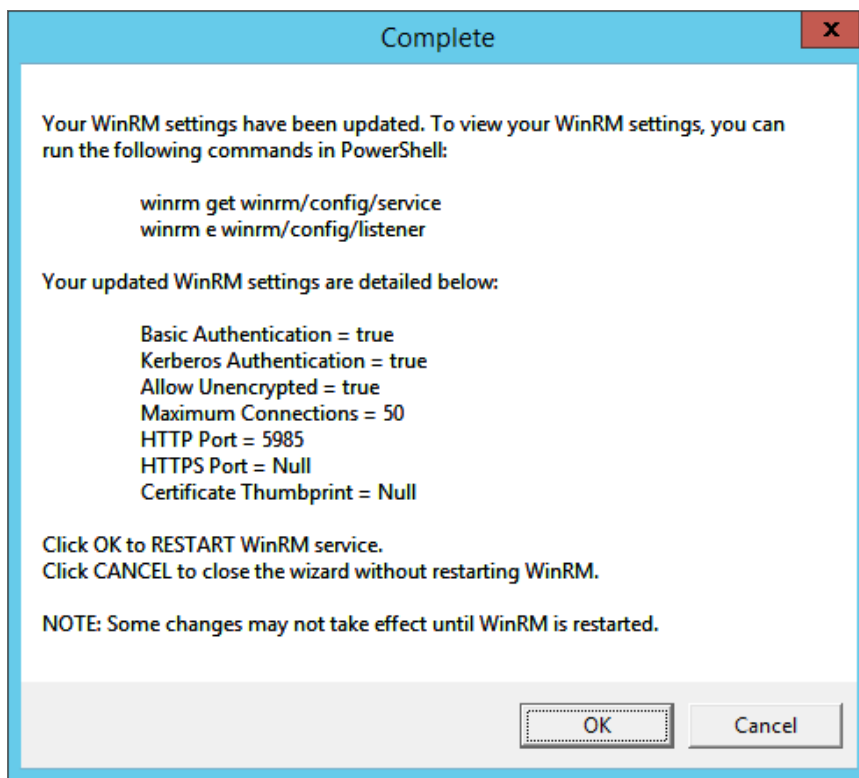


NOTE: If the certificate structure for your certificate thumbprint is incomplete or incorrect, an error message appears indicating that the WinRM client cannot process the request. If you think you made an error, click [OK] and try to correct it. Otherwise, contact a system administrator for help.

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



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



18. Exit the PowerShell session.

Option 2: Manually Configuring Windows Remote Management

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

1. Log in to the server as an administrator.
2. Right-click on the PowerShell icon in the taskbar and select *Run as Administrator*.
3. Execute the following command:

```
Get-ExecutionPolicy
```

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

```
Set-ExecutionPolicy RemoteSigned
```

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

```
winrm quickconfig
```

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

```
winrm quickconfig -transport:https
```

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

```
winrm get winrm/config
```

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

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

```

11. In the Service section, if the parameter **AllowRemoteAccess** is set to *false*, execute the following command:

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

```
Set-Item WSMAN:\localhost\Service\AllowRemoteAccess -value true
```

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

```
Set-Item WSMAN:\localhost\Winrs\AllowRemoteShellAccess -value true
```

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

```
Set-Item WSMAN:\localhost\Service\AllowUnencrypted -value true
```

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

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

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

```
Set-Item WSMAN:\localhost\Service\Auth\Kerberos -value true
```

NOTE: ScienceLogic recommends using an Active Directory account.

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

```
Set-Item WSMAN:\localhost\Service\Auth\Basic -value true
```


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

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

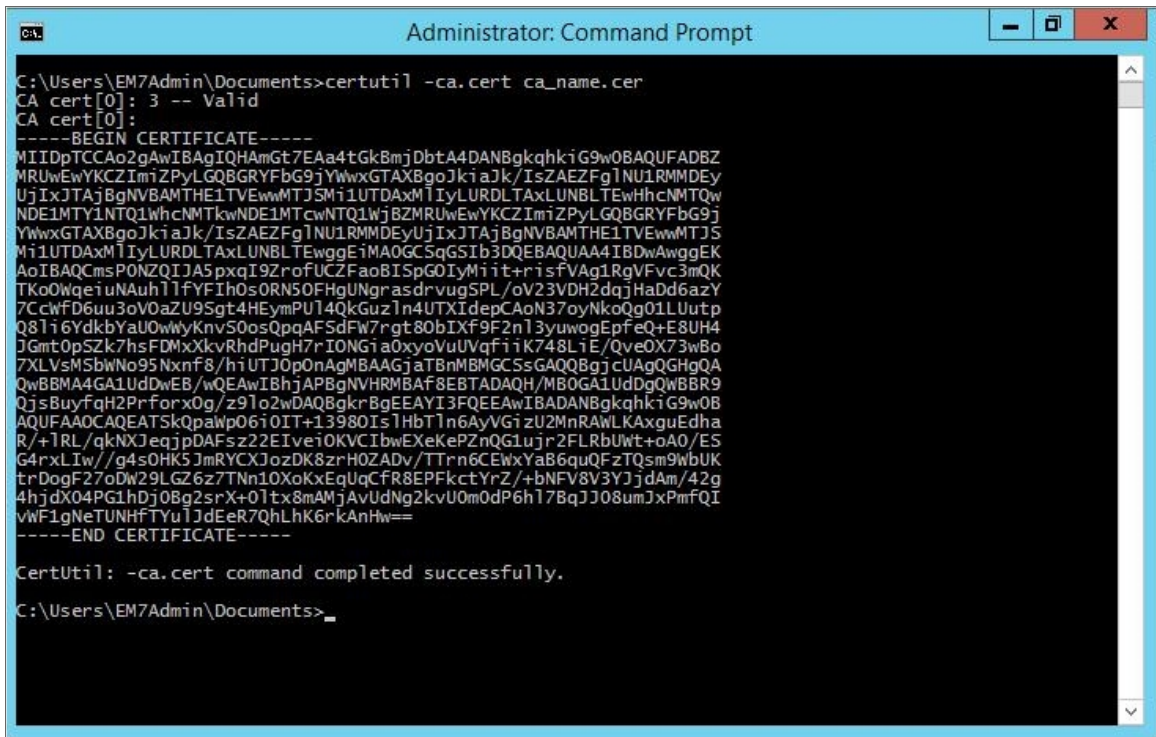
- A registry key to enable Local Account access to Windows Remote Management
- Firewall rules
- Certificates
- HTTP and HTTPS listeners, including authentication and encryption settings
- Service start and recovery settings

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

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

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

```
certutil.exe -ca.cert ca_name.cer
```



```
Administrator: Command Prompt
C:\Users\EM7Admin\Documents>certutil -ca.cert ca_name.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDpTCCAo2gAwIBAgIQHAMgt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ
MRUwEwYKZIm1ZPyLQGBGRYFbG9jYWwzGTAXBgoJkiaJk/IsZAEZFglNU1RMMDEy
UjIxJTAjBgNVBAMTHE1TVWwMTJSMi1UTDAxMlIyLURDLTAxLUNBLTEwHhcnMTQw
NDE1MTY1NTQ1WhcNMtKwNDE1MTcwNTQ1WjBZMRUwEwYKZIm1ZPyLQGBGRYFbG9j
YWwzGTAXBgoJkiaJk/IsZAEZFglNU1RMMDEyUjIxJTAjBgNVBAMTHE1TVWwMTJSMi
1UTDAxMlIyLURDLTAxLUNBLTEwggEiMA0GC5qGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCmsP0NZQIJA5pxqI9ZrofUCZFaoBISpG0IyMitt+r1sfVAg1RgVFvc3mQK
TKo0WqeiuNAuh11FYFIh0s0RN50FHgUNgrasdrvugSPL/ov23VDH2dqjHaDd6azY
7CwfD6uu3oV0aZU9Sgt4HEymPUT4QkGuz1n4UTXIdpCAoN37oyNkoQg01LUutp
Q81i6YdkbYaU0wWyKvS0osQpqAF5dFW7rgt80bIXF9F2n13yuwogEpfEQ+E8UH4
JGmt0pSzk7hsFDMxXkvRhdPugh7rIONGi0xyoVuUVqfiik748LiE/Qve0X73wBo
7XLVsMSbWNo95NxnF8/hiUTJOp0nAgMBAAGjaTBnMBMGCSsGAQQBgjcUAgQHhgQA
QwBBMA4GA1UdDwEB/wQEAwIBhjAPBgNVHRMBAF8EBTADAQH/MB0GA1UdDgQWBBR9
QjsBuyfQh2PrForx0g/z91o2wDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B
AQUFAAOCQEATSkQpawp06i0IT+13980Is1HbT1n6AyVGizU2MnRAWLKAxguEdha
R/+1RL/gkNXJegjpdAFsz22EiveiOKVCIbwEXeKePZnQG1ujr2FLRbUwt+oAO/ES
G4rxLIw//g4s0HK5JmRYCXJozDK8zrHOZADV/TTrn6CEwxYaB6quQFzTQsm9wbUK
trDogF27oDw29LGZ6z7TnN10XoKxEqUqCFR8EPPkctYrZ/+bNFV8V3YjdAm/42g
4hjdX04PG1hDj0Bg2srX+01tx8mAmjAvUdNg2kvU0m0dP6h17BqJJ08umJxPmfQI
vWF1gNeTUNHFYU1JdEeR7QhLhK6rkAnHw==
-----END CERTIFICATE-----

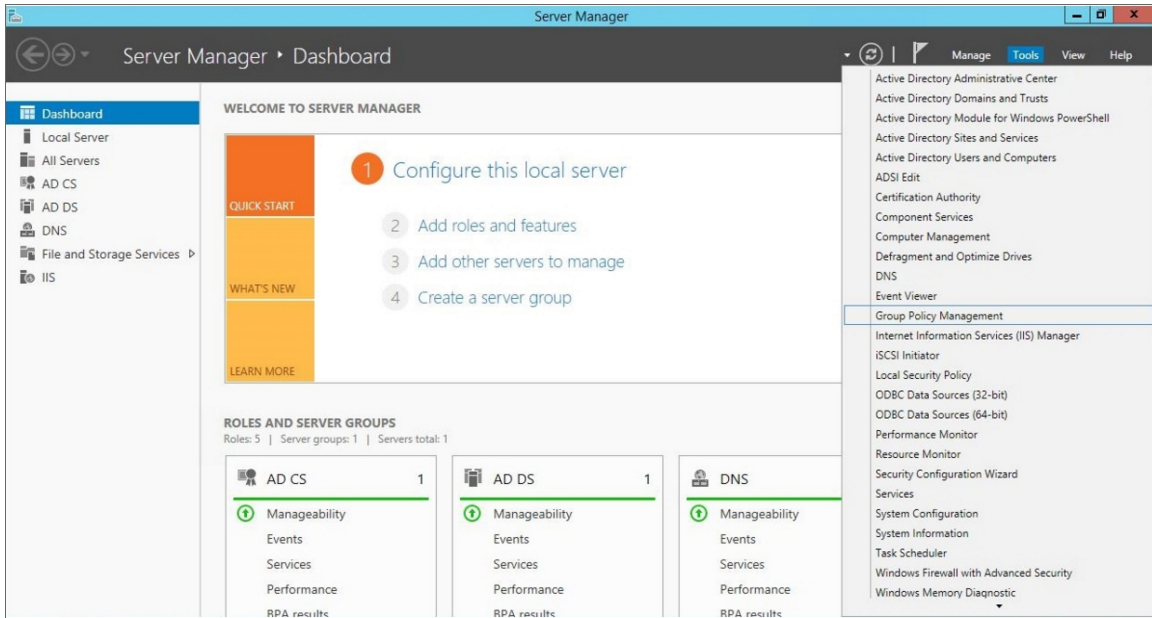
CertUtil: -ca.cert command completed successfully.

C:\Users\EM7Admin\Documents>
```

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

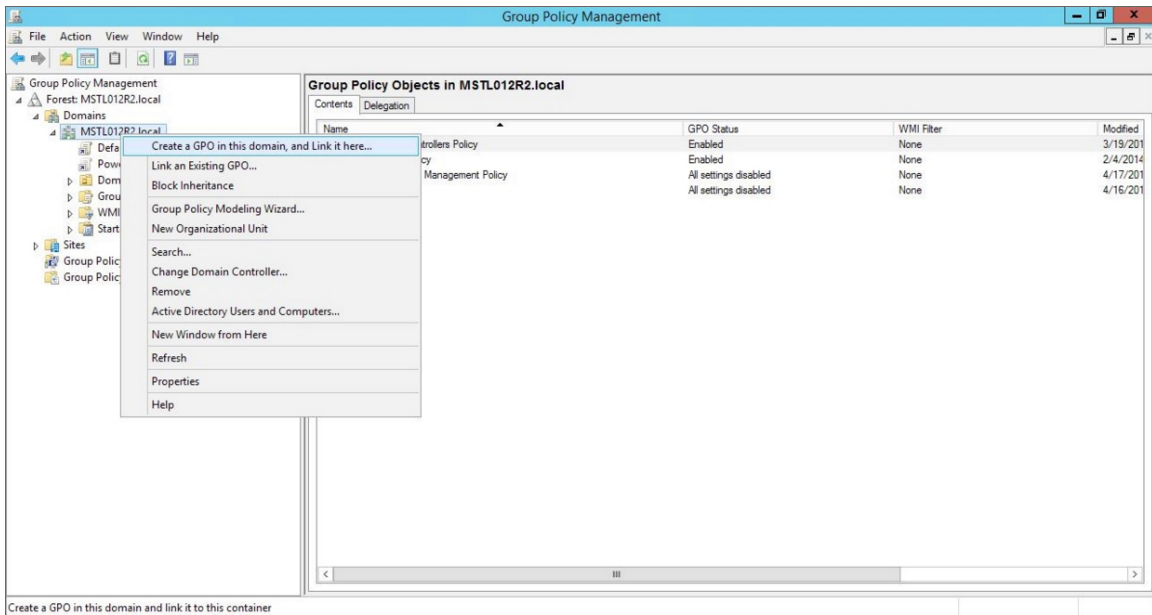
5. Exit the command prompt.
6. Log in to a domain controller in your Active Directory forest and navigate to the System Manager dashboard.

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

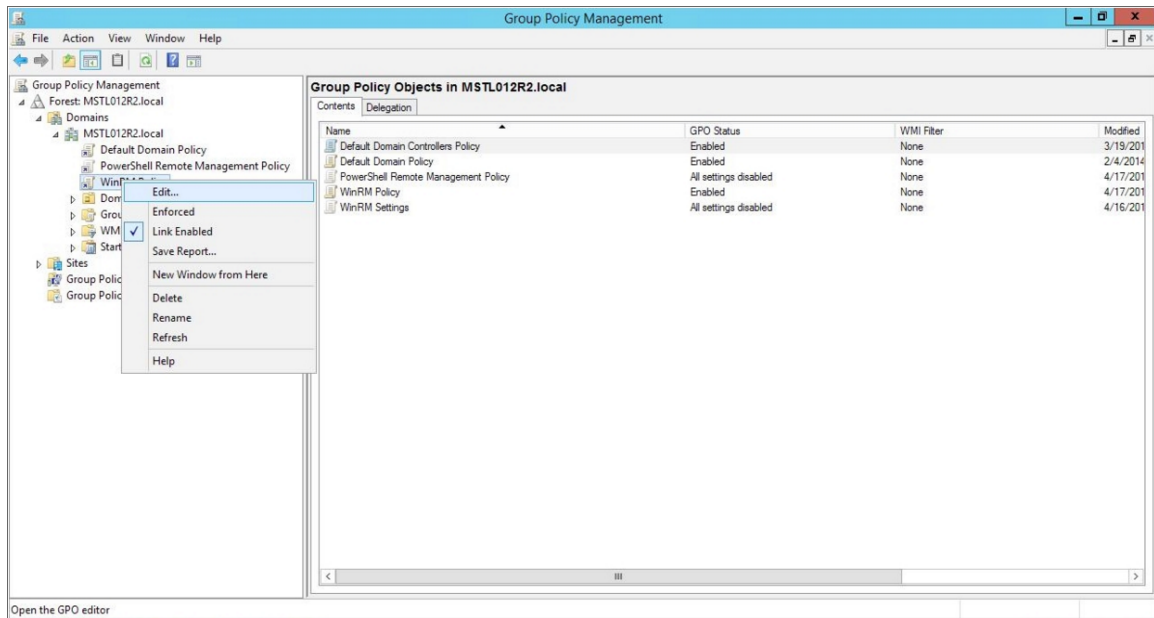


3

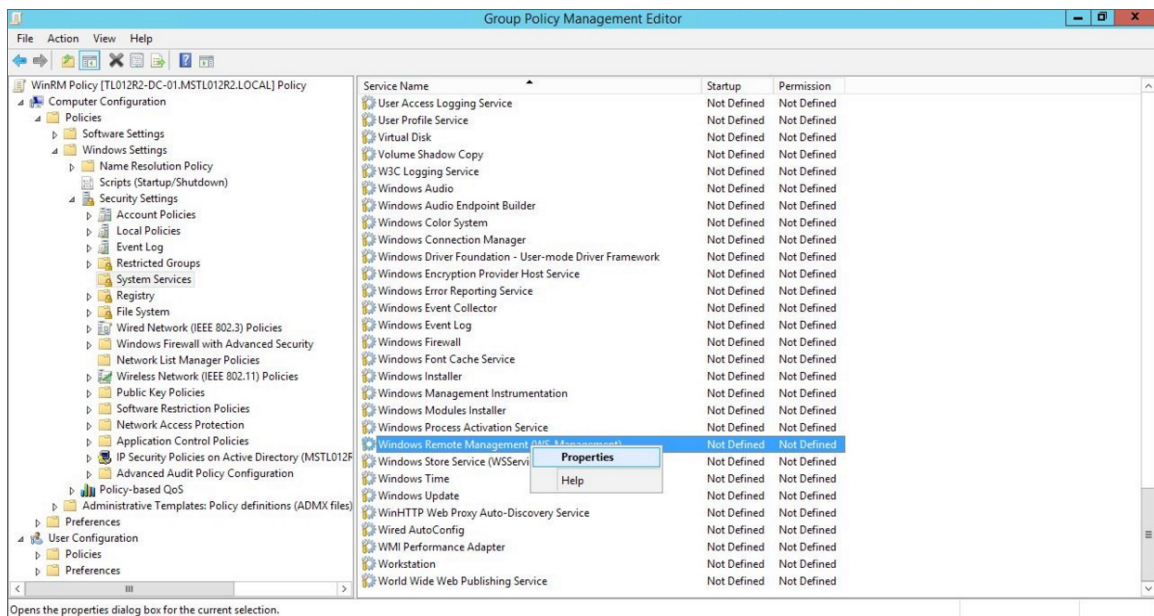
- On the **Group Policy Management** page, in the left panel, right-click the domain name where you want the new group policy to reside and then select *Create a GPO in this domain and Link it here*.



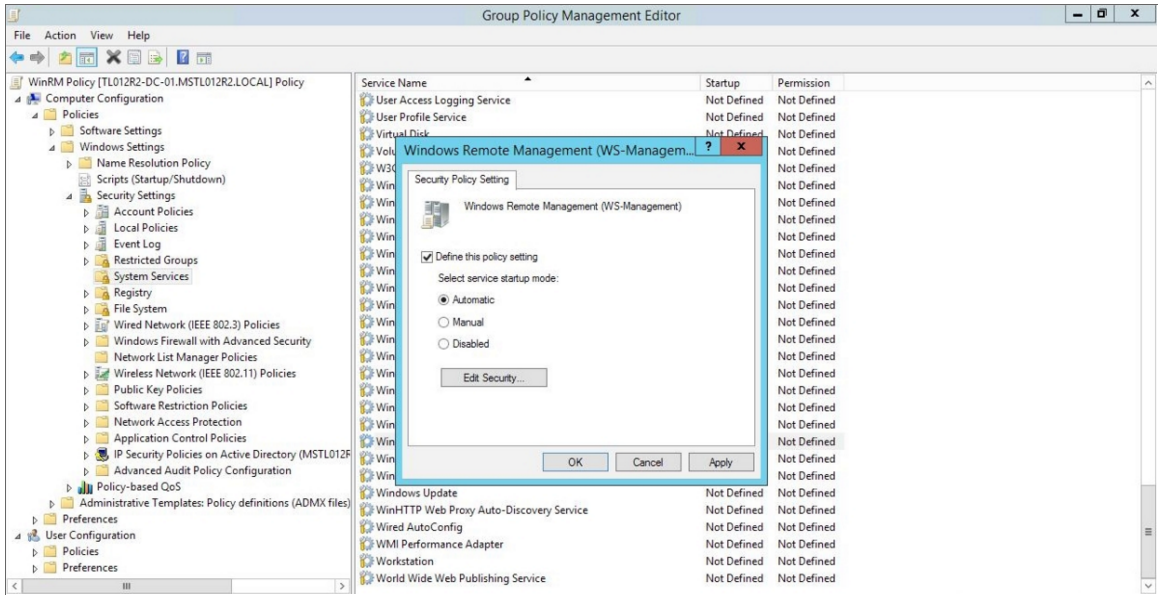
- In the left panel, right-click the new group policy and select *Edit*. The **Group Policy Management Editor** page for the new Windows Remote Management group policy appears.



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

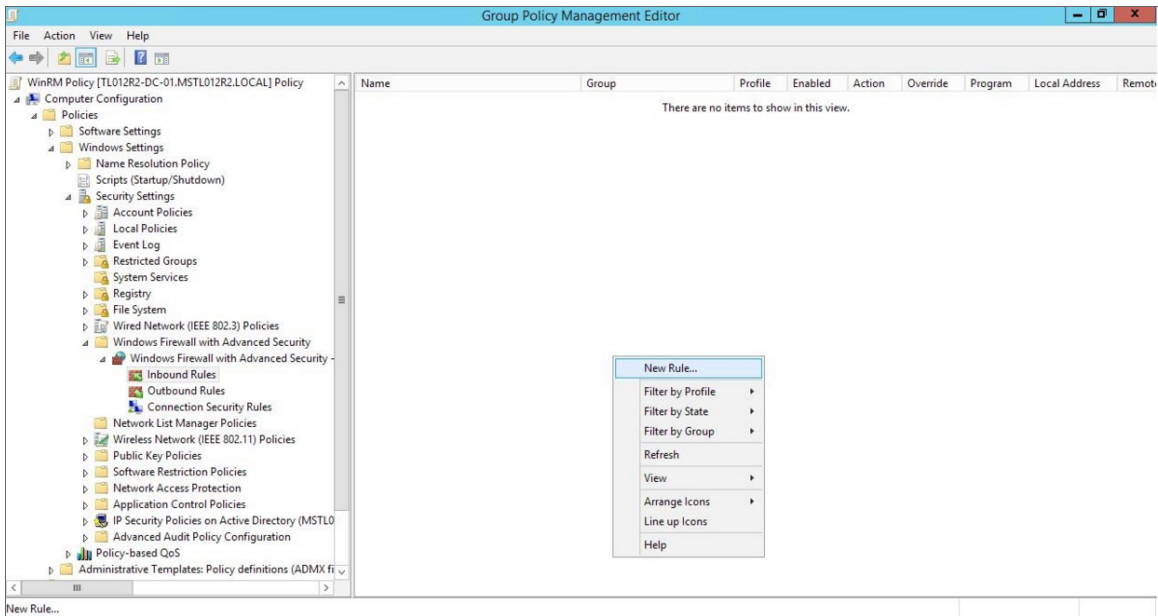


- The **Windows Remote Management (WS-Management)** modal page appears. Select the **Define this policy setting** check box and the **Automatic** radio button, then click **[OK]**.

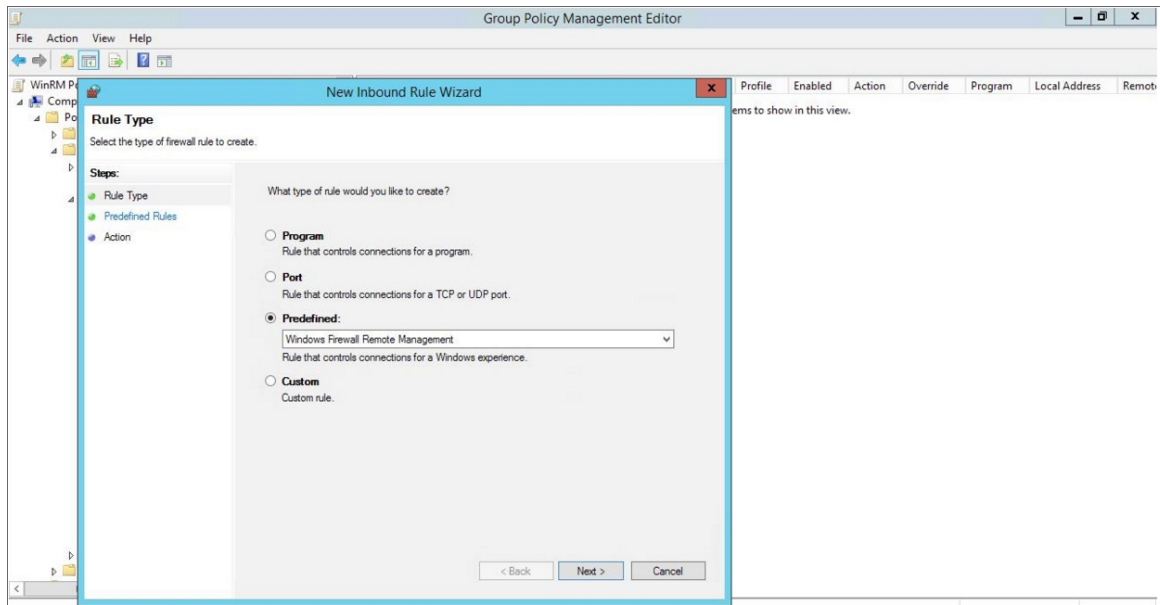


3

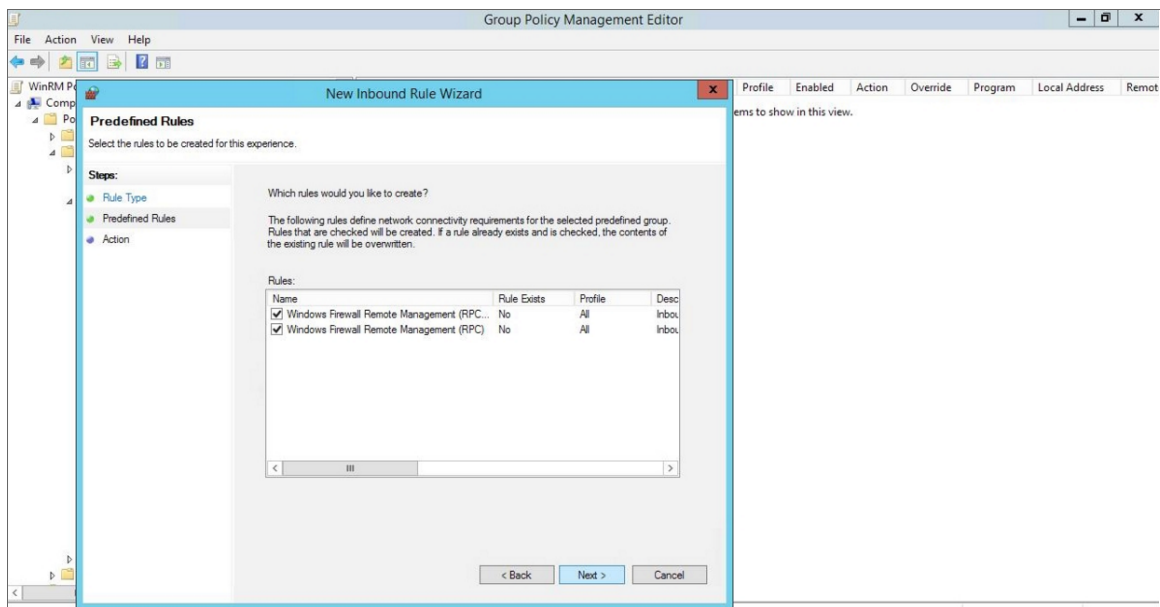
- In the left panel of the **Group Policy Management Editor** page, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security - LDAP > Inbound Rules**. In the right panel, right-click and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



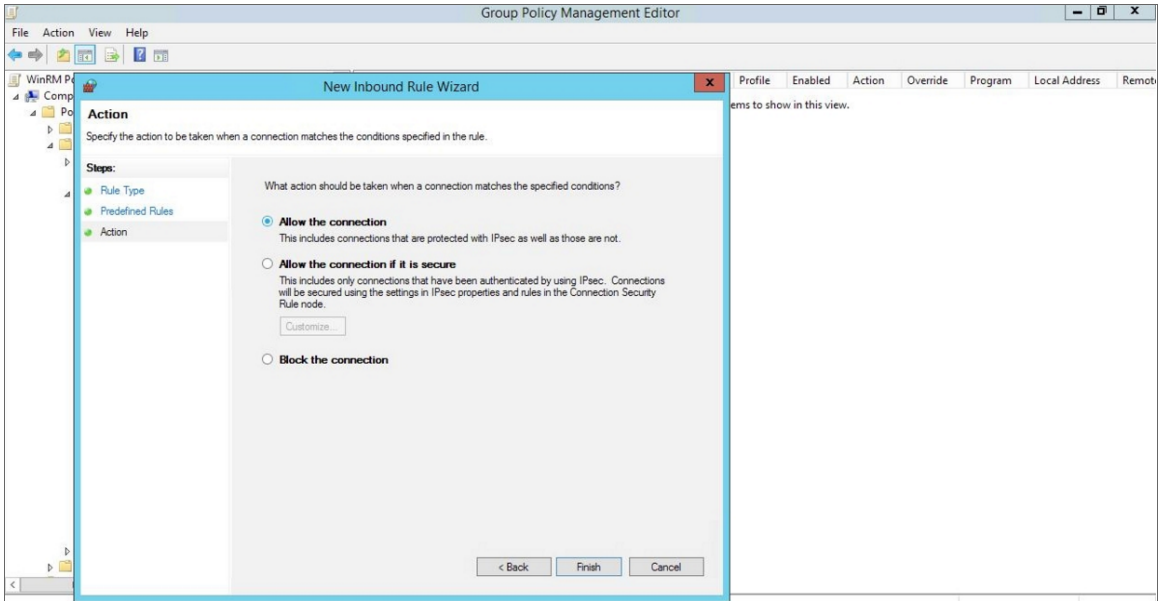
- The **New Inbound Rule Wizard** modal page appears. Click the **Predefined** radio button, select *Windows Firewall Remote Management* from the list, and then click **[Next]**.



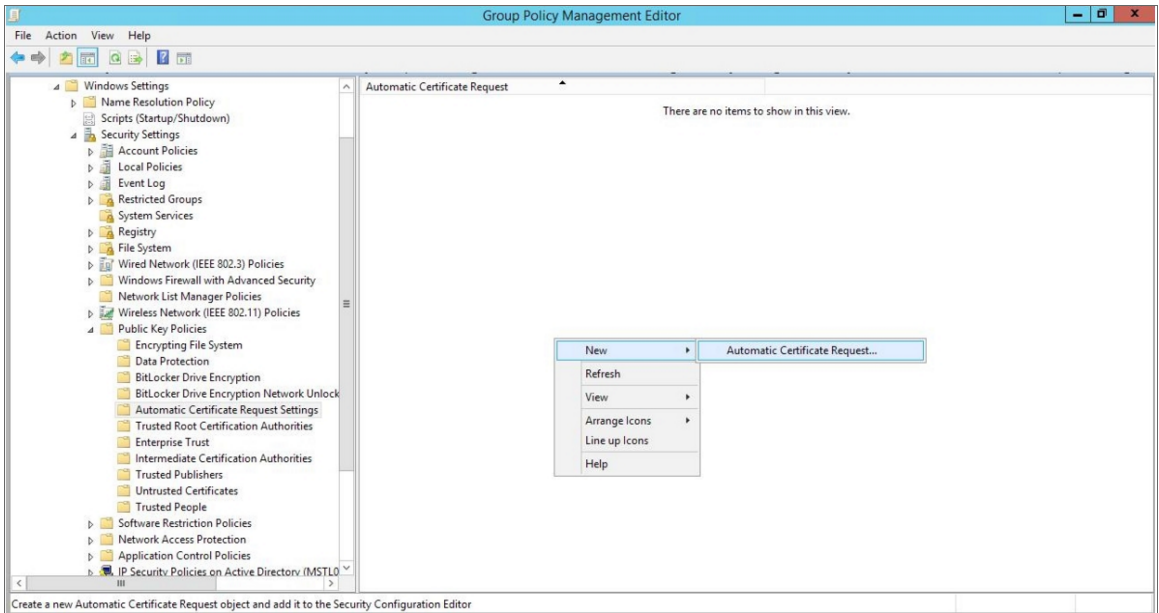
- Select the *Windows Firewall Remote Management (RPC)* and *Windows Firewall Remote Management (RPC-EPMAP)* check boxes, then click **[Next]**.



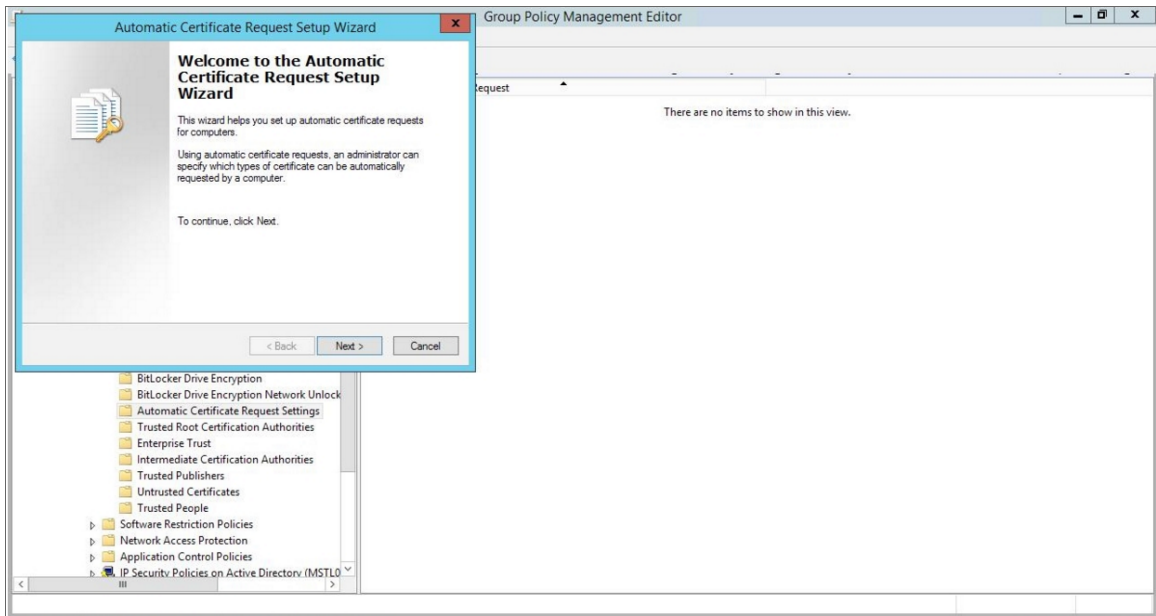
15. Select the *Allow the connection* radio button, then click **[Finish]**.



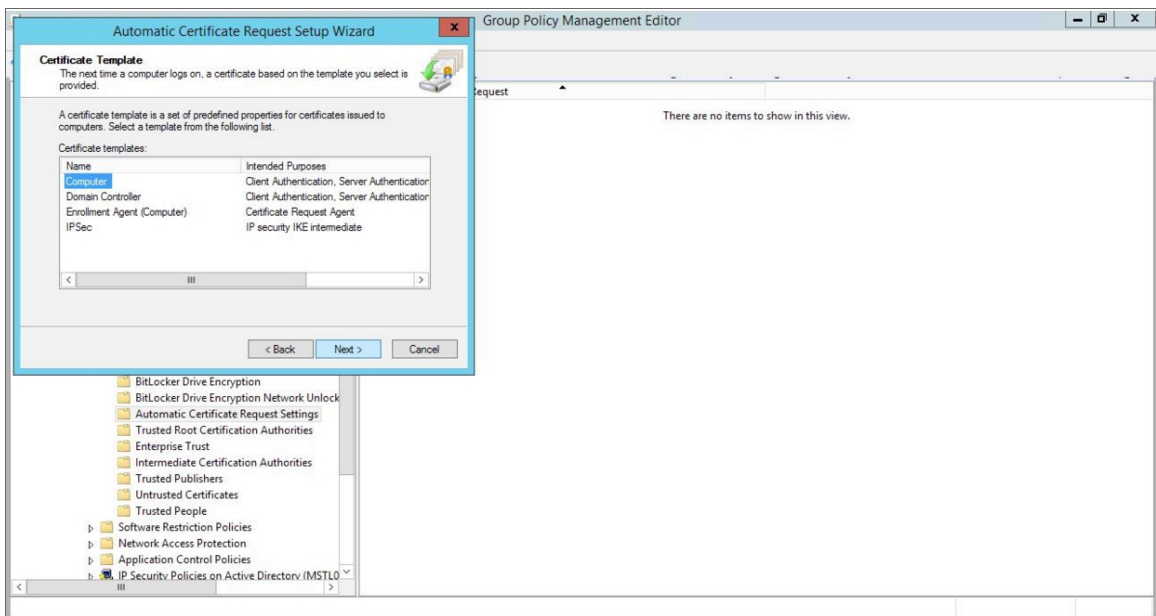
16. In the left panel of the **Group Policy Management Editor** page, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Automatic Certificate Request Settings**. In the right panel, right-click and select **New > Automatic Certificate Request**.



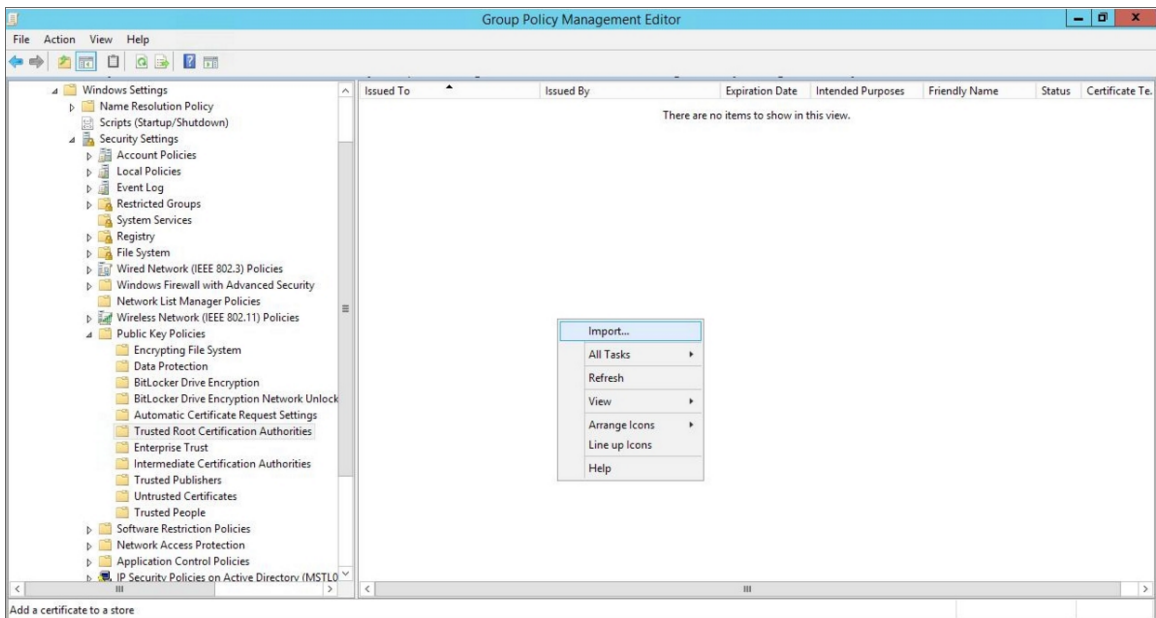
17. The **Automatic Certificate Request Setup Wizard** modal page appears. Click **[Next]**.



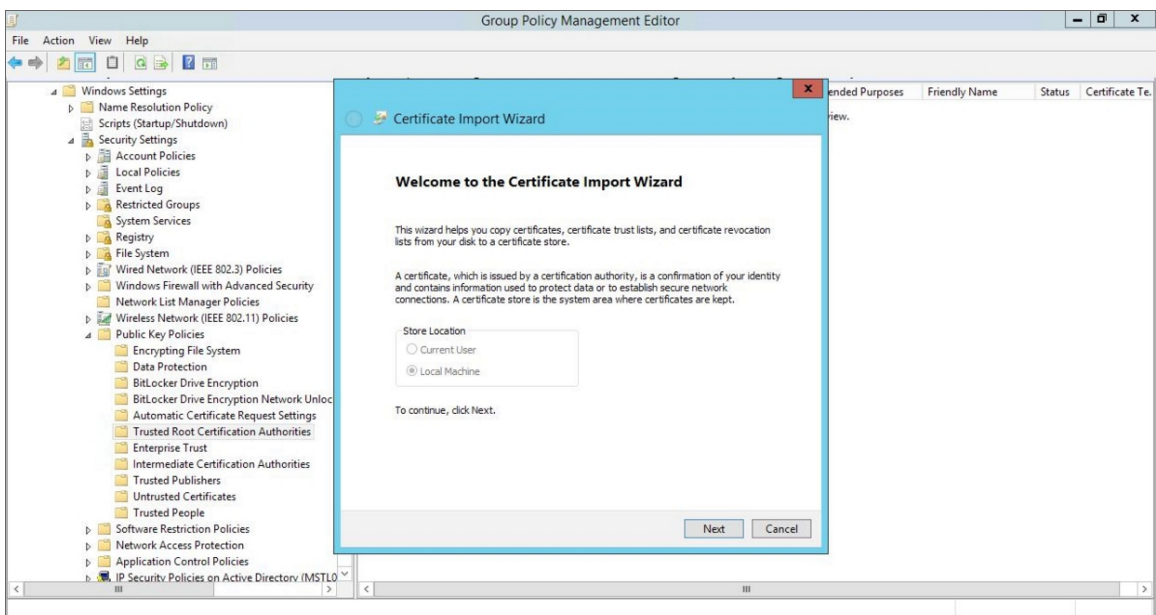
18. Select the *Computer* certificate template. Click **[Next]**, and then click **[Finish]**.



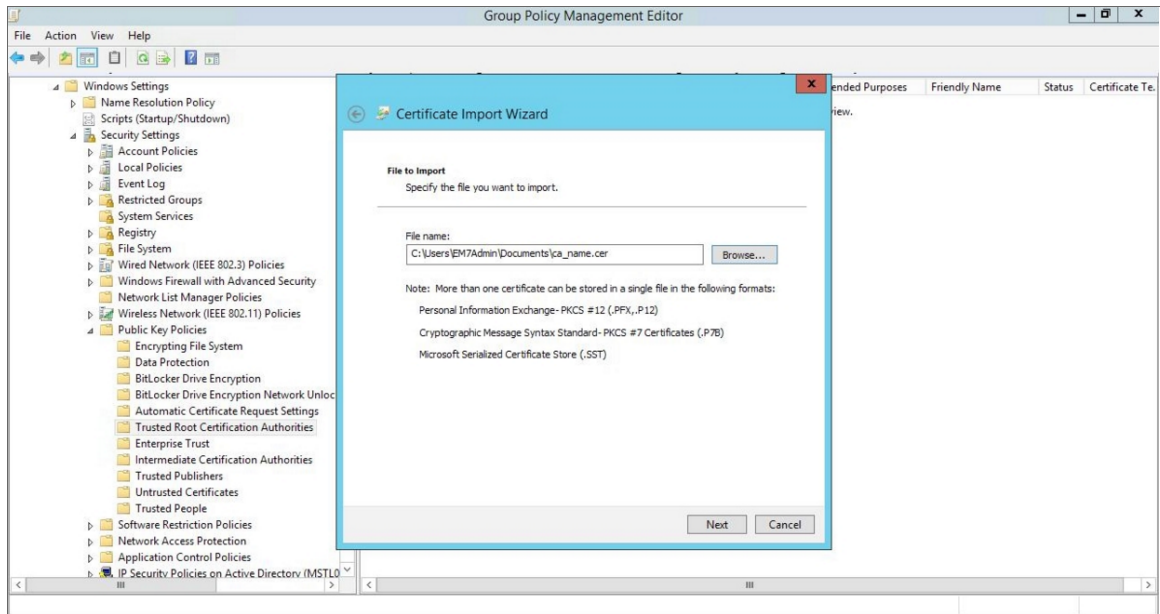
19. In the left panel of the **Group Policy Management Editor** page, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**. In the right panel, right-click and select **Import**.



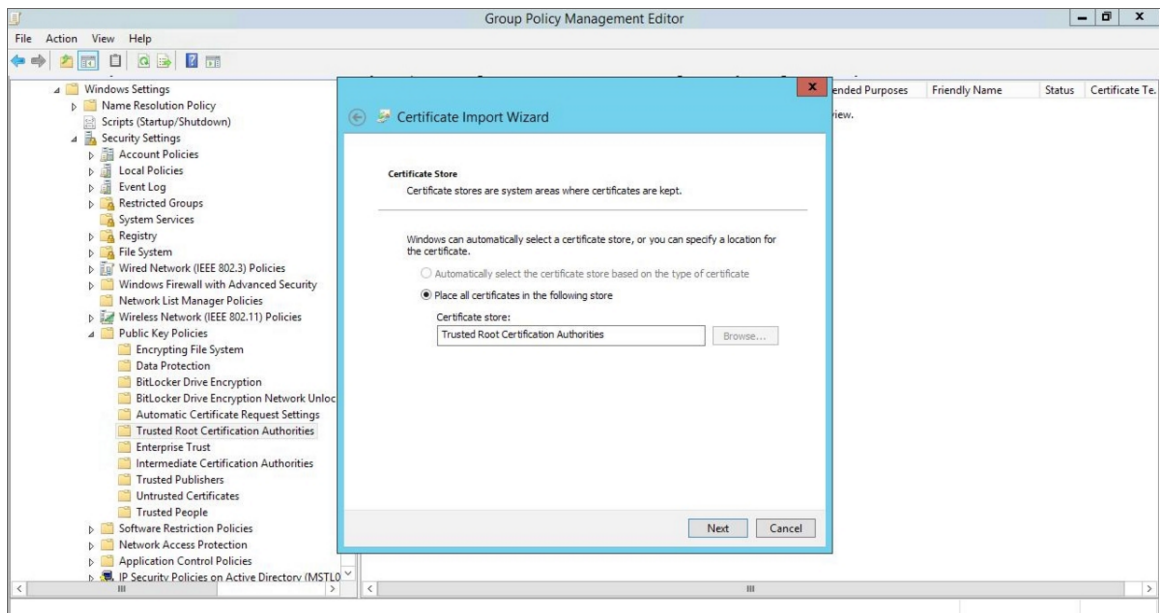
20. The **Certificate Import Wizard** modal page appears. Click **[Next]**.



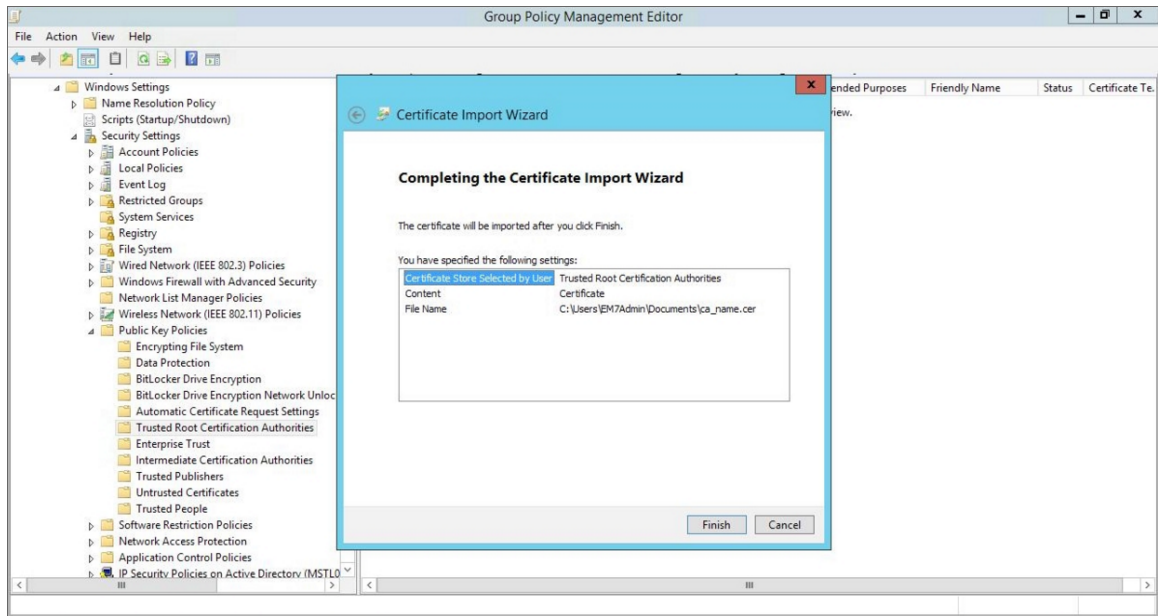
21. Browse to the Certification Authority certificate that you saved to your local directory in step 4, then click [Next].



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

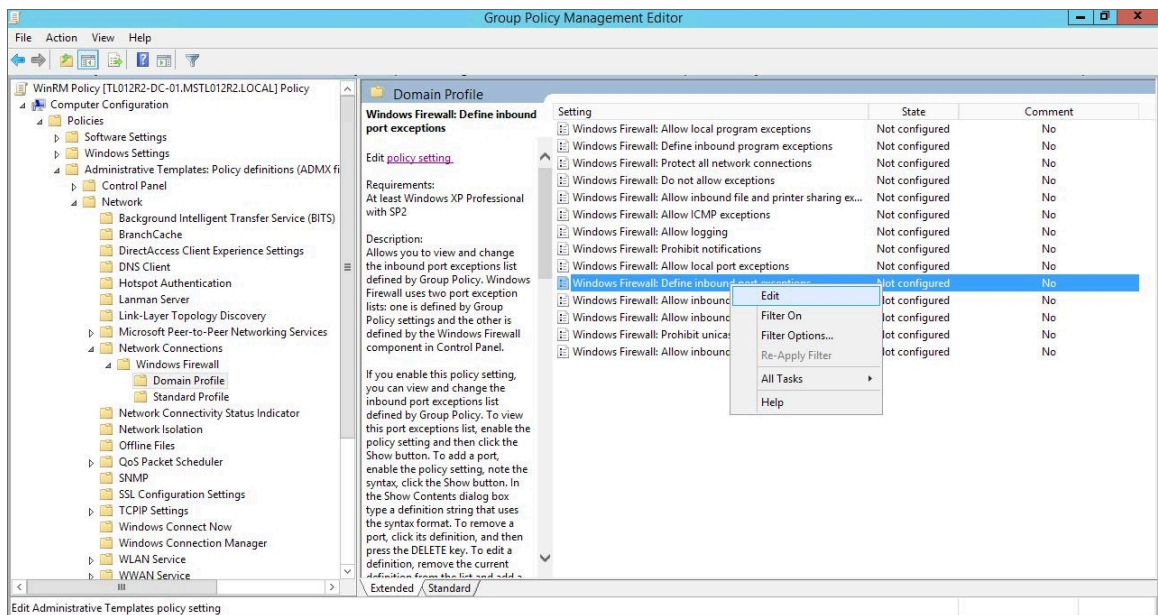


- Click **[OK]** to confirm that the certificate was successfully imported, and then click **[Finish]**.



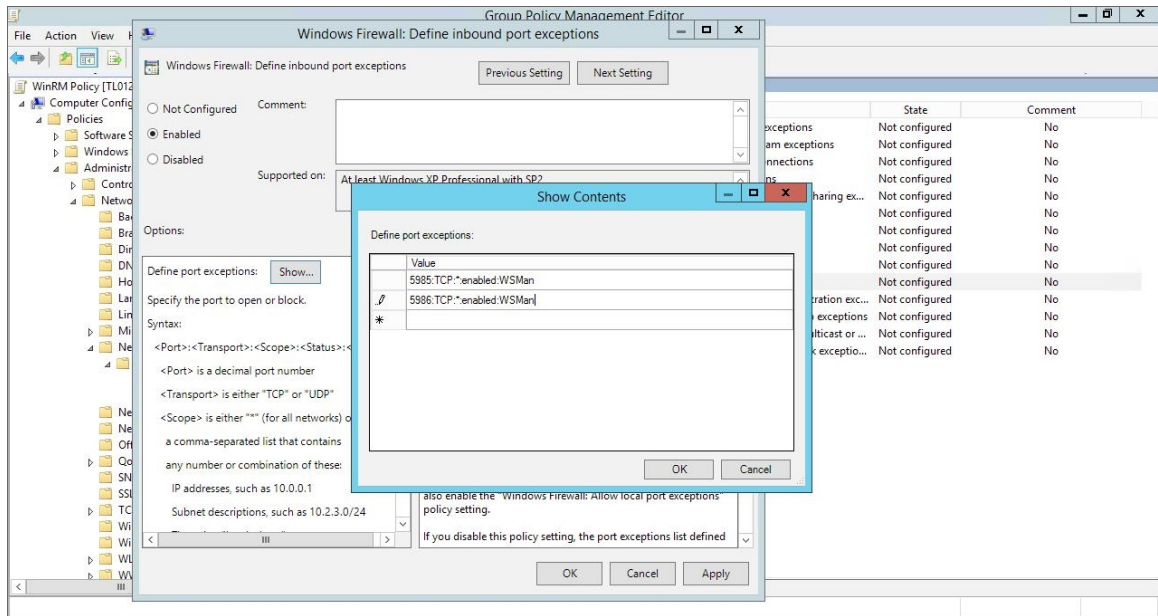
3

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



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

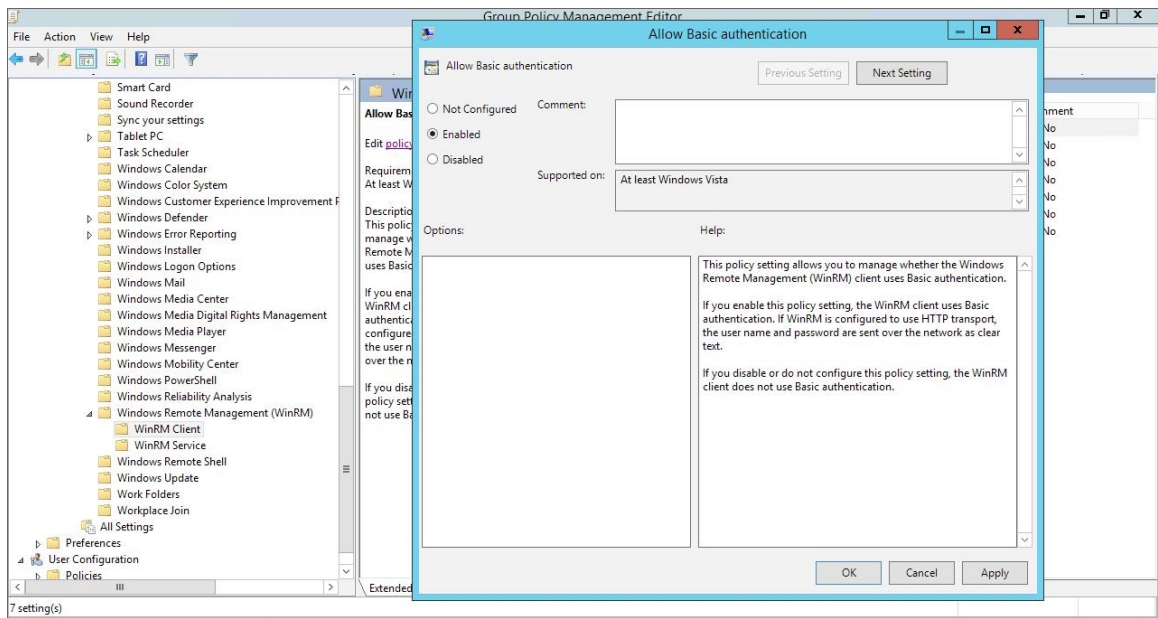
26. The **Show Contents** modal page appears. Enter the following values:



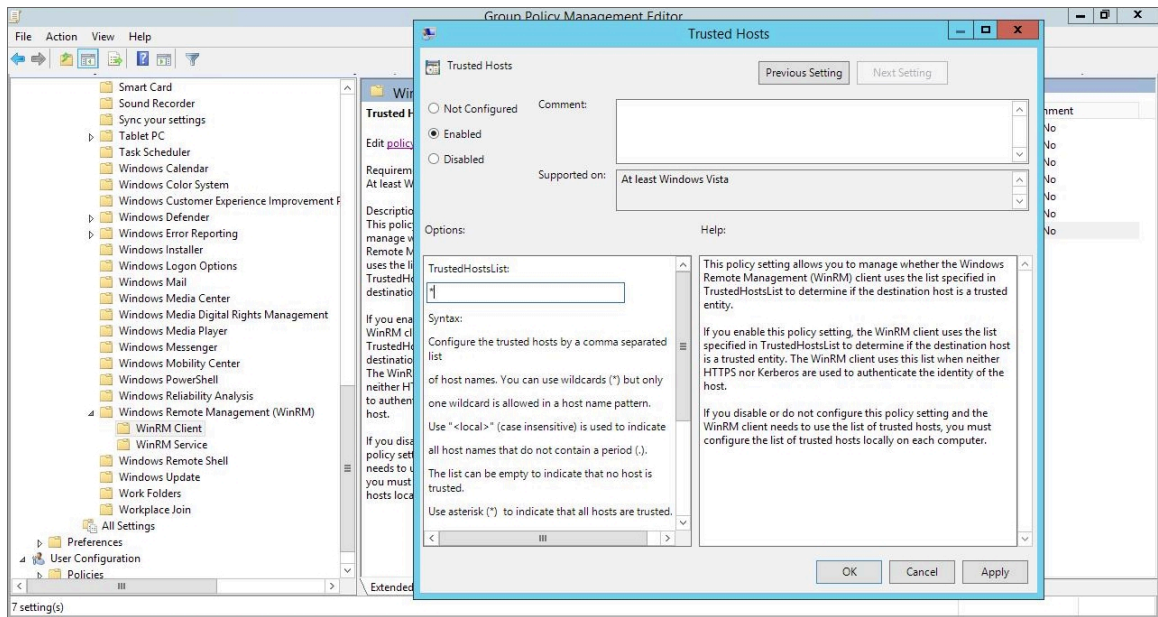
- 5985:TCP:*:enabled:WSMan
- 5986:TCP:*:enabled:WSMan

27. Click **[OK]**, then click **[OK]** again.

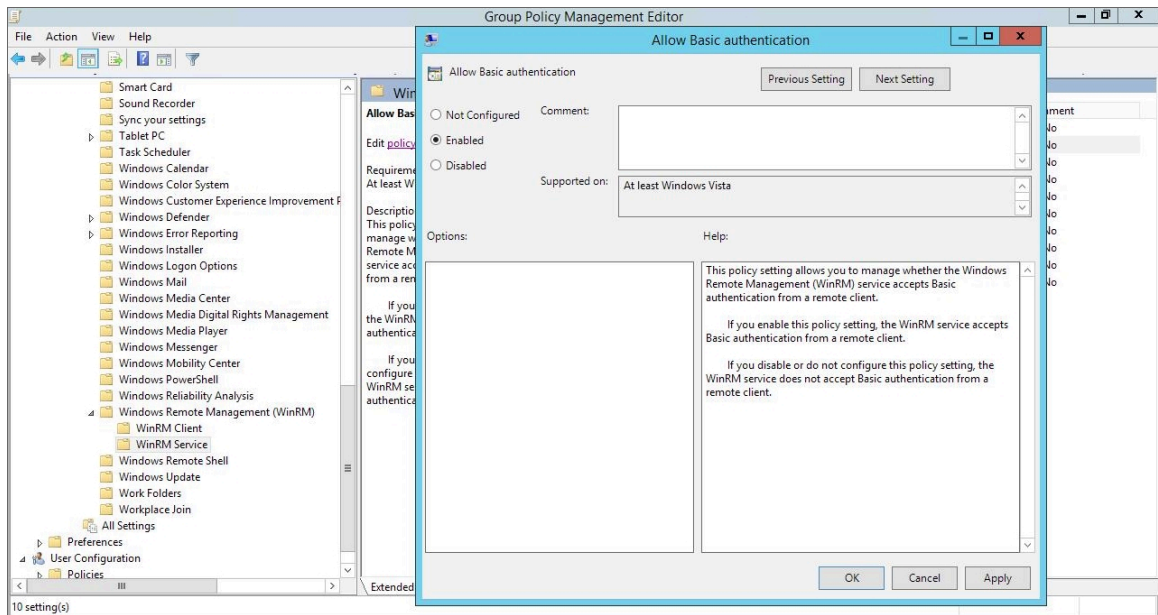
28. In the left panel of the **Group Policy Management Editor** page, navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client**. In the right panel, double-click the **Allow Basic authentication** setting.



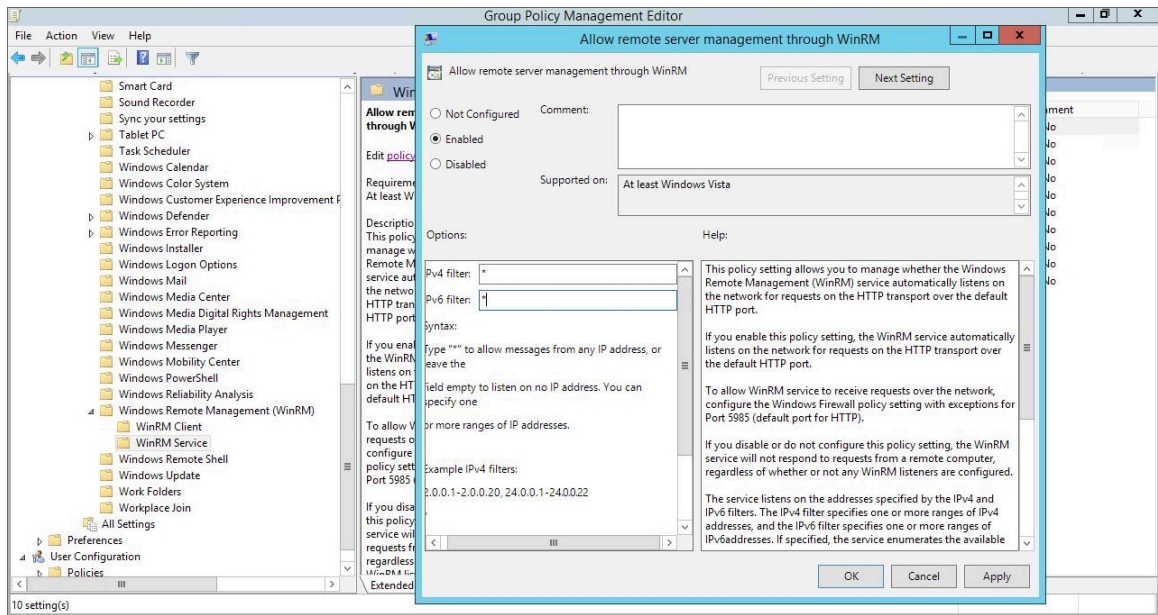
29. Select the **Enabled** radio button, then click [OK].
30. Repeat steps 28 and 29 for the **Allow unencrypted traffic** setting.
31. Double-click the **Trusted Hosts** setting. Select the **Enabled** radio button, enter an asterisk (*) in the **TrustedHostsList** field (under **Options**), and then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



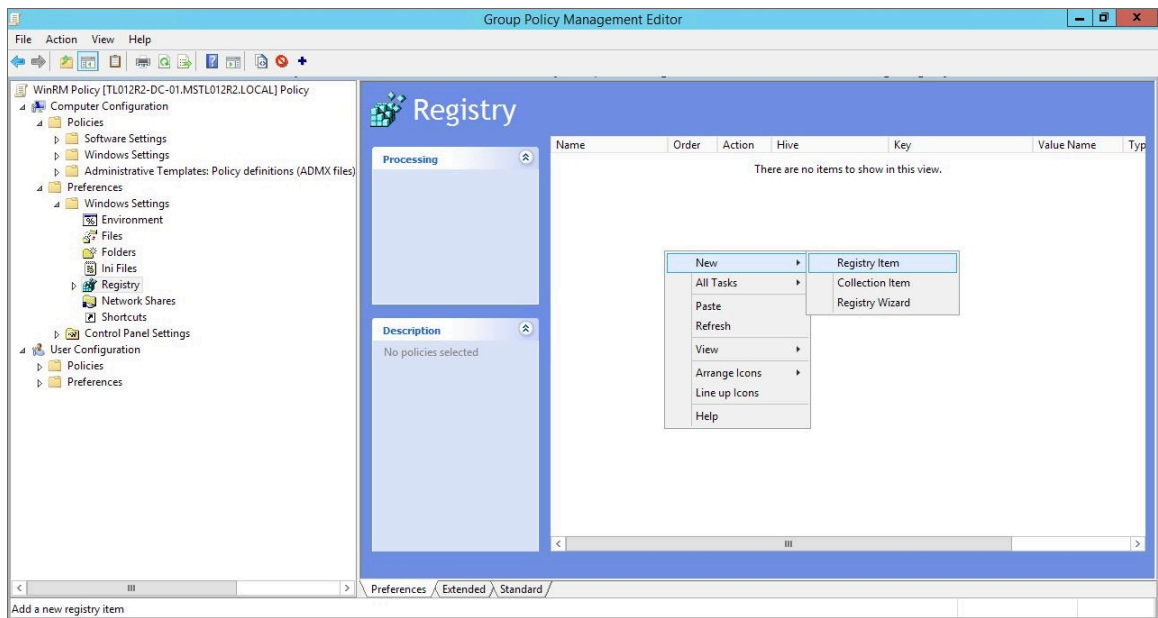
32. In the left panel of the **Group Policy Management Editor** page, navigate to **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service**. In the right panel, double-click the **Allow Basic authentication** setting.



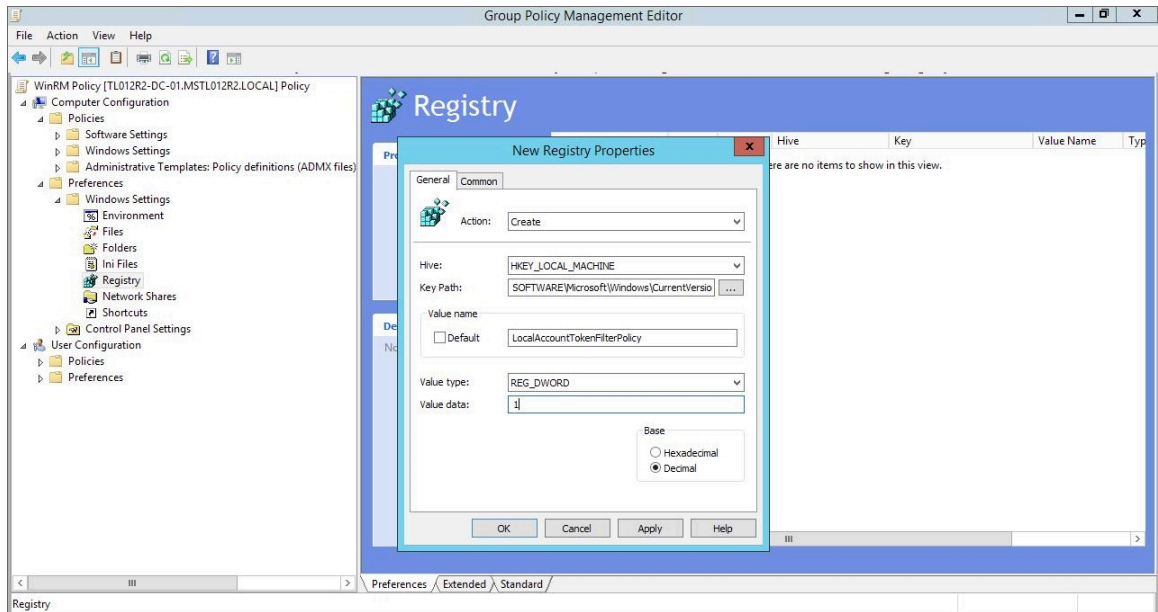
33. Select the **Enabled** radio button, then click [OK].
34. Repeat steps 32 and 33 for the **Allow unencrypted traffic** setting.
35. Double-click the **Allow remote server management through WinRM** setting. Select the **Enabled** radio button, enter an asterisk (*) in the **Pv4 filter** and **Pv6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



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



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



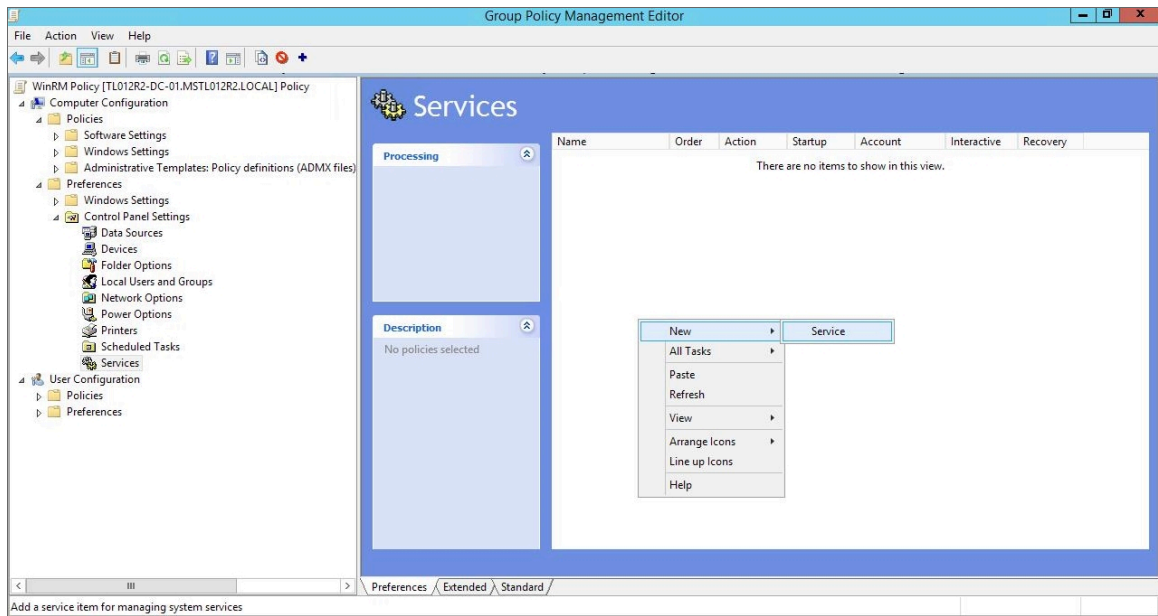
- **Action**. Select *Create*.
- **Hive**. Select *HKEY_LOCAL_MACHINE*.
- **Key Path**. Enter "SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system".
- **Value name**. Enter "LocalAccountTokenFilterPolicy".
- **Value type**. Enter "REG_DWORD".
- **Value data**. Enter "1".
- **Base**. Select *Decimal*.

38. Click the [OK] button.

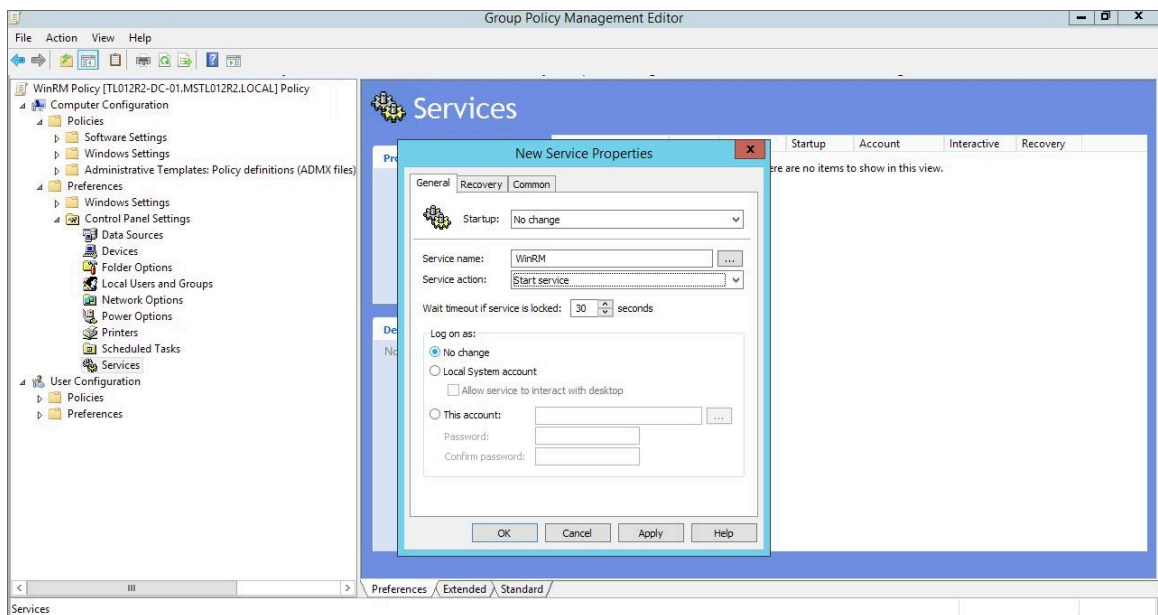
39. Repeat steps 36-38 to make an additional registry change to increase the maximum number of users who can access Windows Remote Management. In the **New Registry Properties** modal page, edit the following values:

- **Action**. Select *Create*.
- **Hive**. Select *HKEY_LOCAL_MACHINE*.
- **Key Path**. Enter "SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\".
- **Value name**. Enter "WinRS!MaxConcurrentUsers".
- **Value type**. Enter "REG_DWORD".
- **Value data**. Enter "0x64 (100)".
- **Base**. Select *Decimal*.

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



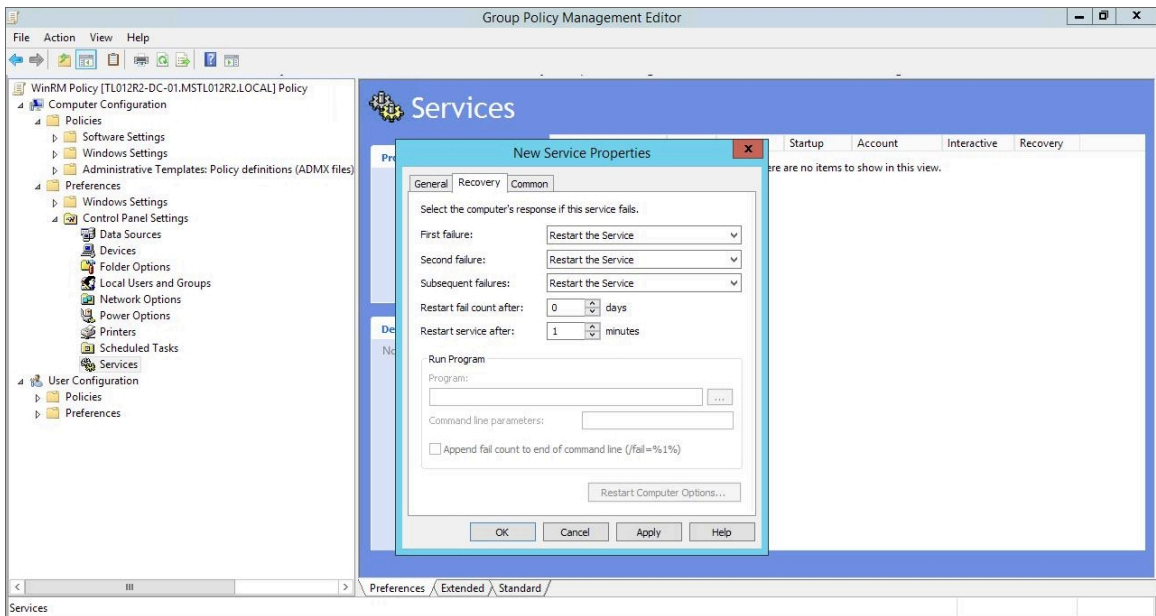
41. In the **New Service Properties** modal page, edit the values in one or more of the following fields:



- **Startup.** Select *No change*.

- **Service name.** Enter "WinRM".
- **Service action.** Select *Start service*.
- **Wait timeout if service is locked.** Select 30 seconds.
- **Log on as.** Select *No change*.

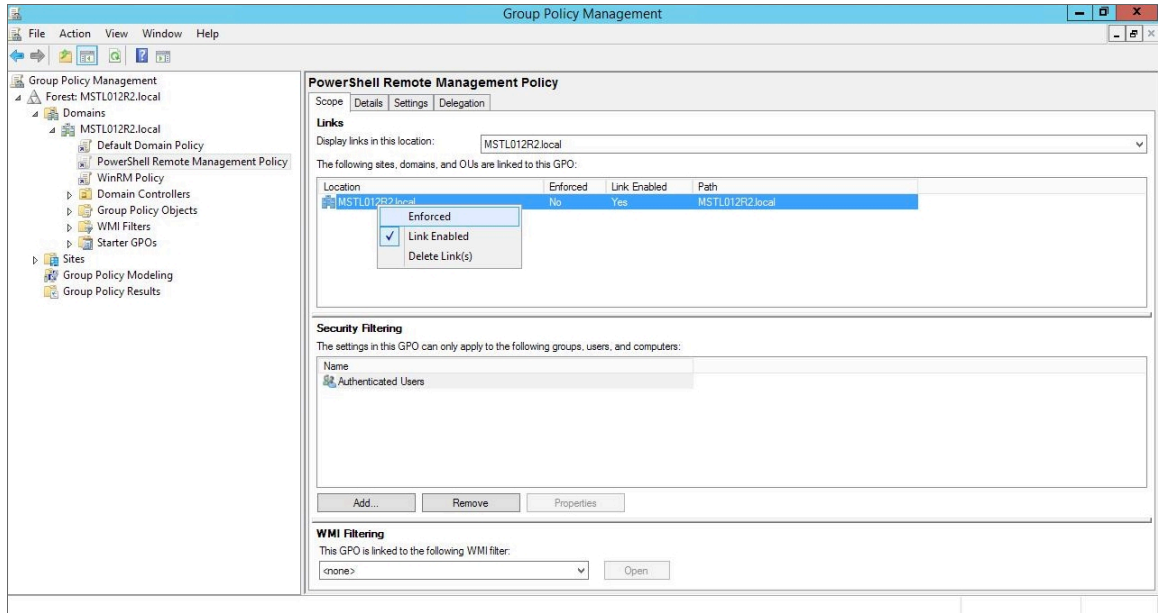
42. Click the **[Recovery]** tab, then edit the values in one or more of the following fields:



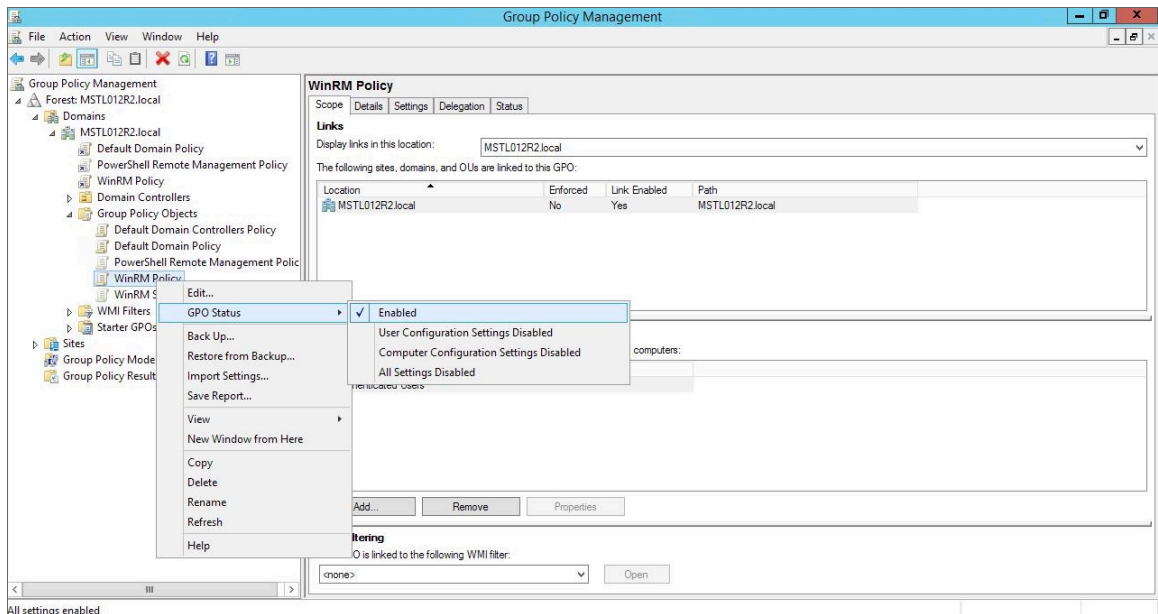
- **First failure.** Select *Restart the Service*.
- **Second failure.** Select *Restart the Service*.
- **Subsequent failures.** Select *Restart the Service*.
- **Restart fail count after.** Select 0 days.
- **Restart service after.** Select 1 minute.

43. Click the **[OK]** button.

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



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



Step 4: Configuring a Windows Management Proxy

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

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

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

1. Configure a user account that the platform will use to connect to the proxy server and the proxy server will use to connect to the target server. The user account can either be a local account or an Active Directory account; however, the user account must have the same credentials on the target and proxy servers and be in the Local Administrator's group on both servers.
2. If you have created a local user account on the Windows Server instead of an Active Directory account, you must configure encrypted communication between the platform and the Windows server. To do this, you must [configure a Server Authentication certificate](#).
3. [Configure Windows Remote Management](#) on the target server and the proxy server.
4. Log in to the proxy server as an administrator.
5. Open the PowerShell command window.
6. Right-click on the PowerShell icon in the taskbar and select *Run as Administrator*.
7. Execute one of the following commands on the proxy server to allow the proxy server to trust one or more target servers:
 - To allow the proxy server to trust all servers (not recommended), execute the following command:

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -value *
```
 - To allow the proxy server to trust only specific target servers, execute the following command, inserting a list that includes the IP address for each target server. Separate the list of IP addresses with commas.

```
Set-Item WSMAN:\localhost\Client\TrustedHosts -value <comma-delimited-list-of-target-server-IPs>
```
8. Execute the following command on the proxy server to configure the LocalAccountTokenFilterPolicy:

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

NOTE: If the proxy server is in a different Windows domain (domain A) than the target servers (domain B), and the proxy server uses a user account from Active Directory, and Active Directory is in the same Windows domain as the target servers (domain B), you must perform the following to allow the proxy server to send PowerShell commands to the target servers:

- On the domain controller for each domain (domain A and domain B), create new forward-lookup zones and reverse-lookup zones that allow name resolution to work between the two domains.
- On the domain controller for each domain (domain A and domain B), create a non-transitive realm trust between the two domains.
- Login to the proxy server and add the Active Directory account (from domain A) to the Local Administrator's group for the proxy server. You should be able to select the account on the proxy server after you create the non-transitive realm trust between the two domains.

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

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

To do so:

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

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

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

```
Restart-Service WinRM
```

4. Repeat these steps on each Windows server that will be monitored by the ScienceLogic platform.

SNMP and PowerShell Dynamic Applications for Windows Devices

Overview

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

<i>SNMP Dynamic Applications for Windows Devices</i>	70
<i>PowerShell Dynamic Applications</i>	70
<i>Microsoft: Active Directory Server</i>	70
<i>Microsoft: DHCP Server</i>	71
<i>Microsoft: DNS Server</i>	71
<i>Microsoft: Exchange Server</i>	72
<i>Microsoft: Exchange Server 2010</i>	72
<i>Microsoft: Hyper-V Server</i>	73
<i>Microsoft: IIS Server</i>	74
<i>Microsoft: Lync Server 2010</i>	74
<i>Microsoft: SharePoint Server</i>	75
<i>Microsoft: Skype for Business</i>	75
<i>Microsoft: SQL Server</i>	76
<i>Microsoft: Windows Server</i>	77
<i>Microsoft: Windows Server Services</i>	78
<i>Run Book Automations and Actions Associated with PowerShell Dynamic Applications for Windows Servers</i>	78
<i>Error Messages for PowerShell Collection</i>	79

SNMP Dynamic Applications for Windows Devices

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

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

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

PowerShell Dynamic Applications

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

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

The following PowerPacks include PowerShell Dynamic Applications for Microsoft Servers.

Microsoft: Active Directory Server

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

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

- Microsoft: Active Directory Address Book Performance
- Microsoft: Active Directory Async Thread Queue Performance
- Microsoft: Active Directory Database Performance
- Microsoft: Active Directory Directory Services Reads Performance
- Microsoft: Active Directory Directory Services Searches Performance
- Microsoft: Active Directory Directory Services Writes Performance
- Microsoft: Active Directory DRA Performance

- Microsoft: Active Directory LDAP Performance
- Microsoft: Active Directory Security Account Management Performance
- Microsoft: Active Directory Services General Performance
- Microsoft: Active Directory Web Service Performance

Microsoft: DHCP Server

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

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

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

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

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

Microsoft: DNS Server

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

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

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

- Microsoft: DNS WINS Performance
- Microsoft: DNS Zone Transfer Performance

Microsoft: Exchange Server

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

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

Microsoft: Exchange Server 2010

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

- Microsoft: Exchange 2010 CAS Address Book Load Performance
- Microsoft: Exchange 2010 CAS Address Book Service Performance
- Microsoft: Exchange 2010 CAS Availability Service Performance
- Microsoft: Exchange 2010 CAS OWA Performance
- Microsoft: Exchange 2010 CAS Performance
- Microsoft: Exchange 2010 CAS RPC Client Access Load Performance
- Microsoft: Exchange 2010 CAS RPC Client Access Performance
- Microsoft: Exchange 2010 MBS Client-Related Search Performance
- Microsoft: Exchange 2010 MBS Database Performance

- Microsoft: Exchange 2010 MBS Info Store RPC Processing Stats
- Microsoft: Exchange 2010 MBS Information Store Performance
- Microsoft: Exchange 2010 MBS Message Queuing Performance
- Microsoft: Exchange 2010 MBS Replay Log I/O Latency Requirements
- Microsoft: Exchange 2010 MBS RPC Client Throttling Performance
- Microsoft: Exchange 2010 MBS Store Client Request Performance
- Microsoft: Exchange 2010 TPS Disk Performance
- Microsoft: Exchange 2010 TPS Transport Database Performance
- Microsoft: Exchange 2010 TPS Transport Load Assessment Stats
- Microsoft: Exchange 2010 TPS Transport Queue Length Performance
- Microsoft: Exchange 2010 UMS General Performance

Microsoft: Hyper-V Server

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

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

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

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

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

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

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

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

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

Microsoft: IIS Server

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

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

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

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

- Microsoft: IIS Server Configuration

Microsoft: Lync Server 2010

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

- Microsoft: Lync 2010 Announcement Service Performance
- Microsoft: Lync 2010 AS MCU Performance
- Microsoft: Lync 2010 Auto Attendant Performance
- Microsoft: Lync 2010 AV MCU Performance
- Microsoft: Lync 2010 AV SIP/MRAS/QOE Performance
- Microsoft: Lync 2010 Call Park Service Performance
- Microsoft: Lync 2010 Conferencing Compatibility Performance
- Microsoft: Lync 2010 Data Conferencing Performance
- Microsoft: Lync 2010 IM MCU Performance
- Microsoft: Lync 2010 Response Group Performance
- Microsoft: Lync 2010 SIP Load Management Performance
- Microsoft: Lync 2010 SIP Networking Performance

- Microsoft: Lync 2010 SIP Peers Performance
- Microsoft: Lync 2010 SIP Protocol Performance
- Microsoft: Lync 2010 SIP Response Performance
- Microsoft: Lync 2010 SipEps Incoming Message Performance
- Microsoft: Lync 2010 User Services Performance
- Microsoft: Lync 2010 Web Services Performance

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

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

Microsoft: SharePoint Server

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

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

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

Microsoft: Skype for Business

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

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

- Microsoft: Lync 2013 AS MCU Performance
- Microsoft: Lync 2013 AV MCU Performance
- Microsoft: Lync 2013 AV SIP/MRAS/QOE Performance
- Microsoft: Lync 2013 Bandwidth Services Performance
- Microsoft: Lync 2013 Call Park Service Performance
- Microsoft: Lync 2013 Data Conferencing Performance

- Microsoft: Lync 2013 IM MCU Performance
- Microsoft: Lync 2013 Mediation Server Performance
- Microsoft: Lync 2013 Response Group Performance
- Microsoft: Lync 2013 SIP Load Management Performance
- Microsoft: Lync 2013 SIP Networking Performance
- Microsoft: Lync 2013 SIP Peers Performance
- Microsoft: Lync 2013 SIP Protocol Performance
- Microsoft: Lync 2013 SIP Response Performance
- Microsoft: Lync 2013 SipEps Incoming Message Performance
- Microsoft: Lync 2013 User Services Performance
- Microsoft: Lync 2013 Web Services Performance

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

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

Microsoft: SQL Server

NOTE: The Dynamic Applications in this PowerPack support SQL Server 2008, 2012, 2014, and 2016.

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

- Microsoft: SQL 2008 Buffer Pages Performance
- Microsoft: SQL Buffer Performance
- Microsoft: SQL Database Performance
- Microsoft: SQL Memory Performance
- Microsoft: SQL Plan Cache Performance
- Microsoft: SQL Query Performance
- Microsoft: SQL Session Performance
- Microsoft: SQL Table Lock/Latch Performance

Microsoft: Windows Server

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2008 R2, 2012, 2012 R2, and 2016, as well as Windows 10.

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

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

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

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

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

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

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

The following Snippet Dynamic Application, which uses PowerShell requests to collect data, can be used to collect journal data from Windows servers:

- Microsoft: Windows Server Process List

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

- Microsoft: Windows Server IC Availability
- Microsoft: Windows Server IC Detail
- Microsoft: Windows Server IC Filesystem Inventory
- Microsoft: Windows Server IC Filesystem Performance
- Microsoft: Windows Server IC Interface Inventory
- Microsoft: Windows Server IC Interface Performance

Microsoft: Windows Server Services

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

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

- Microsoft: Windows Server Service Configuration

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

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

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

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

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

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

Error Messages for PowerShell Collection

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

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

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

Creating SNMP and PowerShell Credentials for Windows Devices

Overview

The following sections describe how to create SNMP and PowerShell credentials for Windows devices that you want to monitor with the ScienceLogic platform, as well as how to discover component devices on Hyper-V systems:

<i>Creating an SNMP Credential</i>	81
<i>Creating a PowerShell Credential</i>	84
<i>Testing Windows Credentials</i>	86
<i>SNMP Credential Test</i>	87
<i>PowerShell Credential Test</i>	87
<i>Running a Windows Credential Test</i>	87
<i>Discovering Component Devices on Hyper-V Systems</i>	88
<i>Viewing Component Devices</i>	89

Creating an SNMP Credential

SNMP Credentials (called "community strings" in earlier versions of SNMP) allow the ScienceLogic platform to access SNMP data on a managed device. The platform 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).

Profile Name	Organization	RO Use	RW Use	DS Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions
1. Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	AWS Account Access	example.com	80	2000	1	2015-05-16	Create SNMP Credential
2. Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential
3. Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<SUBSCRIPTION_ID_H> %D	--	22	180000	59	2015-05-14	Create SOAP/XML Host Credential
4. Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14	Create LDAP/AD Credential
5. Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	{USER_GOES_HERE}	--	161	1500	2	2015-05-14	Create Basic/Snippet Credential
6. Cisco ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	Create PowerShell Credential
7. Cisco ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	
8. Cloudkick - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES}	127.0.0.1	443	5000	9	2015-05-14 11:25:31	
9. GUCM Perfmon/Service 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	%D	8443	2000	4	2015-05-14 11:25:12	
10. EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:28:41	
11. EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43	
12. EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:28:32	
13. EM7 DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:28:32	
14. EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:28:32	
15. EM7 DB - Ssl.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:28:32	
16. EM7 Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42	
17. EM7 Default V3	[all orgs]	--	--	--	SNMP	em7defaultv3	--	161	500	11	2015-05-14 11:25:42	
18. EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	
19. GoGrid - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES}	127.0.0.1	443	5000	16	2015-05-14 11:25:51	
20. IP-SLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14	
21. LifeSize - Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	18	2015-05-14 11:25:58	
22. LifeSize - Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	
23. Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	192.0.0.189	80	5000	22	2015-05-14 11:28:11	
24. NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:28:20	
25. NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:28:20	
26. NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:28:20	
27. Nexus netconf	[all orgs]	--	--	--	Basic/Snippet	--	%D	22	10000	6	2015-05-14 11:25:16	
28. Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16	
29. Polycom - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:28:24	
30. Polycom - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:28:24	
31. Polycom - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:28:24	

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

Credential Editor X

Create New SNMP Credential Reset

Basic Settings

Profile Name: SNMP Version: [SNMP V2]

Port: Timeout(ms): Retries:

SNMP V1/V2 Settings

SNMP Community (Read-Only): SNMP Community (Read/Write):

SNMP V3 Settings

Security Name: Security Passphrase:

Authentication Protocol: [MD5] Security Level: [Authentication Only] SNMP v3 Engine ID:

Context Name: Privacy Protocol: [DES] 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 the platform 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 the platform will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
- **Retries.** Number of times the platform 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 the ScienceLogic platform.

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

Creating a PowerShell Credential

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

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

To define a PowerShell credential in the ScienceLogic platform:

1. Collect the information you need to create the credential:
 - The username and password for a user on the Windows device.
 - If the user is an Active Directory account, the hostname or IP address of the Active Directory server and the domain.
 - Whether an encrypted connection should be used.
 - If you are using a Windows Management Proxy, the hostname or IP address of the proxy server.
2. Go to the **Credential Management** page (System > Manage > Credentials).

- In the **Credential Management** page, click the **[Actions]** menu. Select **Create PowerShell Credential**.

Profile Name	Organization	RO Use	RW Use	DA Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions
1. Amazon Web Services Credential	SOAP/XML Host	[AWS Account Access]	example.com	80	2000	1	2015-05-14	Create SNMP Credential
2. Azure Credential - SOAP/XML	[All Orgs]	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential
3. Azure Credential - SSHKey	[All Orgs]	SSHKey	<SUBSCRIPTION_ID_H	%D	22	180000	50	2015-05-14	Create SOAP/XML Host Credential
4. Cisco SNMPv2 - Example	[All Orgs]	SNMP	---	---	161	1500	3	2015-05-14	Create Basic/Snippet Credential
5. Cisco SNMPv3 - Example	[All Orgs]	SNMP	[USER_GOES_HERE]	---	161	1500	2	2015-05-14	Create SSH/Key Credential
6. Cisco ACI	[All Orgs]	Basic/Snippet	admin	173.36.210.46	443	0	62	2015-05-14 15:25:24	Create PowerShell Credential
7. Cisco ACI Credential	[All Orgs]	Basic/Snippet	admin	198.18.133.200	443	0	81	2015-05-14 14:32:20	...
8. Cloudkick - Example	[All Orgs]	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	9	2015-05-14 11:25:31	...
9. CUCM PerformanceService 8.0 Example	[All Orgs]	SOAP/XML Host	---	---	8443	2000	4	2015-05-14 11:26:12	...
10. EM7 Central Database	[All Orgs]	Database	root	localhost	7706	0	51	2015-05-14 11:26:41	...
11. EM7 Collector Database	[All Orgs]	Database	root	%D	7707	0	14	2015-05-14 11:25:43	...
12. EM7 DB	[All Orgs]	Database	root	%D	7706	0	35	2015-05-14 11:26:32	...
13. EM7 DB - DR Info	[All Orgs]	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:26:32	...
14. EM7 DB - My conf	[All Orgs]	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:26:32	...
15. EM7 DB - Slic conf	[All Orgs]	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:26:32	...
16. EM7 Default V2	[All Orgs]	SNMP	---	---	161	1500	10	2015-05-14 11:25:42	...
17. EM7 Default V3	[All Orgs]	SNMP	em7default3	%D	161	500	11	2015-05-14 11:25:42	...
18. EMC - Example	[All Orgs]	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	...
19. GIGrid - Example	[All Orgs]	Basic/Snippet	[SECURITY KEY GOES]	127.0.0.1	443	5000	16	2015-05-14 11:25:51	...
20. IPSLA Example	[All Orgs]	SNMP	---	---	161	1500	5	2015-05-14 11:25:14	...
21. iReSite - Endpoint SNMP	[All Orgs]	SNMP	control	%D	161	3000	18	2015-05-14 11:25:58	...
22. iReSite - Endpoint SNMPCLI	[All Orgs]	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	...
23. Local API	[All Orgs]	Basic/Snippet	em7admin	10.0.0.180	80	5000	22	2015-05-14 11:26:11	...
24. NetApp 7-mode	[All Orgs]	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:26:20	...
25. NetApp w/SSL Option	[All Orgs]	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:26:20	...
26. NetApp w/SSL Option Off	[All Orgs]	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:26:20	...
27. Nexus redconf	[All Orgs]	Basic/Snippet	---	%D	22	100000	8	2015-05-14 11:25:16	...
28. Nexus snmp	[All Orgs]	SNMP	---	---	161	10000	7	2015-05-14 11:25:16	...
29. Polycom - Advanced	[All Orgs]	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:26:24	...
30. Polycom - CDR	[All Orgs]	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:26:24	...
31. Polycom - Interface	[All Orgs]	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:26:24	...

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

Credential Editor

Create New PowerShell Credential Reset

Basic Settings

Profile Name: Account Type: [Active Directory]

Hostname/IP: Timeout(ms): 10000

Username: Password:

Encrypted: [yes] Port: 5986 PowerShell Proxy Hostname/IP:

Active Directory Settings

Active Directory Hostname/IP: Domain:

Save

- Profile Name.** Name of the credential. Can be any combination of alphanumeric characters.
- Hostname/IP.** Hostname or IP address of the device from which you want to retrieve data.
 - You can include the variable **%D** in this field. The platform will replace the variable with the IP address of the current device (device that is currently using the credential).
 - You can include the variable **%N** in this field. The platform will replace the variable with the hostname of the current device (device that is currently using the credential). If the platform cannot determine the hostname, the platform will replace the variable with the primary, management IP address for the current device.
- Username.** Username for an account on the Windows device to be monitored or on the proxy server.

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

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

5. To save the credential, click the **[Save]** button. To clear the values you set, click the **[Reset]** button.

Testing Windows Credentials

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

SNMP Credential Test

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

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

PowerShell Credential Test

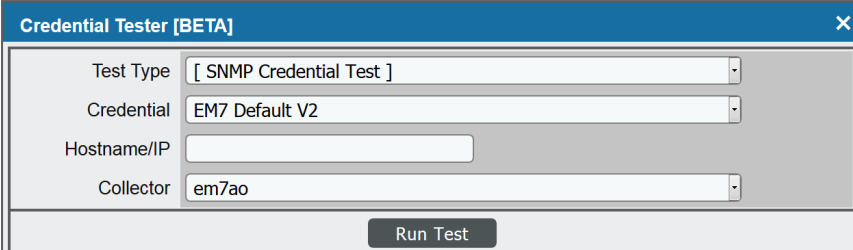
The PowerShell Credential Test can be used to test a PowerShell credential for connectivity. The PowerShell Credential Test performs the following steps:

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

Running a Windows Credential Test

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

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** menu, and then select *Test Credential*. The **Credential Tester** modal page appears:



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

3. Supply values in the following fields:
 - **Test Type.** Select a credential test to run.

- **Credential**. Select the credential you want to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
- **Hostname/IP**. Enter a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
- **Collector**. Select the All-In-One Appliance or Data Collector that will run the test.

4. Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears:

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

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

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

5. Optionally, you can click the **[Execute Discovery Session]** button to run a discovery session using the **Credential**, **Hostname/IP**, and **Collector** you selected in the **Credential Tester** modal page.

Discovering Component Devices on Hyper-V Systems

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

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

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

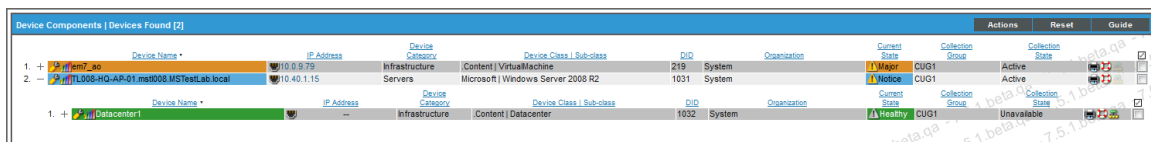
When these Dynamic Applications are aligned to a Hyper-V system, the platform will automatically create a device record for each virtual machine. The platform will also automatically align other Dynamic Applications from the *Microsoft: Hyper-V Server PowerPack* to each virtual machine.

Viewing Component Devices

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

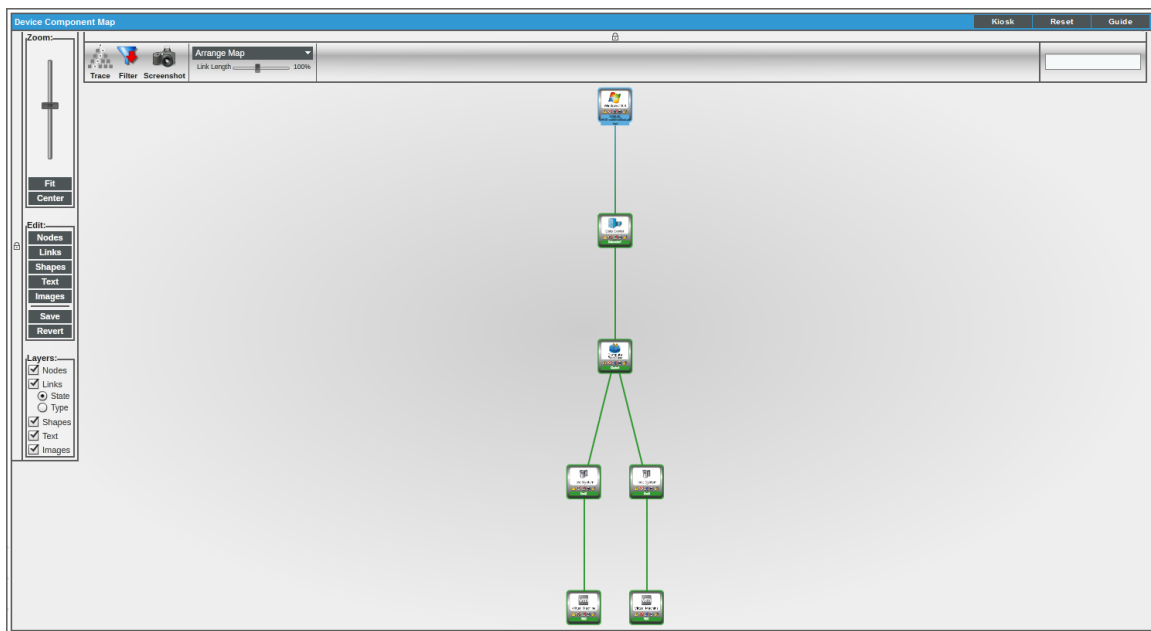
In addition to the **Device Manager** page, you can view the Hyper-V system and all associated component devices in the following places in the user interface:

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



Device Name	IP Address	Device Category	Device Class Sub-class	GUID	System	Organization	Current State	Collection Group	State
1. + [icon] vm7_lab	10.0.0.79	Infrastructure	Content VirtualMachine	218	System		Healthy	CUG1	Active
2. - [icon] TL005-HQ-AP-01.ms1008.MSTestLab.local	10.40.1.15	Servers	Microsoft Windows Server 2008 R2	1031	System		Notice	CUG1	Active
1. + [icon] Datacenter		Infrastructure	Content Datacenter	1032	System		Healthy	CUG1	Unavailable

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



Monitoring a Windows Cluster

Overview

The following sections describe how to monitor a Windows Cluster using the ScienceLogic platform:

<i>Monitoring Windows Clusters in the ScienceLogic Platform</i>	90
<i>Discovering Cluster Nodes</i>	91
<i>Aligning a Dynamic Application with a Cluster Node</i>	91
<i>Disabling Collection of a Dynamic Application on a Device</i>	92
<i>Discovering the Cluster IP Address</i>	93
<i>Aligning Dynamic Applications with the Cluster Device</i>	95
<i>Using a Device Template to Configure Dynamic Applications</i>	96

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 the ScienceLogic platform 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 the ScienceLogic platform 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, the ScienceLogic platform 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 the ScienceLogic platform 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. The ScienceLogic platform will not re-enable collection for those Dynamic Applications.

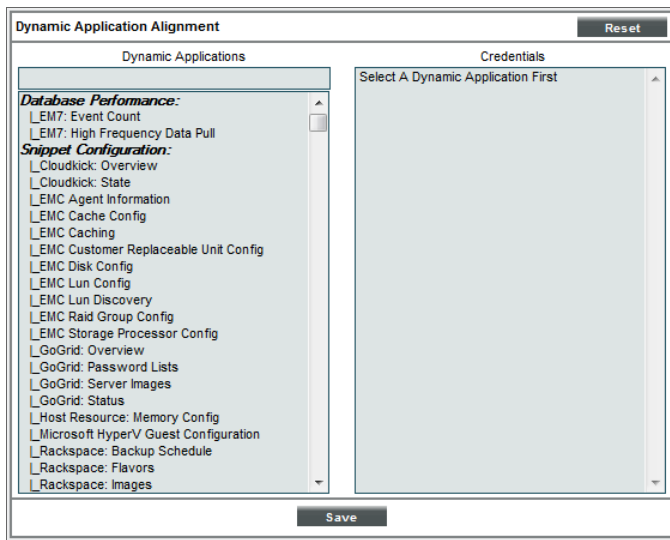
The following sub-sections describe how to manually align a Dynamic Application with a cluster node and how to disable collection of a Dynamic Application on a device. If you are configuring the ScienceLogic platform to monitor multiple clusters that provide the same service, you can speed up both of 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 () 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:



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 () 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:

Dynamic Application™ Collections		Expand	Action	Reset	Guide
ID	Poll Frequency	Type	Credential		
+ Informant: Memory	312 5 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>	
+ Informant: Volumes	314 5 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>	
+ MSSQL: General	84 10 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>	
+ MSSQL: Memory	83 10 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>	
+ MSSQL: SQL Stats	82 10 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>	
+ Host Resource: CPU Config	12 1440 mins	SNMP Configuration	Default SNMP Credential	<input type="checkbox"/>	
+ Host Resource: Software	9 120 mins	SNMP Configuration	Default SNMP Credential	<input type="checkbox"/>	
+ Host Resource: CPU	10 5 mins	Snippet Performance	Default SNMP Credential	<input type="checkbox"/>	
+ Host Resource: Memory	8 5 mins	Snippet Performance	Default SNMP Credential	<input type="checkbox"/>	
+ Host Resource: Memory Config	11 1440 mins	Snippet Configuration	Default SNMP Credential	<input type="checkbox"/>	

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 the ScienceLogic platform 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 the ScienceLogic platform 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:

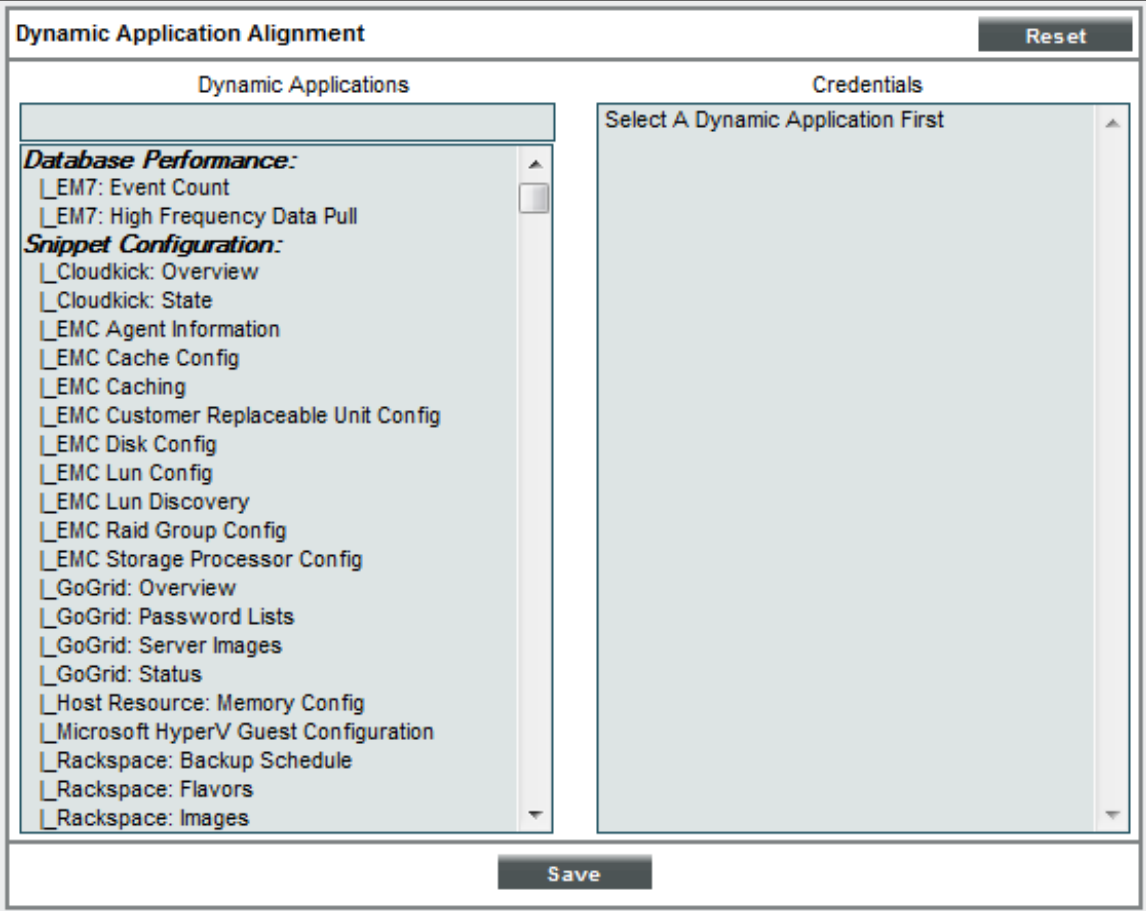
- **IP Address Discovery List**. Enter the shared IP address for the cluster.
- **SNMP Credentials**. Do not select any credentials.
- **Other Credentials**. Do not select any credentials.
- **Discover Non-SNMP**. Select this checkbox.
- **Duplication Protection**. Deselect this checkbox. If you discovered the cluster nodes as SNMP devices, the ScienceLogic platform will have associated the shared IP address for the cluster with one of those nodes. You must disable duplication protection for the ScienceLogic platform 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.

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 () 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:



Dynamic Application Alignment Reset

Dynamic Applications	Credentials
<p>Database Performance:</p> <ul style="list-style-type: none">EM7: Event CountEM7: High Frequency Data Pull <p>Snippet Configuration:</p> <ul style="list-style-type: none">Cloudkick: OverviewCloudkick: StateEMC Agent InformationEMC Cache ConfigEMC CachingEMC Customer Replaceable Unit ConfigEMC Disk ConfigEMC Lun ConfigEMC Lun DiscoveryEMC Raid Group ConfigEMC Storage Processor ConfigGoGrid: OverviewGoGrid: Password ListsGoGrid: Server ImagesGoGrid: StatusHost Resource: Memory ConfigMicrosoft HyperV Guest ConfigurationRackspace: Backup ScheduleRackspace: FlavorsRackspace: Images	Select A Dynamic Application First

Save

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 the ScienceLogic platform 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:

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.

- 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*.
- If you want to configure multiple Dynamic Applications with this device template, repeat steps 4–6 for each additional Dynamic Application.
- 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:

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

The screenshot shows the **Device Template Editor** interface. At the top, there's a breadcrumb trail: **Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)**. A **Reset** button is in the top right. Below the breadcrumb, there's a **Template** dropdown menu set to **New / One-off Template**, a **Save When Applied & Confirmed** checkbox, and a **Template Name** text input field.

The main configuration area is divided into three sections:

- Access & Monitoring:** Contains dropdown menus for **Device Organization** (Acme Corporation), **SNMP Read** (c0sm0s), **SNMP Write** (None), **Availability Protocol** (TCP), **Latency Protocol** (TCP), **Avail+Latency Alert** (Disabled), **Collection** (Enabled), **Coll. Type** (Standard), **Critical Ping** (Disabled), **Event Mask** (Disabled), **Avail Port** (ICMP), **Latency Port** (ICMP), and **Collector Grp** (CUG).
- Device Preferences:** Contains checkboxes for **Auto-Clear Events**, **Scan All IPs**, **Accept All Logs**, **Dynamic Discovery**, **Daily Port Scans**, **Preserve Hostname**, **Auto-Update**, and **Disable Asset Update**.
- Device Retention & Basic Thresholds:** Contains sliders for **System Latency** (500 ms), **Bandwidth Data** (30 days), **Normalized BW Data** (30 days), **Performance Data** (30 days), **Normalized Perf Data** (30 days), **Device Logs Max** (5000 records), **Log Age Max** (30 days), **Number of Availability Pings** (1 pings), and **Ping Packet Size** (100 %).

An **Apply** button is located at the bottom center of the configuration area.

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

Chapter

7

Windows Dashboards

Overview

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

<i>Installing the Microsoft Server Dashboards</i>	98
<i>Microsoft: Active Directory Server Performance</i>	100
<i>Microsoft: DNS Server Performance</i>	103
<i>Microsoft: Exchange Server 2010 Performance</i>	105
<i>Microsoft: Exchange Server 2013 Performance</i>	108
<i>Microsoft: IIS Server Performance</i>	111
<i>Microsoft: Lync Server 2010 Dashboards</i>	113
<i>Microsoft: Lync Server 2010 Performance</i>	113
<i>Microsoft: Lync Server 2010 Utilization</i>	116
<i>Microsoft: Skype for Business Dashboards</i>	119
<i>Microsoft: Lync Server 2013 Performance</i>	119
<i>Microsoft: Lync Server 2013 Utilization</i>	122
<i>Microsoft: SQL Server Performance</i>	125

Installing the Microsoft Server Dashboards

The following PowerPacks contain dashboards for Microsoft servers:

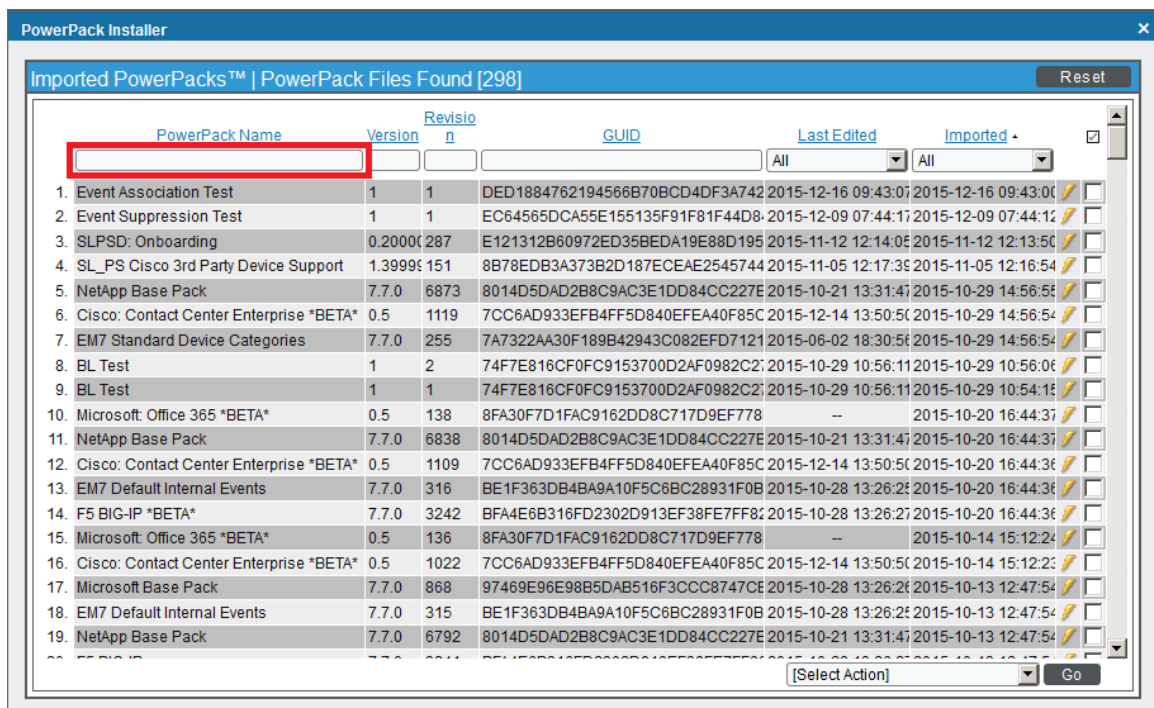
- Microsoft: Active Directory Server Dashboards



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

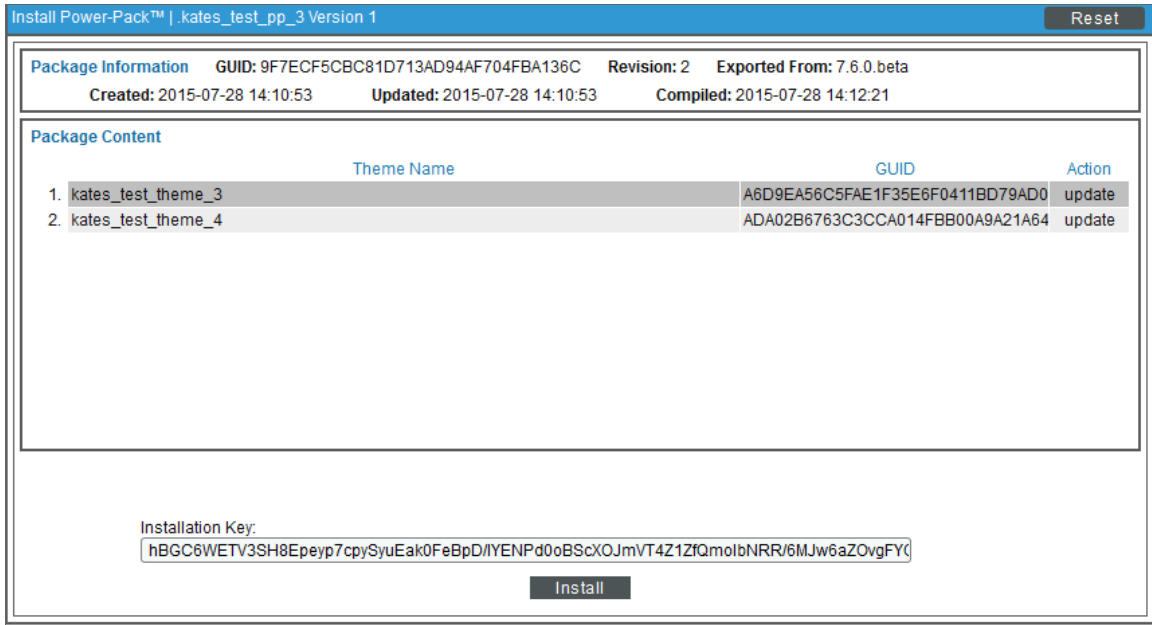
To view these dashboards in the ScienceLogic platform, you must first install the corresponding PowerPack. To do so:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
2. Click the **[Actions]** button, then select *Install PowerPack*. The **Imported PowerPacks** modal page appears.
3. Use the search filter in the **PowerPack Name** column heading to locate the PowerPack you want to install. To do so, enter text to match, including special characters, and the **Imported PowerPacks** modal page displays only PowerPacks that have a matching name.



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

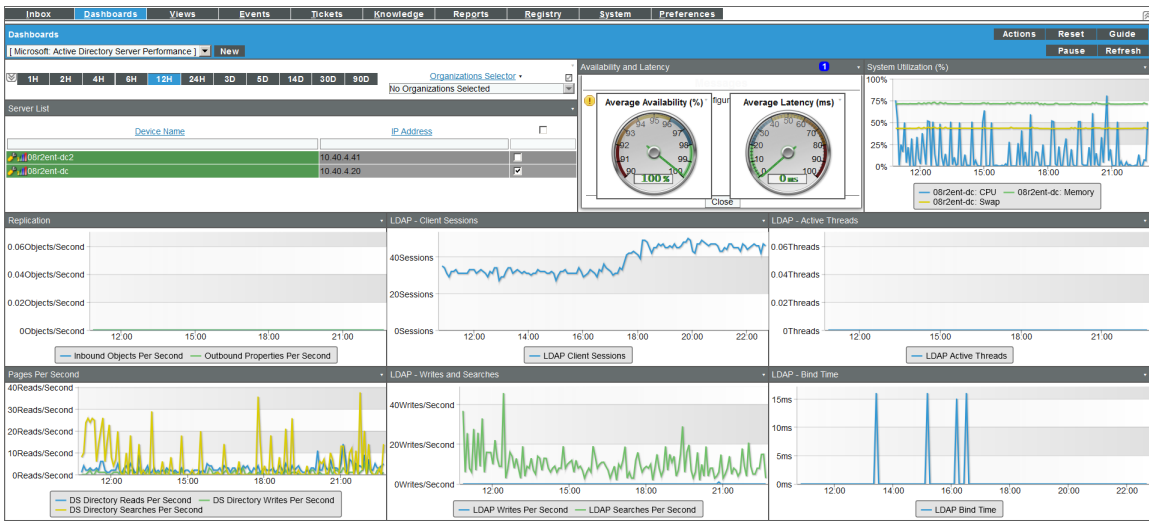
- The **Install PowerPack** modal page appears. To install the PowerPack, click **[Install]**.



- The PowerPack now appears in the **PowerPack Manager** page. The contents of the PowerPack are automatically installed in your ScienceLogic system.

Microsoft: Active Directory Server Performance

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



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



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

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

Availability and Latency. This widget displays two gauges:

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

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

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

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

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

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

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

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

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

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

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

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

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

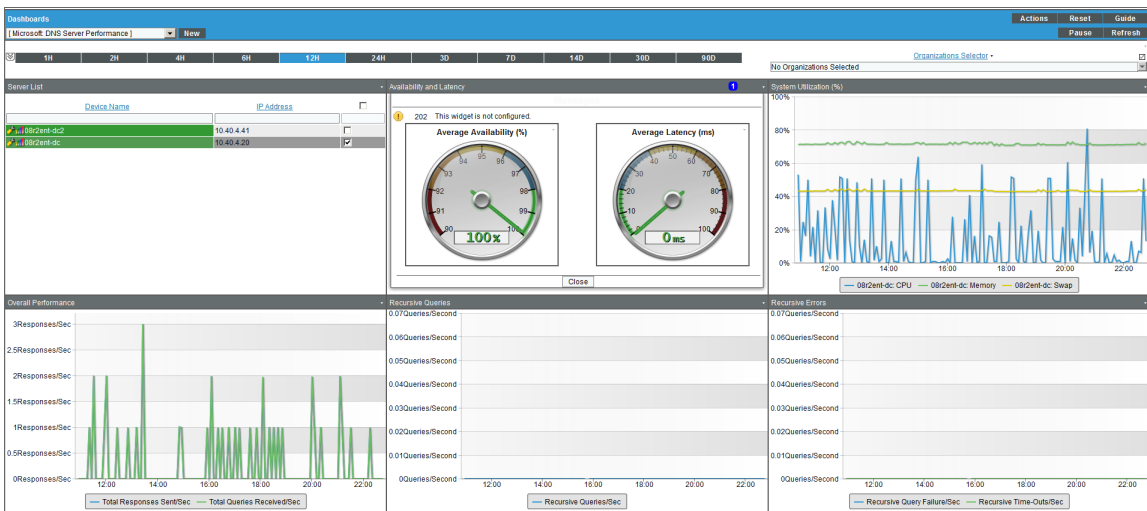
- The y axis displays writers per second and searches per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data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

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

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

Microsoft: DNS Server Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

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

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

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

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

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

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

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

Microsoft: Exchange Server 2010 Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected Exchange 2010 server.

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

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

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

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

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

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

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

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

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

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

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

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

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

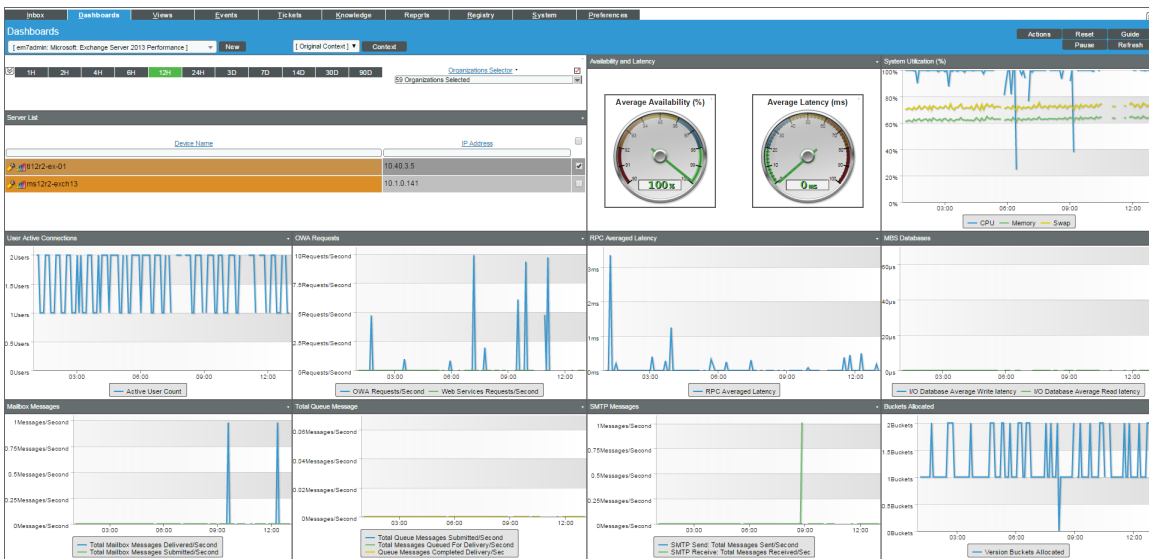
- The y axis displays the number of messages per second.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays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

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

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

Microsoft: Exchange Server 2013 Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Microsoft: IIS Server Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

- Clicking on a data point displays the Device Performance graph for the selected parameter on the selected IIS server.

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

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

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

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

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

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

Pages Per Second. This widget displays a line graph. The line graph displays the number of Pages (served) Per Second.

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

Cache Hit %. The IIS server caches (in memory) frequently requested files. This widget displays a line graph. The line graph displays the ratio of kernel URI cache hits to total cache requests.

- The y axis displays percent of URI cache hits.

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

404 Errors Per Second. This widget displays a line graph. The line graph displays the number of errors due to requests that couldn't be satisfied by the server because the requested document couldn't be found, per second.

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

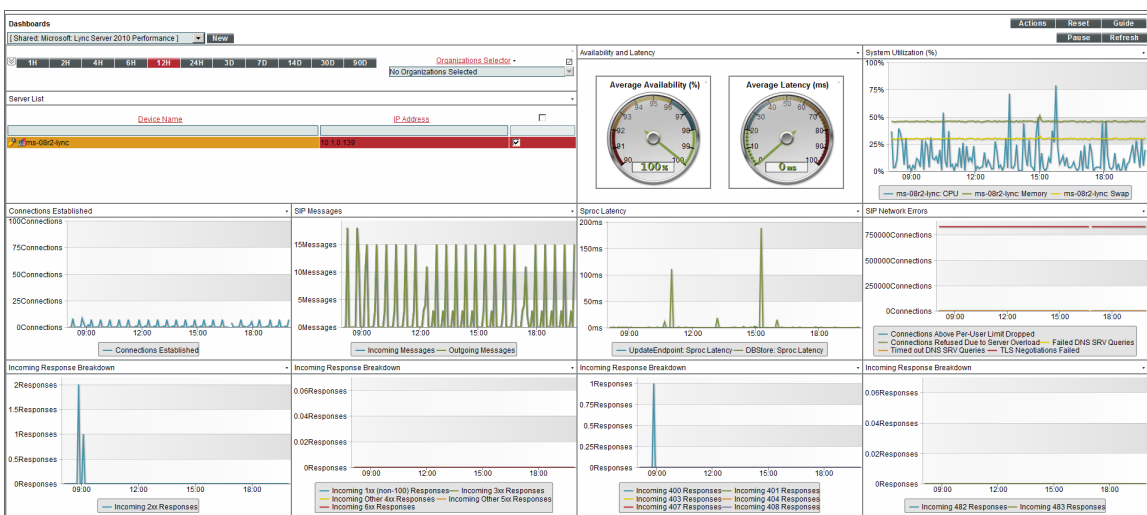
Microsoft: Lync Server 2010 Dashboards

The *Microsoft: Lync Server 2010 Dashboards PowerPack* includes the following dashboards:

- Microsoft: Lync Server 2010 Performance
- Microsoft: Lync Server 2010 Utilization

Microsoft: Lync Server 2010 Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

Connections Established. This widget displays a line graph. The line graph displays Connections Established.

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

SIP Message. SIP is a protocol for instant messaging and VOIP. This widget displays a line graph. The line graph displays Incoming Message and Outgoing Messages. Each parameter is represented by a color-coded line.

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

Sproc Latency. Stored Procedure Call (sproc) latency is the time it takes for the Lync database to process the stored procedure call.

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

SIP Network Errors. This widget displays information about errors during instant messaging or VOIP. This widget displays a line graph. The line graph displays Connections Above Per-User Limit Dropped, Connections Refused Due to Server Overload, Failed DNS SRV Queries, Time Out DNS SRV Queries, and TLS Negotiations Failed. Each parameter is represented by a color-coded line.

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

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 2xx Responses. A 2xx Response means that a connection has been established.

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

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 1xx (non-100) Responses, Incoming 3xx Responses, Incoming Other 4xx Responses, Incoming Other 5xx Responses, and Incoming 6xx Responses. Each parameter is represented by a color-coded line. For a description of SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List_of_SIP_response_codes.

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

Incoming Response Breakdown. This widget displays information about the number of responses generated by the server. This widget displays a line graph. The line graph displays Incoming 400 Responses, Incoming 401 Responses, Incoming Other 403 Responses, Incoming 404 Responses, Incoming 407 Responses, and Incoming 408 Responses. Each parameter is represented by a color-coded line. For a description of SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List_of_SIP_response_codes.

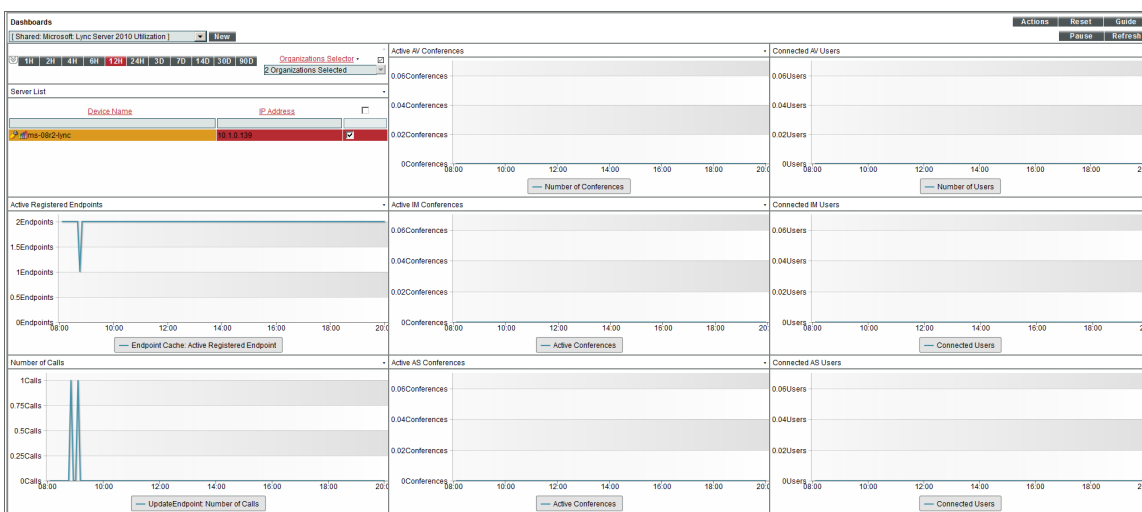
- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the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

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

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

Microsoft: Lync Server 2010 Utilization

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

Active Registered Endpoints. Endpoints are devices that are connected to the Lync front-end server. This widget displays a line graph. The line graph displays Endpoint Cache: Active Registered Endpoints.

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

Active IM Conferences. This widget displays the current number of IM conversations on the Lync server. Conferences usually include more than two users. This widget displays a line graph. The line graph displays Active Conferences.

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

Connected IM Users. This widget displays the current number of connected IM users. This widget displays a line graph. The line graph displays Connected Users.

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

Number of Calls. This widget displays the current number of voice calls on the Lync server. This widget displays a line graph. The line graph displays UpdateEndpoint: Number of Calls.

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

Active AS Conferences. This widget displays the number of active conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Active Conferences.

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

Connected AS Users. This widget displays the number of users connected to conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Connected Users.

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

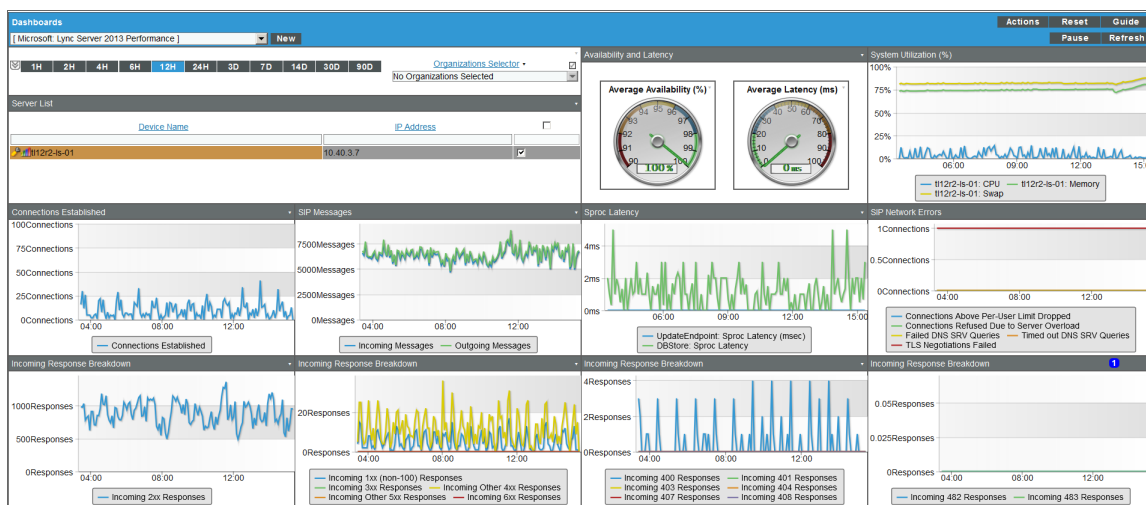
Microsoft: Skype for Business Dashboards

The *Microsoft: Skype for Business Dashboards* PowerPack includes the following dashboards:

- Microsoft: Lync Server 2013 Performance
- Microsoft: Lync Server 2013 Utilization

Microsoft: Lync Server 2013 Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Lync 2013 server during the selected duration. Each parameter is represented by a color-coded line.

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

Connections Established. This widget displays a line graph. The line graph displays Connections Established.

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

SIP Message. SIP is a protocol for instant messaging and VOIP. This widget displays a line graph. The line graph displays Incoming Message and Outgoing Messages. Each parameter is represented by a color-coded line.

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

Sproc Latency. Stored Procedure Call (sproc) latency is the time it takes for the Lync database to process the stored procedure call.

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

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

SIP Network Errors. This widget displays information about errors during instant messaging or VOIP. This widget displays a line graph. The line graph displays Connections Above Per-User Limit Dropped, Connections Refused Due to Server Overload, Failed DNS SRV Queries, Time Out DNS SRV Queries, and TLS Negotiations Failed. Each parameter is represented by a color-coded line.

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

Incoming Response Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 2xx Responses. A 2xx Response means that a connection has been established.

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

Incoming Respond Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 1xx (non-100) Responses, Incoming 3xx Responses, Incoming Other 4xx Responses, Incoming Other 5xx Responses, and Incoming 6xx Responses. Each parameter is represented by a color-coded line. For a description of all SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List_of_SIP_response_codes.

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

Incoming Response Breakdown. This widget displays information about the number of responses that are being generated by the server. This widget displays a line graph. The line graph displays Incoming 400 Responses, Incoming 401 Responses, Incoming Other 403 Responses, Incoming 404 Responses, Incoming 407 Responses, and Incoming 408 Responses. Each parameter is represented by a color-coded line. For a description of all SIP response codes, see the Wikipedia page http://en.wikipedia.org/wiki/List_of_SIP_response_codes.

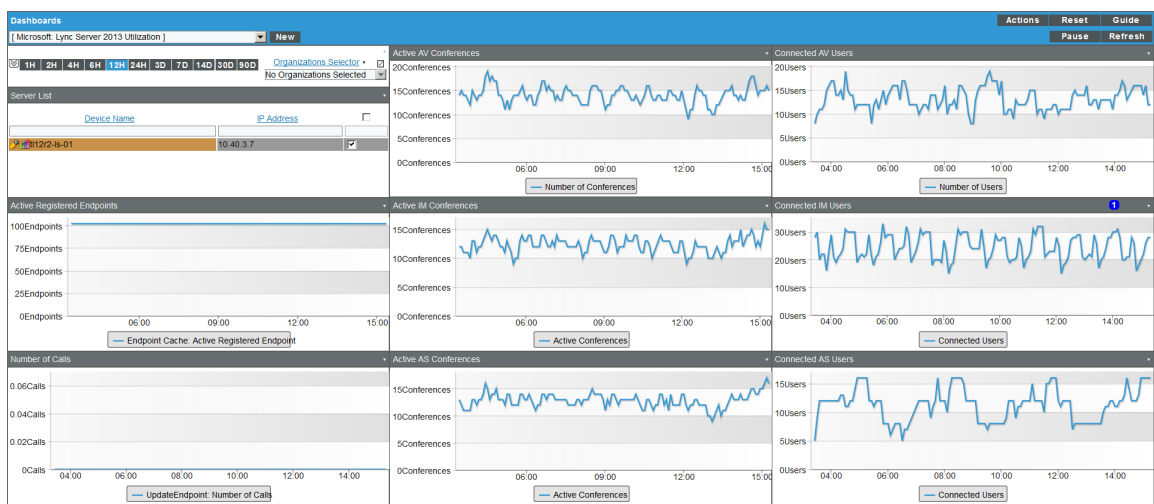
- The y axis displays the number of responses.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays the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

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

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

Microsoft: Lync Server 2013 Utilization

The Microsoft: Lync 2013 Server Utilization dashboard provides an overview of how users are using a selected Lync 2013 server.



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

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

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

Availability and Latency. This widget displays two gauges:

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

System Utilization (%). This widget displays a line graph. The line graph displays memory usage, virtual-memory usage, and CPU usage for the selected Lync 2013 server during the selected duration. Each parameter is represented by a color-coded line.

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

Active Registered Endpoints. Endpoints are devices that are connected to the Lync front-end server. This widget displays a line graph. The line graph displays Endpoint Cache: Active Registered Endpoints.

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

Active IM Conferences. This widget displays the number of IM conversations on the Lync server. Conferences usually include more than two users. This widget displays a line graph. The line graph displays Active Conferences.

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

Connected IM Users. This widget displays the current number of connected IM users. This widget displays a line graph. The line graph displays Connected Users.

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

Number of Calls. This widget displays the current number of voice calls on the Lync server. This widget displays a line graph. The line graph displays UpdateEndpoint: Number of Calls.

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

Active AS Conferences. This widget displays the number of active conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Active Conferences.

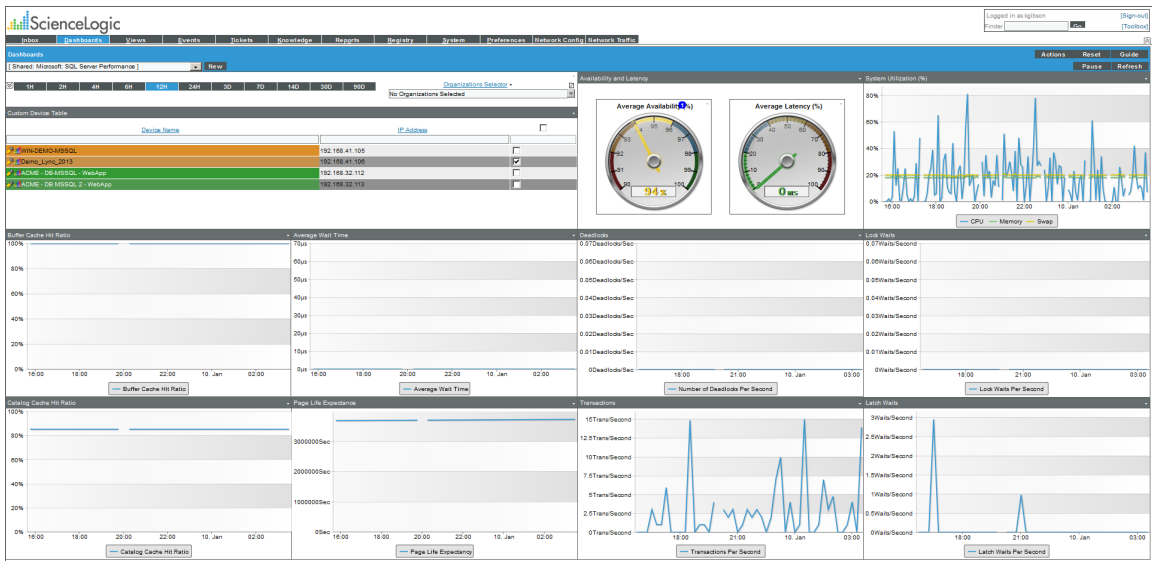
- The y axis displays the number of AS conferences.
- The x axis displays time. The increments vary, depending upon the date range selected in the **Context Quick Selector** widget.
- Mousing over any point in any line displays the average value at that time-point.
- Clicking on a data point displays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

Connected AS Users. This widget displays the number of users connected to conferences using Application Sharing (AS). This widget displays a line graph. The line graph displays Connected Users.

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

Microsoft: SQL Server Performance

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



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

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

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

Availability and Latency. This widget displays two gauges:

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

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

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

Buffer Cache Hit Ratio. This widget displays information about the percentage of page requests that are satisfied by data pages from the buffer cache without having to read from disk. The ratio is the total number of pages found in the buffer divided by the total number of requests. This widget displays a line graph. The line graph displays Buffer Cache Hit Ratio.

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

Average Wait Time. This widget displays information about the average wait time to acquire a lock. This widget displays a line graph. The line graph displays Average Wait Time.

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

Deadlocks. This widget displays information about deadlocks. A deadlock occurs when two or more tasks permanently block each other because each task tries to lock a resource which the other tasks are also trying to lock. This widget displays a line graph. The line graph displays Number of Deadlocks Per Second.

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

Lock Waits. This widget displays information about the number of lock requests per second that require the requester to wait. This widget displays a line graph. The line graph displays Lock Waits Per Second.

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

Catalog Cache Hit Ratio. This widget displays information about the ratio between catalog metadata cache hits and lookups. The ratio is the total number of pages found in the catalog metadata cache divided by the total number of lookups. This widget displays a line graph. The line graph displays Catalog Cache Hit Ratio.

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

Page Life Expectancy. This widget displays information about the number of seconds a page will stay in the buffer pool (memory cache) without references. This widget displays a line graph. The line graph displays Page Life Expectancy.

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

Transactions. A transaction is a sequence of operations that make up a single logical unit of work, usually a change to the database. This widget displays information about the number of transactions per second to the SQL server. This widget displays a line graph. The line graph displays Transactions Per Second.

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

Latch Waits. A latch is an object that ensures data integrity for objects in the buffer pool (memory cache). This widget displays a line graph. The line graph displays Latch Waits Per Second.

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

Chapter

8

Troubleshooting

Overview

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

<i>Troubleshooting WinRM Error Messages</i>	129
<i>Debugging Code 401 Errors</i>	130
<i>Debugging Code 500 Errors</i>	131
<i>Troubleshooting PowerShell Error Messages</i>	132

Troubleshooting WinRM Error Messages

The ScienceLogic platform can generate the following error messages when problems occur in Windows Remote Management (WinRM). For each error message, the top-most cause listed is the most likely reason for the error message.

Error / Message	Cause / Resolution
Incorrect username and/or password provided in the PowerShell Credential.	Bad HTTP response returned from server. Basic authentication failed. Code 401. (For more information, see the section Debugging Code 401 Errors .)
	Pre-authentication failed while getting initial credentials.
	Client not found in Kerberos database.

Error / Message	Cause / Resolution
The device cannot respond to WinRM requests or the PowerShell credential settings do not match the device's WinRM configuration.	Kerberos-based authentication failed. Code 500. (For more information, see the section Debugging Code 500 Errors .)
	[Errno 111] Connection refused.
	ParseError.
Server is offline.	Increase the Timeout value on your ScienceLogic credential.

NOTE: If you receive an error message that is a combination of the first two error messages, then you must run debugging steps for both Code 401 and Code 500.

Debugging Code 401 Errors

If you encounter a Code 401 error, perform the following troubleshooting steps to debug the error:

- Determine if the error is caused by an issue with the Kerberos ticket:
 - Ensure forward and reverse DNS are configured correctly when using Active Directory authentication:

```
# nslookup [IP address]
# nslookup [hostname]
```

- Ensure you are able to run the following command without error from the collector:

```
# kinit [username@DOMAINNAME]
```

- If you see the following error, change the domain name to all capital letters:

```
[root@COM_ISO_AIO ~]# kinit commro@mst108r2.com
Password for commro@mst108r2.com:
kinit(v5): KDC reply did not match expectations while getting initial credentials
```

- Ensure that your WinRM settings match your ScienceLogic credential.
 - To print out current WinRM settings:

```
# winrm get winrm/config
```

- If your ScienceLogic credential says no encryption, AllowUnencrypted should be set to True for both the Client and the Service:

```
# winrm set winrm/config/client '{@AllowUnencrypted="$true"}'
# winrm set winrm/config/service '{@AllowUnencrypted="$true"}'
```

- If you are using local type credentials, basic Authentication should be set to True for both Client and Service:

```
# winrm set winrm/config/client/Auth '@{Basic="$true"}'
# winrm set winrm/config/service/Auth '@{Basic="$true"}'
```

- If you are using AD type credentials, Kerberos Authentication should be set to True for both Client and Service:

```
# winrm set winrm/config/client/Auth '@{Kerberos="$true"}'
# winrm set winrm/config/service/Auth '@{Kerberos="$true"}'
```

- In the ScienceLogic credential, ensure the Active Directory **Hostname/IP** field contains the FQDN and the **LDAP Domain** field includes the domain.
- In the ScienceLogic credential, the value in the **LDAP Domain** field might need to be entered in all capital letters.
- Ensure your ScienceLogic credentials are correct:

- SSH to your Data Collector and try running the following command:

```
# wmic -U 'user%password' //IP "select * from Win32_ComputerSystem"
```

NOTE: If you choose to copy and paste the above command from this document into a shell session, you might have to replace the single and double quotation marks.

- If you are using Windows Servers 2012 and above, make sure that the user you are using belongs to the group: WinRMRemoteWMIUsers__
- If you are using Windows Server 2008, 2008r2, or below, ensure that the user you are using is an administrator. This is a Windows requirement.
- If multiple domains are in use, ensure that they are mapped in the [domain_realm] section of the Kerberos krb5.conf file.
 - The [domain_realm] section provides a translation from a domain name or hostname to a Kerberos realm name.
- Ensure that the username and password are correct and that you can log on to the system.
- Ensure your credential cache is up-to-date:
 - SSH to your Data Collector and cd to the /tmp/ directory.
 - Do an 'ls' to list all the contents of the /tmp/ directory.
 - If you see any files that begin with "krb5cc_", delete those files.

Debugging Code 500 Errors

If you encounter a Code 500 error, perform the following troubleshooting steps to debug the error:

- In the ScienceLogic credential, increase the value in the **Timeout** field (e.g., 180000 ms.).

- Increase the timeout in the WinRM settings:

```
winrm set winrm/config '@{MaxTimeoutms="30000"}'
```

- Increase the maximum number of concurrent operations per user:

```
winrm set winrm/config/service '@{MaxConcurrentOperationsPerUser="100"}'
```

- Increase the maximum number of connections:

```
winrm set winrm/config/service '@{MaxConnections="100"}'
```

- Increase the maximum number of concurrent operations:

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

- Ensure that the Windows device being monitored is not exceeding its resource thresholds. You can do this by opening Resource Monitor on the Windows Device and monitoring the CPU usage.

Troubleshooting PowerShell Error Messages

The ScienceLogic platform can generate the following error message when monitoring Windows devices using PowerShell. This error message usually indicates that an issue with WinRM is not causing the error.

Error / Message	Cause / Resolution
Get-Counter The specified object was not found on the computer.	The PowerShell object was not found on the device that is being monitored. To test this, copy the PowerShell request from the Dynamic Application and run it on the Windows device in a PowerShell shell as Administrator. If you get a similar error message, then the counter does not exist on your Windows device. This means that the user must install the necessary service on the Windows device.

© 2003 - 2018, 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