

## WMI and PowerShell Dynamic Application Development

SL1 version 10.1.4

#### Table of Contents

Introduction	. 1
What is WMI?	. 1
What is PowerShell?	
Prerequisites	2
WMI and PowerShell Dynamic Applications	
WMI Requests	
Defining a WMI Request	
Example WMI Code	
Defining a WBEM Request	
Example WBEM Request Code	
Editing a WMI Request	
Editing a WBEM Request	
Deleting a WMI or WBEM Request	
PowerShell Requests	
Defining a PowerShell Request	
Editing a PowerShell Request	
Deleting a PowerShell Request	
Converting Legacy PowerShell Requests	
WMI and PowerShell Collection Objects	
WMI-Specific Fields for Collection Objects	
PowerShell-Specific Fields for Collection Objects	
Configuring Devices for Monitoring with WMI	
Configuring WMI on Windows 2008 Servers	
Step 1: Configuring Services	
Step 2: Configuring the Windows Firewall	
Step 3: Configuring a User Account and Permissions	
Configuring Namespace and DCOM Security Permissions	
Configuring User Account Control to Allow Elevated Permissions	
Configuring WMI for Windows Desktop Systems	
Step 1: Configuring Services	
Step 2: Configuring Windows Firewall	
Step 3: Setting the Default Namespace Security	
Step 4: Setting the DCOM Security Level	
Step 5: Disabling User Account Control	.47
Configuring Devices for Monitoring with PowerShell	
Configuring PowerShell	
Step 1: Configuring the User Account for SL1	
Option 1: Creating an Active Directory Account	
Option 2: Creating a Local User Account with Administrator Access	
Option 3: Creating a Non-Administrator Local User Account	
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	
Creating a User Group and Adding a User in Active Directory	.54
Setting the Session Configuration Parameters and Group Permissions	.54
Step 2: Configuring a Server Authentication Certificate	
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	56
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	.58
Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	
Step 3: Configuring Windows Remote Management	.59
Option 1: Using a Script to Configure Windows Remote Management	.59

Option 2: Manually Configuring Windows Remote Management	64
Option 3: Using a Group Policy to Configure Windows Remote Management	
Step 4: Configuring a Windows Management Proxy	
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	86
Creating a PowerShell Credential	
Error Messages for PowerShell Collection	89
Concurrent PowerShell Collection	
Enabling and Disabling Concurrent PowerShell for Collector Groups	91
Enabling Concurrent PowerShell on All Collector Groups	
Disabling Concurrent PowerShell on All Collector Groups	92
Enabling Concurrent PowerShell on a Specific Collector Group	92
Disabling Concurrent PowerShell on a Specific Collector Group	
Credentials for WMI and PowerShell Devices	
Configuring a WMI Credential	
Configuring a PowerShell Credential	96
Creating a WMI Performance Dynamic Application	
Defining the WMI Request	
Adding the WMI Request	
Adding the Collection Objects	
Creating the Presentation Objects	
Creating a Credential	
Manually Aligning the Dynamic Application to a Device	
Viewing the Performance Reports	
Creating a PowerShell Performance Dynamic Application	
Creating the Dynamic Application	
Adding the PowerShell Command	
Adding the Collection Object	
Creating the Presentation Object	
Creating a Credential	
Manually Aligning the Dynamic Application to a Device	
Viewing the Performance Report	120

## Chapter

### Introduction

#### Overview

This manual describes how to use the WMI and PowerShell protocols to define collection objects and create WMI and PowerShell Dynamic Applications.

**NOTE**: This manual uses the WMI nomenclature with equivalent SQL nomenclature in parentheses. For example, instance (row), property (column), and class (table).

This chapter provides an overview of the WMI and PowerShell protocols and WMI and PowerShell Dynamic Applications in SL1. It includes the following topics:

What is WMI?	. 1
What is PowerShell?	2
Prerequisites	. 2
WMI and PowerShell Dynamic Applications	2

#### What is WMI?

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

#### What is PowerShell?

Windows PowerShell is a command-line shell and scripting language for administration of Windows systems. SL1 can execute PowerShell requests on target Windows devices via WinRM (Windows Remote Management). For an overview of Windows PowerShell, see <a href="https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6">https://docs.microsoft.com/en-us/powershell/scripting/powershell-scripting?view=powershell-6</a>.

SL1 supports the following PowerShell versions for monitoring Windows devices:

- PowerShell 3.0
- PowerShell 4.0
- PowerShell 5.1

#### Prerequisites

This manual does not describe how to plan, design, use, or troubleshoot Dynamic Applications for your network. This manual assumes that you are already familiar with the common elements and concepts of Dynamic Applications. For general information on planning, designing, using, and troubleshooting Dynamic Applications, see the manual **Dynamic Application Development**.

WMI Dynamic Applications use the WMI protocol. PowerShell Dynamic Applications use the PowerShell protocol. This manual assumes that you are familiar with either the WMI or PowerShell protocols.

#### WMI and PowerShell Dynamic Applications

In SL1, a WMI Dynamic Application is a Dynamic Application that uses WMI to retrieve data from devices. WMI Dynamic Applications use WMI or WBEM requests to populate collection objects. WMI requests use WQL (WMI Query Language) to query WMI classes (tables) to retrieve data.

WBEM objects are populated with values returned by the wbemcli "get instance" command.

In SL1, a PowerShell Dynamic Application is a Dynamic Application that uses PowerShell to retrieve data from devices. PowerShell Dynamic Applications use PowerShell commands to populate collection objects.

WMI and PowerShell Dynamic Applications have the following elements in common with other Dynamic Applications:

- Archetypes. Defines what data is being collected and how it will be displayed in SL1. WMI and PowerShell Dynamic Applications can use either the Performance or Configuration archetypes.
- Properties. Allows for version control, release notes, collection, and retention settings.

- Collection Objects. Define the individual data-points that will be retrieved by the Dynamic Application. These data points are called collection objects. Defines the type of data that is being collected (gauge, counter, etc) and how it is grouped. Collection objects for WMI and PowerShell Dynamic Applications have settings that are different from collection objects in other types of Dynamic Applications. These settings are described in this manual.
- **Presentations**. For Performance Dynamic Applications, defines how collected values will be displayed by SL1.
- *Thresholds*. Can be used to define a threshold value that can be included in alerts. The threshold appears in the **Device Thresholds** page for each device aligned with the Dynamic Application.
- Alerts. Triggers events based on the values retrieved by the Dynamic Application. If the collected data meets the conditions defined in the alert, the alert can insert a message into device logs and trigger events.
- **Credentials**. Define how authentication should occur for each Dynamic Application on each device. WMI Dynamic Applications use Basic/Snippet credentials; PowerShell Dynamic Applications use PowerShell credentials. There are multiple ways to align a credential with a Dynamic Application (during discovery, as secondary credentials for a device, or manually in the Collections page for a device). For details on how SL1 aligns credentials during discovery and how to manually edit and add new credentials to a device, see the manual **Discovery and Credentials**.
- **Relationships**. Dynamic Applications can be configured to automatically create relationships between devices. For example, the Dynamic Applications in the VMware vSphere and NetApp PowerPacks are configured to create relationships between VMware Datastore component devices and their associated NetApp Volume component devices. Relationships created by Dynamic Applications are used and visualized by the platform in the same manner as relationships created by topology collection, Dynamic Component Mapping, and manually in the user interface. The settings for configuring the creation of relationships in configuration WMI and PowerShell Dynamic Applications are the same as the relationship settings for other Dynamic Application protocols.

## Chapter

2

#### **WMI Requests**

#### Overview

In SL1, each WMI Dynamic Application must include at least one WMI or WBEM request.

Collection objects in WMI Dynamic Applications objects are populated with the values returned by a WMI request. WMI requests use WQL (WMI Query Language) to query WMI classes (tables) to retrieve data. A single WMI request can populate multiple WMI objects by querying for multiple class properties (table columns). WBEM objects are populated with values returned by the wbemcli "get instance" command.

Collection objects for both WMI and WBEM are aligned with properties (columns). The definition of each object specifies the WMI or WBEM request that will populate the collection object and the property name to align with the object. The retrieved values of the property will populate the object.

To more easily understand WMI, you can compare the terminology to standard SQL terminology:

WMI	SQL
Namespace	Database
Class	Table
Property	Column
Instance	Row

This chapter includes the following topics:

Defining a WMI Request	5
Example WMI Code	7
Defining a WBEM Request	. 7
Example WBEM Request Code	. 9
Editing a WMI Request	9
Editing a WBEM Request	10
Deleting a WMI or WBEM Request	10

#### Defining a WMI Request

You can define a WMI request in the WMI Request Editor & Registry page. To define a WMI request:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. In the **Dynamic Applications Manager** page, find the Dynamic Application for which you want to define a WMI request. Select its wrench icon (
- 3. Select the **[WMI Requests]** tab for the Dynamic Application.

**NOTE**: The **[WMI Requests]** tab will only appear in Dynamic Applications of type WMI Config and WMI Performance.

4. In the WMI Request Editor & Registry page, enter the following:

Close <u>P</u> roperties <u>C</u> ollections	WMI Requests Thresholds	Alerts Subscribers	_
Dynamic Applications [545]   WMI Request Editor & Regi	atry	Guide Reset	
Cyninic Application [545] Will Request Earlor & Reg	<b>v</b>	UMI Object Key Active State [Enabled]	
	Save		
	There are no WMI requests for this ap	oplication.	

- WMI Request Name. Name of the WMI request.
- WMI Request Type. Specifies whether to use a WMI request (query) or a WBEM request (a wbemcli "get instance" request sent over HTTP).
- WMI Request Namespace. Optional field. In this field, you can specify a WMI namespace. The WMI request will then use this namespace when requesting data. If you do not specify a value in this field, the WMI request will use the default namespace (usually root).
- WMI Object Key. The unique key for each instance (row) returned by the request. This unique key must be a property name, and the request must include that property (column) and return values from that property name (column). You must choose a key that remains constant over all polling periods, for example "Name" or "servicename".
- Active State. Specifies whether SL1 should use this request when performing collection for the Dynamic Application. Choices are:
  - Enabled. SL1 will use the WMI request when performing collection for the Dynamic Application.
  - Disabled. SL1 will not use the WMI request when performing collection for the Dynamic Application.
- WMI Request Query. Enter the WQL query in this field. In most cases, these queries will be of the format:

SELECT [one or more properties (columns), separated by commas] FROM name of WMI class (table) where data is stored]

For more information on WQL, see <u>http://msdn.microsoft.com/en-</u>us/library/aa394606%28VS.85%29.aspx

For more information on WMI classes, see <u>http://msdn.microsoft.com/en-us/library/aa394554</u> (v=VS.85).aspx

For a comparison of WQL and SQL, see <u>http://technet.microsoft.com/en-us/library/cc180454.aspx</u>

#### Example WMI Code

For our example Dynamic Application, we'll use the following WMI request:

 ${\tt SELECT TotalV} is ible {\tt MemorySize,CSName,Caption,SerialNumber FROM Win 32\_OperatingSystem}$ 

In this request, we are retrieving the property (column) values from the WMI class (table) **Win32\_ OperatingSystem**. Win32\_OperatingSystem is a class (table) that stores information about an instance of an operating system running on the monitored device. From this class, the WMI request retrieves the values of the following properties:

- TotalVisibleMemorySize. Total amount, in kilobytes, of physical memory available to the operating system. This value does not necessarily indicate the true amount of physical memory, but only the amount that is reported to the operating system as available to it. In our example Dynamic Application, we can create an object that maps to this property. To map an object to the retrieved value from this property, we must ensure that the WMI Request Arguments field for the object (in the Collection Objects page) contains the value "TotalVisibleMemorySize".
- **CSName**. Name of the computer system (device name as it appears to the operating system). In our example Dynamic Application, we can create an object that maps to this property. To map an object to the retrieved value from this property, we must ensure that the **WMI Request Arguments** field for the object (in the **Collection Objects** page) contains the value "CSName".
- **Caption**. This is a short description of the operating system version. For example, "Microsoft Windows XP Professional Version = 5.1.2500". In our example Dynamic Application, we can create an object that maps to this property. To map an object to the retrieved value from this property, we must ensure that the **WMI Request Arguments** field (in the **Collection Objects** page) contains the value "Caption".
- SerialNumber. Operating system product serial identification number. For example: "10497-OEM-0031416-71674". In our example Dynamic Application, we can create an object that maps to this property. To map an object to the retrieved value from this property, we must ensure that the WMI Request Arguments field (in the Collection Objects page) contains the value "SerialNumber".

#### Defining a WBEM Request

You can define a WBEM request in the **WMI Request Editor & Registry** page. To define a WBEM request in the **WMI Request Editor & Registry** page:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. In the **Dynamic Applications Manager** page, find the Dynamic Application for which you want to define a WBEM request. Select its wrench icon (*P*).
- 3. Select the [WMI Requests] tab for the Dynamic Application.

4. In the WMI Request Editor & Registry page, enter the following:

Close	Properties	<u>C</u> ollections	WMI Requests	<u>T</u> hresholds	Alerts	Subscribers		
Dynamic Applicat	ions [545]   WMI Reque	est Editor & Regis	stry				Guide	Reset
	w	MI Request Name				WMI Object Key	/	
	w	/MI Request Type				Active State		
	[WMI]		•		[Enabled]			
	WMI	Request Namespace						
				WMI Request Query				
				Save				
			_					
			There are no	WMI requests for t	nis application.			

- WMI Request Name. Name of the WBEM request.
- WMI Request Type. Specifies whether to use a WMI request (a query) or a WBEM request (a wbemcli "get instance" request sent over HTTP).
- WMI Request Namespace. Optional field. In this field, you can specify a WMI namespace (database). The WBEM request will then use this namespace (databse) when requesting data. If you do not specify a value in this field, the WBEM request will use the default namespace (usually root).
- WMI Object Key. The unique key for each instance (row) returned by the query. This unique key must be a property name, and the query must include that property (column) and return values from that property name (column).
- Active State. Specifies whether SL1 should use this request when performing collection for the Dynamic Application. Choices are:
  - Enabled. SL1 will use the WBEM request when performing collection for the Dynamic Application.
  - Disabled. SL1 will not use the WBEM request when performing collection for the Dynamic Application.
- WMI Request Query. Enter the wbemcli string in this field. In most cases, this will be of the format:

/[name space]:[class name].property=value (this last argument is optional)

Usually, whemcli requires that the request begins with the full path to the CIM object, including:

http://username:password@hostname or IP:port,

SL1 uses the credentials for the Dynamic Application to automatically append this string to the front of each wbemcli request.

For more information on wbemcli, see <a href="http://linux.die.net/man/1/wbemcli">http://linux.die.net/man/1/wbemcli</a>

5. Select the [Save] button to save the new WBEM request.

#### Example WBEM Request Code

For our example Dynamic Application, we'll use the following WMI request:

/root/cimv2:CIM OperatingSystem

- In this request, we are retrieving value from the namespace (database) called /root/cimv2.
- We are requesting all values from the class (table) called CIM\_OperatingSystem.
- This request will return all values from the class CIM\_OperatingSystem. The values will be returned in the format

property\_name="value"

• Each WBEM object (defined in the **Collection Objects** page) must map to a property name returned by a WBEM request. To map each object, you must have specified a value in the **WMI Request Arguments** field that matches the name of a property returned by this request.

NOTE: Before defining objects for a WBEM request, you must know which property names will be returned.

#### Editing a WMI Request

To edit a WMI request in the WMI Request Editor & Registry page:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. In the **Dynamic Applications Manager** page, find the Dynamic Application for which you want to edit a WMI request. Select its wrench icon (
- 3. Select the **[WMI Requests]** tab for the Dynamic Application.
- In the WMI Request Editor & Registry page, find the WMI request in the WMI Request Registry pane.
   Select its wrench icon (<sup>J</sup>).
- 5. The fields in the top pane are populated with values from the selected WMI request. You can edit the value of one or more fields. For a description of each field, see the section *Defining a WMI Request* in this manual.
- 6. Select the [Save] button to save your changes to the WMI request.

#### Editing a WBEM Request

You can edit a WBEM Request the same way you edit a WMI request. To view these steps, see the section *Editing* a WMI Request in this manual.

#### Deleting a WMI or WBEM Request

To delete a WMI or WBEM request in the WMI Request Editor & Registry page:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. In the **Dynamic Applications Manager** page, find the Dynamic Application for which you want to delete a WMI request or WBEM request. Select its wrench icon (
- 3. Select the [WMI Requests] tab for the Dynamic Application.
- 4. In the WMI Request Editor & Registry page, find the request you want to delete in the WMI Request Registry pane. Select its bomb icon (

Close	Properties Collections WMI Re	quests <u>T</u> hresholds	Alerts Subs	cribers	
Dynamic Applica	ations [545]   WMI Request Editor & Registry   WMI	Request Added Successfully			Guide Reset
SELECT To	WMI Request Name           Example Request           WMI Request Type           [[WMI]]           WMI Request Namespace           vmli Request Namespace	WMI Request Query WMI Request Query DM Win32_OperatingSystem	servicename [[Enabled]	WMI Object Key Active State	
		Save Save As	5		
WMI Request	WMI Reques	t Name		Type State ID WMI Enabled wmi_4	Date Edit (47   2012-06-20 18:09:4

## Chapter



#### **PowerShell Requests**

#### Overview

PowerShell Dynamic Applications must include one or more requests that define how SL1 should request data from a device. Each request specifies a PowerShell command that will gather a response from the device.

Each collection object in a PowerShell Dynamic Application is associated with a request. The collection object definition specifies which property in the response should be used to populate the values for that collection object. A single request can be used to populate multiple collection objects.

This chapter includes the following topics:

Defining a PowerShell Request	11
Editing a PowerShell Request	13
Deleting a PowerShell Request	13
Converting Legacy PowerShell Requests	14

#### Defining a PowerShell Request

To define a request for a PowerShell Dynamic Application:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Locate the Dynamic Application for which you want to define a request. Click its wrench icon (*P*). The **Dynamic Applications Properties Editor** page appears.
- 3. Click the [PowerShell] tab. The Dynamic Applications PowerShell Command Editor & Registry page appears.
- 4. Supply values in the following fields:

- PowerShell Command Name. Enter a name for the command.
- Active State. Specifies whether SL1 should perform this request during collection for this Dynamic Application. Choices are *Enabled* or *Disabled*.
- Response Object Key. This field is not currently used.
- **PowerShell Implicit Remoting**. The mechanism by which a user or application accesses PowerShell cmdlets delivered via the Exchange Management Shell. This mechanism allows Dynamic Applications of type PowerShell to connect to the remote management shell for a Microsoft application and import the cmdlets published by that Microsoft application. Choices are *Enabled* or *Disabled*. If this field is set to *Enabled*, you can reference the imported cmdlets in the **PowerShell Command Query** field.
- **Configuration Name**. Grayed out unless **PowerShell Implicit Remoting** is set to Enabled. Select from a list of configuration names for PowerShell. By default, this field includes:
  - Microsoft.PowerShell
  - Microsoft.Exchange

To enter a custom configuration name, click the plus sign icon (🐨) and enter the custom value.

- **Connection URI**. Grayed out unless **PowerShell Implicit Remoting** is set to *Enabled*. Specifies a Uniform Resource Identifier (URI) that defines the connection endpoint for the session. The URI must be fully qualified. By default, this field includes:
  - http://%D/PowerShell
  - http://%D:%P/WSMAN

**NOTE:** SL1 will replace %D with the hostname or FQDN of the Microsoft server specified in the PowerShell credential.

To enter a custom URI, click the plus sign icon (📌) and enter the custom value.

- **Cmdlets to Import**. Grayed out unless **PowerShell Implicit Remoting** is set to *Enabled*. Enter a comma-separated list of one or more PowerShell cmdlet names that you want to use in this PowerShell session. If you leave this field blank, SL1 will import all cmdlets from the remote management shell for use in this PowerShell session.
- **PowerShell Command Query**. Enter the PowerShell command to execute. The PowerShell command must meet the following requirements:
  - The command must not end with any of the Format-\* cmdlets. This includes the use of their aliases (IE. "fl" for Format-list).
  - The command must return output that can be piped to the Format-list cmdlet.
  - The command must not return whitespace over multiple lines.

- The PowerShell cmdlets you invoke must exist on the target Windows server with the required version of PowerShell.
- The PowerShell cmdlets you invoke must not write to the standard out pipe unless the output needs to be processed and put into a collection object.
- The PowerShell cmdlets you invoke must be synchronous. Do not use asynchronous cmdlets, for example, Invoke-Async or Wait-Job.
- The PowerShell cmdlets you invoke must not be an interactive cmdlet, for example, Enter-PSSession.
- The PowerShell cmdlets you invoke must not query the same property twice.
- If an invoked PowerShell cmdlet creates a new PSSession object, you must invoke the Remove-PSSession cmdlet before the original command ends.

In addition to the requirements listed above, the following best practices are recommended when developing PowerShell commands:

- Perform as much computational work in the PowerShell command as possible to reduce the workload of SL1.
- Query only the pieces of information required to populate the collection objects in the Dynamic Application.
- Per Microsoft guidelines, do not query the Win32\_Product WMI class. For more information, see <a href="http://support.microsoft.com/kb/974524">http://support.microsoft.com/kb/974524</a>.
- 5. Click the **[Save]** button.

#### Editing a PowerShell Request

To edit a PowerShell request:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. In the **Dynamic Applications Manager** page, find the Dynamic Application for which you want to edit a PowerShell request. Select its wrench icon (
- 3. Select the [PowerShell] tab for the Dynamic Application.
- 4. In the **Dynamic Applications PowerShell Command Editor & Registry** page, find the PowerShell request and select its wrench icon (
- 5. The fields in the top pane are populated with values from the selected PowerShell request. You can edit the value of one or more fields. For a description of each field, see the section *Defining a PowerShell Request* in this manual.
- 6. Select the **[Save]** button to save your changes to the PowerShell request.

#### Deleting a PowerShell Request

To delete a PowerShell request in the Dynamic Applications PowerShell Command Editor & Registry page:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. In the **Dynamic Applications Manager** page, find the Dynamic Application for which you want to delete a PowerShell request. Select its wrench icon (
- 3. Select the [PowerShell] tab for the Dynamic Application.
- 4. In the **Dynamic Applications PowerShell Command Editor & Registry** page, find the request you want to delete. Select its bomb icon (

#### Converting Legacy PowerShell Requests

The 7.3 version of SL1 supported the use of PowerShell Dynamic Applications with an SSH-based proxy. Dynamic Applications developed for the SSH-based proxy are not compatible with the "agentless" PowerShell collection introduced in the 7.5 release.

To update a Dynamic Application developed for the SSH-based proxy for use with "agentless" PowerShell collection, edit each PowerShell request in the Dynamic Application and make the following changes to the **PowerShell Command Query**:

- Remove "-Computer %s".
- Remove the "Format-List" cmdlet from the end of the command. If you are using a cmdlet that returns properties that you do not want to collect and you want to continue returning a sub-set of properties, use the "Select" cmdlet instead of "Format-List".

For example, suppose you need to update the following legacy PowerShell command:

```
Get-WmiObject -Computer %s Win32_DiskDrive | Format-List Partitions, DeviceID, Model, Size, Caption
```

The new command would be:

Get-WmiObject Win32\_DiskDrive | Select Partitions, DeviceID, Model, Size, Caption

**NOTE**: In addition to updating the PowerShell requests in the Dynamic Application, you must also use a PowerShell credential with the Dynamic Application instead of a Basic/Snippet credential.

## Chapter

## 4

### **WMI and PowerShell Collection Objects**

#### Overview

This chapter describes how to define collection objects for WMI and PowerShell Dynamic Applications.

**NOTE**: This chapter describes only the fields specific to Defining a Collection Object for a WMI or PowerShell Dynamic Application. All the remaining fields, for both performance and configuration archetypes, are described in detail in the manual **Dynamic Application Development**. All other elements of WMI and PowerShell Collection Objects, such as presentation objects and alerts, behave in the same manner as other Dynamic Application types. For details on other parts of WMI or PowerShell Dynamic Applications, see the manual **Dynamic Application Development**.

This chapter includes the following topics:

WMI-Specific Fields for Collection Objects	. 15	5
PowerShell-Specific Fields for Collection Objects	.16	5

#### WMI-Specific Fields for Collection Objects

Unlike collection objects for other Dynamic Application types, collection objects for WMI Dynamic Applications are based on WMI Requests. Because of this, collection objects for WMI Dynamic Applications have the following unique fields:

• WMI Request Arguments. When you request data from WMI or WBEM, you are requesting data from a class (table), which returns data in tabular form. In this field, you must specify the name of the property (table column) to associate with this object. This property name must be included in the WMI request, specified in the WMI Request field.

- WMI Request. Name of the WMI request associated with this object. The WMI requests in this drop-down list are defined in one of two places:
  - If No Caching or Cache Results is selected in the Caching field in the Dynamic Applications
     Properties Editor page for this Dynamic Application, this list contains all WMI Requests defined in the
     [WMI Requests] tab for this Dynamic Application. Select from the list of WMI requests defined for this
     Dynamic Application.
  - If Consume cached results is selected in the Caching drop-down list in the Dynamic Applications Properties Editor page, this list contains all WMI Requests defined in WMI Dynamic Applications that have Cache results selected in the Caching field in the Dynamic Applications Properties Editor page. Select from the list of cached WMI requests.

NOTE: If Consume cached results is selected in the **Caching** field in the **Dynamic Applications Properties Editor** page for a Dynamic Application, the **[WMI Requests]** tab is hidden and you cannot define WMI Requests for this Dynamic Application. You can only reference WMI Requests that reside in Dynamic Applications that cache results.

#### PowerShell-Specific Fields for Collection Objects

Unlike collection objects for other Dynamic Application types, collection objects for PowerShell Dynamic Applications are based on PowerShell Requests. Because of this, collection objects for PowerShell Dynamic Applications have the following unique fields:

- **PowerShell Arguments**. Enter the property that is associated with this collection object. This property must be included in the PowerShell command you select in the **PowerShell Request** field.
- **PowerShell Request**. Select the PowerShell request associated with this collection object, i.e. the PowerShell command that collects values for this collection object.

For example, suppose you have defined the following PowerShell request:

Get-WmiObject Win32\_DiskDrive | Select Partitions, DeviceID, Model, Size, Caption

This request returns the properties Partitions, DeviceID, Model, Size, and Caption. To store the values returned for each of the five properties, you would create five collection objects. For each of the five collection objects, supply the property name in the **PowerShell Arguments** field, e.g. "Partitions".

## Chapter

# 5

## **Configuring Devices for Monitoring with WMI**

#### Overview

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

Configuring WMI on Windows 2008 Servers	
Step 1: Configuring Services	
Step 2: Configuring the Windows Firewall	
Step 3: Configuring a User Account and Permissions	20
Configuring Namespace and DCOM Security Permissions	20
Configuring User Account Control to Allow Elevated Permissions	28
Configuring WMI for Windows Desktop Systems	
Step 1: Configuring Services	
Step 2: Configuring Windows Firewall	
Step 3: Setting the Default Namespace Security	
Step 4: Setting the DCOM Security Level	
Step 5: Disabling User Account Control	

#### Configuring WMI on Windows 2008 Servers

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

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

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

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

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

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

#### Step 1: Configuring Services

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

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

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

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

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

Server Manager						
File Action View Help						
🔄 🔿 🙎 📷 💁 📓 💽 🕨	▶ III II I>					
Server Manager (QA-DOM-CTRL-1)	Services					Actions
🗄 🍢 Roles	Ö. Services					Services
E Features	Services					More Actions
magnostics     for the second se	Select an item to view its description.	Name	Description Status	Startup Type	Log On As	More Actions
Gringuration     Fi (P) Task Scheduler	Select an term to view its description.	Active Directory Domain Services	AD DS Dom Started	Automatic	Local System	11
Windows Firewall with Advanced Secu		Active Directory Web Services	This servic Started	Automatic	Local System	
Services		Application Experience	Processes Started	Manual	Local System	
WMI Control		Application Identity	Determines	Manual	Local Service	
🗉 🚝 Storage		Application Information	Facilitates Started	Manual	Local System	
-	1	Application Layer Gateway Service	Provides s	Manual	Local Service	
	1	Application Management	Processes i	Manual	Local System	
	1	Background Intelligent Transfer Service	Transfers f Started	Manual	Local System	
		Base Filtering Engine	The Base F Started	Automatic	Local Service	
		Certificate Propagation	Copies use Started	Manual	Local System	
		CNG Key Isolation	The CNG k	Manual	Local System	
		COM+ Event System	Supports S Started	Automatic	Local Service	
		COM+ System Application	Manages t	Manual	Local System	
		Computer Browser	Maintains a	Disabled	Local System	
		Credential Manager	Provides s	Manual	Local System	
		Cryptographic Services	Provides fo Started	Automatic	Network S	
		DCOM Server Process Launcher	The DCOM Started	Automatic	Local System	
		Desktop Window Manager Session Manager	Provides D Started	Automatic	Local System	
		OFS Namespace	Enables vo Started	Automatic	Local System	
		OFS Replication	Enables yo Started	Automatic	Local System	
		O DHCP Client	Registers a Started	Automatic	Local Service	
		Diagnostic Policy Service	The Diagno Started	Automatic (D	Local Service	
		Diagnostic Service Host	The Diagno	Manual	Local Service	
		Diagnostic System Host	The Diagno	Manual	Local System	
		Disk Defragmenter	Provides Di	Manual	Local System	
		Distributed Link Tracking Client	Maintains I	Manual	Local System	
	1	Distributed Transaction Coordinator	Coordinate Started	Automatic (D	Network S	
	1	a DNS Client	The DNS Cl Started	Automatic	Network S	
	1	ONS Server	Enables DN Started	Automatic	Local System	
	1	Encrypting File System (EFS)	Provides th	Manual	Local System	
	1	Extensible Authentication Protocol	The Extens	Manual	Local System	
	1	File Replication Service	Synchroniz Started	Automatic	Local System	-1
( )	Extended Standard					-
	(1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.					

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

COM+ Event System	m Properties (QA-DOM-CTRL-1)	×
General Log On	Recovery Dependencies	
Service name:	EventSystem	
Display name:	COM+ Event System	
Description:	Supports System Event Notification Service (SENS), A which provides automatic distribution of events to	
Path to executable C:\Windows\syste	e: m32\svchost.exe -k LocalService	
Startup type:	Automatic	
Help me configure	service startup options.	
Service status:	Started	
Start	Stop Pause Resume	
You can specify th from here.	e start parameters that apply when you start the service	
Start parameters:		
	OK Cancel Apply	

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

#### Step 2: Configuring the Windows Firewall

To configure Windows Firewall to accept remote WMI requests, execute the following two commands at the console:

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

#### Step 3: Configuring a User Account and Permissions

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

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

#### Configuring Namespace and DCOM Security Permissions

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

To configure the Namespace and DCOM security permissions:

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

3. In the WMI Control Properties window, click the [Security] tab:

WMI Con	trol Properties			?	×
General	Backup/Restore	Security	Advanced		
Namesp	ace navigation allo	ws you to s	et namespace spe	cific security.	
±	Root				
				Security	
		OF	Cance	Арр	ly

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

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

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

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

Advanced	Security Settings for Root			_	
Owner: Permissions	Administrators (DESKTOP-SR36F Auditing	855\Administrators) C	hange		
For addition Permission e	al information, double-click a perm	nission entry. To modify	y a permission entry, select	t the entry and click Edit (if av	ailable).
Туре	Principal	Access	Inherited from	Applies to	
🚨 Allow	Administrators (DESKTOP-SR3	Special	None	This namespace and s	ubname
Allow	no_admin (DESKTOP-SR36R55	Enable Account	None	This namespace only	
Add	Remove View				
Disable in	heritance				
			[	OK Cancel	Apply

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

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

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

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

Permission	Entry for Root		-		×
Principal:	no_admin (DESKTOP-SR36R55\no_admin) Select a principal				
Type:	Allow				
Applies to:	This namespace and subnamespaces $\qquad \lor$				
Permission:	Z Execute Methods     G     Full Write     Partial Write	∑ Enable Account	[	Clear a	Π
			OK	Can	cel

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

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

Component Services			
🍖 File Action View Window I	Help		_ <del>.</del> .
🗢 🔿 🙍 🔚 🗶 🗐 🧔 😖	🛛 🗖   🎦 🗄 🏛 🏛		
Console Root	Name	Actions	
🖃 💩 Component Services	COM+ Applications	My Computer	
<ul> <li>Computers</li> <li>Image: Image is the second se</li></ul>	DCOM Config	More Actions	•
🛨 🚼 Event Viewer (Local)	Running Processes		
🕀 🎑 Services (Local)			
	7		

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

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

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

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

15. Select the [COM Security] tab:

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

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

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

#### Configuring User Account Control to Allow Elevated Permissions

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

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

#### **Option 1: Disabling User Account Control**

To disable User Account Control:

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

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

😌 User Account Control Settings		_		×
User Account Control he	e notified about changes to your computer elps prevent potentially harmful programs from making changes to Account Control settings	your computer.		
	<ul> <li>Never notify me when:</li> <li>Apps try to install software or make changes to my computer</li> <li>I make changes to Windows settings</li> </ul>			
– 💶 – Never notify	i Not recommended.			
	Фок	Cancel	]	

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

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

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

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

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

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

#### Configuring WMI for Windows Desktop Systems

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

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

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

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

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

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

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

#### Step 1: Configuring Services

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

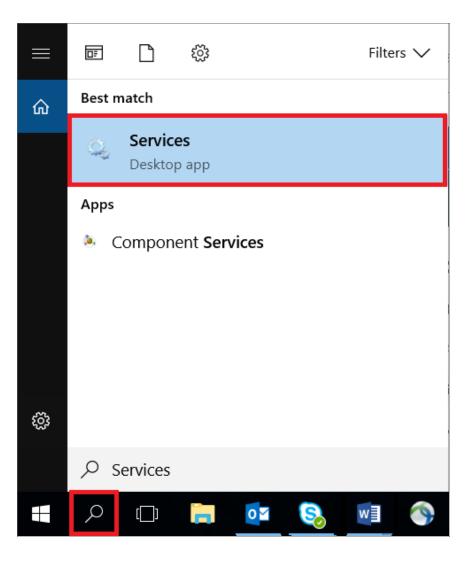
**NOTE**: ScienceLogic recommends you set all these services to start automatically.

COM+ Event System

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

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

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



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

							- [	
ile Action View	Help							
• 🔿 🗖 🐨 🤇	🗟 📑 📲 🖬 🕨 🖬 💵 🕨							
Services (Local)	Services (Local)							
	Workstation	Name	Description	Status	Startup Type	Log On As		
	Stop the service Pause the service Restart the service Description: Creates and maintains client network connections to remote servers using the SMB protocol. If this service is stopped, these connections will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.	Windows Perception Service     Windows Push Notifications System Service 1b4e     Windows Push Notifications User Service 1b4e     Windows Neuh Notifications User Service 1b4e     Windows Remote Management (WS-Managem     Windows Store Install Service     Windows Store Install Service     Windows Update     Windows Office     Windows Office     Windows Office     Windows Office     Windows Office     Workstation     Workstation     Workstation     Workstation     Xbox Scame Monitoring	Enables spat. This service -, This service -, Provides infr Windows Re. Provides infr Maintains d. Enables the WinHTTP im. The Wired A. The Wired A. The Wired A. The Wired A. The Wired A. The Wired A. The Service This service This service	Running Running Running Running Running Running	Annual (frigg_ Automatic Automatic Manual (frigg_ Manual Automatic (De. Manual Manual (frigg_ Manual Manual Automatic Manual Automatic Manual Manual Manual Manual Manual Manual (frigg_ Manual (frigg_	Local Service Local System Local System Local System Local System Local System Local System Local Service Local System Local System		
		<ul> <li>Xbox Live Auth Manager</li> <li>Xbox Live Game Save</li> <li>Xbox Live Networking Service</li> </ul>	Provides aut This service This service		Manual Manual (Trigg Manual	Local System Local System Local System		

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

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

Workstati	on Prope	erties (Local	Computer)			×
General	Log On	Recovery	Dependencies	;		
Service	name:	LanmanWo	orkstation			
Display	name:	Workstation	n			
Descript	tion:		nd maintains clie vers using the S			
Path to	executabl	e:				
C:\WIN	DOWS\Sy	stem32\svch	ost.exe -k Netw	orkService -p		-1
Startup	type:	Automatic			~	
Service	status:	Running				
S	Start	Stop	P	ause	Resume	
You car from he		he start para	meters that app	ly when you st	art the service	
Start pa	rameters:					
			014	0		1
			OK	Cancel	Apply	

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

### Step 2: Configuring Windows Firewall

To configure Windows Firewall to accept remote WMI requests:

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

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

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

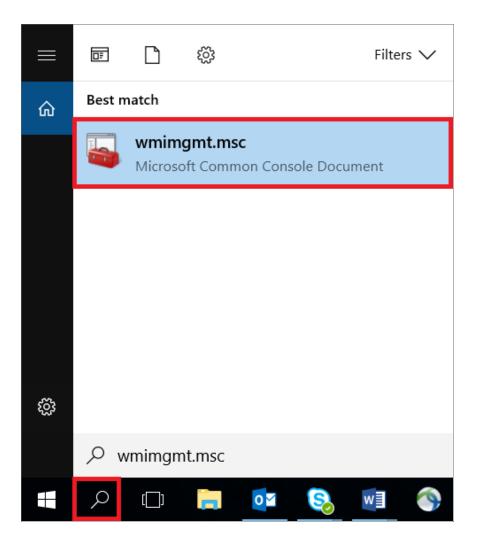
```
netsh firewall set service remoteadmin enable
netsh advfirewall firewall set rule group="remote administration" new enable=yes
```

### Step 3: Setting the Default Namespace Security

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

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

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



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

ᡖ WmiMgmt - [Console	Root\WMI Control (Local)]		-	
🚡 File Action View	Favorites Window Help			- 8 ×
🖛 🏟 🞽 📰 📓	? 📷			
Console Root			Actions	
🚔 WMI Control (Local	Connect to another computer	* Instrumentation (WMI)	WMI Control (Local)	<b>^</b>
		ws Management Instrumentation (WMI)	More Actions	•
	View New Window from Here	with wardgement instrumentation (with)		
	New Taskpad View			
	Properties			
	Help			
Opens the properties dialog	box for the current selection.		1	
i and harden and a state of the				

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

WMI Con	trol (Local) Prope	erties			?	×
General	Backup/Restore	Security	Advanced			
Namesp	ace navigation allo	ws you to s	et namespa	ce specific s	ecurity.	
···· 🔃	Root					
				Se	ecurity	
		Ok	(	Cancel	Ap	ply

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

Security for Root		×
Security Group or user names: Administrators (DESKTOP-SR no_admin (DESKTOP-SR36R		ators)
Pemissions for no_admin Execute Methods Full Write Partial Write Provider Write Enable Account Remote Enable For special pemissions or advance click Advanced.	Add Allow	Remove Deny
ОК	Cancel	Apply

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

Adv	/anced S	ecurity Settings for Root			— 🗆
Own	er:	Administrators (DESKTOP-SR3	6R55\Administrators)	Change	
Pern	nissions	Auditing			
	additiona		mission entry. To modif	y a permission entry, select	t the entry and click Edit (if available).
	Туре	Principal	Access	Inherited from	Applies to
97	Allow	Administrators (DESKTOP-SR3.	Special	None	This namespace and subname
2	Allow	no_admin (DESKTOP-SR36R55.	Enable Account	None	This namespace only
	Add isable inl	Remove Edit	]		
_					

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

Permission	Entry for Root		–
Principal:	no_admin (DESKTOP-SR36R55\no_admin) Select	a principal	
Туре:	Allow	~	
Applies to:	This namespace and subnamespaces	~	
Permission	Execute Methods	Enable Account	
	Full Write	🖂 Remote Enable	
	Partial Write Provider Write	Edit Security	
	ly these permissions to objects and/or containers w		Clear all
	y these permissions to objects and, or containers w		
			OK Cancel

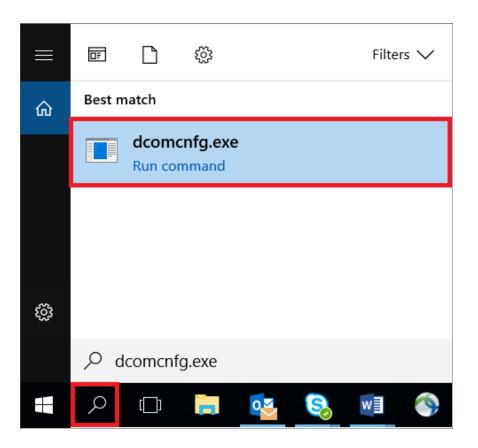
- Type. Select Allow.
- Applies to. Select This namespace and subnamespaces.
- **Permissions**. Select the Execute Methods, Full Write, Partial Write, Provider Write, Enable Account, Remote Enable, Read Security, and Edit Security checkboxes.
- 8. Click **OK** in this window and the following windows,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

### Step 4: Setting the DCOM Security Level

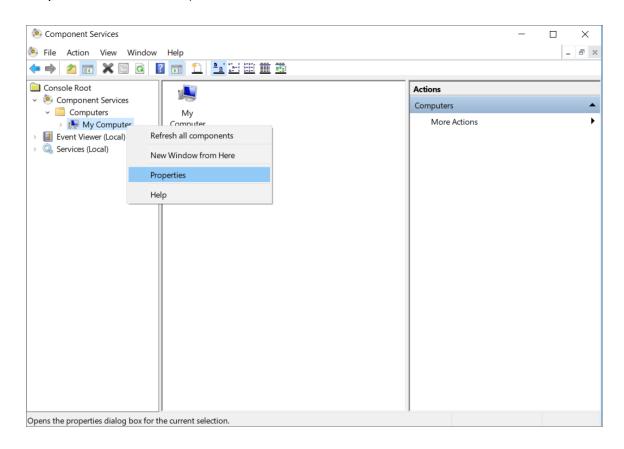
To set the DCOM Security Level, perform the following steps:

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

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



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



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

My Computer Properties			?	$\times$
Default Protocols General	COM Sec Options	urity Default Pr	MSDTC operties	
Enable Distributed COM		]		
□ Enable COM Internet Se				
Default Distributed COM The Authentication Level			Ι.	
Default Authentication	Level:			
Connect		Ť		
The impersonation level s who is calling them, and using the client's identity.	whether the applic			
Default Impersonation		_		
Identify		~		
Security for reference trac and that the default impe			on is used	
Provide additional se	curity for reference	tracking		
Learn more about <u>setting t</u>	nese properties.			
	ОК	Cancel	Арр	y

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

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

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

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

aunch and Activation Permission	1	?	$\times$
Default Security			
Group or user names:			
SYSTEM			
Administrators (SILO2461\Adr	ministrators)		
Sealer Interactive			
	Add	Remove	
Permissions for Administrators	Allow	Deny	
Permissions for Administrators			
	Allow	Deny	
Local Launch	Allow	Deny	
Local Launch Remote Launch	Allow 2 , 2 ,	Deny	
Local Launch Remote Launch Local Activation	Allow , , , , ,	Deny	
Local Launch Remote Launch Local Activation	Allow , , , , ,	Deny	
Local Launch Remote Launch Local Activation	Allow , , , , ,	Deny	
Local Launch Remote Launch Local Activation	Allow , , , , ,	Deny	
Local Launch Remote Launch Local Activation	Allow , , , , ,	Deny	

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

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

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

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

Launch and Activation Permission		? >	×
Security Limits			
Group or user names:			_
Everyone ALL APPLICATION PACKAG S-1-15-3-1024-2405443489-8 Administrators (SILO2461\Adr Performance Log Users (SILO	74036122-428603 ninistrators)		
<		>	
	Add	Remove	
Permissions for Administrators	Allow	Deny	_
Local Launch	☑.		
Remote Launch	$\checkmark$		
Local Activation			
Remote Activation			
		Cancel	

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

### Step 5: Disabling User Account Control

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

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

2. Include the following in the file .:

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

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

## Chapter



## Configuring Devices for Monitoring with PowerShell

### Overview

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

Configuring PowerShell	50
Step 1: Configuring the User Account for SL1	50
Option 1: Creating an Active Directory Account	51
Option 2: Creating a Local User Account with Administrator Access	51
Option 3: Creating a Non-Administrator Local User Account	52
Optional: Configuring the User Account for Remote PowerShell Access to Microsoft Exchange Server	53
Optional: Configuring the User Account for Remote PowerShell Access to Hyper-V Servers	54
Creating a User Group and Adding a User in Active Directory	54
Setting the Session Configuration Parameters and Group Permissions	54
Step 2: Configuring a Server Authentication Certificate	55
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate	
Option 1: Using the Microsoft Management Console to Create a Self-Signed Authentication Certificate . Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	
	58
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate	58 58
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate	58 58 <b>59</b>
Option 2: Using the MakeCert Tool to Create a Self-Signed Authentication Certificate Option 3: Using PowerShell Commands to Create a Self-Signed Authentication Certificate Step 3: Configuring Windows Remote Management	58 58 <b>59</b> 59

Step 4: Configuring a Windows Management Proxy	85
Step 5: Increasing the Number of PowerShell Dynamic Applications That Can Run Simultaneously	86
Creating a PowerShell Credential	86
Error Messages for PowerShell Collection	89

## Configuring PowerShell

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

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

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

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

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

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

## Step 1: Configuring the User Account for SL1

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

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

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

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

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

- Microsoft Exchange Server
- Hyper-V Servers

### **Option 1: Creating an Active Directory Account**

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

After creating your Active Directory account:

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

### Option 2: Creating a Local User Account with Administrator Access

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

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

After creating your local user account with Local Administrator access:

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

### Option 3: Creating a Non-Administrator Local User Account

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

After creating your domain user account or local user account:

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

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

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

winrm configsddl default

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

- Select the Execute Methods, Enable Account, and Remote Enable permission checkboxes, and then click [OK] several times to exit the windows opened for setting WMI permissions.
- 14. Restart the WMI Service from services.msc.

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

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

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

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

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

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

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

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

If you use SL1 to monitor Microsoft Exchange Servers:

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

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

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

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

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

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

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

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

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

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

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

Set-PSSessionConfiguration -ShowSecurityDescriptorUI -Name Microsoft.PowerShell

3. When prompted, select A.

4. The **Permissions** dialog appears.

PSSession Creators (MSTEST	LAB\PSSession	Creators)
Administrators (MSTESTLAB-	THE R. LEWIS CO., LANSING MICH.	and the second se
🔏 Remote Management Users (N	ISTESTLAB-HV	01\Remote .
	1	
1	Add	Bemove
emissions for PSSession		
eators	Allow	Deny
Full Control(All Operations)	~	
Read(Get, Enumerate, Subscribe)		
Write(Put.Delete.Create)		
Execute(Invoke)		
Special permissions		
	1775-	107752

- 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.

### Step 2: Configuring a Server Authentication Certificate

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

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

**NOTE:** For details on configuring WinRM on your Windows servers to use HTTPS, see https://support.microsoft.com/en-us/help/2019527/how-to-configure-winrm-for-https. The sections below describe how to configure a Server Authentication Certificate on the Windows Server. This is only one task included in configuring an HTTPS listener. However, not all users need to configure a Server Authentication Certificate. You can find out if your Windows computer has a digital certificate installed for Server Authentication by running 'Get-ChildItem -Path Cert:\LocalMachine\My -EKU "\*Server Authentication\*"' from a PowerShell command shell.

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

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

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

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

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

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

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

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

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

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

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

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

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

• For information on the MakeCert tool, see:

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

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

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

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

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

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

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

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

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

## Step 3: Configuring Windows Remote Management

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

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

There are three ways to configure Windows Remote Management:

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

#### Option 1: Using a Script to Configure Windows Remote Management

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

To use the PowerShell script, perform the following steps:

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

Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process -Force

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

8. After the warning text, select Y.

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

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

.\winrm\_configuration\_wizard.ps1 -user <domain>\<username>

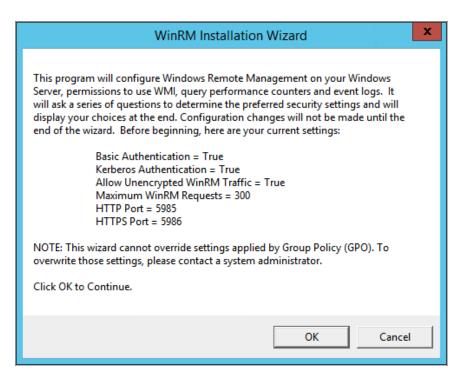
The user account you wish to use for SL1 collection must be specified with the -user command-line argument regardless of other arguments used. You can obtain the full help for the PowerShell configuration script by entering the following:

```
help .\winrm configuration wizard.ps1 -full
```

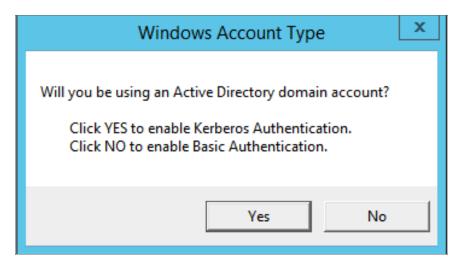
The most common way to run the script is silently:

.\winrm\_configuration\_wizard.ps1 -user <domain>\<username> -silent

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



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

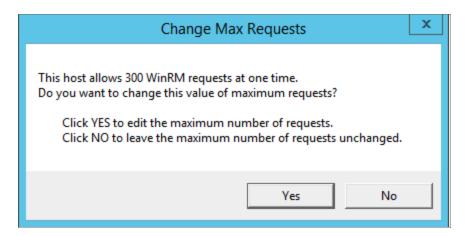


12. The Set Encryption Policy modal page appears. Select the appropriate choice for your environment.

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

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

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



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

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

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

Set HT	Set HTTP/HTTPS Ports				
New HTTP port:	5985				
New HTTPS port:	5986				
		ОК			

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

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

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

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

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

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

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

19. Exit the PowerShell session.

### Option 2: Manually Configuring Windows Remote Management

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

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

Get-ExecutionPolicy

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

Set-ExecutionPolicy RemoteSigned

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

winrm get winrm/config

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

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

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

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

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

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

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

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

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

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

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

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

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

NOTE: ScienceLogic recommends using an Active Directory account.

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

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

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

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

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

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

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

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

certutil.exe -ca.cert ca\_name.cer

C:4.	Administrator: Command Prompt	_ 0 ×
A cert[0]: 3 Valid A cert[0]: BEGIN CERTIFICATE- IIIDpTCCAo2gAwIBAgIQHAm IRUwEwYKC2Imi2PyLGQBGRY JixJTAjBgNVBAMTHEITVEW DDEIMTYINTQ1WhcNMTkwNDE WwxGTAXBg0JkiaJk/IsZAE IiUTDAxMIJyLURDLTAxLUN OIBAQCmsPONZQIJA5pxqI9 KoOWqeiuNAuh11fYFIhOsO CcWfDGuu3oVOaZU9Sgt4HE 821iGYdkbYaUOwWyKnvSOos GmtOpSZk7hsFDMxXkvRhdP XLVsMSbWNo95Nxnf8/hiUT wBBMA4GA1UdDwEB/wQEAwI JjsBuyfqH2PrforxOg/z91o QUFAAOCAQEATSkQpaWpO6i (+1RL/qkNXJeqjpDAFsz22 4rxLIw//g4SOHKSJmRYCX3 rDogF270DW9LGZ6Z7TNn1 HjdX04PG1hDj0Bg2srX+01 WF1gNeTUNHFTYuJJdEeR7Q END CERTIFICATE	Gt7EAa4tGkBmjDbtA4DANBgkqhkiG9w0BAQUFADBZ FbG9jYWwxGTAXBgoJkiaJk/IsZAEZFg1NUIRMMDEy wMTJSMi1UTDAxMlIyLURDLTAxLUNBLTEwHhcNMTOw IMTcwNTQ1WjBZMRUwEwYKCZImiZPyLGQBGRYFbG9j ZFg1NU1RMMDEyUjIxJTAjBgNVBAMTHE1TVEwwMTJS BLTEwggEiMAOGCSqGSIb3DQEBAQUAA4IBDwAwggEK ZrofUCZFaoBISpGOIJMiit+risfVAg1RgVFvc3mQK RNSOFHgUNgrasdrvugSPL/oV23VDH2dq1HaDd6azY ymPU14QkGuz1n4UTXIdepCAON37oyNkoQg01LUutp QpqAFSdFW7rgt8ObIXf9F2n13yuwogEpfeQ+E8UH4 ugH7rIONGia0xyoVuUVqfiiK748LiE/Qve0X73wBo JOPOnAgMBAAGjaTBnMBMGCSsGAQQBgjcUAgQGHgQA BhjAPBgVHRMBAF8EBTADAQH/MBOGA1UdDQMBBR9 2wDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0B 0TF+13980Is1HbT1n6AyVG7zU2MnRAWLKAxguEdha EIvei0KVCIbwEXeKePZnQG1ujr2FLRbUWt+oA0/ES ozDK8zrH0ZADV/TTrn6CEWxYaB6quQFzTQsm9wbUK 0XoKxEqUqCfR8EPFkctYrZ/+bNFV8V3YJjdAm/42g tx8mAMjAvUdNg2kvU0m0dP6h17BqJJ08umJxPmfQI hLK6KAnHw==	
:\Users\EM7Admin\Docum	ents>_	

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

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

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

<b>b</b>	Server Manager	_ <b>_</b> ×
$\frown$	Ianager   Dashboard  Welcome to SERVER MANAGER   Outck START  2 Add roles and features	C     Manage Tools View Help     Active Directory Administrative Center     Active Directory Module for Windows PowerShell     Active Directory Users and Services     Active Directory Users and Computers     ADSI Edit     Certification Authority     Component Services     Computer Management     Defragment and Optimize Drives
m Fine and storage services ⊭	Add other servers to manage      Add other servers to manage      A     Create a server group  LEARN MORE  ROLES AND SERVER GROUPS Roles: 5   Server groups: 1   Servers total: 1	Dengineria and optimize Drives DNS Event Viewer Group Policy Management Internet Information Services (IIS) Manager ISCSI Initiator Local Security Policy ODEC Data Sources (32-bit) ODEC Data Sources (32-bit) Performance Monitor
	🙀 AD CS 1 🛱 AD DS 1 🗟 DNS	Resource Monitor Security Configuration Wizard Services
	Manageability     Manageability       Events     Events       Services     Services       Performance     Performance       BPA results     BPA results	System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows Memory Diagnostic

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

	Group Policy Management						- 0 ×		
Group Policy Management Cortexts MSTIDI2ELiocal Cortexts Delegation MSTIDI2ELiocal Cortexts Delegation MSTIDI2ED Iorall MSTIDI2ED Iorall MSTIDI2ED Iorall MSTIDI2ED Iorall MSTIDI2ED Iorall MSTIDI2ED Iorall Manae Policy Management Policy Objects in MSTLD12R2.local Cortexts Delegation Manae Policy All settings diabled None Management Policy Management Polic							_ 8 ×		
Crete: MSTL0122.local     Crete: GPO in this domain, and Link it here     Crete: GPO in this domain, and Link it here     Crete: GPO in this domain, and Link it here     Crete: GPO in this domain, and Link it here     Group Policy     Group Police     Group Police     Refresh     Poperties     Help	🗢 🄿 🙍 🛅 📋	0							
Image: MSTID(7)P2/10-at     Name     A     GPO Status     WMR Ref     Modified       Image: Power     Link an Existing GPO     Enabled     None     2/4/2014       Image: Power     Link an Existing GPO     Enabled     None     2/4/2014       Image: Power     Biock Inheritance     Group Policy     All settings dasabled     None     4/16/201       Image: Power     Group Policy     Group Policy     All settings dasabled     None     4/16/201       Image: Power     Search     Change Domain Controller     Remove     All settings dasabled     None     4/16/201       Image: Power     All settings dasabled     None     Management Policy     Height Policy     Hei	A Forest: MSTL012R2.local     A      Domains								
Image: Point			Name	•	GPO Status	WMI Filter	Modified		
Power Points Refresh Heip       Image Power Points     Link an Existing GPO     Py     Enabled Mone     2/4/201       Image Power Points     Block Inheritance     All settings disabled     None     4/16/201       Image Power Points     Refresh     Properties     Heip     Heip     Heip			d Link it here						
Image: Start     Group Policy Modeling Wizard       Image: Start     New Organizational Unit       Image: Start     Search       Image: Start     Change Domain Controller       Remove     Active Directory Users and Computers       New Window from Here     Properties       Image: Help     Help	ji Powi ⊳ 📮 Dom				All settings disabled	None	4/17/201		
Image: Group Polic     Search       Group Polic     Group Polic       Active Directory Users and Computers       New Window from Here       Refresh       Properties       Help	Þ 🎒 WMI Þ 🧊 Start								
Refresh       Properties       Help	R Group Polic	Change Domain Controller Remove	puters						
Properties Help		New Window from Here							
Help		Refresh							
		Properties							
		Help							
			<		ш		>		
Treate a GPO in this domain and link it to this container									

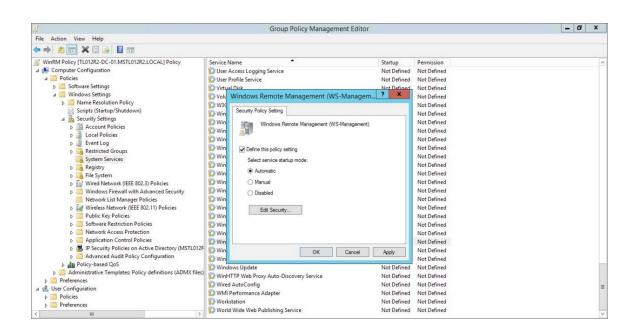
9. In the left panel, right-click the new group policy and select *Edit*. The **Group Policy Management Editor** page for the new Windows Remote Management group policy appears.

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

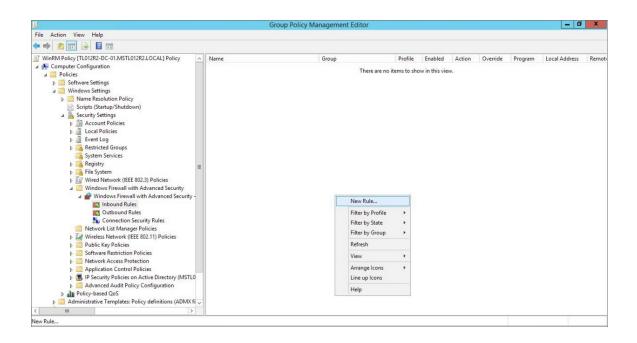
 In the left panel, navigate to Computer Configuration > Policies > Windows Settings > Security Settings > System Services. In the right panel, locate the Windows Remote Management (WS-Management) service. Right-click the service, then select Properties.

	Group Pol	icy Management Editor	r		_ 0
le Action View Help					
🔿 🖄 📷 🗶 🖼 💀 📓					
WinRM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy	Service Name		Startup	Permission	
👰 Computer Configuration	🗱 User Access Logging Service		Not Defined	Not Defined	
a 🧮 Policies	User Profile Service		Not Defined	Not Defined	
Software Settings	🗱 Virtual Disk		Not Defined	Not Defined	
⊿ 🧾 Windows Settings	🗱 Volume Shadow Copy		Not Defined	Not Defined	
Name Resolution Policy	W3C Logging Service		Not Defined	Not Defined	
Scripts (Startup/Shutdown)	Windows Audio		Not Defined	Not Defined	
A Security Settings	Windows Audio Endpoint Builder		Not Defined	Not Defined	
Account Policies     Account Policies	Windows Color System		Not Defined	Not Defined	
	Windows Connection Manager		Not Defined	Not Defined	
Event Log Restricted Groups	Windows Driver Foundation - User	mode Driver Framework	Not Defined	Not Defined	
System Services	Windows Encryption Provider Host Service Windows Error Reporting Service Windows Event Collector Windows Event Loa		Not Defined	Not Defined	
> Registry			Not Defined	Not Defined	
File System			Not Defined	Not Defined	
Wired Network (IEEE 802.3) Policies			Not Defined	Not Defined	
Windows Firewall with Advanced Security	Windows Firewall		Not Defined	Not Defined	
Network List Manager Policies	Windows Font Cache Service		Not Defined	Not Defined	
	Windows Installer		Not Defined	Not Defined	
Public Key Policies	Windows Management Instrument	ation	Not Defined	Not Defined	
Software Restriction Policies	Windows Modules Installer		Not Defined	Not Defined	
Network Access Protection	Windows Process Activation Service	e	Not Defined	Not Defined	
Application Control Policies	Windows Remote Management A	(teemeet 2)	Not Defined	Not Defined	
IP Security Policies on Active Directory (MSTL012F)	Windows Store Service (WSServi	Properties	Not Defined	Not Defined	
Advanced Audit Policy Configuration	Windows Time	Help	Not Defined	Not Defined	
Policy-based QoS	Windows Update	(1) (1) (1)	Not Defined	Not Defined	
Administrative Templates: Policy definitions (ADMX files)	WinHTTP Web Proxy Auto-Discove	ry Service	Not Defined	Not Defined	
Preferences	Wired AutoConfig		Not Defined	Not Defined	
User Configuration     Policies	WMI Performance Adapter		Not Defined	Not Defined	
Policies     Preferences	Workstation		Not Defined	Not Defined	
	World Wide Web Publishing Servic	e	Not Defined	Not Defined	
ш >					

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



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



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

J		Group Policy Management Edito	r						- 0	x
	View Help									
🗢 🔿 🖄										
WinRM Pe MinRM Pe Comp     MinRM Pe     MinR	<i>2</i>	New Inbound Rule Wizard	x	Profile	Enabled	Action	Override	Program	Local Address	Remot
4 🧾 Po				ems to show	v in this vie	w.				
	Select the type of firewall rule	to create.								
Þ	Steps:									
4	Rule Type	What type of rule would you like to create?								
	Predefined Rules									
	<ul> <li>Action</li> </ul>	<ul> <li>Program</li> <li>Rule that controls connections for a program.</li> </ul>								
		O Port								
		Rule that controls connections for a TCP or UDP port.								
		Predefined:								
		Windows Firewall Remote Management								
		Rule that controls connections for a Windows experience.								
		O Custom								
		Custom rule.								
Þ Þ 🚞		< Back Next > Canc	al l							
<		Cook IVEX > Cark								
			_							

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

J		C	Group Policy	Manageme	ent Editor							- 0	x
File Action	View Help												
WinRM P		New Inbound Rule Wizard				x	Profile	Enabled	Action	Override	Program	Local Address	Remot
⊿ 🌺 Comp ⊿ 🧰 Po ▷ 📫 ⊿ 🧰	Predefined Rules Select the rules to be created for	or this experience.					ems to sho	w in this vie	w.				
Þ	Steps:		Which rules would you like to create?										
4	<ul> <li>Rule Type</li> </ul>												
	Predefined Rules	The following rules define network connectivity requi	The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of										
	<ul> <li>Action</li> </ul>	the existing rule will be overwritten.		Chocked, are co									
		Name	Rule Exists	Profile	Desc								
		Windows Frewall Remote Management (RPC.     Windows Frewall Remote Management (RPC)		Al Al	inbou Inbou								
		<			>								
¢		C	< Back	Next >	Cancel								

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

J		Group Policy Management Editor							- 0	x
File Action	View Help									
	📅 🔒 🕜 🎞									
WinRM Pe	<b>@</b>	New Inbound Rule Wizard	x	Profile	Enabled	Action	Override	Program	Local Address	Remot
▲ ₩ Comp	Action	When a connection matches the conditions specified in the rule.  What action should be taken when a connection matches the specified conditions?      More the connection This includes connections that are protected with IPsec as well as those are not.      More the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be accured using the settings in IPsec properties and rules in the Connection Security Rule node.      Block the connection		ems to sh	w in this vie	w.				
4		< Back Pnish Cance								

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.

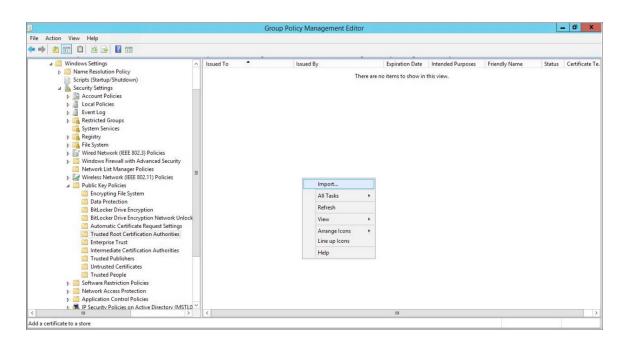
17. The Automatic Certificate Request Setup Wizard modal page appears. Click [Next].

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

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

Automatic Certin	cate Request Setup Wizard	Group Policy Management Editor	- 0
ertificate Template The next time a computer logs on, a provided.	certificate based on the template you select is	P request	
A certificate template is a set of pred computers. Select a template from th Certificate templates:	fined properties for certificates issued to following list.	There are no items to show in this view.	
Name Computer Domain Controller Errollment Agent (Computer) IPSec	Intended Purposes Client Authentication, Server Authentication Client Authentication, Server Authentication Certificate Request Agent IP security IKE intermediate		
< 11	>		
	< Back Next > Cancel ncryption ncryption Network Unlock icate Request Settings		
	tification Authorities		
📔 Enterprise Trust			

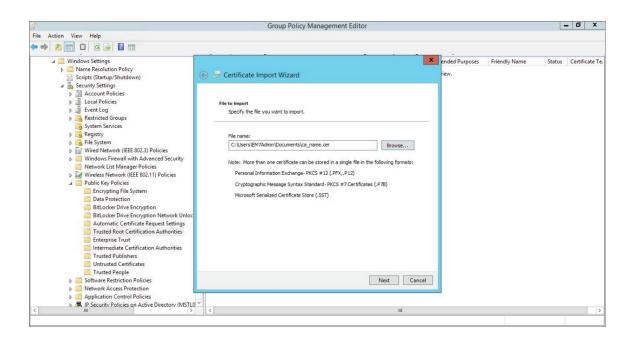
19. In the left panel of the Group Policy Management Editor page, navigate to Computer Configuration
 > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification
 Authorities. In the right panel, right-click and select Import.



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

J	Group Policy Ma	nagement Editor			L	- 0	x
ile Action View Help							
▲      ▲      Windows Settings     ↓      ■ Name Resolution Policy     ☆ Scripts (Startup/Shutdown)     ▲      ➡ Security Settings	) 😼 Certificate Import Wizard		ended Pu	rposes Friendly Name	e Status	Certifi	icate Te
<ul> <li>Account Policies</li> <li>Local Policies</li> <li>Local Policies</li> <li>Event Log</li> <li>Restricted Groups</li> </ul>	Welcome to the Certificate	Import Wizard					
iii System Services ▷ iii Registry ▷ iii System ▷ iii Wired Network (IEEE 802.3) Policies	lists from your disk to a certificate store.	tificate trust lists, and certificate revocation					
Wind vetwork (iEE 00:3) Pointes     Windows Firewall with Advanced Security     Metwork List Manager Policies     Wireless Network (IEEE 802.11) Policies	and contains information used to protect d connections. A certificate store is the syste	on authority, is a confirmation of your identity ata or to establish secure network m area where certificates are kept.					
Public Key Policies Encrypting File System Data Protection	Store Location Current User Local Machine						
BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc	To continue, dick Next,						
Automatic Cettificate Request Settings Tusted Root Cettification Authorities Intermediate Cettification Authorities Tusted Publishers Tusted Qublishers Tusted Qublishers Tusted Qublishers Tusted Qublishers Tusted Qublishers							
Software Restriction Policies     Tosteo People     Software Restriction Policies     Software Restriction		Next Cano	el				
Application Control Policies      B. IP Security Policies on Active Directory (MSTL0							
	<	ш				_	>

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



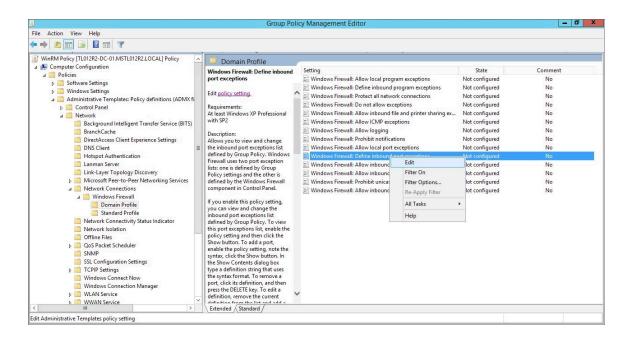
22. Select the **Place all certificates in the following store** radio button, then select the Trusted Root Certification Authorities certificate store and click [Next].

<b>B</b>	Group Policy Management Editor			Ŀ	- 0	x
File       Action       View       Help         Image: Second Sec	Certificate Store Certificate Store Certificate stores are system areas where certificates are kept. Windows can automatically select a certificate store, or you can specify a location for the certificate. Windows can automatically select the certificate store, or you can specify a location for the certificate store Automatically select the certificate store based on the type of certificate Place all certificates in the following store Certificate store: Trusted Root Certification Authorities Browse	ended Purposes view.	Friendly Name	Status	Certific	
	V Cancel					>

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

	Group Policy Management Editor	_ 0 ×
le Action View Help		
• 🔿 🙍 🖬 🗎 💁 📓 🖬		
▲      ■ Windows Settings     ▶      ■ Name Resolution Policy      B Scripts (Startup/Shutdown)     ▲      ▶ Security Settings		ended Purposes Friendly Name Status Certificate Tr     iew.
Account Policies     Galacal Policies     Galacal Policies     Galacal Policies     Galacada Control Contro Control Control Contro Control Control Contro	Completing the Certificate Import Wizard	
<ul> <li>System Services</li> <li>Registry</li> <li>File System</li> </ul>	The certificate will be imported after you click Finish. You have specified the following settings:	
<ul> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Security</li> </ul>	Certificate Store Selected by User Trusted Root Certification Authorities Continue Store Selected by User Trusted Root Certification Authorities	
<ul> <li>Network List Manager Policies</li> <li>Wireless Network (IEEE 802.11) Policies</li> <li>Public Key Policies</li> <li>Encrypting File System</li> </ul>	File Name C: Users/EM7Admin/Documents/ca_name.cer	
Data Protection BitLocker Drive Encryption BitLocker Drive Encryption Network Unloc		
Automatic Certificate Request Settings Trusted Root Certification Authorities Enterprise Trust		
<ul> <li>Intermediate Certification Authorities</li> <li>Trusted Publishers</li> <li>Untrusted Certificates</li> <li>Trusted People</li> </ul>		
Fusted People Software Restriction Policies	Finish Cano	cel
Network Access Protection		
Application Control Policies		
IP Security Policies on Active Directory (MSTL0)		(

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

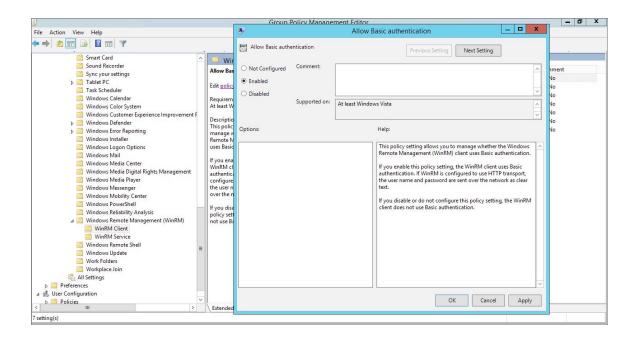


25. The Windows Firewall: Define inbound port exceptions modal page appears. Under Options, click [Show].

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

<u>.</u>	Group Policy Management Editor	_ 0 ×
File Action View H	Se Windows Firewall: Define inbound port exceptions	
🔶 🌒 🙎 🔜 💽	Windows Firewall: Define inbound port exceptions Previous Setting Next Setting	
WinRM Policy [TL01: ▲ Computer Config ▲ Policies ↓ Software S ↓ Sof	Value     V	ot configured No ot configured No
▶ 🚰 TC 🚞 Wi 🚞 Wi	Subnet descriptions, such as 10.2.3.0/24     v       <	
↓ 1	OK Cancel Apply	

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



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

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

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

<u>.</u>	Group	Policy Manage	jement Editor	- 8 ×
File Action View Help			Allow Basic authentication	x
<ul> <li></li></ul>		entication Comment:	Previous Setting Next Setting	ment
Sync your setungs     Table PC     Task Scheduler     Windows Calendar     Windows Customer Experience Improvement F     Windows Customer Experience Improvement F	<ul> <li>Enabled</li> <li>Disabled</li> </ul>	Supported on:	X At least Windows Vista	<ul> <li>∧ ment</li> <li>√ ko</li> <li>√ ko</li> <li>√ ko</li> <li>√ ko</li> <li>√ ko</li> <li>√ ko</li> </ul>
<ul> <li>▶ Windows Strof Reporting</li> <li>Windows Strof Reporting</li> <li>Windows Strof Reporting</li> <li>Windows Installer</li> <li>Windows Logan Options</li> <li>Windows Media Digtal Rights Management</li> <li>Windows Media Digtal Rights Management</li> <li>Windows Media Payer</li> <li>Windows Resenger</li> <li>Windows Relability Analysis</li> <li>Windows Remote Nanagement (WinRM)</li> <li>Windows Remote Nanagement (WinRM)</li> <li>Windows Remote Shell</li> <li>Work Folders</li> </ul>	Options:		Help:         This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client.         If you enable this policy setting, the WinRM service accepts Basic authentication from a remote client.         If you disable or do not configure this policy setting, the WinRM service does not accept Basic authentication from a remote client.	Чo
b Policies     C Extended     ID setting(s)			OK Cancel Apply	

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

	Group Policy Management Editor – 🗖	x
File Action View Help	Allow remote server management through WinRM 📃 🗖 🗙	
	Allow compto concer management through WigPM	
Smart Card Sund Recorder Syncy our settings ) Tablet PC Task Scheduler Windows Color System Windows Color System Windows Customer Experience Improvement F ) Windows Customer Experience Improvement F Windows Customer Experience Improvement F Windows Nedia Digital Rights Management Windows Media Digital Rights Management Windows Redia Digital Rights Management Windows Update Windows Remote Shell Windows Remote Shell	Previous Setting     Not Configured     Comment:     Onto Configured     Comment:     Onto Configured     Supported on:     At least Windows Vista     Options:     At least Windows Vista     Options:     Help:     Disabled     Options:     Help:     This policy setting allows you to manage whether the Windows     No     No     Pu6 filter:     Image:     Junction     Junction	
10 setting(s)		

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

<b>1</b>	Group Pol	icy Management Edit	or		- 0 ×
File Action View Help					
🗢 🔿 🙆 🛅 📾 🙆 📾 📓 🖬 🙆 🛇 🛨					
WinFM Policy (TL0)222-DC-01.MSTL01222.LOCAL] Policy         ▲ Policies         ▶ Software Settings         ▶ Windows Settings         ▶ Windows Settings         ▶ Mindows Settings         ■ Preferences         ■ Windows Settings         ■ Preferences         ■ Windows Settings         ■ Network Shares         ■ Software         ■ Softwares         ■ Policies         ▶ Policies         ▶ Preferences	Processing (* Processing (*) Processing (*)	Neme	Order Action Hive There are n All Tasks • Paste Refresh Kefresh Une up kons Help	Key no items to show in this view. Registry Item Collection Item Registry Wizard	Value Name Typ
< III >	Preferences / Extended / Standard	1			
Add a new registry item					

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

WinRM Policy (TL012R2-DC-01 MSTL012R2.LOCAL) Policy     WinRM Policy (TL012R2-DC-01 MSTL012R2.LOCAL) Policy     Police     Police     Police     Police     Police     Policy definitions (ADMX file     Poli		Group Policy Management Editor	- 0 X
WinRM Adicy (TU012R2-DC-01.MSTU012R2.LOCAL) Policy         WinRM Adicy (TU012R2-DC-01.MSTU012R2.LOCAL) Policy         Preferences         Preferences         Preferences         Windows Settings         Files         Freidering         Freidering         Preferences         Windows Settings         Windows Settings         Freidering         Freidering         Freidering         Freidering         Preferences         Windows Settings         Windows Settings         Freidering         Freidering         Freidering         Freidering         Wendows Settings         Wendows Settings         Freidering         Freidering         Freidering         Stortcuts         Stortcuts         Peloicie         Preferences         Value type:         REG_DWORD         Value data:         Base         Hexadecinal         Peterences / Estended / Standard /	File Action View Help		
Computer Configuration Computer Configuration Configuration Control Panel Settings Control Panel Settings Control Panel Settings Preferences Value type: Registry Value type: Registry Registry Value type: Registry Value type: Registry Value type: Registry Walke type: Registry Value type: Registry Walke type: Registry Value type: Registry Walke type: Registry Walke type: Registry Value type: Registry Walke type: Registry Registry Registry Registry Reg	🗢 🔿 📶 📋 🛲 🖬 🗟 🖬 🔤		
< III > Preferences / Extended > Standard /	WinRM Policy (TL012R2-DC-01.MSTL012R2LOCAL) Policy         ▲ Computer Configuration         ▲ Policies         ▶ Software Settings         ▶ Windows Settings         ▶ Preferences         ■ Windows Settings         ■ Preferences         ■ Windows Settings         ■ Freferences         ■ Windows Settings         ■ Freferences         ■ Preferences         ■ Preferences         ■ Stricts         ■ IniFiles         ■ Network Shares         ■ Control Panel Settings         ■ Control Panel Settings         ■ Control Panel Settings         ■ Control Panel Settings	Pr     New Registry Properties     X       Hive     Key       Action:     Create       Value     HKEY_LOCAL_MACHINE       Value     Value       Value     SOFTWARE/Nerrosoft/Windows/CurrentVersio       Value     Nerrosoft/Windows/CurrentVersio       Value     REG_DWORD       Value     4	Value Name Typ
			>
		\Preferences \Extended \Standard /	

- 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.

File Action View Help  WinNAM Policy [TL012R2-DC-01.MSTL012R2.LOCAL] Policy  Computer Configuration  Policies  Policies  Policies  Policies  Pocessing  Name Order Action Startup Account Interactive Recovery  Processing  Pocessing  Pocessing  Pocessing  Pocessing  Pocessing  Pocessing  Name Order Action Startup Account Interactive Recovery  Pocessing  Name Order Action Startup Account Interactive Recovery  Pocessing  Pocessing  Pocessing  Pocessing  Pocessing  Pocessing  Pocessing  Pocessing  Name Order Action Startup Account Interactive Recovery  Pocessing  Pocessing  Name Order Action Startup Account Interactive Recovery  Pocessing  Pocessing  Name Order Action Startup Account Interactive Recovery  Pocessing  Pocessing  Name Order Action Startup Account Interactive Recovery  Pocessing  Pocessi		Group Pol	icy Management	Editor				- 0
WinRM Pholicy [T1012R2-DC-01.MSTL012R2.L0CAL] Policy WinRM Pholics P Software Settings P Software Settings P Generations P Frederences Processing Processing Name Order Action Startup Account Interactive Recovery There are no items to show in this view. Processing Name Order Action Startup Account Interactive Recovery There are no items to show in this view. Processing Name Order Action Startup Account Interactive Recovery There are no items to show in this view. Processing Name Order Action Startup Account Interactive Recovery There are no items to show in this view. Processing Name Order Action Startup Account Interactive Recovery There are no items to show in this view. Processing Name Name Order Action Startup Account Interactive Recovery There are no items to show in this view.	File Action View Help							
<ul> <li>Computer Configuration</li> <li>Policies</li> <li>Software Settings</li> <li>Software Settings</li> <li>Software Settings</li> <li>Control Panel Settings</li> <li>Network Options</li> <li>Scheduled Tasks</li> <li>Scheduled Tasks</li> <li>Policies selected</li> <li>No policies selected</li> <li>No policies selected</li> <li>View +</li> <li>Arrange Icons +</li> </ul>	• 🔿 🙍 🛅 📋 📾 🖬 📓 🖬 🖄 🔕 🔸							
Line up Icons Help	<ul> <li>WinRM Policy [L1012R2-DC-01.MSTL012R2.LOCAL] Policy</li> <li>WonRM Policy (L1012R2-DC-01.MSTL012R2.LOCAL] Policy</li> <li>Policies</li> <li>Software Settings</li> <li>Doi: Windows Settings</li> <li>Preferences</li> <li>Preferences</li> <li>Preferences</li> <li>Doi: Windows Settings</li> <li>Doi: Contol Panel Settings</li> <li>Data Sources</li> <li>Doi: Doitol Panel Settings</li> <li>Doices</li> <li>Policies</li> <li>Power Options</li> <li>Power Options</li> <li>Power Options</li> <li>Scheduled Tasks</li> <li>Services</li> <li>Ver Configuration</li> <li>Poincies</li> </ul>	Processing (*)	Name	New         Image: Constraint of the second sec	Service		Recovery	
	< III > 1	Preferences $\sqrt{\text{Extended }}$ Standard	/					

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

File     Action     View     Help       Image: State of the state of		-	
WinRM Policy [TL012R2-DC-01.MSTL012R2LOCAL] Policy			
M Compute Configuration     Policies     Policies     Policies     Policies     Porterences     Policies     Porterences     Policies     Po	Interactive	Recovery	
< III > Preferences / Extended > Standard / Services			

• Startup. Select No change.

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

File Action View Help     Image: Computer Configuration     Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Image: Computer Configuration   Im	₽	Group Policy Management Editor	- 0 X
Compute Configuration     Policies     Software Settings     Software Settings			
(Therefore Administry	<ul> <li>Computer Configuration</li> <li>Policies</li> <li>Stotware Settings</li> <li>Windows Settings</li> <li>Ministrative Templates: Policy definitions (ADMX files)</li> <li>Preferences</li> <li>Windows Settings</li> <li>Control Panel Settings</li> <li>Devices</li> <li>Control Panel Settings</li> <li>Devices</li> <li>Local Users and Groups</li> <li>Network Options</li> <li>Power Options</li> <li>Scheduled Tasks</li> <li>Services</li> <li>Mer Configuration</li> <li>Devices</li> </ul>	New Service Properties       X       Startup       Account       Interactive       Recover         General       Recovery       Common       Select the computer's response if this service fails.       If a service is service fails.       If a service is service fails.       If a service is service fails.         First failure:       Restart the Service       V         Subsequent failures:       Restart the Service       V         Restart failures:       Restart the Service       V         Restart failures:       Restart the Service       V         Restart service after:       1 ⊕ minutes         Program:	1
	< III > \ Services	Preferences / Extended / Standard /	

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

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

<u>.</u>	Group Policy Management	- 0 X
🔣 File Action View Window Help		_ 8 ×
🗢 🔿 🙍 🖬 🤷 🛛 🗊		
📓 Group Policy Management	PowerShell Remote Management Policy	
▲ ▲ Forest: MSTL012R2.local	Scope Details Settings Delegation	
▲ Commains ▲ MSTL012R2.local	Links	
Default Domain Policy	Display links in this location: MSTL012R2.local	~
PowerShell Remote Management Policy	The following stes, domains, and OUs are linked to this GPO:	
WinRM Policy Controllers	Location Enforced Link Enabled Path	
<ul> <li>I Domain Controllers</li> <li>Group Policy Objects</li> </ul>	MSTL012R2/acai No Yes MSTL012R2/acai	
WMI Filters	Enforced	
Starter GPOs	Link Enabled	
Sites	Delete Link(s)	
Group Policy Modeling Group Policy Results		
Coup Forcy Results		
	Security Filtering	
	The settings in this GPO can only apply to the following groups, users, and computers:	
	Name	
	& Authenticated Users	
	Add Remove Properties	
	WMI Filtering This GPO is linked to the following WMI filter:	
	(none) V Open	

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

Group Policy Management							
🔜 File Action View Window Help		_ 8 ×					
🗢 🔿 🙍 🔁 🗎 🗶 💁 👘							
Group Policy Management     A	WinRM Policy           Scope Details         Settings         Delegation         Status           Unkes         Delegation:         MSTL012R2.local           The following ates, domains, and OUs are linked to this GPO:         Status GPO:	v					
Vinite Foury     Group Policy Objects     Group Policy Objects     Default Domain Controllers Policy     Default Domain Policy     PowerShell Remote Management Polic     WinRM Police	Location A Enforced Link Enabled Path						
WinRM S Edit							
WMI Filters GPO Status	► V Enabled						
<ul> <li>▷ (m) Starter GPOs</li> <li>▷ (m) Sites</li> <li>Back Up</li> <li>Back Up</li> <li>Restore from Backup</li> <li>Group Policy Result</li> <li>Import Settings</li> <li>Save Report</li> </ul>	User Configuration Settings Disabled Computer Configuration Settings Disabled All Settings Disabled The lucase views						
View New Window from He							
Copy Delete Rename Refresh	Add Propeties						
Help	C is linked to the following WMI filter:						
< 111	(none> Y Open						
< III > All settings enabled							

# Step 4: Configuring a Windows Management Proxy

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

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

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

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

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

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

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

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

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

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

To do so:

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

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

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

Restart-Service WinRM

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

### Creating a PowerShell Credential

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

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

To define a PowerShell credential in SL1:

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

dential Management   Credentia													roato SM	MP Credentia	
		RO	RW	DA										abase Crede	
Profile Name *	Organization	ROUse	Use	DA Use	Type	Credential User		Host	Port	Timeout (ms	<u>s) ID</u>	135			
												AI	reate SO	AP/XML Host	Crede
Amazon Web Services Credential	👔 System				SOAP/XML Host	[ AWS Account Access ]	example.com		80	2000	1	2015-05-18			
Azure Credential - SOAP/XML	👔 [all orgs]				SOAP/XML Host	<ad_user></ad_user>	login.windows.net		443	60000	60	2015-05-14	reate Bas	ic/Snippet Cr	redenti
Azure Credential - SSH/Key	[all orgs]				SSH/Key	<subscription_id_h< td=""><td>%D</td><td></td><td>22</td><td>180000</td><td>59</td><td>2015-05-14</td><td>reate SSI</td><td>H/Key Creder</td><td>fial</td></subscription_id_h<>	%D		22	180000	59	2015-05-14	reate SSI	H/Key Creder	fial
A Cisco SNMPv2 - Example	[all orgs]				SNMP				161	1500	3	2015-05-		verShell Cred	
P Cisco SNMPv3 - Example	(all orgs)				SNMP	[USER_GOES_HERE]			161	1500	2	2015-05-4			
A Cisco: ACI	🚯 [all orgs]			126	Basic/Snippet	admin	173.36.219.46		443	0	62	2015-05-14 15	05:24	:m7admin	
A Cisco: ACI Credential	(all orgs]				Basic/Snippet	admin	198.18.133.200		443	0	61	2015-05-14 14	32.20 6	m7admin	
P Cloudkick - Example	[all orgs]				Basic/Snippet	(SECURITY KEY GOES	127.0.0.1		443	5000	9	2015-05-14 11	25:31 e	em7admin	
CUCM PerfmonService 8.0 Example	(all orgs)				SOAP/XML Host		%D		8443	2000	4	2015-05-14 11	:25:12 e	em7admin	
P EM7 Central Database	[all orgs]				Database	root	localhost		7706	0	51	2015-05-14 11	26:41 6	m7admin	
A EM7 Collector Database	(all orgs)				Database	root	%D		7707	0	14	2015-05-14 11	25:43 6	m7admin	
A EM7 DB	(all orgs)				Database	root	%D		7706	0	35	2015-05-14 11	26:32 e	em7admin	
PEM7 DB - DB Info	(all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 11	26:32 0	em7admin	
PEM7 DB - My.cnf	[all orgs]				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 11	26:32 6	m7admin	
A EM7 DB - Silo.conf	(all orgs)				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 11	26:32 6	m7admin	
EM7 Default V2	(all orgs)				SNMP				161	1500	10	2015-05-14 11	25:42 e	em7admin	
P EM7 Default V3	(all orgs)				SNMP	em7defaultv3			161	500	11	2015-05-14 11	25:42 0	em7admin	
P EMC - Example	[all orgs]				Basic/Snippet	root	%D		443	10000	15	2015-05-14 11	25:47 6	m7admin	
@ GoGrid - Example	(all orgs)				Basic/Snippet	(SECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 11	25:51 6	m7admin	
PIPSLA Example	all orgs]				SNMP	-			161	1500	5	2015-05-14 11	25:14	m7admin	
P LifeSize: Endpoint SNMP	(all orgs)				SNMP	control			161	3000	18	2015-05-14 11	25:58	m7admin	
P LifeSize: Endpoint SSH/CLI	[all orgs]				Basic/Snippet	auto	%D		22	3	17	2015-05-14 11	25:58 6	m7admin	
(A Local API	(all orgs)				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 11	26:11 6	m7admin	
NetApp 7-mode	(all orgs)				Basic/Snippet	root	%D		443	3000	24	2015-05-14 11	26:20	m7admin	
A NetApp w/SSL Option	(all orgs)				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 11	26:20	m7admin	
P NetApp w/SSL Option Off	(all orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 11	26:20 6	m7admin	
A Nexus netconf	(all orgs)				Basic/Snippet		%D		22	10000	6	2015-05-14 11	25:16 6	m7admin	
A Nexus snmp	(all orgs)				SNMP				161	10000	7	2015-05-14 11	25:16	em7admin	
Polycom - Advanced	[all orgs]				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 11	26:24 (	m7admin	
Polycom - CDR	all orgs]				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 11	26:24 6	m7admin	
Polycom - Interface	(all orgs)				SOAP/XML Host	admin	%D		80	20000	29	2015-05-14 11	26:24 6	em7admin	

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

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

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

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

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

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

# Error Messages for PowerShell Collection

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

Error Message	Possible Issue(s)
Preauthentication failed while getting initial credentials	Incorrect Password (Active Directory Accounts only)
Client not found in Kerberos database	Username does not exist in Active Directory (Active Directory Accounts only)
KRB5 error code 68 while getting initial credentials	Incorrect domain name (Active Directory Accounts only)

Error Message	Possible Issue(s)
Bad HTTP response returned from server. Code 401, basic auth failed	Incorrect username/password or target server does not allow user account to perform WinRM operations.
ParseError	Incorrect port specified in credential
[Errno 111] Connection refused	Mismatch between server configuration and credential, e.g. encryption option selected but not enabled on server.
Hostname cannot be canonicalized	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
Cannot resolve network address for KDC in requested realm	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
Configuration file does not specify default realm	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
No credentials cache found	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance
Server not found in Kerbers database	Forward and/or reverse name resolution are not working from the Data Collector or All-In-One Appliance

# Chapter

# 7

# **Concurrent PowerShell Collection**

### Overview

This chapter describes how to configure and use concurrent PowerShell collection.

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

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

This chapter covers the following topics:

# Enabling and Disabling Concurrent PowerShell for Collector Groups

To improve the process of collecting data via PowerShell, you can enable Concurrent PowerShell Collection. Concurrent PowerShell Collection allows multiple collection tasks to run at the same time with a reduced load on Data Collectors. Concurrent PowerShell Collection also prevents missed polls and data gaps because collection will execute more quickly. As a result, Data Collectors can collect more data using fewer system resources.

When you use the PowerShell Collector for Concurrent PowerShell Collection, the collection process can bypass failed or paused collections, reduce collection time, and reduce the number of early terminations (sigterms) that occur with data collection. The PowerShell Collector is an independent service running as a container on a Data Collector.

You can enable one or more Collector Groups to use concurrent PowerShell collection, and you can collect metrics for concurrent PowerShell collection.

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

### Enabling Concurrent PowerShell on All Collector Groups

To enable concurrent PowerShell collection service for all collector groups:

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

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

### Disabling Concurrent PowerShell on All Collector Groups

To disable concurrent PowerShell collection service for all collector groups:

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

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

#### Enabling Concurrent PowerShell on a Specific Collector Group

To enable concurrent PowerShell collection for a specific collector group:

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

```
INSERT INTO master.system_custom_config (`field`, `field_value`, `cug_filter`)
VALUES ('enable_powershell_service_CUGx', '1', 'collector_group_ID');
```

where:

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

#### Disabling Concurrent PowerShell on a Specific Collector Group

To disable concurrent PowerShell collection for a specific collector group:

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

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

where:

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

# Chapter



# **Credentials for WMI and PowerShell Devices**

### Overview

This chapter describes how to configure credentials for WMI and PowerShell Dynamic Applications. It includes the following topics:

Configuring a WMI Credential	94
Configuring a PowerShell Credential	96

### Configuring a WMI Credential

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

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

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

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

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Select the [Create] button in the upper right of the page. Select Basic/Snippet Credential.

	Profile Name *	Organization	RO Use	RW Use	DA Use	Tupe	Credential User		Hast	Port	Timeout (ma)			SNMP Crede		R
1	P9.160	(all crost)			350	SOAPXWL Host	-	%D	1000	443	20030	53	2013-03-12	Database C	redential	
	99.163	(all orgs)	-		449	SOAPOOL Host	-	50		443	20000	54	2013-03-12	SOAP/XML I	fost Credential	
	COSTOS	(all orgs)	57		7	SNMP				161	2000	38	2013-02-27		adaptial	
	Polismos (Longer Timeout)	(Mall orgs)	-		-	SNMP	-		-	161	5000	39	2013-02-27			
. 6	Cloudkick - Example	a la				Basic/Snippet	ISECURITY KEY GOES HER	127.0.0.1		443	5000	12	2013-02-27	Basic/Snipp	et Credential	
	PCUCM 7	(all orgs)	-		8	SOAP/ONL Host	em7app	%D		8443	10000	52	2013-03-11 11	28:23 jft	ak .	
	POUCH 8	Stat orgs]			8	SOAP/OWL Host	em7app	%D		8443	10000	51	2013-03-11 11:	27:23 11	*	
	CUCM PerfmonService 8.0 Example	(all orgs)	-		-	SOAP/XML Host	-	%D		8443	2000	13	2013-03-11 11:	22:51 10	ek.	
. 6	PEM7 Collector Database	(all orgs)				Detabase	reat	50		7707	0	14	2013-03-29 17	15:24 10	ak .	
	PEM7 Default V2	(all orgs)	54			SNMP				161	1500	18	2013-02-27 16	19.40 et	n7admin	
. 6	PEM7 Default V3	a fall orgs]	9			SNMP	em7defaultv3			161	500	19	2013-02-27 16	19.40 et	n7admin	
	PEVC - Example	(all orgs)	-		-	Basic/Snippet	reot	50		443	10000	7	2013-03-29 17	14:21 if	ak.	
	GLaDOS Cred	(all orgs)				SNMP				161	1500	80	2013-03-29 11	29.01 er	n7admin	
	PGoGrid - Example	(Mall orgs)				Basic/Snippet	ISECURITY KEY GOES HER	127.0.0.1		443	5000	16	2013-02-27 16	19.36 er	n7admin	
	PLifeSize: Endpoint SNMP	a (all cras)				SNMP	centrel		-	161	3000	10	2013-02-27 16		n7admin	
	LifeSize: Endpoint SSH/CLI	(all orgs)	-			Basic/Snippet	auto	%D		22	3	9	2013-03-25 17		ak.	
	Printest	(all orgs)			1	Database	postgres	10.168.44.220		5432	0	58	2013-03-21 16	45:56 m	hussain	
	PHSSQL	(Mall gras)				Database	58	10.0.9.241				35	2013-02-27 16		n7admin	
. 6	PHySQL	a la				Detabase	reot	50		7706	0	38	2013-02-27 18	35:07 er	n7admin	
	PNetApp	(all orgs)				Basic/Snippet	reat	50		443	3000	15	2013-03-29 17	15:00 if:	k	
	PNetApp w/SSL Option	(all orgs)				SOAPOOL Host	root	160		443	3000	82	2013-03-29 17		k	
	PNetApp w/SSL Option Off	(all crost)				SOAP/XIVL Host		50		443	3000	81	2013-03-29 17		ak.	
	Pnew cred name	2 (0:0t]	-			Database	usert	my.host		162	1600	65	2013-03-26 17		n7admin	
1	Pnew cred name	(none)				Database	usert	my host		162	1600	70	2013-03-26 17	44-46 m	n7admin	
	Pnew cred name	(none)				Database	usert	my.host		162	1600	75	2013-03-26 17		n7admin	
	POracle	(all orgs)				Detabase	EW7ADWN	10.0.9.151		1521	0	32	2013-02-27 16		n7admin	
	Polycom - Advanced	(all orgs)				SDAROWL Host		50		80	20000	3	2013-03-22 16		replowitz	
	Protycom - Interface	al al orgs)				SDAROWI Host	admin	160		80	20000	4	2013-02-27 16		n7admin	
	Protycom - Network	a (all cras)				SOAP/XWL Host	afmin	50		80	20000	5	2013-02-27 16		n7admin	
	Polycom - System	(all orgs)				SOAPOWL Host		50		80	20000	2	2013-02-27 16		n7admin	
	Prelycom CDR	(all orgs)				SDAROWI Host	admin	50		80	20000	6	2013-02-27 16	19:09 01	n7admin	
	Prostores	(all orgs)			-	Detabase		192,168,11,135			0	33	2013-02-27 16	34:43 01	n7admin	
	Postores	(all cros)				Detabase		192.168.11.135		5432	0	50	2013-03-07 11		n7admin	
	POALDAP	(multiple orgs)				LDARIAD	uid: %u cu: People donacie	10.0.9.81		389	1000	57	2013-03-15 16	26:27 b	ethanabotia	
	Rackspace - Example	(Mall orgs)				Basio/Snippet	IUSERNAME GOES HEREI			443	5000	28	2013-02-27 16		n7admin	
	Sig AD	(all crost)	-		-	LDAP/AD	Su@%d	192,168,40,11		389	1000	40	2013-02-27 16		n7admin	
	Snippet Cred Test	(all orgs)				Basic/Solpoet	em7admin	10.0.9.52		22	3000	55	2013-03-13 15		hussain	
	SNMP Public V1	(all orgs)	309			SNMP				161	1500	20	2013-02-27 16		n7admin	
	PSNMP Public V2	(all crost)	7		4	SNMP	-		-	161	1500	21	2013-02-27 16	19.40 et	n7admin	
	Sybase	(all orgs)	-		-	Detabase	88	10.0.9.242		5010	0	34	2013-02-27 16		n7admin	
	Tandberg Endpoint - Config	(all orgs)					USERNAME HERE	50		80	10000	24	2013-02-27 16		n7admin	
	PTandberg Endpoint - History	al al orgs)					USERNAVE HERE	160		80	10000	25	2013-02-27 16		n7admin	
	PTandberg Endpoint - Status	a (al cros)	-				USERNAVE HERE	SD		80	10030	23	2013-02-27 16		n7admin	
	Tandberg: HTTPS	(all orgs)				SOAPOWL Host		50		443	10000	29	2013-03-13 14		hussain	
	Tandberg: XML Configuration	(all orgs)						50		443	5000	31	2013-03-13 14		hussain	

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

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

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

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

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

## Configuring a PowerShell Credential

To define a PowerShell credential in SL1:

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

ential Management   Credentia	ils Found [62]													Reset	Gu
												Cr	eate SI	NMP Credentia	
Profile Name *	Organization	RO Use	RW Use	DA Use	Type	Credential User		Host	Port	Timeout (ms		Last		atabase Crede	
												AICI	eate S	DAP/XML Host	Cred
Amazon Web Services Credential	System				SOAP/XML Host	AWS Account Access	example.com		80	2000	1	2015-05-18 Cr		DAP/AD Crede	
Azure Credential - SOAP/XML	all orgs]				SOAP/XML Host	<ad user=""></ad>	login.windows.net		443	60000	60	2015-05-14	eate B	asic/Snippet C	rede
Azure Credential - SSH/Key	all orgs]				SSH/Key	<subscription_id_h< td=""><td>%D</td><td></td><td>22</td><td>180000</td><td>59</td><td>2015 05 11</td><td></td><td>SH/Key Creder</td><td></td></subscription_id_h<>	%D		22	180000	59	2015 05 11		SH/Key Creder	
Cisco SNMPv2 - Example	all orgs]				SNMP				161	1500	3	2015-05-			
Cisco SNMPv3 - Example	(all orgs)				SNMP	[USER_GOES_HERE]			161	1500	2	2015-05- 4	eate P	owerShell Crea	denti
Cisco: ACI	[all orgs]			126	Basic/Snippet	admin	173.36.219.46		443	0	62	2015-05-14 15:0	15:24	em7admin	_
Cisco: ACI Credential	all orgs]				Basic/Snippet	admin	198.18.133.200		443	0	61	2015-05-14 14:3	32:20	em7admin	
Cloudkick - Example	(all orgs)				Basic/Snippet	(SECURITY KEY GOES	127.0.0.1		443	5000	9	2015-05-14 11:2	5:31	em7admin	
CUCM PerfmonService 8.0 Example	(all orgs)				SOAP/XML Host		%D		8443	2000	4	2015-05-14 11:2	25:12	em7admin	
EM7 Central Database	[all orgs]				Database	root	localhost		7706	0	51	2015-05-14 11:2	6:41	em7admin	
EM7 Collector Database	(all orgs)				Database	root	%D		7707	0	14	2015-05-14 11:2	5:43	em7admin	
PEM7 DB	(all orgs)				Database	root	%D		7706	0	35	2015-05-14 11:2	6:32	em7admin	
EM7 DB - DB Info	(all orgs)				SOAP/XML Host	root	%D		80	3000	38	2015-05-14 11:2	6:32	em7admin	
EM7 DB - My.cnf	[all orgs]				SOAP/XML Host	root	%D		80	3000	37	2015-05-14 11:2	6:32	em7admin	
EM7 DB - Silo.conf	(all orgs)				SOAP/XML Host	root	%D		80	3000	36	2015-05-14 11:2	6:32	em7admin	
EM7 Default V2	(all orgs)				SNMP				161	1500	10	2015-05-14 11:2	25:42	em7admin	
EM7 Default V3	(all orgs)				SNMP	em7defaultv3			161	500	11	2015-05-14 11:2	5:42	em7admin	
EMC - Example	[all orgs]				Basic/Snippet	root	%D		443	10000	15	2015-05-14 11:2	5:47	em7admin	
GoGrid - Example	(all orgs)				Basic/Snippet	(SECURITY KEY GOES	127.0.0.1		443	5000	16	2015-05-14 11:2	5.51	em7admin	
PIPSLA Example	(all orgs)				SNMP				161	1500	5	2015-05-14 11:2	25:14	em7admin	
LifeSize: Endpoint SNMP	(all orgs)				SNMP	control			161	3000	18	2015-05-14 11:2	5:58	em7admin	
LifeSize: Endpoint SSH/CLI	[all orgs]				Basic/Snippet	auto	%D		22	3	17	2015-05-14 11:2	5:58	em7admin	
A Local API	(all orgs)				Basic/Snippet	em7admin	10.0.0.180		80	5000	22	2015-05-14 11:2	26:11	em7admin	
NetApp 7-mode	(all orgs)				Basic/Snippet	root	%D		443	3000	24	2015-05-14 11:2	6:20	em7admin	
NetApp w/SSL Option	[all orgs]				SOAP/XML Host	root	%D		443	3000	26	2015-05-14 11:2	6:20	em7admin	
NetApp w/SSL Option Off	[all orgs]				SOAP/XML Host	root	%D		443	10000	25	2015-05-14 11:2	6:20	em7admin	
Nexus netconf	(all orgs)				Basic/Snippet		%D		22	10000	6	2015-05-14 11:2	25:16	em7admin	
Nexus snmp	all orgs]				SNMP				161	10000	7	2015-05-14 11:2	25:16	em7admin	
Polycom - Advanced	(all orgs)				SOAP/XML Host	admin	%D		80	20000	28	2015-05-14 11:2	6:24	em7admin	
Polycom - CDR	all orgs]				SOAP/XML Host	admin	%D		80	20000	31	2015-05-14 11:2	6.24	em7admin	
Polycom - Interface	(all orgs)				SOAP/XML Host	admin	%D		80	20000	29	2015-05-14 11:2	6:24	em7admin	

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

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

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

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

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

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

# Example

# Creating a WMI Performance Dynamic Application

### Overview

In this example, we will create a WMI Dynamic Application. Our Dynamic Application will collect the following information from a network interface running on a Windows computer: Total bytes, current bandwidth, name, packets per second, outbound errors, and received errors.

**NOTE**: This example Dynamic Application is included in the *Microsoft Base Pack* PowerPack, version 1.5 and later.

The following steps are covered in this example:

Defining the WMI Request	100
Adding the WMI Request	100
Adding the Collection Objects	101
Creating the Presentation Objects	
Creating a Credential	108
Manually Aligning the Dynamic Application to a Device	109
Viewing the Performance Reports	110

### Defining the WMI Request

To create the Dynamic Application and define the general properties for this Dynamic Application, perform the following steps:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the [Actions] button, and then select Create New Dynamic Application. The Dynamic Applications Create New Application page appears.
- 3. Supply values in the following fields:

Close	Properties	<u>C</u> ollections	Presentati <u>o</u> ns	<u>W</u> MI Req	uests	Thresholds	Alerts	Subscri	bers	
Dynamic Applicati	ons [307]   Properti	es Editor							Guide	Reset
Windows In	Application Name terface		Operational (	State	[	Abando [Default]	n Collection	0	Compon	ent Mapping
[WMI Perfo	Application Type mance]	<b>v</b> 🚱			[	C	ontext	•	s	ave
[Version 1.2	Version Number	- 3	Poll Freque [Every 5 Minutes]		[	Ca [ No caching ]	aching	0		ve As

- Application Name. Enter Windows Interface in this field.
- Application Type. Select WMI Performance.
- Poll Frequency. Select Every 5 Minutes.
- 4. For this example, you can leave the remaining fields at their default value. Select the **[Save]** button to save the Dynamic Application.

### Adding the WMI Request

In SL1, each WMI Dynamic Application must include at least one WMI or WBEM request.

WMI objects are populated when the Dynamic Application executes a WMI request. WMI requests use WQL (WMI Query Language) to query WMI classes (tables) to retrieve data. A single WMI request can populate multiple WMI objects by querying for multiple class properties (table columns).

WMI objects are aligned with properties (column). The definition of each object specifies the WMI request that will populate the object and the property name to align with the object. The retrieved values of the property will populate the object.

For more details on WMI requests, see the WMI Requests section.

To create the WMI request for this Dynamic Application:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the wrench icon (*P*) for the Windows Interface Dynamic Application. The **Dynamic Applications**

Properties Editor page appears.

- 3. Select the [WMI Requests] tab. The WMI Request Editor & Registry page appears.
- 4. Supply values in the following fields:

Close <u>P</u> roperties <u>C</u> ollections	Presentations WMI Requests	Thresholds	<u>A</u> lerts	Subscribers	
Dynamic Applications [307]   WMI Request Editor & Regis	try   Editing Snippet [448]			Guide	Reset
Win Request Name Win32_PerformatedDas_Topp_Networkt Will Request Type [WMI] WMI Request Type Select Name, Byter TotalPerSec, Packet/PerSec, CurrentBandy	WMI Request Query	Name [Enabled] Ærrors From Win32_Per	WM Object K	•	
	Save Save	15			

- WMI Request Name. We named our WMI Request "Win32\_PerfFormattedData\_Tcpip\_ NetworkInterface"
- WMI Request Type. Select WMI.
- WMI Object Key. The unique key for each instance (row) returned by the request. This unique key must be a property (column) name, and the request must include that property (column) and return values from that property name (column). The selected property (column) must return the same values over all polling periods. The "Name" property (column) meets these criteria. Enter "Name" in this field.
- Active State. Select Enabled.
- WMI Request Query. This Dynamic Application is getting values from the Win32\_ PerfFormattedData\_Tcpip\_NetworkInterface class (table), and will collect the following values: Interface name, total bytes, current bandwidth, name, outbound errors, and received errors. We entered the following in the WMI Request Query:

Select Name, BytesTotalPerSec, PacketsPerSec, CurrentBandwidth, PacketsOutboundErrors, PacketsReceive dErrors From Win32 PerfFormattedData Tcpip NetworkInterface

5. Select the [Save As] button to save the WMI Request.

### Adding the Collection Objects

Our example Dynamic Application has six collection objects:

- Total Bytes per second
- Current Bandwidth
- Interface Name

- Packets per second
- Outbound errors
- Received errors

To create these collection objects, perform the following steps:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the wrench icon (*P*) for the Windows Interface Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
- 3. Select the [Collections] tab. The Dynamic Applications | Collections Objects page appears.
- 4. To create the collection object for Total Bytes, supply values in the following fields:

	Close P	roperties <u>C</u> ollections	Presentati <u>o</u> n	IS <u>W</u> MLF	Requests	<u>T</u> hresholds	<u>A</u> lerts	Subscribers		-
C	Jynamic Applications [307	Collection Objects   Object	Saved [ 2549 ]					Guide	Reset	
	Object Name WMI Request Arguments	Network Interface\Bytes Total/sec BytesTotalPersec			over ea Should	ch network adap	ter, including ork Card Speed	on h bytes are sent and g framing characters i X 2 (for duplex) X		
	Class Type	[4 Performance Gauge]		.:: •			Formula	1	.::	1
	WMI Request	[Win32_PerfFormattedData_Tcpip_	Network Interface]							μ
	Group Number	[Group 1]		Index: 🕅						
				Save	Save	As		Disable Object Main	tenance	

- Object Name. We named our collection object "Network Interface\Bytes Total/sec"
- WMI Request Argument. In this field, you must specify the name of the property (table column) to associate with this object. Enter "BytesTotalPersec" in this field.
- **Class Type**. Total bytes per second is a number that can go up or down between polls. Select 4 *Performance Gauge* in this field.
- WMI Request. Name of the WMI request associated with this object. Select Win32\_ PerfFormattedData\_Tcpip\_NetworkInterface.
- Group Number. Select Group 1. For performance Dynamic Applications, SL1 uses the Group Number setting to associate performance values with the appropriate labels. For the performance graph for this example to display labels correctly, all the collection objects must be in the same group.
- **Description**. A description of the object. This is an optional field. We provided a summary of the object in this field.
- 5. For this example, you can leave the remaining fields set to their default values.
- 6. Select the **[Save]** button.
- 7. Select the **[Reset]** button to clear the form fields.
- To create the following Collection Objects for Current Bandwidth, Packets Per Second, Outbound Errors, and Received Errors collection objects, repeat step 4, using the following values in the WMI Request Argument field. These values match the properties defined in the WMI Request for this Dynamic Application.

Collection Object	WMI Request Argument
Network Interface/Current Bandwidth	Current Bandwidth
Network Interface/Packets/sec	PacketsPerSec
Network Interface/Outbound Errors	PacketsOutbandErrors
Network Interface/Received Errors	PacketsReceivedErrors

9. To create the Interface Name collection object, which will be the label for the performance report, supply the following values in the **Dynamic Applications | Collections Objects** page:

Clo	ose <u>P</u>	roperties	<u>Collections</u>	Presentation	s <u>W</u> MI	Requests	Thresholds	Alerts	Subscribers	
Dynamic	Applications [307	Collection C	Objects						Guide	Reset
	Object Name	Network Interfac	>e\Name			Name of	the interface	Description	1	
WMI Req	quest Arguments	Name			.::					:
	Class Type	[104 Label (Alw	ays Polled)]		×			Formula		
	WMI Request	Win32_PerfFor	mattedData_Tcpip_I	NetworkInterface						
	Group Number	[Group 1]		•	Index: 🔽					.::
					Save	Save	As		Disable Object Maintena	ince

- Object Name. We named this collection object "Network Interface\Name".
- WMI Request Argument. In this field, you must specify the name of the property (table column) to associate with this object. Enter "Name" in this field.
- **Class Type**. Select Label (Always Polled) in this field. In performance Dynamic Applications, collection objects that use this class type are string values that SL1 uses to label the lines on a performance graph.
- WMI Request. Name of the WMI request associated with this object. Select Win32\_ PerfFormattedData Tcpip NetworkInterface.
- **Group Number**. Select Group 1. For performance Dynamic Applications, SL1 uses the **Group Number** setting to associate performance values with the appropriate labels. For the performance graph for this example to display labels correctly, all the collection objects must be in the same group.
- **Description**. A description of the object. This is an optional field. We provided a summary of the object in this field.
- 10. For this example, you can leave the remaining fields set to their default values.
- 11. Select the **[Save]** button.

### Creating the Presentation Objects

When you create a collection object in a Dynamic Application of type Performance, SL1 automatically creates a presentation object that corresponds to that collection object. In this example, we will remove these presentation objects and create new presentation objects for each collection object defined above.

To create the presentation objects:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the wrench icon ( *for the Windows Interface Dynamic Application*.
- 3. Select the [Presentations] tab. The Dynamic Applications Presentation Objects page appears.
- 4. In the **Dynamic Applications Presentation Objects** page, each collection object created in the **Adding** the Collection Objects section has been created by default. Select each presentation object's bomb icon (

🚅) to delete them.

5. Select the **[Reset]** button. To create the presentation object that displays Total Bytes Per Second, enter values in the following fields:

Close	Properties	Collections	Presentations	<u>W</u> MI Requests	<u>T</u> hresholds	Alerts	Subscribers		
Dynamic Applications	[307]   Presentatio	on Successfully S	aved [ 868 ]   Pres	entation Objects				Guide Re	eset
Report Name	e Bytes Total per Sec	ond		Formula Editor (o_2549)					
Active State	[Enabled]								
Data Uni	Bytes/Second								
Abbreviation / Suffix	в			7 8	9 2549: Ne	twork Interface\Bytes	Total/sec	<u>^ 0 (</u>	CE
Show as Percent	t [No]			4 5 1 2		twork Interface\Packe twork Interface\Curren		- ( /	)
Vitals Link	[Disabled]			0		Add		-	•
Guide Text									
				ceived over each or duplex) X 75%			aming ;	Save Save As	1

- Report Name. Enter "Bytes Total per Second" in this field.
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Bytes/Second" into this field.
- Abbreviation / Suffix. Enter "Bps" into this field.
- Show as Percent. Select No. The graph will not display percent values.
- 'Formula Editor. In this field, enter the object ID for the Total Bytes Per Second collection object, surrounded by parentheses.
- 6. For this example, you can leave the remaining fields set to their default values.
- 7. Select the [Save] button to save the presentation object.

8. Select the [**Reset**] button. For the Current Bandwidth presentation object, enter the following values in the **Dynamic Applications Presentation Objects** page:

Close	Properties	Collections	Presentati <u>o</u> ns	WMI Requests	Thresholds	Alerts	Subscrib	ers	
Dynamic Applications	[307]   Presentatio	n Objects					1	Guide	Reset
Report Name	Current Bandwidth			Formula Editor					
Active State	[Enabled]								
Data Unit	Byte per second								
Abbreviation / Suffix	Bps			7 8	9 2549: Netwo	ork Interface\Bytes T	otal/sec	× 0	.::: CE
Show as Percent	[No]		•	4 5 1 2		ork Interface\Packet ork Interface\Current		- (	)
Vitals Link	[Disabled]			0		Add		-	•
Guide Text									
	or those where	no accurate es	timation can be	second (bps). For made, this value			in This	Sav	

- Report Name. Enter "CurrentBandwidth" in this field.
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Bytes per second" into this field.
- Abbreviation / Suffix. Enter "Bps" into this field.
- Show as Percent. Select No. The graph will not display percent values.
- Vitals Link. Select Disabled.
- **Formula Editor**. In this field, enter the object ID for the Current Bandwidth collection object, surrounded by parentheses.
- 9. For this example, you can leave the remaining fields set to their default values. Select the **[Save]** button to save the presentation object.
- 10. Select the **[Reset]** button. For the Interface Utilization presentation object, enter the following values in the **Dynamic Applications Presentation Objects** page:

Close	Properties	<u>C</u> ollections	Presentati <u>o</u> ns	<u>W</u> MIRequests	<u>T</u> hresholds	Alerts	Subscrib	ers
Dynamic Applications	[307]   Presentatio	n Objects					1	Guide Reset
Report Name	Interface Utilization			Formula Editor	? ( (8 * o_25	49) / 0_2552)	: 0)	
Active State	[Enabled]		•					
Data Unit	Percent							.:
Abbreviation / Suffix	%			7 8	9 2549: Netv	vork Interface\Bytes	Total/sec	<ul> <li>() CE</li> </ul>
Show as Percent	[Yes]			4 5 1 2		vork Interface\Packe vork Interface\Curren		- ( ) / ·
Vitals Link	[Disabled]			0		Add		- +
Guide Text								
0. If the inte	erface rate is	positive, then	the Bytes/sec a	h bits/sec. If t are turned into b arface from the a	its/sec by mult	iplying by 8,	then the	Save Save As

- Report Name. Enter "Interface Utilization" in this field.
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Percent" into this field.

- Abbreviation / Suffix. Enter "%" into this field.
- Show as Percent. Select Yes. The graph will display percent values.
- Formula Editor. In this field, enter the following formula:

((<object ID for Current Bandwidth> > 0) ? ((8 \* <object ID for Bytes Total/sec>) / <object ID for Current Bandwidth>) : 0)

For example, if the object ID for Current Bandwidth is o\_7034 and the object ID for Bytes Total/sec is o\_7031, enter:

This formula includes a collection object as a divisor. To prevent an error from occurring when the divisor returns zero, the formula includes a ternary operator that tests to see if the divisor is zero. If the divisor is zero, the formula returns zero. If the divisor is greater than zero, the formula converts the "Bytes Total/sec collection object in to Bits Total/sec, then divides the total bits/second by the speed of the interface.

- 11. For this example, you can leave the remaining fields set to their default values. Select the **[Save]** button to save the presentation object.
- 12. Select the **[Reset]** button. For the Packets Per Second presentation object, enter the following values in the **Dynamic Applications Manager** page:

	Close	Properties	<u>C</u> ollections	Presentati <u>o</u> ns	WN	ll Requests	Threshol	ds	Alerts	Subscrib	ers	
	Dynamic Applications	[307]   Presentation	Successfully S	aved [ 869 ]   Prese	entat	ion Objects					Guide	Reset
	Report Name	Packets per Second				rmula Editor o_2551)						
	Active State	[Enabled]										
	Data Unit	Packets/Second										
	Abbreviation / Suffix	P/s				7 8	9 25	49: Network	Interface\Bytes	Total/sec		CE
	Show as Percent	[No]				4 5 1 2	25	51: Network	Interface\Pack Interface\Curren	ets/sec	- (	)
	Vitals Link	[Disabled]			-	0			Add		-	•
ľ	Guide Text										1	
	Packets/sec is	the rate at whi processor bottl					ork interf	ace. 1	fonitor ove	r time.	Sat	

- Report Name. Enter "Packets per Second" in this field.
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Packets/Second" into this field.
- Abbreviation / Suffix. Enter "P/s" into this field.
- Show as Percent. Select No. The graph will not display percent values.
- Formula Editor. In this field, enter the object ID for the Packets Per Second collection object, surrounded by parentheses.
- 13. For this example, you can leave the remaining fields set to their default values. Select the **[Save]** button to save the presentation object.

14. Select the **[Reset]** button. For the Outbound Errors presentation object, enter the following values in the **Dynamic Applications Manager** page:

Close	Properties Co	ollections	Presentati <u>o</u> ns	<u>W</u> MI Requests	<u>T</u> hresholds	<u>A</u> lerts	Subscrib	ers	
Dynamic Applications	[307]   Presentation Ob	jects						Guide	Reset
Report Name	Packets Outbound Errors			Formula Editor					
Active State	[Enabled]		•						
Data Unit	Errors								
Abbreviation / Suffix	Errors			7 8	9 2549: Netw	ork Interface\Bytes	Total/sec	<u>^</u> 0	CE
Show as Percent	[No]			4 5 1 2	6 2551: Netw 2552: Netw	ork Interface\Packe ork Interface\Curren	its/sec it Bandwidth	- (	)
Vitals Link	[Disabled]			0		Add		-	+
Guide Text									
Number of outbo	ound packets that c	ould not b	e transmitted b	ecause of errors.			.:		ave Ne As

- Report Name. Enter "PacketsOutboundErrors" in this field.
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Errors" into this field.
- Abbreviation / Suffix. Enter "Errors" into this field.
- Show as Percent. Select No. The graph will not display percent values.
- Formula Editor. In this field, enter the object ID for the Outbound Errors collection object, surrounded by parentheses.
- 15. For this example, you can leave the remaining fields set to their default values. Select the **[Save]** button to save the presentation object.
- 16. Select the **[Reset]** button. For the Inbound Errors presentation object, enter the following values in the **Dynamic Applications Manager** page:

Close	Properties	<u>C</u> ollections	Presentati <u>o</u> ns	WMI Requests	<u>T</u> hresholds	<u>A</u> lerts	Subscribe	rs	
Dynamic Applications	[307]   Presentatio	n Successfully S	aved [ 873 ]   Prese	entation Objects				Guide	Reset
Report Name	PacketsInboundErro	ß		Formula Editor					
Active State	[Enabled]		-						
Data Unit	Errors								
Abbreviation / Suffix	Errors			7 8	9 2549: Net	work Interface\Bytes	Total/sec	<b>^</b> (	.;;
Show as Percent	[No]		•	4 5 1 2		work Interface\Packe work Interface\Curren		- (	)
Vitals Link	[Disabled]		•	0		Add		-	•
Guide Text									
	ind packets tha	t contained er	rors preventing	delivery to a hi	gher-layer pro	tocol.	.::		ave ve As

- Report Name. Enter "PacketsInboundErrors" in this field.
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Errors" into this field.
- Abbreviation / Suffix. Enter "Errors" into this field.

- Show as Percent. Select No. The graph will not display percent values.
- **Formula Editor**. In this field, enter the object ID for the Inbound Errors collection object, surrounded by parentheses.
- 17. For this example, you can leave the remaining fields set to their default values. Select the **[Save]** button to save the presentation object.

#### Creating a Credential

To use the Windows Interface Dynamic Application, we must include a Basic/Snippet credential. To create the Basic/Snippet credential:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Select the [Create] button, and then select Basic/Snippet Credential. The Create New Basic/Snippet Credential page appears.
- 3. Define values in the following fields:

Credential Editor		Clos	se / Esc
Create New Basic/Snippet Credential		Re	set
Basic Settings			
	Credential Name		
Windows Interface WMI			
Hostname/IP	Port	Timeout(ms)	
%D	1521	5000	
Use	rname	Password	
Administrator		•••••	
L			
	Save		

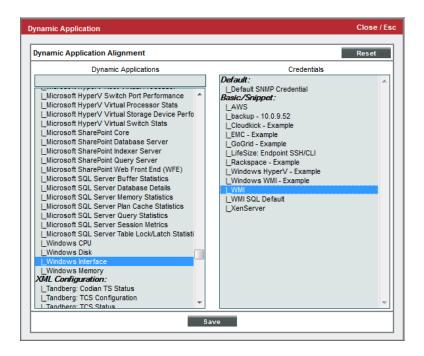
- Credential Name. Enter "Windows Interface WMI" in this field.
- [Hostname/IP]. Enter "%D" in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
- Port. Enter "1521" in this field. This is the default port for WMI.
- *Timeout*. Enter "5000" in this field. SL1 will stop trying to communicate with the authenticating server after 5000 seconds.
- **Username**. Enter the username for a user account in this field that will provide access to the monitored Windows device.
- **Password**. Enter a password for a user account that will provide access to the monitored Windows device
- 4. Select the [Save] button to save the credential.

## Manually Aligning the Dynamic Application to a Device

In this example we will align the Dynamic Application to a Windows device running WMI. By manually aligning the Dynamic Application to a device, we can immediately view the interface data in the presentation objects we defined.

To manually align the Dynamic Application to a device:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- In the Device Manager page, find the device you want to align the Dynamic Application to. In this example, we are aligning the Dynamic Application to a Windows device running WMI. Select the device's wrench icon (*P*).
- 3. The Device Properties page appears. Select the [Collections] tab.
- 4. In the **Dynamic Application Collections** page, select the **[Action]** button and select Add Dynamic Application. The **Dynamic Application Alignment** page appears.



- 5. Select the Windows Interface Dynamic Application in the Dynamic Applications pane, and select Windows Interface WMI in the Credentials pane.
- 6. Select the [Save] button to add the Dynamic Application.

#### Viewing the Performance Reports

After the Dynamic Application has collected the data specified in the collection objects, you can view the performance report for the device into the device. To view the performance report for the device with the *Windows Interface* Dynamic Application aligned to it:

- 1. From the **Dynamic Application Collections** page, select the **[Reset]** button to update the page with the latest information.
- 2. Locate the **Windows Interface** Dynamic Application. If the graph icon (<sup>111</sup>) is colored, the performance report is available. Select the graph icon for the presentation object you want to view.

Or:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. In the **Device Manager** page, find the test device you aligned the *Windows Interface* Dynamic Application to. Select the device's graph icon (
- 3. The Device Summary page appears. Select the [Performance] tab.
- 4. In the left NavBar, select any of the presentation objects you created in the section **Creating the Presentation Objects** in this chapter. In this example, we selected Bytes Total per Second.

Close <u>S</u> ummary Logs Events	Performa Ticket		Profile	T <u>o</u> pology Processe		onfigs ervices	TCP Ports	<u>I</u> nterf Organi		Asset	
Device Name LAB-2007-DC.skl IP Address / ID 10.168.44.214 [ 9 Class Microsoft Organization System Collection Mode Active Description Hardware: Intel64	74	Stepping 2 A	T/AT COMPATI	Mar	aged Type P Category S Sub-Class W Uptime 4 otion Time 2	iysical Device ervers findows Cluste 21 days, 10:50 012-06-21 17:5 JG3   em7_cu3	r Point 17				
Overview	Options	Report			Wind	ows Interface	>   Bytes Total			Reset	Guide
Place Systems     Place Systems     Place Transmission     Place Transmission     Place Transmission     Place Transmission     Porter Transmission     Place Transmission     Place Transmission     Placets Received Errors     Placets Received Errors	60,000 Bps 50,000 Bps 40,000 Bps 30,000 Bps 20,000 Bps 10,000 Bps										
	0 Bps	17:05	17:10	17:15	17:20	17:25	17:30	17:35	17:40	17:45	17:50
	Currently Visit Date Rang Start 06/19/ End 06/21/	Jun 20 le: 06/21/ le Selection:	2012 16:59		12:00 12 17:54 Graph Type line v	]	se-over	Jun 21	Range: 6 Ho Max	ur 12 Hour	12:00 1 Day Max Ran Nos Nos Nos Nos Pol 0 57 30,959 57 0 57

- 5. The Windows Interface | Bytes Total per Second report is displayed.
  - The report displays the collected values from the collection object Network Interface\Bytes Total/sec.
  - You can mouseover different data points on the report, and the report will display the total bytes moving through the interface at the time selected on the graph.

- The amount of bytes is shown to the left of the report.
- The values for each label object are displayed in the graph key at the bottom of the page.
- 6. To learn more about performance reports, see the manual *Monitoring Device Infrastructure Health*.

# Example

# 2

## Creating a PowerShell Performance Dynamic Application

### Overview

In this example, we will create a PowerShell Dynamic Application. Our Dynamic Application will collect the Processor Queue Length from a Windows computer.

**NOTE**: This example Dynamic Application is included in the *Microsoft: Windows Server* PowerPack, version 1.0 and later. This example describes how to create only one of the requests, collection objects, and presentation objects that are included in the *Microsoft: Windows Server* PowerPack version of this Dynamic Application.

The following steps are covered in this example:

Creating the Dynamic Application	.113
Adding the PowerShell Command	.114
Adding the Collection Object	. 115
Creating the Presentation Object	. 116
Creating a Credential	. 117
Manually Aligning the Dynamic Application to a Device	. 119
Viewing the Performance Report	.120

## Creating the Dynamic Application

To create the Dynamic Application and define the general properties for this Dynamic Application, perform the following steps:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the **[Actions]** button, and then select Create New Dynamic Application. The **Dynamic Applications Create New Application** page appears.

3. Supply values in the following fields:

C lo se	Create												
Dynamic Applications   Create New Application Guide Rese													
Application	Application Name		Version Number [Version 1.0]	Abandon Collection [Default] 2		ollup of Data							
	Performance [22] Caching	• •	Operational State [Enabled]	Null Row Option	Compone	ent Mapping							
No caching	Device Dashboard	@ @	Poll Frequency Every 5 Minutes	- values T 😧 Null Column Option - values T 😪	S	ave							

- Application Name. Enter "Microsoft: Windows Server CPU Performance" in this field.
- Application Type. Select PowerShell Performance.
- Polling Frequency. Select Every 5 Minutes.
- 4. For this example, you can leave the remaining fields at their default value. Select the **[Save]** button to save the Dynamic Application.

## Adding the PowerShell Command

In SL1, each PowerShell Dynamic Application must include at least one PowerShell Command.

The collection objects in a PowerShell Dynamic Application are populated when SL1 executes a PowerShell Command.

Collection objects in PowerShell Dynamic Applications are aligned with properties (columns). The definition of each object specifies the PowerShell command that will populate the object and the property name to align with the object. The retrieved values of the property will populate the object.

To create the PowerShell command for this Dynamic Application:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the wrench icon for the "Microsoft: Windows Server CPU Performance" Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
- 3. Select the [PowerShell] tab. The PowerShell Command Editor and Registry page appears.

4. Supply values in the following fields:

Close	<u>P</u> roperties	<u>C</u> ollections	Presentati <u>o</u> ns	Power <u>S</u> hell	<u>T</u> h	resholds	<u>A</u> lerts	Subscribe	rs	
Dynamic Applicat	ions [705]   PowerShell C	ommand Editor & F	Registry   Editing Si	nippet [773]					Guide	Reset
	PowerSi Server CPU Processor Q	nell Command Name	•				Response Ob	ject Key		
		Active State					PowerShel	І Туре		
	[Enabled]		<u>-</u>	PowerShell Command	Query	[Not Exchange]			-	
(Get-Coun	ter "\System\Process	or Queue Lengt				kedValue				
				Save Sav	e As					

- **PowerShell Command Name**. We named our PowerShell Command "Server CPU Processor Queue-Length".
- Active State. Select Enabled.
- **PowerShell Command Query**. This Dynamic Application collects the CookedValue property from \System\Processor Queue Length: . We entered the following in the **PowerShell Command Query** field:

(Get-Counter "\System\Processor Queue Length").CounterSamples | Select-Object CookedValue

5. Select the [Save As] button to save the PowerShell command.

## Adding the Collection Object

Our example Dynamic Application has one collection object: Processor Queue Length.

To create the collection object, perform the following steps:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the wrench icon (*P*) for the "Microsoft: Windows Server CPU Performance" Dynamic Application. The **Dynamic Applications Properties Editor** page appears.
- 3. Select the [Collections] tab. The Dynamic Applications | Collections Objects page appears.

4. To create the collection object for Processor Queue Length, supply values in the following fields:

Close P	operties <u>C</u> ollection	ns Presentati <u>o</u> ns	Pov	/er <u>S</u> hell	Thresholds	<u>A</u> lerts	Subscribers	
Dynamic Applications [705]	Collection Objects					Guide	e Reset	
Object Name PowerShell Arguments	Processor Queue Length CookedValue			queue. counter There i multipl process	Unlike the disk shows ready the s a single queue e processors. The ors, you need to	<pre>c counters, this reads only, not f e for processor f nerefore, if a co o divide this val </pre>	f threads in the pr counter counters, threads that are rr time even on comput mputer has multip Lue by the number o Istained processor	this inning. cers with .e
Class Type PowerShell Request	[4 Performance Gauge] [Server CPU Processor Que	ue-Length ]					normally acceptable	
Group / Usage Type	[No Group] [Standard]	-						
Enable Deviation Alerting:	max weeks data: 0	min weeks data: 0	Save	Save	As		Disable Object Ma	intenance

- Object Name. We named our collection object "Processor Queue Length".
- **PowerShell Argument**. In this field, you must specify the name of the property to associate with this object. Enter "CookedValue" in this field.
- Class Type. Processor Queue Length is a number that can go up or down between polls. Select 4 Performance Gauge in this field.
- **PowerShell Request**. Name of the PowerShell request associated with this object. Select Server CPU Processor Queue Length.
- **Group Number**. Select No Group. For performance Dynamic Applications, SL1 uses the Group Number setting to associate performance values with the appropriate labels.
- **Description**. A description of the object. This is an optional field. We provided a summary of the object in this field.
- 5. For this example, you can leave the remaining fields set to their default values.
- 6. Select the **[Save]** button.

#### Creating the Presentation Object

When you create a collection object in a Dynamic Application of type Performance, SL1 automatically creates a presentation object that corresponds to that collection object. In this example, we will edit the presentation object for the Processor Queue Length to create a new presentation object for the Processor Queue Length.

To create the Processor Queue Length presentation object:

- 1. Go to the **Dynamic Applications Manager** page (System > Manage > Applications).
- 2. Select the wrench icon ( I for the "Microsoft: Windows Server CPU Performance".
- 3. Select the [Presentation] tab. The Dynamic Applications Presentation Objects page appears.

4. In the **Dynamic Applications Presentation Objects** page, the Processor Queue Length collection object created in the Adding the Collection Objects section has been created by default. Select the Processor

Queue Length presentation object's wrench icon (🥓) to edit it.

5. To create the presentation object that displays the Processor Queue Length, supply values in the following fields:

Close	<u>P</u> roperties	<u>C</u> ollections	Presentati <u>o</u> ns	Power <u>S</u> hell	<u>T</u> hresholds	<u>A</u> lerts	Subscribe	ers	
Dynamic Applications	[705]   Presentation	Objects						Guide	Reset
Report Name	Processor Queue Le	ngth		Formula Editor (o_7813)					
Active State	[Enabled]		<u>•</u>						
Data Unit	Threads								
Abbreviation / Suffix	Threads			7 8	9 7812: CPU U	Jtilization			CE
Show as Percent	[No]	Precedence [50	]	4 5 1 2	6 7813: Proce 7834: Cores	ssor Queue Length			)
Label Group	No Label	+ Label [NA	<u> </u>	0		Add		-	+
Guide Text									
counters, this time even on co this value by t processor is no	counter shows ro mputers with mu he number of pro rmally acceptab	eady threads on ltiple processo ocessors servic le, dependent o	ly, not threads t rs. Therefore, it ing the workload.	that are running. F a computer has A sustained pro Sustained valu	e the disk counte There is a sing multiple processo cessor queue of l es > 2 X # of CPU	le queue for p rs, you need to ess than 10 th	rocessor o divide reads per		ve e As

- Report Name. Enter "Processor Queue Length".
- Active State. Select Enabled. SL1 will generate a report of the presentation object.
- Data Unit. Enter "Threads" into this field.
- Abbreviation / Suffix. Enter "Threads" into this field.
- Show as Percent. Select No. The graph will not display percent values.
- 6. For this example, you can leave the remaining fields set to their default values. Select the **[Save]** button to save the presentation object.

#### Creating a Credential

To use the "Microsoft: Windows Server CPU Performance" Dynamic Application, we must create a PowerShell credential. To create the PowerShell credential:

- 1. Go to the **Credential Management** page (System > Manage > Credentials).
- 2. Select [Create] button, and then select PowerShell Credential. The Create New PowerShell Credential page appears.

3. Supply values in the following fields:

Credential Editor [62]	Close / Esc
Edit PowerShell Credential #62	New Reset
Basic Settings	
Profile Name	Account Type
PowerShell 2k12r2 [AD]	[Active Directory]
Hostname/IP	Timeout(ms)
%D	3000
Username	Password
Em7admin	
Encrypted Port	PowerShell Proxy Hostname/IP
[no] 5985	
Active Directory Settings	
Active Directory Hostname/IP	Domain
TL012R2-DC-01.MSTL012R2.LOCAL	MSTL012R2.LOCAL
Save Save As	

- **Profile Name**. Enter a credential name in this field. We entered "PowerShell 2k12R2 [AD]" in this example.
- Account Type. Select the account type of the user that will provide access to the monitored Windows device.
- Hostname/IP. Enter "%D" in this field. SL1 will replace the variable with the IP address of the device that is currently using the credential.
- *Timeout (ms)*. Enter "3000" in this field. SL1 will stop trying to communicate with the authenticated server after 3000 ms.
- Username. Enter the username for a user that will provide access to the monitored Windows device.
- Password. Enter the password for the user account you entered in the Username field.
- *Encrypted*. Select whether encryption is configured on the monitored Windows device.
- Port. The port should be automatically selected after selecting a value in the Encrypted field.
- **PowerShell Proxy Hostname**./IP. Do not enter a value this field unless you have configured a Windows device to serve as an intermediary proxy to retrieve PowerShell data from the target Windows device.
- Active Directory Hostname/IP. If you are using an active directory user account, enter the Hostname or IP address of the managed device's corresponding domain controller from the active directory forest.
- **Domain**. Enter your Active Directory Domain.
- 4. Select the [Save] button to save the credential.

## Manually Aligning the Dynamic Application to a Device

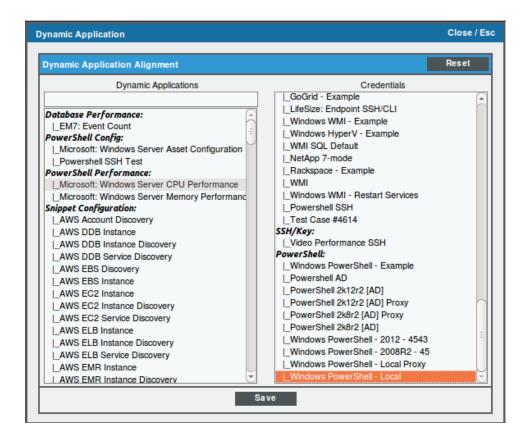
In this example we will align the Dynamic Application to a Windows device that is configured for monitoring via PowerShell. By manually aligning the Dynamic Application to a device, we can immediately view the performance data in the presentation object we defined.

To manually align the Dynamic Application to a device:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. In the **Device Manager** page, find the device you want to align with the Dynamic Application. In this example, we are aligning the Dynamic Application to a Windows device that is configured for monitoring via

PowerShell. Select the wrench icon for the device (

- 3. The Device Properties page appears. Select the [Collections] tab.
- 4. In the **Dynamic Application Collections** page, select the **[Action]** button and select Add Dynamic Application. The **Dynamic Application Alignment** page appears:



- 5. Select the "Microsoft: Windows Server CPU Performance" Dynamic Application in the **Dynamic Applications** field, and select the appropriate PowerShell credential in the **Credentials** field.
- 6. Select the [Save] button to add the Dynamic Application.

#### Viewing the Performance Report

After the Dynamic Application has collected the data specified in the collection objects, you can view the performance report for the device. To view the performance report for the device with the "Microsoft: Windows Server CPU Performance" Dynamic Application aligned to it:

- 1. From the **Dynamic Application Collections** page, select the **[Reset]** button to update the page with the latest information.
- 2. Locate the "Microsoft: Windows Server CPU Performance" Dynamic Application. If the graph icon is colored, the performance report is available. Select the graph icon (1) for the presentation object you want to view.

Or:

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. In the **Device Manager** page, find the test device you aligned the "Microsoft: Windows Server CPU Performance" Dynamic Application. Select the device's graph icon.
- 3. The Device Summary page appears. Select the [Performance] tab.
- 4. In the left NavBar, select the presentation object you created in the section **Creating the Presentation Objects**:

Close <u>S</u> ummary Logs <u>E</u> vents		pology <u>C</u> onf ftware Proce		Interfaces TCP Ports	Organization	
Device Name TL008-HO-SP-0 IP Address / ID 10.0.6.34   61 Class Microsoft Organization System Collection Mode Active Descice Hostname	1.MSTL008.local 4 Family 6 Model 44 Stepping 2 AT//		Managed Type Physical Dev Category Servers Sub-Class Windows Ser Uptime 0 days, 20:38 Collection Time 2014-03-27 ( roup / Collector CUG_213   er	ver 2008 R2 9:27 99:50:00		
-Overview	Options Report	Microsoft	: Windows Server CPU Pe	rformance   Processor		Reset Guide
He Systems     Network Interfaces     Host Resource: Memory     Host Resource: CPU     Host Resource: CPU     Performance     CPU Utilization     Processor Queue Length     Hicrosoft: Windows Server Memory     Performance	Zoom 6H 12H 1D Max 6 5 4 2 1 2				From: 03/25	/201403:03   To: 03/26/201407:12
Find	0 03:30 4) Date Range Selection: Start 03/25/2014 09:55:3 End 03/27/2014 09:55:3 Presets Set Custom	04:00 C	Graph Type Trend	05:30 12:00 Mouse-over -	Min Max	06:30 07:00 27. Mar 27. Mar Avg Polis 11.000 0.330 287

- 5. The Microsoft: Windows Server CPU Performance | Processor Queue Length report is displayed.
  - The report displays the collected values from the collection object Processor Queue Length.
  - You can mouse over different data points on the report, and the report will display the queue length value at the time selected on the graph.
  - The values for the Processor Queue Length label object are displayed in the graph key at the bottom of the page.

To learn more about performance reports, see the manual Device Management.

#### © 2003 - 2020, ScienceLogic, Inc.

#### All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

#### Copyrights and Trademarks

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

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

- ScienceLogic<sup>™</sup>
- EM7<sup>™</sup> and em7<sup>™</sup>
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management<sup>™</sup>

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

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

#### Other

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

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



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

International: +1-703-354-1010