



Cisco UCS Performance Manager Installation Guide

First Published: October 2014

Release 1.0.0

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014-2015 Cisco Systems, Inc. All rights reserved.

Contents

Preface.....	4
 Chapter 1: Welcome to Cisco UCS Performance Manager.....	6
Preparing Network Devices.....	6
Preparing Storage Devices.....	7
Preparing Server Devices.....	8
Preparing Hypervisor Devices.....	8
 Chapter 2: Installing with VMware vSphere.....	10
Deploying a VMware virtual machine for Cisco UCS Performance Manager.....	10
Setting the root password.....	11
 Chapter 3: Installing with Hyper-V Manager.....	13
Creating a Hyper-V virtual machine for Cisco UCS Performance Manager.....	13
Installing Cisco UCS Performance Manager.....	14
 Chapter 4: Setting up Cisco UCS Performance Manager.....	17
Accepting the License Agreement.....	17
Setting up Users.....	18
Providing a license key.....	18
Adding UCS Domains.....	19
Adding Infrastructure Devices.....	20
 Chapter 5: Maintaining Cisco UCS Performance Manager.....	24
Downloading Cisco UCS Performance Manager software.....	24
Updating the Cisco UCS Performance Manager server operating system.....	24
Configuring network device settings.....	25
Configuring DNS settings.....	27
 Appendix A: Configuring HTTPS communications.....	29
Creating a self-signed SSL certificate.....	29
Configuring the nginx server.....	30
 Appendix B: Preparing Windows Systems.....	33

Preface

Cisco UCS Performance Manager Installation Guide provides detailed instructions for installing Cisco UCS Performance Manager Express or Cisco UCS Performance Manager. Cisco UCS Performance Manager Express provides monitoring for Cisco UCS Domains, and Cisco UCS Performance Manager provides monitoring both Cisco UCS Domains and other infrastructure devices. For convenience, this document uses "Cisco UCS Performance Manager" generically. When needed, differences between the two products are noted explicitly.

Minimum system requirements

Cisco UCS domain size		Cisco UCS Performance Manager virtual machine size		
Category	Monitored Servers	Cores	Memory	Storage
Small	1-50	4	32GB	50GB
Medium	51-100	8	64GB	100GB
Large	101-500	12	96GB	150GB

Note Cisco UCS Performance Manager requires a storage subsystem that supports a minimum of 500 IOPS (input/output operations per second).

Supported client and browser combinations

Note All browsers must have Adobe® Flash® Player 11 installed, or a more recent version.

Client OS	Supported Browsers
Windows 7 and 8.1	Internet Explorer 10 and above (compatibility mode is not supported)
	Firefox 30 and above
	Chrome 30 and above
Macintosh OS/X	Firefox 30 and above
	Chrome 30 and above
	Safari 7 and above
Linux/RHEL	Firefox 30 and above
	Chrome 30 and above

Related publications

Title	Description
<i>Cisco UCS Performance Manager Administration Guide</i>	Provides an overview of Cisco UCS Performance Manager architecture and features, as well as procedures and examples to help use the system.
<i>Cisco UCS Performance Manager Getting Started Guide</i>	Provides specific instructions for using Cisco UCS Performance Manager in the UCS environment.
<i>Cisco UCS Performance Manager Installation Guide</i>	Provides detailed information and procedures for installing and upgrading Cisco UCS Performance Manager.

Title	Description
<i>Cisco UCS Performance Manager Release Notes</i>	Describes known issues, fixed issues, and late-breaking information not already provided in the published documentation set.

Documentation feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

Welcome to Cisco UCS Performance Manager

1

Cisco UCS Performance Manager provides visibility from a single console into UCS components for performance monitoring and capacity planning. It provides data center assurance of integrated infrastructures and ties application performance to physical and virtual infrastructure performance. This allows you to optimize resources and deliver better service levels to your customers.

Cisco UCS Performance Manager software is distributed as the following, self-contained packages:

- A self-installing ISO package for Microsoft Hyper-V systems
- A VMware OVA package for vSphere systems

The packages include both the run-time environment (CentOS 6.5) and the application software, and are ready to install on virtual machines. Once a package is installed, the Cisco UCS Performance Manager Setup Wizard guides you through the process of setting up UCS domains, defining users, and providing your license key. If your license is Cisco UCS Performance Manager, the Setup Wizard also includes a convenient way to add infrastructure devices.

Cisco UCS Performance Manager uses standard management APIs to collect performance data, so no proprietary agents are installed on infrastructure devices. However, Cisco recommends that you review the following sections, and verify that the devices to monitor are ready to respond to requests for data.

Note If your license is Cisco UCS Performance Manager Express, skip the following sections.

Preparing Network Devices

Cisco UCS Performance Manager uses SNMP to provide customized or generalized support for many Cisco products.

The following table associates Cisco products with the customized Cisco UCS Performance Manager device types that support them. Device types are listed in the **Network** area of the **Add Infrastructure** wizard, which is both part of the setup wizard and available through the Cisco UCS Performance Manager web interface.

Cisco product	Device type
Cisco Catalyst 6500 and 3560 Series Switches	Cisco 6500 (SNMP)
Cisco Nexus 5000 Series Switches	Cisco Nexus 5000 (SNMP)
Cisco Nexus 1000v Series Switches	Cisco Nexus 1000V (SNMP)
Cisco Nexus 3000 Series Switches	Cisco Nexus 3000 (SNMP)

Cisco product	Device type
Cisco Nexus 9000 Series Switches	Cisco Nexus 9000 (SNMP)
Cisco Catalyst 6500 Series Virtual Switching Systems	Cisco VSS (SNMP)
Cisco MDS 9000 Series Multilayer Switches	Cisco MDS 9000 (SNMP)

In addition, Cisco UCS Performance Manager provides two generalized device types.

Cisco product	Device type
Cisco CatOS-based switches or routers	Generic Switch/Router (SNMP)
Cisco IOS-based switches or routers	Cisco IOS (SNMP)

To prepare a switch or router device for monitoring, verify that an SNMP agent on the device is running.

Preparing Storage Devices

Legacy NetApp Filers

Cisco UCS Performance Manager uses SNMP to monitor legacy NetApp Filers that do not support the Data ONTAP® API (ZAPI).

Note The data gathered are approximate, because the values for many objects (Aggregate, Volume, Plex, and RAID group) are not exposed by the NetApp MIB.

To prepare a legacy NetApp Filer for monitoring, verify that SNMPv2 is installed, and then start an SNMP agent.

Recent NetApp Filers

Cisco UCS Performance Manager uses HTTP to monitor NetApp Filers that support the Data ONTAP® API (ZAPI).

To prepare a recent NetApp Filers for monitoring, verify the following conditions:

- The Filer is running in 7-Mode or C-Mode.
- ZAPI is installed and enabled. Version 8.x, or a more recent version, is required.

Also, you need the username and password of an account on the Filer that is authorized to use ZAPI.

Note Many of the graphs for components types of EMC arrays display NaN when statistics logging is disabled on the EMC device. The logging feature has a low default timeout value, and must be set to a higher value or turned on again periodically.

EMC Storage Arrays

Cisco UCS Performance Manager uses the Web-Based Enterprise Management (WBEM) protocol to send queries to EMC Storage Management Initiative Specification (SMI-S) providers associated with EMC VMAX and VNX storage arrays.

To prepare EMC arrays for monitoring, verify that at least one EMC SMI-S provider is running for each type of array to monitor. (The VMAX and VNX data models are different.) In addition, you need the following information:

- The username and password of a user account that is authorized to collect data on each SMI-S provider.
- The IP address of each SMI-S provider.
- The port number at which each SMI-S provider listens for requests.

Cisco recommends verifying that an SMI-S provider is responding to requests before adding it to Cisco UCS Performance Manager.

Verifying an SMI-S provider

To perform this procedure, you need a Linux host that has a network path to the SMI-S providers of the arrays to monitor.

Note Do not perform this procedure on the Cisco UCS Performance Manager host.

Perform this procedure to verify that the SMI-S providers associated with EMC arrays are configured correctly, and are responding to WBEM queries from command line tools.

- 1 Log in to a Linux host as `root`, or as a user with superuser privileges.
- 2 Install a WBEM command-line interface package, such as `wbemcli`.
- 3 Verify the SMI-S provider. Replace the variables with values that are valid in your environment.

```
wbemcli IP-Address:Port -u admin -p 'Password' -n root/emc --no-ssl
ei('EMC_DiskDrive')
```

The expected result is a list of Disk Drive classes.

Preparing Server Devices

Linux Servers

Cisco UCS Performance Manager uses SNMP or SSH to monitor Linux servers.

To prepare a Linux server for SNMP monitoring, install an SNMP package on the server (for example, [Net-SNMP](#)) and start the agent.

To prepare a Linux server for SSH monitoring, install an SSH server package (for example, [OpenSSH](#)) and start the SSH daemon. Also, obtain the username and password of a user account on the server that has standard user privileges (root privileges are not required).

Windows Servers

Cisco UCS Performance Manager uses SNMP or WinRM to monitor the following Microsoft Windows systems:

- Microsoft Windows Server 2012 and 2012 R2
- Microsoft Windows Server 2008 R2

To prepare a Windows system for SNMP monitoring, start the SNMP service.

To prepare a Windows system for WinRM monitoring, refer to Appendix B, Preparing Windows Systems.

Preparing Hypervisor Devices

VMware vSphere servers

Cisco UCS Performance Manager uses SOAP to monitor VMware vSphere servers running vSphere 4.1, 5.0, or 5.1.

To prepare a VMware vSphere server for monitoring, verify the software version, and obtain the username and password of an account on the server that is authorized to use the vSphere API.

Microsoft Hyper-V servers

Cisco UCS Performance Manager uses WinRM to monitor the following Microsoft Hyper-V systems:

- Microsoft Hyper-V Server 2012 and 2012 R2
- Microsoft Hyper-V Server 2008 and 2008 R2

To prepare a Hyper-V Server for WinRM monitoring, refer to Appendix B, Preparing Windows Systems.

2

Installing with VMware vSphere

This procedure installs the Cisco UCS Performance Manager OVA package on a virtual machine managed by vSphere Server version 5.0.0, using VMware vSphere Client 5.0.0. The procedure is slightly different with different versions of VMware vSphere Client.

Note VMware vSphere Client 5.0.0 does not include a library that is needed to deploy compressed OVA files. You may uncompress the OVA package and then deploy it, or [download and install the missing library](#). Cisco recommends installing the library.

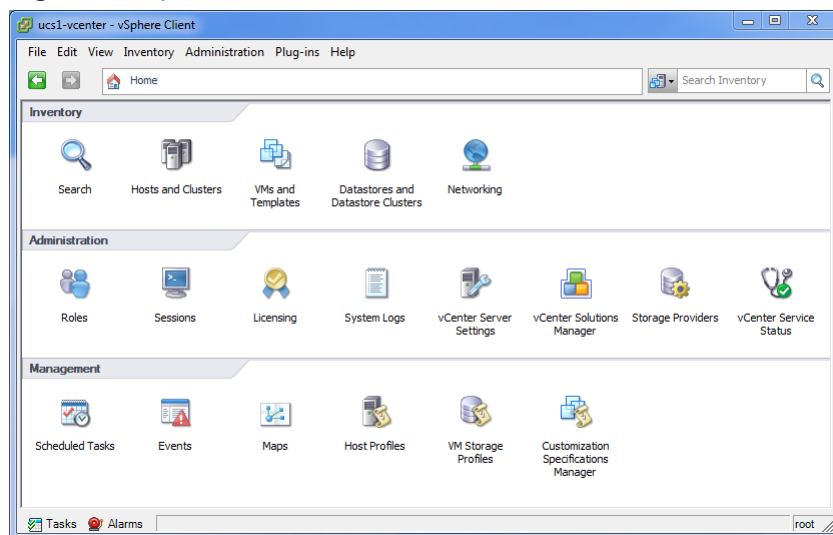
From start to finish, installing Cisco UCS Performance Manager with VMware vSphere takes approximately 10 minutes or less.

Use the minimum system requirement information in the following table to create a new virtual machine for Cisco UCS Performance Manager.

Cisco UCS domain size		Cisco UCS Performance Manager virtual machine size		
Category	Monitored Servers	Cores	Memory	Storage
Small	1-50	4	32GB	50GB
Medium	51-100	8	64GB	100GB
Large	101-500	12	96GB	150GB

Deploying a VMware virtual machine for Cisco UCS Performance Manager

- 1 Download the Cisco UCS Performance Manager package for VMware vSphere servers to your workstation. For more information, see [Downloading Cisco UCS Performance Manager software](#) on page 24.
- 2 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home** view.

Figure 1: vSphere client Home view

- 3 From the **File** menu, select **Deploy OVF Template....**
- 4 In the **Source** panel, specify the path of the Cisco UCS Performance Manager package, and then click **Next >**.
- 5 In the **OVF Template Details** panel, click **Next >**.
- 6 In the **Name and Location** panel, provide a name and a location for the server.
 - a In the **Name** field, enter a new name or use the default.
 - b In the **Inventory Location** area, select a data center for the virtual machine.
 - c Click **Next >**.
- 7 In the **Host / Cluster** panel, select a host system, and then click **Next >**.
- 8 In the **Storage** panel, select a storage system with sufficient space for your UCS system, and then click **Next >**.
- 9 In the **Disk Format** panel, select **Thin Provision**, and then click **Next >**.
- 10 In the **Ready to Complete** panel, review the deployment settings, and then click **Finish**.
You may check the check box labeled **Power on after deployment**, or wait until the deployment is complete and then power on the virtual machine.
- 11 In the **Home > Inventory > Hosts and Clusters** panel, click the **Summary** tab, and then make a note of the IP address of the newly-deployed host.

Note If DHCP is not available in your environment, or if you want to change networking settings, see [Configuring network device settings](#) on page 25.

Setting the root password

Perform this task immediately after deploying and starting a VMware virtual machine for Cisco UCS Performance Manager.

- 1 Use the VMware vSphere Client to log in to vCenter as `root`, or as a user with superuser privileges, and then display the **Home** view.
- 2 In the **Home > Inventory > Hosts and Clusters** panel, click the **Console** tab of the newly-deployed host.
- 3 In the console window of the host, log in as the `root` user, with password `zenoss`.

Figure 2: Example login prompt

```

Welcome to Cisco UCS Performance Manager 1.0.0

To access the UCS-PM Management Console, please browse to:

    http://10.87.209.233:8080

Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _

```

- 4 The system prompts you to replace the default password with a new password.

Figure 3: Change password prompt

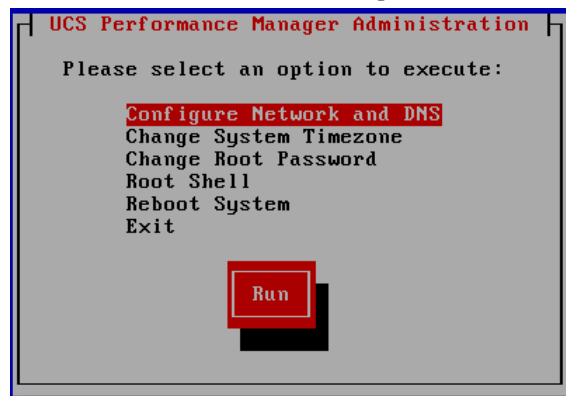
```

Linux Kernel 2.6.32-431.23.3.el6.x86_64 on an x86_64
localhost login: root
Password:
You are required to change your password immediately (root enforced)
Changing password for root.
(current) UNIX password: _

```

- a Enter the default password, zenoss.
- b Enter a new password, twice.

The Cisco UCS Performance Manager Administration menu displays.



- c Use the down-arrow key to select **Exit**, then press Enter.

Proceed to [Setting up Cisco UCS Performance Manager](#) on page 17.

3

Installing with Hyper-V Manager

This install procedure requires Microsoft Remote Desktop Client.

From start to finish, installing Cisco UCS Performance Manager with Hyper-V Manager takes approximately 30 minutes.

Use the minimum system requirement information in the following table to create a new virtual machine for Cisco UCS Performance Manager.

Cisco UCS domain size		Cisco UCS Performance Manager virtual machine size		
Category	Monitored Servers	Cores	Memory	Storage
Small	1-50	4	32GB	50GB
Medium	51-100	8	64GB	100GB
Large	101-500	12	96GB	150GB

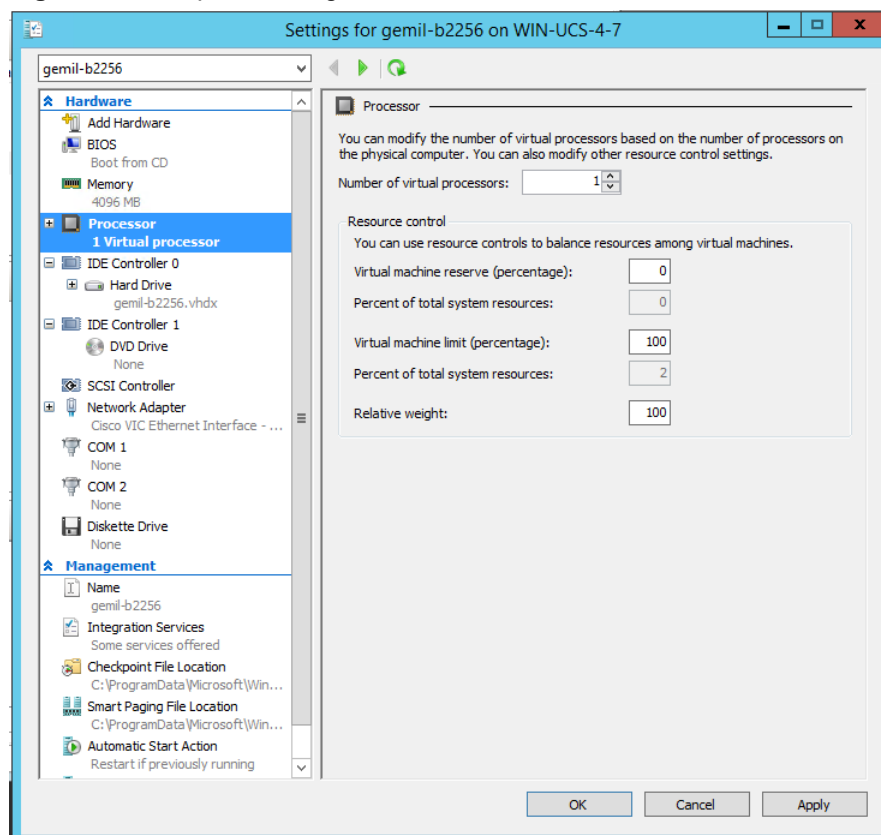
Creating a Hyper-V virtual machine for Cisco UCS Performance Manager

- 1 Use Remote Desktop Connection to log in to a Hyper-V server as Administrator, or as a user with Administrator privileges.
- 2 Download the Cisco UCS Performance Manager package for Hyper-V servers.
For more information, see [Downloading Cisco UCS Performance Manager software](#) on page 24.
- 3 Start **Hyper-V Manager**.
- 4 From the **Action** menu, select **New > Virtual Machine...**
- 5 In the **New Virtual Machine Wizard** dialog, display the **Specify Name and Location** panel.
If the first panel displayed is the **Before You Begin** panel, click **Next >**.
- 6 In the **Specify Name and Location** panel, provide a name for the virtual machine, and then click **Next >**.
- 7 In the **Specify Generation** panel, select **Generation 1**, and then click **Next >**.
- 8 In the **Assign Memory** panel, enter the memory size for the virtual machine in the **Startup memory** field, and then click **Next >**.
For more information about memory size, refer to [Installing with Hyper-V Manager](#) on page 13.
- 9 In the **Configure Networking** panel, select **Cisco VIC Ethernet Interface - Virtual Switch**, and then click **Next >**.
- 10 In the **Connect Virtual Hard Disk** panel, select **Create a virtual hard disk**, enter the disk size for the virtual machine, and then click **Next >**.

For more information about disk size, refer to [Installing with Hyper-V Manager](#) on page 13.

- 11 In the **Installation Options** panel, specify the Cisco UCS Performance Manager ISO package.
 - a Select **Install an operating system from a bootable CD/DVD-ROM**.
 - b Select **Image file (.iso)**, and then specify the location of the Cisco UCS Performance Manager ISO image file.
 - c Click **Next >**.
- 12 In the **Summary** panel, review the virtual machine specification, and then click **Finish**.
Hyper-V Manager creates the new virtual machine, and then closes the **New Virtual Machine Wizard** dialog.
- 13 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Settings...**
- 14 In the **Hardware** area of the **Settings** dialog, select **Processor**.

Figure 4: Example: Starting a new virtual machine



- 15 In the **Processor** area, set the value in the **Number of virtual processors** field to the number of cores recommended for your installation.

For more information about the number of cores, refer to [Installing with Hyper-V Manager](#) on page 13.

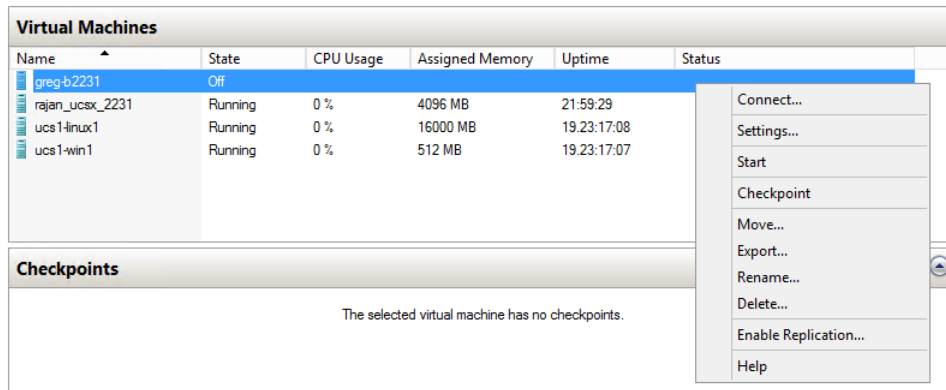
- 16 Click **OK**.

Proceed to [Installing Cisco UCS Performance Manager](#) on page 14.

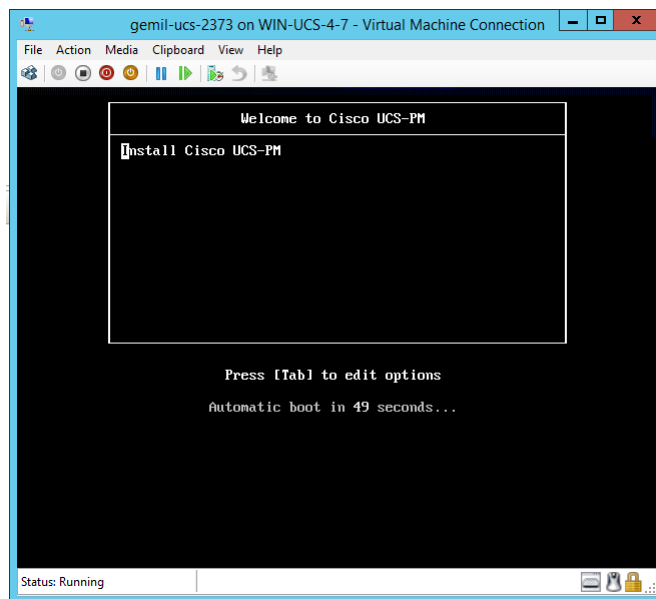
Installing Cisco UCS Performance Manager

Perform this procedure after creating a virtual machine for Cisco UCS Performance Manager in Hyper-V Manager.

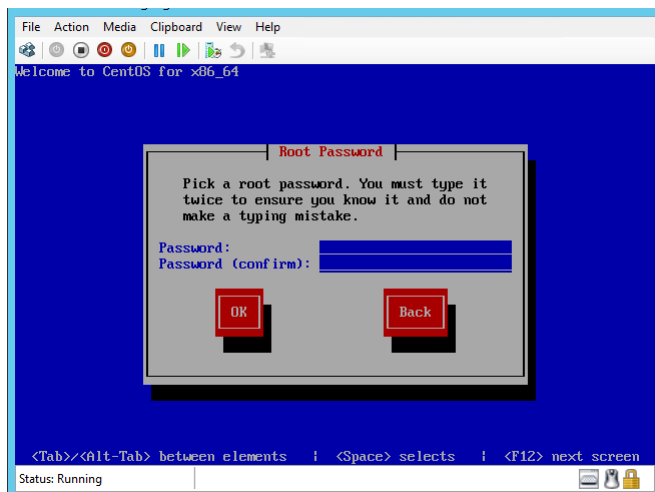
- 1 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Start**.

Figure 5: Example: Starting a new virtual machine

- 2 In the **Virtual Machines** area of Hyper-V Manager, select the new virtual machine, and then right-click to select **Connect**.
- 3 In the **Virtual Machine Connection** window, press ENTER or allow the automatic boot time to expire.

Figure 6: Installation start screen

- 4 In the **Virtual Machine Connection** window, enter a password for the `root` user account, twice.

Figure 7: Root Password screen

- 5 Press the TAB key, and then press ENTER.
The installation runs to completion after this input.
- 6 Write down the URL of the Cisco UCS Performance Manager interface.

Note If DHCP is not available in your environment, or if you want to change networking settings, see [Configuring network device settings](#) on page 25.

```

Welcome to Cisco UCS Performance Manager 1.0.0

To access the UCS-PM Management Console, please browse to:

    http://10.87.209.233:8080

Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _
  
```

Proceed to [Setting up Cisco UCS Performance Manager](#) on page 17.

Setting up Cisco UCS Performance Manager

4

This section describes how to use the Cisco UCS Performance Manager Setup Wizard to set up UCS domains, define users, and provide your license key.

The Setup Wizard runs the first time you log in to the Cisco UCS Performance Manager web interface. (For more information about supported browsers and client operating systems, see [Preface](#) on page 4.)

The Cisco UCS Performance Manager web server listens at port 8080. So, if the IP address of your Cisco UCS Performance Manager virtual machine `my-vm.example.com` is 10.92.10.10, both of the following URLs return the login page.

- `http://my-vm.example.com:8080/`
- `http://10.92.10.10:8080/`

Note The Setup Wizard times out after 20 minutes if you have not completed it. To start it again, close its browser window or tab, and then log in again.

To complete the Setup Wizard, you need the following items:

- Authorization to accept the Cisco UCS Performance Manager end-user license agreement on behalf of your organization.
- A password for the default administrative account (`admin`).
- A username and password for one additional administrative account.
- The license key for your product (Cisco UCS Performance Manager Express or Cisco UCS Performance Manager). To obtain a license key, contact your Cisco representative.
- The hostnames or IP addresses of UCS Domain servers in your environment. In addition, you need the username and password of an account on each server that is authorized for read access to the resources you plan to monitor.

If your license is Cisco UCS Performance Manager, the Setup Wizard includes the **Add Infrastructure** page as the final step. The step is optional, and the page is a standard part of the Cisco UCS Performance Manager interface, so you can use it at any time. To use the **Add Infrastructure** page successfully as part of the Setup Wizard, review the device information in [Welcome to Cisco UCS Performance Manager](#) on page 6.

Accepting the License Agreement

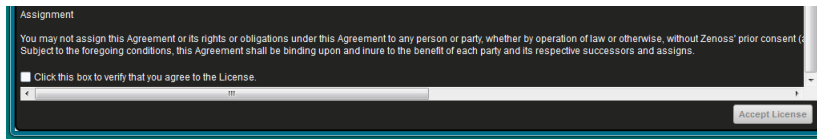
Perform this procedure after installing Cisco UCS Performance Manager on a virtual machine and powering it on.

- 1 In a web browser, navigate to the login page of the Cisco UCS Performance Manager interface.

Cisco UCS Performance Manager redirects the first login attempt to the Setup page, which includes the **End User License Agreement** (EULA) dialog.

- 2 Read through the agreement.
- 3 At the bottom of the EULA dialog, check the check box on the left side, and then click **Accept License** button on the right side.

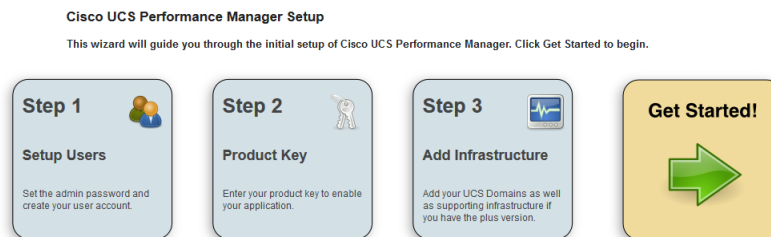
Figure 8: Bottom of EULA dialog



Setting up Users

Perform this procedure after accepting the EULA.

- 1 On the **Cisco UCS Performance Manager Setup** page, click **Get Started!**.



- 2 On the **Setup Users** page, enter a password for the admin user, and create an account for one additional user.

Step 1: Setup Users

<p>Set admin password</p> <p><small>The admin account has extended privileges, similar to Linux's root or Windows' Administrator. Its use should be limited to administrative tasks.</small></p> <p><small>Enter and confirm a password for the admin account.</small></p> <p>Admin password: <input type="password"/></p> <p>Retype password: <input type="password"/></p> <p><input type="button" value="Previous"/></p>	<p>Create your account</p> <p><small>Enter information for your personal user account. You'll use this to perform most tasks.</small></p> <p>Username: <input type="text"/></p> <p>Password: <input type="password"/></p> <p>Retype password: <input type="password"/></p> <p>Your email: <input type="text"/></p> <p><input type="button" value="Next"/></p>
---	--

- a In the **Set admin password** area, enter and confirm a password for the admin user account.
- b In the **Create your account** area, create one additional administrative user account.
- c Click **Next**.

Providing a license key

To perform this procedure, you need a license key for Cisco UCS Performance Manager Express or Cisco UCS Performance Manager.

This is Step 2 of the Setup Wizard.

- 1 In the **Enter your Product Key** field, enter your license key.

Step 2: Add Product Key

Enter your Product Key:

PreviousNext

- 2 Proceed to the next task or repeat the preceding step.
- If the product name matches the product you purchased, click **Next**.
 - If the product name does not match the product you purchased, repeat the preceding step.

Note The Cisco UCS Performance Manager interface includes an option for changing your license key.

Adding UCS Domains

This is Step 3 of the Setup Wizard.

- 1 On the **Add UCS Domains** page, provide connection credentials for one or more domains.

Step 3: Add UCS Domains

Credentials

Hostname or IP Address:

Username:

Password:

Add

Domains

Host/IP Address	Username	Port	SSL	Connection Valid?	Remove
-----------------	----------	------	-----	-------------------	--------

PreviousNext

- a In the **Hostname or IP Address** field, enter the fully-qualified domain name or IP address of a UCS domain server.
- b In the **Username** field, enter the name of a user account in the UCS domain that is authorized for read access to the resources you plan to monitor.
- c In the **Password** field, enter the password of the user account specified in the preceding step.
- d Click **Add**.
- 2 Review the information in the **Connection Valid?** column of the **Domains** table, and then remove a domain, add a domain, or continue.

Step 3: Add UCS Domains

Credentials

Hostname or IP Address:

10.87.208.163

Username:

ucs_viewer

Password:

Add

Domains

Host/IP Address	Username	Port	SSL	Connection Valid?	Remove
10.87.208.163	ucs_vl...	443	true	Success	

PreviousNext

- If the final message in the **Connection Valid?** column is `Authentication failed`, click the button in the **Remove** column, and then try again to add a domain.

- If the final message in the **Connection Valid?** column is **Success**, you may add another domain or continue to the next page.
- 3 Continue to the next page.
 - If your license is Cisco UCS Performance Manager Express, click **Finish** to continue to the **DASHBOARD** page of the web interface.
 - If your license is Cisco UCS Performance Manager, click **Next** to continue to the **Add Infrastructure** page.

Adding Infrastructure Devices

Note This step is not available in Cisco UCS Performance Manager Express.

This is Step 4 of the Setup Wizard.

Step 4: Add Infrastructure

- This step is optional. Click **Finish** to exit the Setup Wizard.
- The Setup Wizard times out after 20 minutes if you have not completed it. You may restart Setup Wizard by closing its browser window or tab, and then logging in again. Also, you may add devices through the **Add Infrastructure** page at any time.

Adding Network Devices

This procedure is one of the options in step 4 of the Setup Wizard. For more information about network devices, see [Preparing Network Devices](#) on page 6.

- 1 In the **Category** area, select **Network**.

Step 4: Add Infrastructure

- 2 In the **Type** list, select the product model of the switch or router to add.

The protocol used to gather data from the device is included in the list, in parentheses. SNMP is the only protocol available for network devices.

- 3 In the **Connection Information** area, specify the devices to add.
 - a In the **Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses** field, enter the hostname or IP address of one or more switch or router devices on your network.
 - b Optional: In the **SNMP Community String** field, change the default (`public`) if necessary.
This field is not used if the selected device supports both SNMP and NETCONF, and you provide a user name and password.
 - c Optional: In the **Username** field, enter the name of a user account on the device.
This field is only present when the selected device supports both SNMP and NETCONF. By providing a user name and password, you select NETCONF protocol.
 - d Optional: In the **Password** field, enter the password of the user account specified in the previous field.
This field is only present when the selected device supports both SNMP and NETCONF. By providing a user name and password, you select NETCONF protocol.
 - e Click **Add**.

If you are finished adding devices, click **Finish**.

Adding Storage Devices

This procedure is one of the options in step 4 of the Setup Wizard. For more information about storage devices, see [Preparing Storage Devices](#) on page 7.

- 1 In the **Category** area, select **Storage**.

Step 4: Add Infrastructure

- 2 In the **Type** list, select the product model of the storage device to add.
The protocol used to gather data from the device is included in the list, in parentheses.
- 3 In the **Connection Information** area, specify the devices to add.
 - a In the **Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses** field, enter the hostname or IP address of one or more storage devices on your network.
 - b Optional: In the **Username** field, enter the name of a user account on the device.
This field is not present when the device protocol is SNMP.
 - c Optional: In the **Password** field, enter the password of the user account specified in the previous field.
This field is not present when the device protocol is SNMP.
 - d Optional: In the **Port** field, enter the port at which the device listens for data collection requests.
This field is present only when the device protocol is SMIS Proxy.
 - e Check the **Use SSL?** check box to use secure communications to collect data, or uncheck the check box to use insecure communications.
This field is not present when the device protocol is SNMP.
 - f Click **Add**.

If you are finished adding devices, click **Finish**.

Adding Server Devices

This procedure is one of the options in step 4 of the Setup Wizard. For more information about server devices, see [Preparing Server Devices](#) on page 8.

- 1 In the **Category** area, select **Servers**.

Step 4: Add Infrastructure

- 2 In the **Type** list, select the operating system and monitoring protocol of the server to add.
The protocol used to gather data from the device is included in the list, in parentheses.
- 3 In the **Connection Information** area, specify the servers to add.
 - a In the **Enter multiple similar devices, separated by a comma, using either hostname or IP Addresses** field, enter the hostname or IP address of one or more server devices on your network.
 - b Optional: In the **SNMP Community String** field, change the default (`public`) if necessary.
This field is not present when the device protocol is SNMP.
 - c Optional: In the **Username** field, enter the name of a user account on the device.
This field is not present when the device protocol is SNMP.
 - d Optional: In the **Password** field, enter the password of the user account specified in the previous field.
This field is not present when the device protocol is SNMP.
 - e Optional: In the **AD Domain Controller** field, enter the IP address or hostname of the Active Directory Domain Controller on your network.
This field is only present when the device protocol is WinRM.
 - f Click **Add**.

If you are finished adding devices, click **Finish**.

Adding Hypervisor Devices

This procedure is one of the options in step 4 of the Setup Wizard. For more information about hypervisor devices, see [Preparing Hypervisor Devices](#) on page 8.

- 1 In the **Category** area, select **Hypervisor**.

Step 4: Add Infrastructure

Category <input type="radio"/> Network <input type="radio"/> Storage <input type="radio"/> Server <input checked="" type="radio"/> Hypervisor	Type <div>vSphere EndPoint (SOAP) ▼</div>	Connection Information Device Name: <input type="text"/> Hostname / IP Address: <input type="text"/> Username: <input type="text" value="admin"/> Password: <input type="password"/> Use SSL?: <input checked="" type="checkbox"/> <input type="button" value="Add"/>
--	---	---

- 2 In the **Type** list, select the hypervisor service to add.
- 3 In the **Connection Information** area, specify the service to add.
 - a In the **Device Name** field, enter the name of the hypervisor service.
 - b In the **Hostname / IP Address** field, enter the hostname or IP address of the hypervisor service.
 - c In the **Username** field, enter the name of a user account on the host.
 - d In the **Password** field, enter the password of the user account specified in the previous field.
 - e Optional: Check the **Use SSL?** check box to use secure communications to collect data (recommended).
This field is only present when the device protocol is SOAP.
 - f Optional: From the **Version** list, select the operating system version of the hypervisor's host.
This field is only present when the device protocol is WinRM.
 - g Click **Add**.

If you are finished adding devices, click **Done**.

Maintaining Cisco UCS Performance Manager

5

Maintenance tasks include updating Cisco UCS Performance Manager software and updating the Cisco UCS Performance Manager server operating system.

Downloading Cisco UCS Performance Manager software

To perform this procedure, you need permission to download Cisco UCS Performance Manager software from the Cisco support site.

- 1 In a web browser, navigate to the [Cisco UCS Performance Manager](#) site.
- 2 Select a package file to download.

File	Description
cisco-ucs-perf-mgr-*.x86_64.iso	Microsoft Hyper-V server installation package
cisco-ucs-perf-mgr-*.ova	VMware vSphere server installation package

Updating the Cisco UCS Performance Manager server operating system

To perform this procedure, you need the following items:

- Access to the console window of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V
- The password of the `root` account on the Cisco UCS Performance Manager virtual machine

This procedure requires some Cisco UCS Performance Manager downtime. Restarting Cisco UCS Performance Manager requires approximately 3 minutes, and restarting the operating system requires approximately 5 to 10 minutes.

- 1 Gain access to the console interface of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V.


```

Welcome to Cisco UCS Performance Manager 1.0.0

To access the UCS-PM Management Console, please browse to:

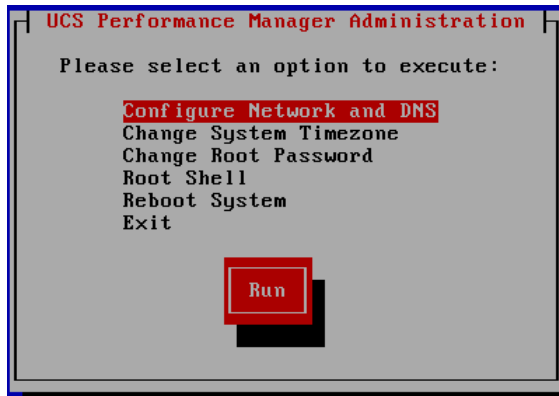
    http://10.87.209.233:8080

Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _

```

- 2 Log in to the virtual machine as root.



- 3 From the **UCS Performance Manager Administration** menu, use the UP-ARROW or DOWN-ARROW key to select **Root Shell**, and then press ENTER.
- 4 Start the operating system update.

```
yum -y update
```

Monitor the packages that are downloaded and installed, to determine whether the update includes a new kernel.
- 5 Restart the server or restart Cisco UCS Performance Manager.

- If the update includes a new kernel, restart the server.

```
reboot
```

- If the update does not include a new kernel, restart Cisco UCS Performance Manager, and then exit.

```
service zenoss restart; exit
```

Configuring network device settings

To perform this procedure, you need the following items:

- Access to the console window of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V
 - The password of the root account on the Cisco UCS Performance Manager virtual machine
- 1 Gain access to the console interface of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V.

```

Welcome to Cisco UCS Performance Manager 1.0.0

To access the UCS-PM Management Console, please browse to:

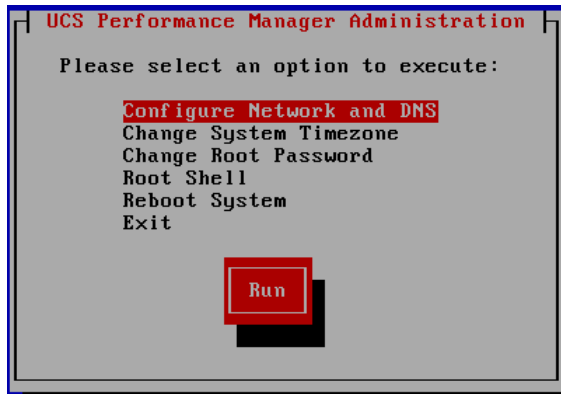
  http://10.87.209.233:8080

Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

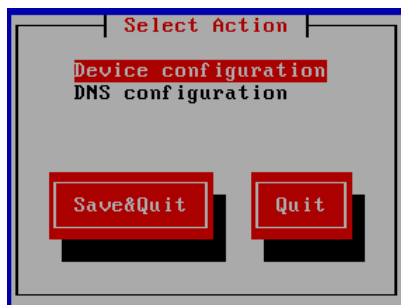
Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _

```

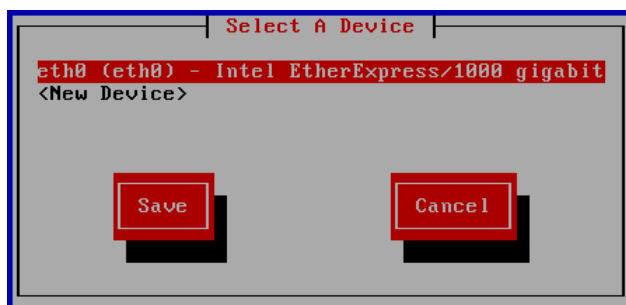
- 2 Log in to the virtual machine as root.



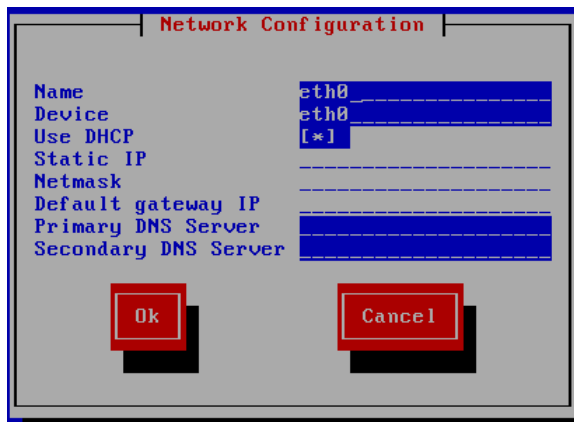
- 3 From the **UCS Performance Manager Administration** menu, use the UP-ARROW or DOWN-ARROW key to select **Configure Network and DNS**, and then press ENTER.



- 4 Select **Device Configuration**, and then press ENTER.



- 5 Select an ethernet controller device, and then press ENTER.



- 6 In the **Network Configuration** screen, modify the device settings.
 - To move down through the fields, use TAB. To move up, use SHIFT-TAB.
 - To select or deselect **Use DHCP**, use SPACE.
- 7 Select **OK** and press ENTER to save the settings and return to the **Select a Device** screen.
- 8 Select **Save** and press ENTER to save the device configuration and return to the **Configure Network and DNS** screen.
- 9 Select **Save&Quit** and press ENTER to save the changes and return to the **UCS Performance Manager Administration** menu.
- 10 Use the UP-ARROW or DOWN-ARROW key to select **Reboot System**, and then press ENTER.

Configuring DNS settings

To perform this procedure, you need the following items:

- Access to the console window of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V
 - The password of the `root` account on the Cisco UCS Performance Manager virtual machine
- 1 Gain access to the console interface of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V.

```

Welcome to Cisco UCS Performance Manager 1.0.0

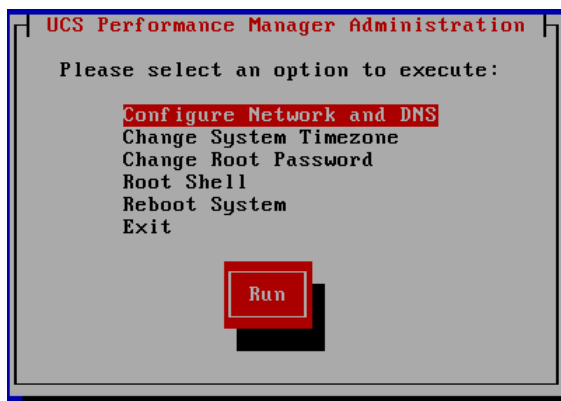
To access the UCS-PM Management Console, please browse to:

  http://10.87.209.233:8080

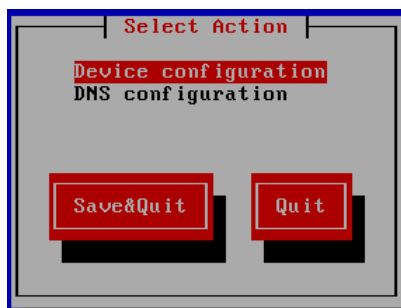
Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _
  
```

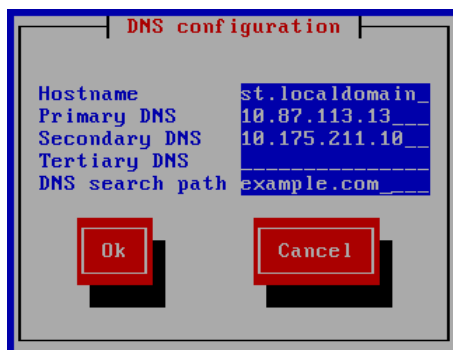
- 2 Log in to the virtual machine as `root`.



- 3 From the **UCS Performance Manager Administration** menu, use the UP-ARROW or DOWN-ARROW key to select **Configure Network and DNS**, and then press ENTER.



- 4 Select **DNS Configuration**, and then press ENTER.



- 5 In the **DNS Configuration** screen, modify the settings.

To move down through the fields, use TAB. To move up, use SHIFT-TAB.

Note Cisco recommends not changing the hostname of a Cisco UCS Performance Manager virtual machine after installation.

- 6 Select **OK**, and then press ENTER, to save the settings and return to the **Select Action** screen.
- 7 Select **Save&Quit**, and then press ENTER, to save the changes and return to the **UCS Performance Manager Administration** menu.
- 8 Use the UP-ARROW or DOWN-ARROW key to select **Exit**, and then press ENTER.

A

Configuring HTTPS communications

Cisco UCS Performance Manager employs `nginx` as a load balancer for the Zope application server. The procedures in this appendix configure `nginx` for HTTPS (HTTP/SSL) communications.

Creating a self-signed SSL certificate

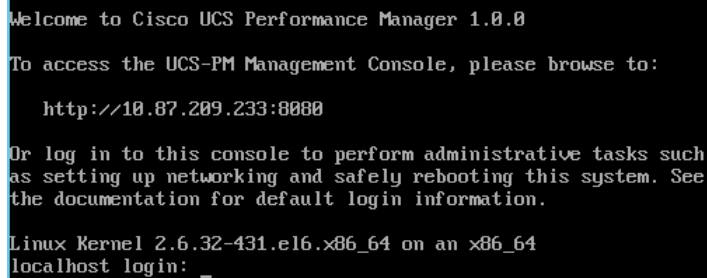
To perform this procedure, you need the following items:

- Access to the console window of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V
- The password of the `root` account on the Cisco UCS Performance Manager virtual machine

Perform this procedure if you do not have an SSL certificate signed by a certificate authority.

Note The default security settings of most browsers trigger warning messages when a web server presents a self-signed SSL certificate. The warnings are not displayed when a web server presents an SSL certificate signed by a certificate authority.

- 1 Gain access to the console interface of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V.

A screenshot of a terminal window showing the Cisco UCS Performance Manager 1.0.0 boot sequence. The text is as follows:

```
Welcome to Cisco UCS Performance Manager 1.0.0

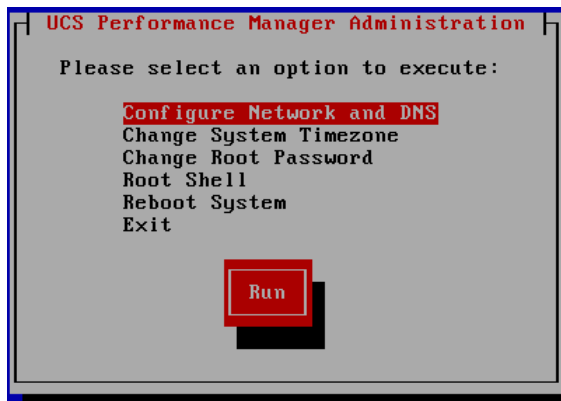
To access the UCS-PM Management Console, please browse to:

    http://10.87.209.233:8080

Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _
```

- 2 Log in to the virtual machine as `root`.



- 3 From the **UCS Performance Manager Administration** menu, use the UP-ARROW or DOWN-ARROW key to select **Root Shell**, and then press ENTER.
- 4 Switch user to zenoss.

```
su - zenoss
```
- 5 Create a directory for the certificate and key files, and then make the new directory the current directory.

```
mkdir /opt/zenoss/etc/ssl && cd /opt/zenoss/etc/ssl
```
- 6 Create a private key.

```
openssl genrsa -des3 -out zenoss.key 1024
```

The openssl command prompts for a passphrase. You may enter any string as the passphrase. Subsequent steps remove the passphrase from the key.
- 7 Create the signing request.

```
openssl req -new -key zenoss.key -out zenoss.csr
```

The openssl command prompts for the passphrase you entered in the previous step, and then presents additional prompts, for certificate information.
- 8 Remove the pass phrase requirement.

```
cp zenoss.key zenoss.key.orig  
openssl rsa -in zenoss.key.orig -out zenoss.key
```

The openssl command prompts for the passphrase you entered previously.
- 9 Sign the certificate.

```
openssl x509 -req -days 365 -in zenoss.csr -signkey zenoss.key -out zenoss.crt
```

Configuring the nginx server

To perform this procedure, you need the following items:

- Access to the console window of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V
- The password of the root account on the Cisco UCS Performance Manager virtual machine
- A self-signed SSL certificate or an SSL certificate signed by a certificate authority

Cisco UCS Performance Manager includes `zenwebserver`, a script for managing the integration between the nginx load balancer and the Zope application server. The `zenwebserver` configuration file contains customized directives that `zenwebserver` translates into nginx directives for nginx configuration files.

This procedure briefly disables access to the Cisco UCS Performance Manager interface.

- 1 Gain access to the console interface of the Cisco UCS Performance Manager virtual machine, through VMware vSphere or Microsoft Hyper-V.

```

Welcome to Cisco UCS Performance Manager 1.0.0

To access the UCS-PM Management Console, please browse to:

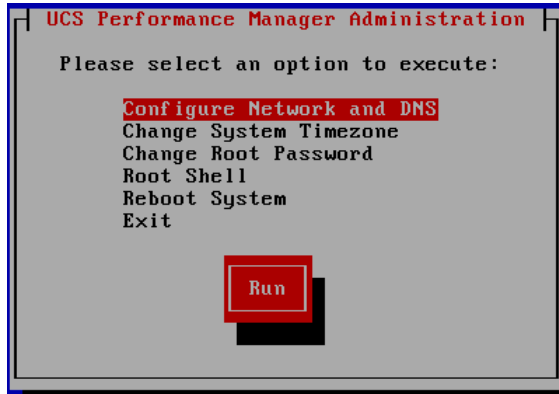
    http://10.87.209.233:8080

Or log in to this console to perform administrative tasks such
as setting up networking and safely rebooting this system. See
the documentation for default login information.

Linux Kernel 2.6.32-431.el6.x86_64 on an x86_64
localhost login: _

```

- 2 Log in to the virtual machine as root.



- 3 From the **UCS Performance Manager Administration** menu, use the UP-ARROW or DOWN-ARROW key to select **Root Shell**, and then press ENTER.
- 4 Switch user to zenoss.
`su - zenoss`
- 5 Create a directory for the certificate and key files, and then make the new directory the current directory. Subsequent steps assume the certificate and key files are located in the `/opt/zenoss/etc/ssl` directory. Files in the `/opt/zenoss/etc` hierarchy are preserved during upgrades.

- If you performed the preceding procedure to create a self-signed certificate, enter the following command.

```
cd /opt/zenoss/etc/ssl
```

- If you have an SSL certificate signed by a certificate authority, enter the following commands:

```
mkdir /opt/zenoss/etc/ssl && cd /opt/zenoss/etc/ssl
```

- 6 Optional: Download your certificate and key files to the current directory. If you performed the preceding procedure to create a self-signed certificate, proceed to the next step.

- 7 Stop the Cisco UCS Performance Manager web server daemons.

```
zenwebserver stop
```

- 8 Change the ownership and permissions of the nginx executable.

The following commands prompt for the root password.

```
TARGET=$(readlink /opt/zenoss/bin/nginx)
su -c "chown root:zenoss $TARGET && chmod 04750 $TARGET"
```

- 9 Verify the ownership and permissions of the nginx executable.

```
ls -lL /opt/zenoss/bin/nginx
```

The first portion of the result of the preceding command should match the following text.

```
-rwsr-x---. 1 root zenoss
```

- 10 Edit `/opt/zenoss/etc/zenwebserver.conf` to configure nginx for SSL communications.
 - a Change the value of the `useSSL` directive from `False` to `True`.
 - b Remove the number sign character (`#`) from the beginning of the line that contains the `sslPort` directive.
You may change the value, if desired. 443 is the standard port for HTTPS communications, but any available port less than 1024 may be used.
 - c Remove the number sign character (`#`) from the beginning of the line that contains the `sslCert` directive.
If you are using an SSL certificate signed by a certificate authority, change the value to the name of your certificate file.
 - d Remove the number sign character (`#`) from the beginning of the line that contains the `sslKey` directive.
If you are using an SSL certificate signed by a certificate authority, change the value to the name of your key file.
- 11 Start the Cisco UCS Performance Manager web server daemons.
`zenwebserver start`
- 12 Reconfigure the nginx load balancer.
`zenwebserver configure`
- 13 Restart nginx.
`zenwebserver reload`

Appendix B: Preparing Windows Systems

This appendix includes procedures for preparing Microsoft Windows Server 2012 R2, 2012, and 2008R2 for monitoring in Cisco UCS Performance Manager. The procedures are standardized around a low security configuration using local system credentials, rather than domain credentials, and no encryption of credentials or payload. This scenario provides a good base configuration for ease of setup and testing, but in production the use of a single domain service for authentication simplifies administration. The use of a domain service account requires the use of Kerberos to encrypt credentials, which improves security. Security can be improved further still by configuring WinRM to encrypt its payload using SSL. Each section of this document includes these additional configurations for administrators who need to implement them. These higher security configurations are recommended in production environments.

About Windows Authentication for WinRM Monitoring

Cisco UCS Performance Manager must authenticate to the Windows systems it will monitor using either local system or Windows domain credentials. The Windows user account used for WinRM authentication must have specific permissions granted on each Windows system to be monitored. By default, Windows Administrator accounts already have the necessary permissions, but best practices dictate that Administrator accounts not be used for purposes such as WinRM monitoring. Instead, a dedicated User account (a “service account”) should be created specifically for the purpose of WinRM monitoring with only the necessary permissions granted to the account.

Instead of manually editing the necessary permissions, a Windows PowerShell®, hereafter referred to as *PowerShell*, script can be used to modify the necessary permissions in a single step. For convenience, Cisco provides a sample script that modifies the permissions necessary for an example service. The script is available at the Cisco UCS Performance Manager section of the Cisco Support site. The file can be edited as necessary to suit specific production environments.

Note: The sample script includes two lines that must be located and deleted before the functions in the script will execute. These lines have been deliberately included to encourage administrators to thoroughly review the script before deploying it to ensure (i) that administrators fully understand the functions it performs and (ii) they have made any necessary edits before deploying it.

The relevant sections below describe methods to configure Windows system permissions using a PowerShell script such as *zenoss-lpu.ps1* that has been tailored to a specific environment.

Windows Server 2012 & 2012 R2

The following sections describe how to configure Windows Server 2012 and Windows Server 2012 R2.

Note: Windows 2012 R2 is specifically called out only when there is a difference in method between the two Windows server versions.

Configuring Windows Server 2012 Using Group Policy (Basic Authentication, no Encryption)

Note: This configuration uses a local user account on each monitored Windows system for authentication instead of a domain account. The local user account must be present on each system before Cisco UCS Performance Manager can monitor it.

1. Log on to a domain controller as a user with 'Domain Admin' privileges.
2. On Server 2012 (non R2), press the **Windows** key on the keyboard to display the *Start* screen, then click the **Group Policy Management** tile.
3. On Server 2012 R2, press the **Windows** key on the keyboard to display the *Start* screen, then click Server Manager. Click **Tools** in the upper right, then choose **Group Policy Management**.
4. Navigate to your target domain in the tree at the left:
 - i. Expand the section for the domain Forest you want to edit.
 - ii. Expand **Domains**.
 - iii. Expand your target domain.
5. Right-click **Group Policy Objects** and select *New*. In the form that displays:
 - i. Enter a name for your new Group Policy Object, for example, *WinRM_Monitoring*.
 - ii. Leave "(none)" in the **Source Starter GPO** field.
 - iii. Click **OK** to save and exit the form.
6. Select your new **Group Domain Policy Object**, *WinRM_Monitoring*, for example.
7. Right click your new **Group Domain Policy Object** and select *Edit* to open the Group Policy Management Editor.
8. Expand the **Computer Configuration** section of the tree and navigate the tree to:

```
Policies\Administrative Templates:Policy...\Windows  
Components\Windows Remote Management (WinRM)
```
9. Enable remote server management:
 - i. Click on **WinRM Service** to access the *WinRM Service Group Policy* settings in the right pane.
 - ii. Double-click the **Allow remote server management through WinRM** property.
 - iii. Click the **Enabled** radio button.
 - iv. Place an asterisk as a wildcard (' * ') in the *IPv4 filer* and *IPv6 fields* or specify a range of IP addresses for WinRM to listen on.
 - v. Click **OK** at the bottom to submit the form.
10. Enable authentication:
 - i. Double-click the **Allow Basic authentication** property in the right pane.
 - ii. Select the **Enabled** radio button.
 - iii. Click **OK** at the bottom to submit the form.
11. Specify unencrypted traffic:
 - i. Double-click the **Allow unencrypted traffic** property.
 - ii. Select the **Enabled** radio button.
 - iii. Click **OK** at the bottom to submit the form.
12. Select *Windows Remote Shell* in the left pane to set its **Group Policy** settings. This is located in the

group policy tree in the following location (which might be located right below *WinRM* service in the tree):

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell

13. Configure remote shell access:

- i. In the right pane, double-click **Allow Remote Shell Access**.
- ii. Select the **Enabled** radio button.
- iii. Click **OK** at the bottom to submit the form.

14. Configure shell processes:

- i. In the right pane, double-click **Specify maximum number of processes per Shell**.
- ii. Select the **Enabled** radio button.
- iii. Enter the value **2,000,000,000** (without commas or spaces) in the *MaxProcessPerShell* field.
- iv. Click **OK** at the bottom to submit the form.

15. Configure the number of remote shells:

- i. In the right pane, double-click **Specify maximum number of remote shells per user**.
- ii. Select the **Enabled** radio button.
- iii. Enter the value **2,000,000,000** (without commas or spaces) in the *MaxShellsPerUser* field.
- iv. Click **OK** at the bottom to submit the form.

16. Configure shell timeout value:

- i. In the Right pane, double-click **Specify Shell Timeout**.
- ii. Select the **Enabled** radio button.
- iii. Enter the value **7,200,000** (without commas or spaces) in the *ShellTimeOut* field.
- iv. Click **OK** at the bottom to submit the form.

Windows Server 2012: Configuring Firewall Group Policies

WinRM listens on port 5985 when data payload encryption is not used and on port 5986 when encryption is used. Additionally, ICMP (ping) requests must be enabled because Cisco UCS Performance Manager uses them as a source of availability monitoring.

The appropriate port must be opened on the firewalls of monitored servers. You can use Group Policy to open the required ports on all servers across the organization.

1. In the Group Policy Manager Editor, navigate to:

Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security - LDAP;...\Inbound Rules

2. Create a new *Inbound Rules* policy for **Windows Remote Management**:

- i. Right click **Inbound Rules** in the left pane.
- ii. Select **New Rule...**
- iii. Select the **Predefined** radio button.
- iv. Select **Windows Remote Management** from the drop down list.
- v. Click **Next**.
- vi. Ensure that all items in the list are checked.
- vii. Click **Next**.
- viii. Ensure that the **Allow the connection** radio button is selected.
- ix. Click **Finish**.

3. Create a new *Inbound Rules* policy for **Echo Request ICMP** (ping) requests:

- i. Right click **Inbound Rules** in the left pane.
- ii. Select **New Rule...**
- iii. Select the **Predefined** radio button.
- iv. Select **File and Printer Sharing** from the drop down list.
- v. Click **Next**.
- vi. Ensure the check boxes for the following items are selected:
 - **File and Printer Sharing (Echo Request-ICPMv4-IN)**
 - **File and Printer Sharing (Echo Request-ICPMv6-IN)**You can de-select any additional check boxes unless you require them specifically.
- vii. Click **Next**.
- viii. Ensure that the **Allow the connection** radio button is selected.
- ix. Click **Finish**.

4. Exit the *Group Policy Management Editor*:

Select **File > Exit**

5. Link your new GPO to one or more Organizational Units (OU) containing servers to which you wish to have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

Note: Substitute a specific OU for the domain if you want to link only to a subset of servers.

- i. Right-click your domain in the left pane of the *Group Policy Management* window.
- ii. Choose **Link an Existing GPO...**
- iii. Select your new GPO, *WinRM_Monitoring* for example, from the list that displays.

- iv. Click **OK** to complete the process.
6. Exit the Group Policy Management window:
- Select **File > Exit**
7. Before adding servers to Cisco UCS Performance Manager for monitoring, wait a sufficient amount of time for Group Policy to automatically refresh on the server(s). Alternatively, you can manually refresh Group Policy from the command prompt of target servers using this command:
- ```
gpupdate /force
```

## Windows Server 2012: Configuring Windows Credentials in Cisco UCS Performance Manager

When one or more servers are ready for addition to Cisco UCS Performance Manager, perform the following steps within the Cisco UCS Performance Manager web interface. If the same user account name was created on each server, the following procedure will specify it for all servers in the device class:

1. Navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. In the right pane, set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

**Note:** For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled About Windows Authentication for WinRM Monitoring for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems or the section titled Windows Server 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration.

6. Click **See All**.
7. Add windows servers using the web interface or `ZenBatchload`.

**Note:** If the user names and passwords used on servers are different, each server must be added and its individual *zWinRMUser* and *zWinRMPassword* configuration properties must be set. Perform the following steps to add the server information:

- i. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding as follows:
  - If you are adding via the web interface, leave the **Model Device:** box unchecked.
  - If you are adding through the `zenbatchload` command, be sure the device has the `--nomodel` flag set.
- ii. When the device displays in the device list, click on its name.
- iii. Click on **Configuration Properties** in the left pane, and set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.
- iv. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

## Windows Server 2012: Improving Security by Using a Domain Service Account & Encrypting Credentials with Kerberos

**Note:** When switching from the use of local system accounts for authentication to a single domain service account, the use of Kerberos to encrypt credentials is mandatory.

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment the AD Server also acts as the Key Distribution Center (KDC). The `zWinKDC` configuration property in Cisco UCS Performance Manager must be set to the IP address of the AD Server. Each collector used to monitor Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Cisco UCS Performance Manager, perform the following steps:

1. In the Cisco UCS Performance Manager web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class in the left pane.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. Edit the configuration property in the right pane for `zWinKDC`. Double click `zWinKDC` and specify the IP address of your Active Directory Server.
6. Edit the value for `zWinRMUser` name to be the *complete domain name* of the user, for example, `user@test.loc`.

**Note:** A `zWinRMUser` name value in the form of `user@domain` is the trigger for Cisco UCS Performance Manager to (i) use a domain account rather than a local system account and (ii) to use Kerberos encryption for credentials. When the value of `zWinRMUser` name takes the form of `user[only]` instead of `user@domain`, Cisco UCS Performance Manager will use a local user account on the system being monitored.

**Note:** For ease of setup and testing, the local Administrator account might be preferable to use in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled About Windows Authentication for WinRM Monitoring for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems or the section titled Windows Server 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration.

**Note:** The Cisco UCS Performance Manager server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

- i. Configuring the Cisco UCS Performance Manager server to access the Windows DNS server for its DNS resolutions.
- ii. Manually entering PTR records for each server in to the `/etc/hosts` file.

For example, the server `r2d2.example.com` at the IP address **77.77.77.77** has the following PTR record:

`77.77.77.77 r2d2.example.com`

iii. Using the `zWinRMServerName` property as follows:

- Specify the monitored server's name with the `zWinRMServerName` property field.

**Note:** The `zWinRMServerName` property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory. For example, if *myserver1* is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address *192.51.100.21*, but IP address *192.51.100.21* resolves to *www.example.com*, you must set the `zWinRMServerName` property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Cisco UCS Performance Manager
  - set `zWinRMServerName` to `${here/titleOrId}` at the */Server/Microsoft/Windows* device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Cisco UCS Performance Manager does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.



# Windows Server 2012: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption)

Perform the following steps to configure WinRM and WinRS:

1. Log on to the target server as a user with *Domain Admin* or local *Admin* privileges.
2. Press the **Windows** key on the keyboard to display the *Start* screen.
3. Click the **Windows PowerShell** tile.

- i. Configure the system to accept WS-Management requests from other systems. Enter the following at the command prompt:

```
winrm quickconfig
```

- ii. Specify *http* instead of *https* (SSL) connections. Enter the following command:

```
winrm s winrm/config/service '@{AllowUnencrypted="true"}'
```

- iii. Configure the maximum number of concurrent operations per user. Use the following command:

```
winrm s winrm/config/service
'@{MaxConcurrentOperationsPerUser="4294967295"}'
```

- iv. Configure the *maximum number of shells per user*. Enter the following command:

```
winrm s winrm/config/winrs '@{MaxShellsPerUser="2147483647"}'
```

- v. Configure the *idle timeout*. Enter the following command:

```
winrm s winrm/config/winrs '@{IdleTimeout="7200000"}'
```

- vi. Specify *Basic Authentication*. Enter the following command:

```
winrm s winrm/config/service/auth '@{Basic="true"}'
```

- vii. Exit PowerShell:

```
exit
```

4. Configure the firewall to allow connections on port 5985.
  - i. Press the **Windows** key on the keyboard to display the *Start* screen.
  - ii. Click the **Server Manager** tile.
  - iii. Click **Local Server** on the left.
  - iv. Edit the firewall profile currently in use. Click the value to the right of **Windows Firewall** to change it.  
For example, "Windows Firewall" might display in grey font and to the right of it, in blue colored font, "Domain: On." In this case, click the blue **Domain On** value to display the *Windows Firewall* page.
  - v. In the left pane of the *Windows Firewall* page, click **Allow an app or feature through Windows Firewall**.

- vi. Scroll down through the list that displays and confirm that **Windows Remote Management** is checked for the current firewall profile in use (and any other profiles required).  
**Note:** Remote management includes allowing connections on port 5985.
  - vii. Click **OK**.
5. If your firewall settings are NOT set by group policy, perform the following, depending on your server, to enable response to ping requests that are necessary for Cisco UCS Performance Manager to perform availability monitoring:

**Windows 2012 R2:**

- i. In *Server Manager*, click **Local Server** in the left pane.
- ii. In the right pane, click the entry for *Windows Firewall Domain: On* (in blue letters) to display the *Windows Firewall* dialog.
- iii. Click **Allow an app or feature through Windows Firewall** to display the *Allowed apps* dialog.
- iv. Click **File and Printer Sharing**.
- v. Click **Next**.
- vi. Ensure the boxes are checked for:
  - **File and Printer Sharing (Echo Request - ICMPv6-In)**
  - **File and Printer Sharing (Echo Request - ICMPv4-In)**

This enables the response to ping requests, you can uncheck any additional boxes unless you require them specifically.
- vii. Click **OK**.

**Windows 2012**

- i. In *Server Manager*, click **Local Server** in the left pane.
  - ii. In the right pane, click the entry for *Windows Firewall Domain: On* (in blue letters) to display the *Windows Firewall* dialog.
  - iii. In the left pane of the *Windows Firewall* page, click **Allow an app or feature through Windows Firewall** to display the *Allowed apps* dialog.
  - iv. Scroll down through the list that displays and confirm that **Windows Remote Management** is checked for the current firewall profile in use (and any other profiles required).  
**Note:** Choosing remote management opens port 5985.
  - v. Click **OK**.
6. Configure Cisco UCS Performance Manager to monitor the server. Perform the following steps within the Cisco UCS Performance Manager web interface:
- i. Navigate to the **Infrastructure** page.
  - ii. Select the **Server/Microsoft/Windows** device class.
  - iii. Click the **Details** icon.
  - iv. Click **Configuration Properties** in the left pane.
  - v. In the right pane, confirm that the configuration properties for *zWinRMUser* and *zWinRMPassword* match the appropriate Windows credentials on the system being monitored.

**Note:** For ease of setup and testing, the local Administrator account may be preferable to use in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled [About Windows Authentication for WinRM Monitoring](#)

for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled [Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems](#) or the section titled [Windows Server 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration](#).

If the credentials listed are correct, click **See All** and add the server to Cisco UCS Performance Manager.

- vi. If the credentials listed are not appropriate to the target server, the server must be added and the server's individual `zWinRMUser` and `zWinRMPassword` configuration properties must be set. Perform the following steps to add the server information:
  - a. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding it:
    - If you are adding via the web interface, leave the **Model Device:** box unchecked.
    - If you are adding via the zenbatchload command, be sure the device has the `--nomodel` flag set.
  - b. When the device displays in the device list, click on its name.
  - c. Click on **Configuration Properties**, and set the configuration properties for `zWinRMUser` and `zWinRMPassword`, supplying the appropriate Windows credentials.
  - d. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

## Windows Server 2012: Configuring Individual Servers to Use a Domain Service Account & Encrypt Credentials with Kerberos

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment, the AD Server also acts as the Key Distribution Center (KDC). The `zWinKDC` configuration property in Cisco UCS Performance Manager must be set to the IP address of the AD Server. Each collector that monitors Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Cisco UCS Performance Manager, perform the following steps:

1. In the Cisco UCS Performance Manager web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click **Details**.
4. Edit the configuration property for `zWinKDC` to specify the IP address of your Active Directory Server.
5. Edit the value for `zWinRMUserName` to be the complete domain name of the user, for example, `administrator@test.loc`.

**Note:** A `zWinRMUserName` value in the form of `user@domain` is the trigger for Cisco UCS Performance Manager to use Kerberos encryption for credentials. When the value of `zWinRMUsername` takes the form of `user[only]` instead of `user@domain`, Cisco UCS Performance Manager will not use Kerberos.

**Note:** For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled [About Windows Authentication for WinRM Monitoring](#) for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator service account, see the section below titled [Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems](#) or the section titled [Windows Server 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration](#).

**Note:** The Cisco UCS Performance Manager server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

- i. Configuring the Cisco UCS Performance Manager server to access the Windows DNS server for its DNS resolutions.
- ii. Manually entering PTR records for each server in to the `/etc/hosts` file.

For example, the server `r2d2.example.com` at the IP address **77.77.77.77** has the following PTR record:

```
77.77.77.77 r2d2.example.com
```

- iii. Using the `zWinRMServerName` property as follows:

- Specify the monitored server's name with the `zWinRMServerName` property field.

**Note:** The `zWinRMServerName` property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory.

For example, if `myserver1` is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address `192.51.100.21`, but IP address `192.51.100.21` resolves to `www.example.com`, you must set the `zWinRMServerName` property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Cisco UCS Performance Manager
  - set **`zWinRMServerName`** to `${here/titleOrId}` at the `/Server/Microsoft/Windows` device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Cisco UCS Performance Manager does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.

## Windows Server 2012: Improving Individual Server Security - Specify SSL for WinRM & WinRS

To successfully encrypt the payload between Resource Manager and Windows clients, you must install a *Server Authentication* certificate on each monitored server. Log on to your Certificate Authority server as a user with Administrator privileges to create a Certificate Template for use in creating each server's certificate. This step only needs to be completed once because the new Certificate Template is then used repeatedly to create each server's certificate. In the following steps, the standard *Web Server Certificate Template* is duplicated to create a new Certificate Template.

1. Press the **Windows** key on the keyboard to display the *Start* screen.
2. Click the **Windows PowerShell** tile.
3. Launch the **Microsoft Management Console** (mmc). Enter the following command:

```
mmc
```

Within the mmc create the duplicate template:

- i. Click the **File** menu, and select **Add/Remove Snap-in...** to display the *Add or Remove Snap-ins* dialog.
  - ii. From the list on the left, select **Certificate Templates**.  
**Note:** If the **Certificate Templates** option does not display in the list, you must add the CA role to your server.
  - iii. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
  - iv. Click **OK**.
  - v. Click on **Certificate Templates ([server name])** in the window on the left to display the full list of Certificate Templates.
  - vi. Scroll down the list and locate **Web Server**.
  - vii. Right click the *Web Server* template and select **Duplicate Template** to display the *Properties of New Template* window.
  - viii. Select the **Request Handling** tab, and check the box next to *Allow private key to be exported*.
  - ix. Select the **General** tab and specify a value for *Template display name*.
  - x. Select the **Security** tab and add the certificate authority computer account to the template with at minimum *Enroll* permissions.
  - xi. Click **OK** to save the changes and exit the *Properties of New Template* window.
4. In the mmc, configure the *Certificate Template*:
  - i. Click the **File** menu.
  - ii. Select **Add/Remove Snap-in...**
  - iii. From the list on the left, select **Certification Authority**.
  - iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.  
If a window titled *Certification Authority* displays:
    - a. Select the radio button next to *Local computer* under *This snap-in will always manage:*
    - b. Click **Finish**.
    - c. Click **OK**.
  - v. Expand the list under **Certification Authority (Local)** and the list under your server name.
  - vi. Right click **Certificate Templates** in the list under your server name.
  - vii. Select **New => Certificate Template to Issue**.
  - viii. In the *Enable Certificate Templates* window, select the new template you created in the

- previous steps.
- ix. Click **OK**.
- x. Exit the mmc:

Select **File > Exit**

## Creating a Certificate for Each Server

In the following steps, use the new certificate template to create a certificate for each server you want to monitor using SSL encryption. These steps are repeated for each server.

1. If necessary, launch the Microsoft Management Console (mmc). Press the **Windows** key on the keyboard to display the *Start* screen.
2. Click the Windows PowerShell tile.
3. Launch the **Microsoft Management Console** (mmc) with the following command:

```
mmc
```

In the mmc:

- i. Click the **File** menu.
  - ii. Select **Add/Remove Snap-in...**
  - iii. From the list on the left, select **Certificates**.
  - iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
  - v. In the *Certificates* snap-in window, select *Compute account* under **This snap-in will always manage certificates for:**
  - vi. Click **Next** (or **Finish** if your using an existing mmc console).
  - vii. Click **Local computer** under **This snap-in will always manage:** if you are presented with the *Select Computer* dialogue (which occurs if opening a new mmc console).
  - viii. Click **Finish**.
  - ix. Click **OK**.
4. Request and enroll the new certificate. In the *Certificate* mmc:
  - i. Navigate to **Console Root > Certificates (Local Computer) > Personal > Certificates**.
  - ii. Select **Action** in the menus at the top of the mmc to display the drop down list.
  - iii. Select **All Tasks > Request New Certificate**.
  - iv. Click **Next** to display the next window with *Active Directory Enrollment Policy* highlighted.
  - v. Click **Next**.
  - vi. Place a check mark in the box next to your copied certificate template and click the link to launch the *Properties* edit window.
    - a. In the **Subject** tab, choose **Common name** from the *Type:* drop-down of the *Subject name* field. Enter the fully qualified domain name of the server to be monitored (for example, *mytestmachine.mynetwork.com*) in the **Value:** field.
    - b. Click **Add**.
    - c. If desired, enter additional identification information, including the organization, street address, etc., in the same manner.
    - d. Select the **General** tab and populate the *friendly name* field.
  - vii. Click **OK**.

- viii. Click **Enroll**.
  - ix. Click **Finish**.
- 5. Expand the tree under **Certificates**.
- 6. Expand the tree under **Personal**.
- 7. Click on **Certificates** to highlight it and display a list of certificates on the right.
- 8. Right click the new certificate and select **All Tasks**.
  - i. Select **Export**.
  - ii. In the *Certificate Export Wizard* window, click **Next**.
  - iii. Select the radio button next to **Yes, export the private key**.
  - iv. Click **Next**.
- 9. On the next page:
  - i. Verify that the radio button next to **Personal Identification Exchange - PKCS #12 (.pfx)** is selected.
  - ii. Verify that the checkbox next to Include all certificates in the certification path if possible is checked.
  - iii. Click **Next**.
- 10. On the *Security* page of the wizard:
  - i. Check the box next to **Password**.
  - ii. Create a password to secure the private key.
  - iii. Click **Next**.
- 11. On the *File to Export* page:
  - i. Select a *destination* for the key export.
  - ii. Create a *file name*.
  - iii. Click **Save**
  - iv. Click **Next**.
- 12. On the *Completing the Certificate Export Wizard* page, click **Finish**.
- 13. Click **OK** to close *the Certificate Export Wizard*.
- 14. Move or copy the exported certificate to the target (monitored) server.

## Installing the Certificate on the Target Computer

1. On the target computer, launch the Microsoft Management Console (mmc) with the following command:
 

```
mmc
```
2. In the mmc:
  - i. Click the **File** menu.
  - ii. Select **Add/Remove Snap-in...**
  - iii. From the list on the left, select **Certificates**.
  - iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
  - v. In the *Certificates* snap-in window, select **Computer account** under **This snap-in will always**

#### manage certificates for:.

- vi. Click **Next**.
- vii. On the *Select a computer page*, click the radio button next to **Local computer**.
- viii. Click **Finish**.
- ix. Click **OK** on the *Add or Remove Snap-ins* page.

## Importing the Certificate

1. In the mmc console, expand the **Certificates (Local Computer)** branch of the tree.
2. Right click **Personal**.
3. Select **All Tasks => Import**.
4. On the first page of the *Certificate Import Wizard*, click **Next**.
5. On the *File to import* page:
  - i. Click **Browse**.
  - ii. Navigate to the location of the certificate copied to the target system above.
  - iii. Select the file.  
**Note:** You might need to change the file type in the file browser window to *Personal Information Exchange* for the file to display.
  - iv. Select the certificate file.
  - v. Click **Open**.
  - vi. Click **Next**.
6. On the *Private key protection* page:
  - i. Enter the password for the key.
  - ii. Verify that the checkboxes for **Include all Extended Properties** and **Mark this key as exportable** are selected.
  - iii. Click **Next**.
7. On the *Certificate Store* page:
  - i. Select the radio button next to **Place all certificates in the following store**.
  - ii. Verify that *Personal* appears in the field for **Certificate Store**.
  - iii. Click **Next**.
8. On the *Completing the Certificate Import Wizard* page, click **Finish**.
9. Click **OK** to exit the *Certificate Wizard*.

## Verifying the Details and Copying the Thumbprint

1. In the mmc console:
  - i. Expand the *Certificates (Local Computer)* branch of the tree.
  - ii. Expand *Personal*.
  - iii. Click on **Certificates**.
  - iv. Double click on the certificate to view its details.
2. In the **General** tab of the *Certificate* window:
  - i. Verify that the *hostname* is correct for the target server.
  - ii. Select the **Details** tab



- iii. Scroll down to **Thumbprint** in the *Field* list.
  - iv. Click on **Thumbprint**.
  - v. Copy the thumbprint from the lower window for use in later steps.
3. If the server has not been previously configured for monitoring using WinRM, complete the steps listed above in the section *Windows Server 2012: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption)* on page 9 and omit the step that specifies SSL not be used. Substitute the steps in the following section, [Configuring the Firewall](#) (below) for firewall configuration. If the server has previously been configured for monitoring but without using SSL, proceed directly to the section, [Configuring the Firewall](#) (below).

## Configuring the Firewall

1. Configure the firewall to allow connections on port 5986 on individual servers. If desired, use these instructions to instead modify a Group Policy object (for example as directed in Page 4 of this document) to make the change on large numbers of servers.
  - i. Press the **Windows** key on the keyboard to display the *Start* screen.
  - ii. Click the **Server Manager** tile.
  - iii. Click **Local Server** on the left.
  - iv. Edit the Firewall profile currently in use. Click the value to the right of **Windows Firewall** to change the value.  
For example, you might see *Windows Firewall* in grey font and to the right of it, in blue font, **Domain: On**.  
In this case, click the blue **Domain On** value.
  - v. Click on **Advanced Settings** on the left.
2. In the *Windows Firewall with Advanced Security* window:
  - i. Click on **Inbound Rules** on the left.
  - ii. Click on **New Rule...** on the far right under **Actions**.
3. In the *New Inbound Rule Wizard* window:
  - i. Select the radio button next to **Port**.
  - ii. Click **Next**.
  - iii. Verify that the radio buttons next to **TCP** and **Specific local ports** are selected.
  - iv. Enter the value 5986 in the field for **Specific local ports**.
  - v. Click **Next**.
  - vi. On the next page, verify that the radio button next to **Allow the connection** is selected.
  - vii. Click **Next**.
  - viii. On the next page, select the firewall profiles for which the rule should apply.
  - ix. Click **Next**.
  - x. On the next page, give the rule a name.
  - xi. Click **Finish**.

## Creating the WinRM Listener Using SSL

1. Press the **Windows** key on the keyboard to display the *Start* screen.
2. Click the *Windows PowerShell* tile.
3. At the PowerShell command line, type the following command, substituting your values for the certificate *thumbprint* and *serverfqdn* (server fully qualified domain name of the monitoring server):

```
winrm create
winrm/config/Listener?Address=*&Transport=HTTPS '@{Hostname="[serverfqdn]";CertificateThumbprint="[thumbprint]"}'
```

for example:

```
winrm create winrm/config/Listener?Address=*&Transport=HTTPS '@{Hostname="mytestmachine.mynetwork.com";CertificateThumbprint="07bfff656edab6d9b4dd27f020f768f54fee5eb8"}'
```

**Note:** The thumbprint value must be entered without the spaces displayed in the *Detail* tab of the *Certificate information* window. For example, the displayed value: 07 bf ff 65 6e da ... must be entered as: 07bfff656eda...

4. Specify *https* (SSL) instead of *http* connections. Enter the following command:

```
winrm s winrm/config/service '@{AllowUnencrypted="false"}'
```

**Note:** If this is already controlled through a policy, an error displays. In that case, modify the appropriate GPO. The instructions on Page 2 of this document can be used as a guide.

## Adding the Server to Cisco UCS Performance Manager

In the Cisco UCS Performance Manager web UI:

1. Navigate to the **Infrastructure** page.
2. If the server has not yet been added to Cisco UCS Performance Manager, add it the **Server/Microsoft/Windows** device class and opt out of modeling.
3. Click on the name of the target (monitored) server (or on the **Server/Microsoft/Windows** device class if you would like these changes to apply to all Windows servers).
4. Click on Configuration Properties.
5. Edit the configuration property for *zWinScheme* to be *https*.
6. Edit the value for *zWinRMPort* to be *5986*.
7. Verify that the values for *zWinRMUser* and *zWinRMPassword* are correct. Correct means the appropriate Windows credentials. Edit as necessary.
8. To verify that all settings are correct, model the device. Click the **Action Wheel** (gear-shaped) icon in the lower left and select **Model Device...**

## Windows Server 2012: Configuring a WinRM Service Account on Individual Windows Systems

See the section above titled [\*About Windows Authentication for WinRM Monitoring\*](#) if necessary for more background on Windows permissions requirements when monitoring with WinRM.

**Note:** You cannot create a local service account if the machine is configured as a domain controller (AD DS) because the *local users and groups* options no longer exist in that configuration. There are no local accounts on a domain controller, only domain accounts.

Complete the following steps on each non-domain controller server to configure your service account:

1. Add a new local user for use as a service account:
  - i. Open *Server Manager*.
  - ii. Click on **Tools** in the upper right and select **Computer Management** from the menu that displays.
  - iii. In the left pane of the *Computer Management* window, expand **Local Users and Groups**.
  - iv. Right click on **User** and select **New User** from the menu that displays.
  - v. Complete the *New User* form. Uncheck **User must change password at next logon** and check (if desired) the **Password never expires** box.
  - vi. Click **Create**.
  - vii. Click **Close** to exit the *New User* form.
2. Copy your permissions configuration script, for example an edited version of the *zenoss-lpu.ps1* script, to the target server.
3. Run the PowerShell Script:
  - i. Press the **Windows** key on the keyboard to display the *Start* screen.
  - ii. Click the **Windows PowerShell** tile.
  - iii. Run your service account configuration script by typing the full path to the script in the command line, then appending the script with the `-u` option and the name of your service account. For example, if you are using an edited version of the *zenoss-lpu.ps1* script and your service account is named "benny," enter the command at the PowerShell prompt:

```
C:\tmp\zenoss-lpu-ps1 -u benny
```

**Note:** depending on the security policies enforced on your server, you might encounter an error such as:

```
File C:\tmp\zenoss-lpu-ps1 cannot be loaded because running scripts is disabled on this system....
```

If you encounter this error, you can bypass the security restrictions for this script by including the `-executionpolicy bypass` option, for example:

```
Powershell -executionpolicy bypass -file C:\tmp\zenoss-lpu.ps1 -u benny
```

# Windows Server 2012: Group Policy Deployment of a PowerShell Script for Service Account Configuration

Refer to the section above titled [About Windows Authentication for WinRM Monitoring](#) for background on service account requirements.

## Prerequisites for Configuring a Service Account

The prerequisites for configuring a service account include:

- Creation of a domain user account for use as the service account.
- Completion of the appropriate preparatory sections.

## Creating the Domain User (Service) Account

Perform the following to create a new domain user (service) account, if necessary:

1. Log on to an Active Directory server for the domain.
2. Open *Server Manager* and click **Tools** in the upper right.
3. Select **Active Directory Users and Computers** from the drop-down list.
4. In the left pane of the *Active Directory Users and Computers* window, find and expand your domain, for example, *doctest.loc*.
5. Right-click *Users* and select **New > User**
6. In the *New Object – User* window, provide a **First name** and a **User logon name**, *zenny* for example.
7. Verify the domain field has the correct domain identification. For example, *@doctest.loc*
8. Click **Next** to display the password dialog for the new user.
9. In the *Password* fields, enter and verify the new user password.
10. Uncheck the **User must change password at next logon**.
11. Check the option for **Password never expires**. We recommend this option to prevent issues later on because your new domain user (*zenny* in this example) never logs on as a human user.
12. Click **Next**.
13. Click **Finish**. Your new user, *zenny* for example, displays in the list of users for the domain.

## Completing Preparatory Sections

The following procedure assumes that you have completed the following preparatory sections:

- [Windows Server 2012: Configuring Firewall Group Policies](#)

**Note:** This method of deploying a PowerShell script across a large group of Windows systems is most likely to be employed in combination with the use of a single domain service account for WinRM authentication. The use of a domain service account mandates the use of Kerberos to encrypt credentials. See the relevant section in this document for instructions on configuring a domain service account and Kerberos if you have not already:

- [Windows Server 2012: Improving Security](#)

## PowerShell Script Deployment

Perform the following procedure to create a new GPO and to deploy the PowerShell script.

1. Create your service account configuration script (or edit, as appropriate, the sample script referenced above in the section titled [About Windows Authentication for WinRM Monitoring](#)).
2. Copy the script (for example “*zenoss-lpu.ps1*”) to a *Netlogon* folder such as  
`\\yourdomain\SYSVOL\yourdomain\scripts`
3. Open *Group Policy Management*, from the **Server Manager** console:

Click **Tools** in the upper right, and then choose **Group Policy Management**.

4. Create a new policy.
  - i. In the left pane, navigate to:  
**Forest: yourdomain > Domains > yourdomain > Group Policy Objects**
  - ii. Right click **Group Policy Objects**
  - iii. Select **New** to display the *NEW GPO* dialog.
  - iv. Name your policy, for example: *zenoss\_lpu*
  - v. Click **OK** to save and exit the *New Policy* window.
5. Edit your new policy.
  - i. In the left pane, navigate to your new *Group Policy Object*. For example:  
**Forest: yourdomain > Domains > yourdomain > Group Policy Objects > zenoss\_lpu**
  - ii. Right click the policy and select **Edit** to display the *Group Policy Management Editor*.
  - iii. In the left pane of the Group Policy Management window, navigate to:  
**Computer Configuration\Policies\Windows Settings\Scripts (Startup/Shutdown)**
  - iv. Click **Scripts (Startup/Shutdown)**.
  - v. In the right pane (Scripts (Startup/Shutdown), double-click **Startup** to launch the *Startup Properties* dialog.
  - vi. In the *Startup Properties* dialog box, select the **PowerShell Scripts** tab.
  - vii. Click **Add** to display the *Add a Script* dialog box:
    - a. Specify the script name and path. In the *Script Name* field, enter the path to the script, or click *Browse* to locate the script file.  
**Note:** Scripts should be located in the Netlogon shared folder on the domain controller.  
For example:  
`\\yourdomain\sysvol\yourdomain\scripts`
    - b. Select the *zenoss-lpu.ps1* PowerShell script.
    - c. Click **Open**.
    - d. In the **Script Parameters** box, enter *-u yourusername@yourdomain* for a domain user or *-u yourusername* for basic authentication of a local computer account user.  
  
**Note:** Basic authentication relies on local computer accounts. To successfully authenticate to any particular computer, you must have a local account on that machine.
    - e. Click **OK** to save the information and exit the *Add a Script* window.  
  
If you have multiple scripts and want them to run in a particular order, use the Up and Down buttons in the Startup Properties window to set their run order.
    - f. Click **OK** to exit the *Startup Properties* window.
6. Exit the *Local Group Policy Editor*:  
**File > Exit**
7. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want to have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.  
  
**Note:** Substitute a specific OU for the domain if you want to link only to a subset of servers.
  - i. Right-click your domain in the left pane of the *Group Policy Management* window.
  - ii. Choose **Link an Existing GPO...**

- iii. Select your new GPO from the list that displays.
- iv. Click **OK** to complete the process.

8. Exit the Group Policy Management window:

**File > Exit**

9. Manually refresh Group Policy from the command prompt of target servers:

```
gpupdate /force
```

10. Reboot your member servers to have the script run for the first time.

# Windows Server 2008R2

## Configuring Windows Server 2008 Using Group Policy (Basic Authentication, no Encryption)

1. Log on to a domain controller as a user with 'Domain Admin' privileges.
2. Launch the Group Policy Editor. Use one of the following methods:
  - Click the **Start** button and navigate to **All Programs > Administrative Tools > Group Policy Management**.
  - Click **Start**, enter the word *Group* in the search field and select **Group Policy Management**.
3. Right-click **Group Policy Objects** and select *New*. In the form that displays:
  - i. Enter a name for your new Group Policy Object, for example, *WinRM\_Monitoring*.
  - ii. Leave "(none)" in the **Source Starter GPO** field.
  - iii. Click **OK** to save and exit the form.
4. Select your new **Group Domain Policy Object**, *WinRM\_Monitoring*, for example.
5. Right click your new **Group Domain Policy Object** and select *Edit* to open the Group Policy Management Editor.
6. In the Group Policy Management Editor window, expand the Computer Configuration section of the tree and navigate the tree to:

```
Policies\Administrative Templates:Policy...\Windows Components\Windows Remote Management (WinRM)
```
7. Enable remote server management:
  - i. Click on **WinRM Service** to access the *WinRM Service Group Policy* settings in the right pane.
  - ii. Double-click the Allow automatic configuration of listeners property.
  - iii. Click the **Enabled** radio button.
  - iv. Place an asterisk as a wildcard (' \* ') in the *IPv4 filer* and *IPv6 fields* or specify a range of IP addresses for WinRM to listen on.
  - v. Click **OK** at the bottom to submit the form.
8. Enable authentication:
  - i. Double-click the **Allow Basic authentication** property in the right pane.
  - ii. Select the **Enabled** radio button.
  - iii. Click **OK** at the bottom to submit the form.
9. Specify unencrypted traffic:
  - i. Double-click the **Allow unencrypted traffic** property.
  - ii. Select the **Enabled** radio button.
  - iii. Click **OK** at the bottom to submit the form.
10. Select *Windows Remote Shell* in the left pane to set its **Group Policy** settings. This is located in the group policy tree at the following path, which should be located right below *WinRM* service in the tree:

```
Computer Configuration\Policies\Administrative Templates\Windows
```

Components\Windows Remote Shell

11. Configure remote shell access:

- i. In the right pane, double-click **Allow Remote Shell Access**.
- ii. Select the **Enabled** radio button.
- iii. Click **OK** at the bottom to submit the form.

12. Configure shell processes:

- i. In the right pane, double-click Specify maximum number of processes per Shell.
- ii. Select the **Enabled** radio button.
- iii. Enter the value 2,000,000,000 (without commas or spaces) in the *MaxProcessesPerShell* field.
- iv. Click **OK** at the bottom to submit the form.

13. Configure the number of remote shells:

- i. In the right pane, double-click Specify maximum number of remote shells per user.
- ii. Select the **Enabled** radio button.
- iii. Enter the value 2,000,000,000 (without commas or spaces) in the *MaxShellsPerUser* field.
- iv. Click **OK** at the bottom to submit the form.

14. Configure the shell timeout value:

- i. In the Right pane, double-click **Specify Shell Timeout**.
- ii. Select the **Enabled** radio button.
- iii. Enter the value 7,200,000 (without commas or spaces) in the **ShellTimeOut** field.
- iv. Click **OK** at the bottom to submit the form.

## Windows 2008: Configuring Firewall Group Policies

Windows firewall must allow incoming ICMP (ping) requests. Additionally, WinRM listens on port 5985 when SSL is not used and on port 5986 when SSL is used. These ports must be opened on the firewalls of monitored servers. You can use Group Policy to open these ports on all servers across the organization.

In the **Group Policy Management Editor**, navigate to:  
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security - LDAP;...\Inbound Rules

1. Create a new *Inbound Rules* policy:

- i. Right click **Inbound Rules** in the left pane.
- ii. Select **New Rule...** to display the *New Inbound Rule Wizard*
- iii. Select the **Predefined** radio button in the right pane.
- iv. Select **Windows Remote Management** from the drop down list.
- v. Click **Next**.
- vi. Ensure that all items in the list are checked.
- vii. Click **Next**.
- viii. Ensure that the **Allow the connection** radio button is selected.
- ix. Click **Finish**.

2. Exit the Group Policy Management Editor:  
Select **File > Exit**

3. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want to



have the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

**Note:** Substitute a specific OU for the domain if you want to link only to a subset of servers.

- i. Right-click your domain in the left pane of the *Group Policy Management* window.
  - ii. Choose Link an Existing GPO...
  - iii. Select your new GPO from the list that displays, *WinRM\_Monitoring*, for example.
  - iv. Click **OK** to complete the process.
4. Exit the *Group Policy Management* window:  
Select **File > Exit**
5. Before adding servers to Cisco UCS Performance Manager for monitoring, wait a sufficient amount of time for Group Policy to automatically update on the server(s). Alternatively, you can manually refresh Group Policy on target servers by typing the following at the command prompt:

```
gpupdate /force
```

## Windows 2008: Configuring Windows Credentials in Cisco UCS Performance Manager

When one or more servers are ready for addition to Cisco UCS Performance Manager, perform the following steps within the Cisco UCS Performance Manager web interface:

1. Navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. In the right pane, set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.

**Note:** For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled [About Windows Authentication for WinRM Monitoring](#) for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator account, see the sections below titled [Windows 2008: Configuring a WinRM Service Account on Individual Servers](#), or [Windows 2008: Using Group Policy to Configure a Service Account on all Servers](#).

6. Click **See All**.
7. Add windows servers using the web interface or `ZenBatchload`.

## Windows 2008: Improving Security by Using a Domain Service Account & Encrypting Credentials with Kerberos

**Note:** When switching from the use of local system accounts for authentication to a single domain service account, the use of Kerberos to encrypt credentials is mandatory.

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment the AD Server also acts as the Key Distribution Center (KDC). The `zWinKDC` configuration property in Cisco UCS Performance Manager must be set to the IP address of the AD Server. Each collector used to monitor Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Cisco UCS Performance Manager, perform the following steps:

1. In the Cisco UCS Performance Manager web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class in the left pane.
3. Click the **Details** icon.
4. Click **Configuration Properties** in the left pane.
5. Edit the configuration property in the right pane for `zWinKDC`. Double click `zWinKDC` and specify the IP address of your Active Directory Server.
6. Edit the value for `zWinRMUser` name to be the *complete domain name* of the user, for example, `administrator@test.loc`.

**Note:** A `zWinRMUser` name value in the form of `user@domain` is the trigger for Cisco UCS Performance Manager to use Kerberos encryption for credentials. When the value of `zWinRMUser` name takes the form of `user[only]` instead of `user@domain`, Cisco UCS Performance Manager will not use Kerberos.

**Note:** The Cisco UCS Performance Manager server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

- i. Configuring the Cisco UCS Performance Manager server to access the Windows DNS server for its DNS resolutions.
- ii. Manually entering PTR records for each server in to the `/etc/hosts` file.

For example, the server `r2d2.example.com` at the IP address **77.77.77.77** has the following PTR record:

```
77.77.77.77 r2d2.example.com
```

- iii. Using the `zWinRMServerName` property by specifying the monitored server's name with the `zWinRMServerName` property field.

**Note:** The `zWinRMServerName` property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory.

For example, if `myserver1` is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address `192.51.100.21`, but IP address `192.51.100.21` resolves to `www.example.com`, you must set the `zWinRMServerName` property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Cisco UCS Performance Manager.
  - set `zWinRMServerName` to `${here}/titleOrId` at the `/Server/Microsoft/Windows`

device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Cisco UCS Performance Manager does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.

## Windows 2008: Configuring WinRM and WinRS on Individual Servers (Basic Authentication, no Encryption)

Perform the following steps to configure WinRM and WinRS:

1. Log on to the target server as a user with *Domain Admin* or local *Admin* privileges.
2. Launch Windows PowerShell:
  - Click the **Windows PowerShell** icon if it exists in the tool bar.
  - Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.
3. Within Windows PowerShell:

- i. Configure the system to accept WS-Management requests from other systems. Enter the following at the command prompt:

```
winrm quickconfig
```

- ii. Specify *http* instead of *https* (SSL) connections. Enter the following command:

```
winrm s winrm/config/service '@{AllowUnencrypted="true"}'
```

- iii. Configure the maximum number of concurrent operations per user. Use the following command:

```
winrm s winrm/config/service
'@{MaxConcurrentOperationsPerUser="4294967295"}'
```

- iv. Configure the *maximum number of shells per user*. Enter the following command:

```
winrm s winrm/config/winrs '@{MaxShellsPerUser="2147483647"}'
```

- v. Configure the *idle timeout*. Enter the following command:

```
winrm s winrm/config/winrs '@{IdleTimeout="7200000"}'
```

- vi. Specify *Basic Authentication*. Enter the following command:

```
winrm s winrm/config/service/auth '@{Basic="true"}'
```

- vii. Exit PowerShell:

```
exit
```

4. Configure the firewall to allow connections on port 5985.

- i. Click the Start button and navigate to All Programs > Administrative Tools > Server Manager.
- ii. In the left pane, navigate to Server Manager > Configuration > Windows Firewall with Advanced Security>Inbound Rules.
- iii. In the right pane, scroll down through the list that displays and confirm that *Windows Remote Management* is enabled for the current firewall profile in use (and any other profiles required).

**Note:** Remote management includes allowing connections on port 5985 when SSL is not being used.

If **Windows Remote Management** does not appear in the right pane:

- a. Right click **Inbound Rules** in the left pane.
  - b. Select **New Rule...**
  - c. Select the **Predefined** radio button.
  - d. Select **Windows Remote Management** from the drop down list.
  - e. Click **Next**.
  - f. Ensure that all items in the list are checked.
  - g. Click **Next**.
  - h. Ensure that the **Allow the connection** radio button is selected.
  - i. Click **Finish**.
5. Configure Cisco UCS Performance Manager to monitor the server. Perform the following steps within the Cisco UCS Performance Manager web interface:
- i. Navigate to the **Infrastructure** page.
  - ii. Select the **Server/Microsoft/Windows** device class.
  - iii. Click the **Details** icon.
  - iv. Click **Configuration Properties** in the left pane.
  - v. In the right pane, confirm that the values for the *zWinRMUser* and *zWinRMPassword* properties are populated with the correct Windows credentials for your Windows servers.

**Note:** For ease of setup and testing, the local Administrator account can be used in test environments. For production environments, the use of a less privileged service account is recommended. See the section above titled [About Windows Authentication for WinRM Monitoring](#) for more on WinRM authentication.

To configure Windows to allow monitoring using a non-Administrator account, see the section below titled [Windows 2008: Configuring a WinRM Service Account on Individual Servers](#).

- vi. If the credentials listed are correct, click **See All** and add the server to Cisco UCS Performance Manager.
- vii. If the credentials listed are not appropriate to the target server, the server must be added and the server's individual *zWinRMUser* and *zWinRMPassword* configuration properties must be set. Perform the following steps to add the server information:
  - a. Add the server to the **Server/Microsoft/Windows** device class, but opt out of modeling the device when adding as follows:
    - If you are adding via the web interface, leave the **Model Device:** box unchecked.
    - If you are adding via the `zenbatchload` command, be sure the device has the `--nomodel` flag set.
  - b. When the device displays in the device list, click on its name.
  - c. Click on **Configuration Properties**, and set the configuration properties for *zWinRMUser* and *zWinRMPassword*, supplying the appropriate Windows credentials.
- viii. Model the device by clicking the Action Wheel (gear-shaped) icon in the lower left and select **Model Device...**

## Windows 2008: Configuring Individual Servers to Use a Domain Service Account & Encrypt Credentials with Kerberos

The Kerberos authentication process requires an available ticket granting server. In the Microsoft Active Directory (AD) environment, the AD Server also acts as the Key Distribution Center (KDC). The `zWinKDC` configuration property in Cisco UCS Performance Manager must be set to the IP address of the AD Server. Each collector that monitors Windows servers must be able to send Kerberos packets to this server. To specify the ticket granting server in Cisco UCS Performance Manager, perform the following steps:

1. In the Cisco UCS Performance Manager web UI, navigate to the **Infrastructure** page.
2. Select the **Server/Microsoft/Windows** device class.
3. Click **Details**.
4. Edit the configuration property for `zWinKDC` to specify the IP address of your Active Directory Server.
5. Edit the value for `zWinRMUserName` to be the complete domain name of the user, for example, `administrator@test.loc`.

**Note:** A `zWinRMUserName` value in the form of `user@domain` is the trigger for Cisco UCS Performance Manager to use Kerberos encryption for credentials. When the value of `zWinRMUsername` takes the form of `user[only]` instead of `user@domain`, Cisco UCS Performance Manager will not use Kerberos.

**Note:** The Cisco UCS Performance Manager server and collectors must be able to resolve the target server's pointer records (PTR) to their Active Directory fully qualified domain name. Administrators can meet this requirement by using one of three methods:

- i. Configuring the Cisco UCS Performance Manager server to access the Windows DNS server for its DNS resolutions.
- ii. Manually entering PTR records for each server in to the `/etc/hosts` file.

For example, the server `r2d2.example.com` at the IP address **77.77.77.77** has the following PTR record:

```
77.77.77.77 r2d2.example.com
```

- iii. Using the `zWinRMServerName` property as follows:
  - Specify the monitored server's name with the `zWinRMServerName` property field.

**Note:** The `zWinRMServerName` property should only be used in conjunction with domain authentication when the DNS PTR record for a monitored server's managed IP address does not resolve to the name by which the server is known in Active Directory. For example, if `myserver1` is known as **myserver1.ad.example.com** by Active Directory and is being managed by IP address `192.51.100.21`, but IP address `192.51.100.21` resolves to `www.example.com`, you must set the `zWinRMServerName` property to **myserver1.ad.example.com** for domain authentication to work.

- If many Windows servers in your environment do not have DNS PTR records that match Active Directory, it is recommended that you:
  - set the monitored device's name to be the fully-qualified Active Directory name in Cisco UCS Performance Manager
  - set `zWinRMServerName` to `${here}/titleOrId` at the `/Server/Microsoft/Windows` device class.

This method avoids setting the `zWinRMServerName` property on every device.

We recommend that you leave the `zWinRMServerName` property blank if local authentication is used, or DNS PTR records match the Active Directory listings. The result is that Cisco UCS Performance Manager does not have to rely on DNS resolution while monitoring and it avoids the additional overhead of configuring the `zWinRMServerName` properties.



# Windows 2008: Improving Individual Server Security - Specify SSL for WinRM & WinRS

## Creating a New Certificate Template

To successfully encrypt the payload between Resource Manager and Windows clients, you must install a *Server Authentication* certificate on each monitored server. Log on to your Certificate Authority server as a user with *Administrator* privileges to create a Certificate Template for use in creating each server's certificate. This step only needs to be completed once because the new Certificate Template is then used repeatedly to create each server's certificate. In the following steps, the standard *Web Server Certificate Template* is duplicated to create a new Certificate Template.

1. Log on to your Certificate Authority server as a user with Administrator privileges.
2. Launch Windows PowerShell:
  - i. Click the **Windows PowerShell** icon if it exists in the tool bar.
  - ii. Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.
3. Launch the **Microsoft Management Console** (mmc). Enter the following command:

```
mmc
```

Within the mmc create the duplicate template:

- i. Click the **File** menu, and select **Add/Remove Snap-in...**
  - ii. From the list on the left, select **Certificate Templates**.
  - iii. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
  - iv. Click **OK**.
4. Click on **Certificate Templates** in the left window to display the full list of Certificate Templates.
  - i. Scroll down the list and locate **Web Server**.
  - ii. Right click the *Web Server* template and select **Duplicate Template**. The *Duplicate Template* dialog displays with radio button choices.
  - iii. Select **Windows Server 2008 Enterprise** and click **OK** to display the *Properties of New Template window*.
  - iv. In the **General** tab specify a value for *Template display name*.
  - v. Select the **Request Handling** tab, and check the box next to *Allow private key to be exported*.
  - vi. Select the **Security** tab and add the certificate authority computer account to the template with at minimum *Enroll* permissions.
  - vii. Click **OK**.
5. In the mmc configure the Certificate Template:
  - i. Click the **File** menu.
  - ii. Select **Add/Remove Snap-in...**
  - iii. From the list on the left, select **Certification Authority**.
  - iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.

If a window titled *Certification Authority* displays:

    - a. Select the radio button next to *Local computer* under **This snap-in will always manage:**
    - b. Click **Finish**.

- c. Click **OK**.
- v. Expand the list under **Certification Authority (Local)** and the list under your server name.
- vi. Right click **Certificate Templates** in the list under your server name.
- vii. Select New => Certificate Template to Issue.
- viii. In the *Enable Certificate Templates* window, select the new template you created in the previous steps.
- ix. Click **OK**.

## Creating a Certificate for Each Server

In the following steps, use the new certificate template to create a certificate for each server you want to monitor using SSL encryption. These steps are repeated for each server.

1. If necessary, launch the Microsoft Management Console (mmc) with the following command:

```
mmc
```

2. Open the Certificates MMC:

- i. Click the **File** menu.
- ii. Select Add/Remove Snap-in...
- iii. From the list on the left, select **Certificates**.
- iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
- v. In the **Certificates** snap-in window, select the option **This snap-in will always manage certificates for Computer account** to display the *Select Computer* window.
- vi. Select the radio button for This snap-in will always manage Local Computer.
- vii. Click **Finish**
- viii. Click **OK**.

3. Request and enroll the new certificate. In the Certificate mmc:

- i. Navigate to Console Root > Certificates (Local Computer) > Personal > Certificates.
- ii. Select **Action** in the menus at the top of the mmc to display the drop down list.
- iii. Select All Tasks > Request New Certificate.
- iv. Click **Next** to display the next window with *Active Directory Enrollment Policy* highlighted.
- v. Click **Next**.
- vi. Place a check mark in the box next to your copied certificate template and click the link to launch the *Properties* edit window.
  - a. In the **Subject** tab, choose *Common name* from the *Type:* drop-down of the *Subject name* field. Enter the fully qualified domain name (for example, *mytestmachine.mynetwork.com*) in the *Value:* field.
  - b. Click **Add**.
  - c. If desired, enter additional identification information, including the *organization*, *street address*, etc., in the same manner.
  - d. Select the **General** tab and populate the *friendly name* field.
- vii. Click **OK**.
- viii. Click **Enroll**.
- ix. Click **Finish**.

4. Export the certificate. In the *Certificates* mmc:

- i. Expand the tree under Certificates - Local Computer > Personal > Certificates.
  - ii. Right click the new certificate and select **All Tasks**.
  - iii. Select **Export** to display the *Certificate Export Wizard*.
  - iv. In the *Certificate Export Wizard* window, click **Next**.
  - v. Select the radio button for *Yes, export the private key*. Click **Next**.
  - vi. On the next page:
    - a. Verify that the **Personal Information Exchange** radio button is selected.
    - b. Select the check box for Include all certificates in the certification path if possible.
    - c. Click **Next**.
5. Create and confirm a password.
6. Click **Next** to display the *File to Export* page.
 

On the *File to Export* page:

  - i. Browse to select a *destination* for the exported key.
  - ii. Create a *file name*.
  - iii. Click **Save**.
  - iv. Click **Next**.
7. On the *Completing the Certificate Export Wizard* page, verify the information. Click **<Back** if you need to edit the information.
8. Click **Finish**.
 

If the export is successful, the *Certificate Export Wizard* displays a success message.
9. Click **OK** to close the message and exit the wizard.
10. Move or copy the exported certificate to the target server.

## Installing the Certificate on the Target Computer

1. On the target computer, launch **Windows PowerShell**:
  - Click the **Windows PowerShell** icon if it exists in the tool bar.
  - or
  - Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.
2. Launch the Microsoft Management Console (mmc):
 

mmc
3. Add the **Certificate** snap-in to the mmc:
  - i. Click the **File** menu.
  - ii. Select Add/Remove Snap-in...
  - iii. From the list on the left, select **Certificates**.
  - iv. Click the **Add>** button in the middle of the window to add it to the *Selected snap-ins* list on the right.
  - v. In the Certificates snap-in window, select **Computer account** under *This snap-in will always manage certificates for:*.
  - vi. Click **Next**.
  - vii. On the *Select a computer* page, select **Local computer**.
  - viii. Click **Finish**.
  - ix. Click **OK** on the *Add or Remove Snap-ins* page.

## Importing the Certificate

1. In the mmc console, expand the **Certificates (Local Computer)** branch of the tree.
2. Highlight and right click **Personal**.
3. Select **All Tasks => Import** to launch the *Certificate Import Wizard*.
4. On the first page of the *Certificate Import Wizard*, click **Next**.
5. On the *File to import* page:
  - i. Click **Browse**.
  - ii. Navigate to the location of the certificate file you copied to the target system and select the file.  
**Note:** If your file name does not display, change the file type in the file browser window to *Personal Information Exchange*.
  - iii. Click **Open**.
  - iv. Click **Next** to display the *Private key protection* page.
6. On the *Private key protection* page:
  - i. Enter the password for the key.
  - ii. Verify that the checkboxes for *Mark this key as exportable* and *Include all Extended Properties* are selected.
  - iii. Click **Next** to display the *Certificate Store* page.
7. On the *Certificate Store* page:
  - i. Select *Place all certificates in the following store*.
  - ii. Verify that *Personal* appears in the field for *Certificate Store*.
  - iii. Click **Next** to display the *Completing the Certificate Import Wizard* page.
8. On the *Completing the Certificate Import Wizard* page, verify the certificate information.
9. Click **Finish** to exit the wizard.  
If the export is successful, The Certificate Export Wizard displays a success message.
10. Click **OK** to close the message and exit the wizard.

## Verifying the Details and Copying the Thumbprint

1. If necessary, launch the mmc with the *Certificate snap-in*. In the mmc console:
  - i. Expand the *Certificates (Local Computer)* branch of the tree.
  - ii. Expand *Personal*.
  - iii. Click on *Certificates*.
  - iv. Double click on the certificate in the right pane to launch the *Certificate* window and view its details.
2. Copy the thumbprint. In the **General** tab of the *Certificate* window:
  - i. Verify that the *hostname* is the correct fully qualified domain name for the target server.
  - ii. Select the **Details** tab
  - iii. Scroll down to **Thumbprint** in the *Field* list.

- iv. Click on **Thumbprint**.
- v. Copy the 40 digit thumbprint from the lower window for use in later steps, for example:

*3a 79 6b ce 83 82 85 55 32 31 30 11 16 e5 bd 14 f0 2d 61 89*

**Note:** The forty digit thumbprint value that displays contains spaces. These spaces must be removed before using it in commands.

**Note:** If the server has not been configured for monitoring using WinRM, complete the steps listed in the section **Windows 2008: Configuring WinRM and WinRS On Individual Servers (Basic Authentication, no encryption)**, and omit the step that specifies SSL not be used. Substitute the steps in the following section, *Configuring the Firewall* (below) for firewall configuration.

If the server has been configured for monitoring but without using SSL, proceed directly to the section, *Configuring the Firewall* (below).

## Configuring the Firewall

1. Configure the firewall to allow connections on port 5986:
  - i. Click the Start button and navigate to All Programs > Administrative Tools > Server Manager.
  - ii. In the left pane, navigate to Server Manager > Configuration > Windows Firewall with Advanced Security>Inbound Rules.
    - i. Create a *New Inbound Rule*. Click on **New Rule...** on the right under **Actions** to display the *New Inbound Rule Wizard* window.
2. Create *New Inbound Rules* and specify ports in the *New Inbound Rule Wizard* window:
  - i. Select the radio button next to **Port**.
  - ii. Click **Next**.
  - iii. Verify that the radio buttons next to **TCP** and **Specific local ports** are selected.
  - iv. Enter the value **5986** in the field for **Specific local ports**.
  - v. Click **Next**.
  - vi. On the next page, verify that the radio button next to **Allow the connection** is selected.
  - vii. Click **Next**.
  - viii. On the next page, select the firewall profiles for which the rule should apply.
  - ix. Click **Next**.
  - x. On the next page, give the rule a name.
  - xi. Click **Finish**.

## Creating the WinRM Listener Using SSL

1. Launch the Windows Power Shell:
  - i. Click the **Windows PowerShell** icon if it exists in the tool bar.  
or
  - ii. Click **Start**, enter the word *Power* in the search field and select **Windows PowerShell**.
2. Create the listener referencing the newly created Certificate. At the PowerShell command line, type the following command, substituting your values for the certificate *thumbprint* and *serverfqdn* (server fully qualified domain name):

```
winrm create
winrm/config/Listener?Address=*&Transport=HTTPS '@{Hostname="[serverfq
```

```
dn]";CertificateThumbprint="[thumbprint]"}
```

For example:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
'@{Hostname="mymachinename.mynetwork.com";CertificateThumbprint="3a796b
ce838285553231301116e5bd14f02d6189"}'
```

**Note:** The thumbprint value must be entered without the spaces that are displayed in the **Detail** tab of the *Certificate Information* window.

3. Specify *https* (SSL) instead of *http* connections. Enter the following command:

```
winrm s winrm/config/service '@{AllowUnencrypted="false"}'
```

**Note:** If this is already controlled through a policy, an error displays.

## Adding the Server to Cisco UCS Performance Manager

In the Cisco UCS Performance Manager web UI:

1. Navigate to the **Infrastructure** page.
2. If the server has not yet been added to Cisco UCS Performance Manager, add it the **Server/Microsoft/Windows** device class and opt out of modeling.
3. Click on the name of the target server.
4. Click on the server's Configuration Properties.
5. Edit the configuration property for *zWinScheme* to be *https*.
6. Edit the value for *zWinRMPort* to be *5986*.
7. Verify that the values for *zWinRMUser* and *zWinRMPassword* are correct. This means the appropriate Windows credentials, for example, *Bill* and *billspassword*, respectively. Edit as necessary.
8. To verify that the settings have been successfully entered, model the device. Click the **Action Wheel** (gear-shaped) icon in the lower left and select **Model Device...**

## Windows 2008: Configuring a WinRM Service Account on Individual Servers

See the section above titled [\*About Windows Authentication for WinRM Monitoring\*](#) if necessary for more background on Windows permissions requirements when monitoring with WinRM. Complete the following steps on each server to configure your service account:

1. Add a new local user for use as a service account:
  - i. Open **Server Manager**.
  - ii. Expand *Configuration* in the left pane.
  - iii. Expand *Local Users and Groups* in the left pane.
  - iv. Right click on **Users** and select **New User** from the menu that displays.
  - v. Complete the New User form. Uncheck **User must change password** at next logon and check (if desired) the **Password never expires** box.
  - vi. Click **Create**.
  - vii. Click **Close** to exit the *New User* form.
2. Copy your permissions configuration script, for example the *zenoss-lpu.ps1* script, to the target server.
3. Run the PowerShell Script:
  - i. Click the *Windows PowerShell* icon, if present, in the Taskbar. If the icon is not present, click **Start** in the taskbar and enter "Powershell" in the search field to locate PowerShell.
  - ii. Run your service account configuration script by typing the full path to the script in the command line and append the script with the *-u* option and the name of your service account. For example, if you are using an edited version of the *zenoss-lpu.ps1* script and your service account is named "benny," enter the following command at the PowerShell prompt:

```
C:\tmp\zenoss-lpu.ps1 -u benny
```

**Note:** depending on the security policies enforced on your server, you might encounter an error such as:

```
File C:\tmp\zenoss-lpu-ps1 cannot be loaded because running scripts is disabled on this system....
```

If you encounter this error, you can bypass the security restrictions for this script by including the

*-executionpolicy bypass* option, for example:

```
Powershell -executionpolicy bypass -file C:\tmp\zenoss-lpu.ps1 -u benny
```

# Windows 2008: Using Group Policy to Configure a Service Account on all Servers

**Important note:** If the Group Policies for your Windows 2008R2 domain have been left at their default settings, Windows may block the execution of PowerShell scripts over the network without active user confirmation at the command line that the script should be permitted to run. This request for user intervention can cause Windows systems to hang on boot for an extended period when a startup script is run, pending user intervention (which cannot be given because administrators cannot log on to the system while it waits). Group Policy objects that work around this issue can be created that do the following:

1. Set the PowerShell execution policy to *allow all scripts*.
2. Add the hostname (or the hosts's domain) of the server hosting the script on a shared directory in the Trusted Sites Internet Zone.
3. Edit registry keys to disable Internet Explorer's Enhanced Security Configuration (this is necessary to add items to the Trusted Sites Internet Zone).

Administrators should weigh the security implications of these policies against the benefits of being able to deploy the PowerShell script from a central location using Group Policy instead of running the script manually on each server to be modified. To make these changes, complete the next section.

## Enabling Script Execution (If Necessary)

1. Click **Start** in the taskbar and enter *Group Policy Management* in the search bar to locate *Group Policy Management*.
  - i. In the left pane of the *Group Policy Manager* window, navigate to **Forest: yourdomain > Domains > yourdomain > Group Policy Objects**  
  
For example:  
`Forest: doctest.loc > Domains > doctest.loc > Group Policy Objects`
  - ii. Right click *Group Policy Objects* and select **New** to display the *NEW GPO* dialog.
  - iii. Name your policy, for example *script\_execution*.
  - iv. Click **OK** to save and exit the *New Policy* window.
2. Edit your new policy.
  - i. In the left pane, navigate to your new Group Policy Object. For example:  
**Forest: doctest.loc > Domains > doctest.loc > Group Policy Objects > script\_execution**
  - ii. Right click the policy and select **Edit** to display the *Group Policy Management Editor*.
    - a. In the left pane of the *Group Policy Management* window, navigate to:  
`Computer Configuration/Policies/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel/Security Page/`
    - b. In the right panel, double click **Site to Zone Assignment List**
    - c. Click the **Enabled** radio button



- d. Add the hostname of the system hosting your PowerShell script (or the domain where it is located if broader permissions are desired) by clicking the **Show** button.  
**Note:** In the right *Help* menu you are provided with guidance on how to add domains or individual hosts.
- e. Choose the value '2' for your site or domain to put it into the *Trusted Sites Zone*.
- f. Click **OK** at the bottom of the form.

iii. In the left pane of the *Group Policy Management* window, navigate to:

Computer Configuration/Policies/Administrative Templates/Windows Components/Windows PowerShell/

- a. In the right pane, double-click **Turn on Script Execution**
- b. In the *Turn on Screen Execution* dialog window, click the **Enabled** radio button.
- c. Click **OK**
- d. In the dropdown list under *Execution Policy*, choose **Allow all scripts**.
- e. Click **OK** at the bottom.

iv. In the left pane of the *Group Policy Management* window, navigate to:

Computer Configuration/Preferences/Windows Settings/Registry/

- a. Right-click on *Registry* and select **New > Registry Item**.
- b. Either enter the following Key Path or use the [...] button to use the *Registry Item Browser* to navigate to:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{A509B1A7-37EF-4b3f-8CFC-4F3A74704073}

- c. In the lower pane, click **IsInstalled**
- d. Click the **Select** button to display the *New Registry Properties* dialog box.
- e. In the *New Registry Properties* dialog box, select the **General** tab and verify the following settings:
  - *Action* is set to **Update**.
  - The *Hive* is **HKEY\_LOCAL\_MACHINE**
  - The *Key Path* is the one specified in step b.
  - The *Value name* is **IsInstalled** and the *Default* box is **unchecked**.
  - The *Value type* is **REG\_DWORD**
  - The checkbox for *Base* is set to **Hexadecimal**
- f. Change the *Value data* entry from the Default of 00000001 (enabled) to the new value of 00000000 (disabled)
- g. Click **OK** to close the dialog and save the changes.

9. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.

**Note:** Substitute a specific OU for the domain if you want to link only to a subset of servers.

- i. Right-click your domain in the left pane of the *Group Policy Management* window.
- ii. Choose **Link an Existing GPO...**
- iii. Select your new GPO from the list that displays.
- iv. Click **OK** to complete the process.

10. Exit the *Group Policy Management* window:

Select **File > Exit**

11. Manually refresh Group Policy from the command prompt of target servers:

```
gpupdate /force
```

**Note:** you may need to reboot the server for the Internet Explorer settings to take effect.

## Creating the Domain User (Service) Account

Perform the following to create a new domain user (service) account, if necessary:

1. In the left panel of Server Manager, Navigate to your target domain in the tree at the left:
  - i. Expand *Roles*
  - ii. Expand *Active Directory Domain Services*
  - iii. Expand *Active Directory Users and Computers*
  - iv. Expand your domain.
2. Right-click *Users* and select **New > User**.
3. In the *New Object – User* window, provide a First name and a User logon name, *zenny* for example.
4. Verify the domain field has the correct domain identification. For example, *@doctest.loc*
5. Click **Next** to display the password dialog for the new user.
6. In the *Password* fields, enter and verify the new user password.
7. Uncheck the selection for **User must change password at next logon**.
8. Check the option for **Password never expires**.
9. Click **Next**.
10. Click **Finish**. Your new user, *zenny* for example, displays in the list of users for the domain.

## Completing Preparatory Sections

The following procedure assumes that you have completed the following preparatory sections:

- [Windows 2008: Configuring Firewall Group Policies](#)
- [Windows 2008: Configuring Windows Credentials in Cisco UCS Performance Manager](#)

This procedure requires the PowerShell script *zenoss-lpu.ps1*, available from the Cisco UCS Performance Manager support site.

## Creating the Script GPO

1. Create your service account configuration script (or edit, as appropriate, the sample script referenced above the section titled [About Windows Authentication for WinRM Monitoring](#)).
2. Copy your configuration script to an appropriate folders shared on the network, for example:  
`\\[yourdomain]\SYSVOL\[yourdomain]\SCRIPTS`
3. Open Group Policy Management, from the *Server Manager Console*, click **Tools > Group Policy Management**
4. Create a new policy.

- i. In the left pane, navigate to:

```
Forest: yourdomain > Domains > yourdomain > Group Policy Objects
```

For example:

**Forest: doctest.loc > Domains > doctest.loc > Group Policy Objects**

- ii. Right click *Group Policy Objects* and select **New** to display the *NEW GPO* dialog.
- iii. Name your policy, for example *zenoss-sa*

- iv. Click **OK** to save and exit the *New Policy* window.
5. Edit your new policy. In the left pane, navigate to your new Group Policy Object.  
For example:  
**Forest:** *doctest.loc* > **Domains** > *doctest.loc* > **Group Policy Objects** > *zenoss-sa*
  - i. Right click the policy and select **Edit** to display the *Group Policy Management Editor*.
  - ii. In the left pane of the *Group Policy Management* window, navigate to:  
  
Computer Configuration\Policies\Windows Settings\Scripts  
(Startup/Shutdown)
  - iii. Click Scripts (Startup/Shutdown).
  - iv. In the right pane (*Scripts (Startup/Shutdown)*), double-click **Startup** to launch the *Startup Properties* dialog.
  - v. In the *Startup Properties* dialog box, select the **PowerShell Scripts** tab.
  - vi. Click **Add** to display the *Add a Script* dialog box:
    - a. Specify the script name and path. In the *Script Name* field, enter the path to the script, or click **Browse** to locate the script file you copied in step 2 above.
    - b. Select the script and click **Open**.
    - c. In the *Script Parameters* box, enter the domain logon information for your service account user in the form of:  
-u *yourusername@yourdomain* for a domain user  
or -u *yourusername* for a local user.
    - d. Click **OK** to save the information and exit the *Add a Script* window.
    - e. If you have multiple scripts and want them to run in a particular order, use the **Up** and **Down** buttons in the *Startup Properties* window to set their run order.
    - f. Click **OK** to exit the *Startup Properties* window.
6. Exit the Local Group Policy Editor:  
**File > Exit**
7. Link your new GPO to one or more Organizational Units (OU) containing servers to which you want the policies applied. Alternatively, you can apply the policies to all Windows servers in the domain by linking the new GPO to the domain itself. To link the GPO to the domain, complete the following process.  
**Note:** Substitute a specific OU for the domain if you want to link only to a subset of servers.
  - i. Right-click your domain in the left pane of the *Group Policy Management* window.
  - ii. Choose Link an Existing GPO...
  - iii. Select your new GPO from the list that displays.
  - iv. Click **OK** to complete the process.
8. Exit the Group Policy Management window:  
Select **File > Exit**

9. Manually refresh Group Policy from the command prompt of target servers:

```
gpupdate /force
```

10. Reboot your member servers to pick up the script changes.