

Cisco UCS Director Bare Metal Agent Installation and Configuration Guide, Release 6.9

First Published: 2024-05-07

Last Modified: 2026-05-05

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.

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

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: https://www.cisco.com/c/en/us/about/legal/trademarks.html. 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. (1721R)

© 2024–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface ix

Audience ix

Recommended Knowledge ix

Conventions x

Related Documentation xi

Documentation Feedback xi

Communications, Services, and Additional Information xi

CHAPTER 1

New and Changed Information for this Release 1

New and Changed Information 1

CHAPTER 2

Overview 3

Cisco UCS Director Bare Metal Agent 3

Minimum System Requirements 3

Guidelines and Limitations 4

Network Configuration Options 5

Provisioning Bare Metal Servers through Bare Metal Agent 7

Upgrade of Bare Metal Agent 7

CHAPTER 3

Installing Cisco UCS Director Bare Metal Agent 9

Installing Cisco UCS Director Bare Metal Agent on VMware vSphere 9

Installing Cisco UCS Director Bare Metal Agent on Microsoft Hyper-V 11

CHAPTER 4

Configuring Cisco UCS Director Bare Metal Agent 13

Adding a Bare Metal Agent Account 13

Configuring the DHCP Server for a Bare Metal Agent Account 15

Associating a Bare Metal Agent to Cisco UCS Director 17
Configuring the Interface for the PXE Network 17
Adding an NFS Mount Point 18
Uploading an OS Image File 18
Generating Custom ESXi ISO Image 19
Viewing and Editing the OS Configuration File Details 21
Cloning an OS Configuration File 22
Swapping the OS Configuration File Details 23
Provisioning an OS Image 23

CHAPTER 5 **Managing Bare Metal Agent** 25
Managing bmaadmin Access 25
Logging in as bmaadmin User 26
Enabling bmaadmin Access 26
Disabling bmaadmin Access 27
Configuring bmaadmin Access 27
Configuring Password Policy 28
Password Management 29
Changing the Default Bare Metal Agent Account 29
Starting and Stopping Bare Metal Agent Services 30
Checking the Status of a Bare Metal Agent 30
Viewing the DHCP Configuration for a Bare Metal Agent Account 31
Using External DHCP Server and Bare Metal Agent 31
Configuring the DHCP Server on Linux OS 33
Configuring the DHCP Server on Windows OS 35
Viewing the DHCP Logs for a Bare Metal Agent Account 37
Viewing the Logs for a Bare Metal Agent Account 38
Viewing Operating System Images 38
Viewing PXE Service Requests 38
Viewing the Network Interface Details for a Bare Metal Agent Account 39
Shelladmin Script for Bare Metal Agent 39
Bare Metal Agent Migration Using Shelladmin Script 40
Online Migration 40
Offline Migration 42

Viewing the Bare Metal Agent Migration Status 45
Setting Up UEFI as Network Boot Manager 45

CHAPTER 6 **Adding Non-Windows OS Images** 47
Adding a Non-Windows OS Image in Bare Metal Agent 47
Non-Windows OS Provisioning through vMedia 48
Downloading Cisco UCS Storage Drivers 48

CHAPTER 7 **Adding Windows OS Images** 51
Windows OS Provisioning through vMedia 51
Windows Operating Systems Supported for Cisco UCS Director Bare Metal Agent 52
Guidelines and Limitations for Windows Operating System Images 52
Windows Server 2008 R2 x64 Operating System Images 53
Prerequisites for Setting Up Windows Server 2008 R2 x64 Operating System Images 53
Creating a Customized WinPE 54
Preparing Windows Server 2008 R2 Installation Files 55
Creating a Boot Configuration Data File 57
Verifying the Installation files For All Editions of Windows 2008 R2 58
Customizing and Copying the WinPE.wim and PXE Boot Files for Windows 2008 R2 59
Copying the Customized Windows Installation Files to the Bare Metal Agent VM 62
Windows Server 2012 x64 and 2012 R2 x64 Operating System Images 63
Prerequisites for Setting Up Windows Server 2012 x64 and 2012 R2 x64 Operating System Images 63
Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2012 64
Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2012 R2 67
Preparing Windows Server 2012 Installation Files 70
Preparing Windows Server 2012 R2 Installation Files 72
Installing and Setting Up the Boot Configuration Data File 74
Copying the Windows Installation Files to the Server Folder 75
Windows Server 2016 x64 Operating System Images 76
Prerequisites for Setting Up Windows Server 2016 x64 Operating System Images 76
Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2016 77
Preparing Windows Server 2016 R2 Installation Files 80
Installing and Setting Up the Boot Configuration Data File 82

Copying the Windows Installation Files to the Server Folder 83
Windows Server 2019 x64 Operating System Images 84
Prerequisites for Setting Up Windows Server 2019 x64 Operating System Images 84
Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2019 85
Preparing Windows Server 2019 x64 Installation Files 88
Installing and Setting Up the Boot Configuration Data File 90
Copying the Windows Installation Files to the Server Folder 91
Windows Server 2022 x64 Operating System Images 92
Prerequisites for Setting Up Windows Server 2022 x64 Operating System Images 92
Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2022 93
Preparing Windows Server 2022 x64 Installation Files 96
Installing and Setting Up the Boot Configuration Data File 98
Copying the Windows Installation Files to the Server Folder 99
Windows Server 2025 x64 Operating System Images 100
Prerequisites for Setting Up Windows Server 2025 x64 Operating System Images 100
Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2025 101
Preparing Windows Server 2025 x64 Installation Files 104
Installing and Setting Up the Boot Configuration Data File 106
Copying the Windows Installation Files to the Server Folder 107
Using MEMDISK for Deploying Multiple Versions of Windows Simultaneously 108
Requirements for Using MEMDISK 108
Creating Bootable WINPE File for Windows Server 2008 R2, 2012, 2012 R2, or 2016 108
Modifying MAC File Template 109
Automating PXE-based Windows OS Deployment 110
Specifying Windows OS Variant to be Deployed 110
Provisioning Windows OS Image 111

CHAPTER 8 **Provisioning OS Images through Orchestration Workflow Tasks 115**
Orchestration Workflow Tasks for PXE/vMedia Boot 115
Prerequisites for Workflows with PXE/vMedia Boot Tasks 116
Execution of the Setup PXE/vMedia Boot Tasks 117
Determining the Windows OS Edition 118
Inputs for the Setup PXE/vMedia Boot Task 119
Inputs for the Setup PXE/vMedia Boot with BMA Selection Task 122

Inputs for the Setup Windows PXE/vMedia Boot Task 125
Outputs from the Setup PXE/vMedia Boot Task and Setup Windows PXE/vMedia Boot Task 128
Creating a PXE Boot Request in Cisco UCS Director 129
Viewing the PXE Request Configuration Files 132
PXE Boot States 132
Monitor PXE/vMedia Boot Setup Task 133
Inputs for the Monitor PXE Boot Task 133
Outputs from the Monitor PXE Boot Task 133
Remove PXE/vMedia Boot Setup Task 133
Inputs for the Remove PXE Boot Setup Task 133
Outputs from the Remove PXE Boot Setup Task 134
Injecting Drivers When Installing RHEL 7 or CentOS 7 on UCS Modular Servers 134
Simultaneous Provisioning of Windows Server Operating Systems 135
Files and Folders Used In Simultaneous Deployment 135
Example: Simultaneous Deployment of Windows Server Operating Systems 136
Prerequisites for Provisioning ESXi OS to Dell, HP, and UCSM Bare Metal Servers through vMedia 139
Prerequisites for Provisioning RHEL OS to Dell, HP, and UCSM Bare Metal Servers through vMedia 139
Prerequisites for Provisioning Windows OS to Dell Bare Metal Servers through vMedia 142
Prerequisites for Provisioning Windows OS to HP Bare Metal Servers through vMedia 143
Prerequisites for Provisioning Windows OS to UCSM Bare Metal Servers through vMedia 144

APPENDIX A **Sample Operating System Configuration Template Files** 145
Encrypting the Root Password 145
Sample Configuration Template Files 145
Sample Linux Configuration Template Files 145
Sample Kickstart Configuration Template File for Linux Operating Systems 145
Sample PXE Configuration Template File for Linux Operating Systems 147
Sample iPXE Configuration Template File for Linux Operating Systems 147
Sample VMware vSphere ESXi Configuration Template Files 147
Sample Kickstart Configuration Template File for VMware vSphere ESXi Operating Systems 147
Sample PXE Configuration Template File for VMware vSphere ESXi Operating Systems 148
Sample iPXE Configuration Template File for VMware vSphere ESXi Operating Systems 149
Sample iPXE UEFI Configuration Template File for Windows 149

Sample Windows Answer File 149

APPENDIX B **Ports** 155

Cisco UCS Director TCP and UDP Port Usage 155

Cisco UCS Director TCP and UDP Port Usage on VMware vSphere 155

Cisco UCS Director TCP and UDP Port Usage on Microsoft Hyper-V 156

Port List 157

Multi-Node Port Requirements 158



Preface

- Audience, on page ix
- Conventions, on page x
- Related Documentation, on page xi
- Documentation Feedback, on page xi
- Communications, Services, and Additional Information, on page xi

Audience

This guide is intended primarily for data center administrators who use Cisco UCS Director and who have responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security
- Virtualization and virtual machines

Recommended Knowledge

To deploy and manage Cisco UCS Director Bare Metal Agent, you should be familiar with the following:

- DHCP configuration
- PXE boot
- TFTP functionality
- HTTP functionality
- Linux
- Virtualization technologies

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

Cisco UCS Director Documentation Roadmap

For a complete list of Cisco UCS Director documentation, see the *Cisco UCS Director Documentation Roadmap* available at the following URL: http://www.cisco.com/en/US/docs/unified_computing/ucs/ucs-director/doc-roadmap/b_UCSDirectorDocRoadmap.html.

Cisco UCS Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

Note The *Cisco UCS B-Series Servers Documentation Roadmap* includes links to documentation for Cisco UCS Manager and Cisco UCS Central. The *Cisco UCS C-Series Servers Documentation Roadmap* includes links to documentation for Cisco Integrated Management Controller.

Documentation Feedback

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

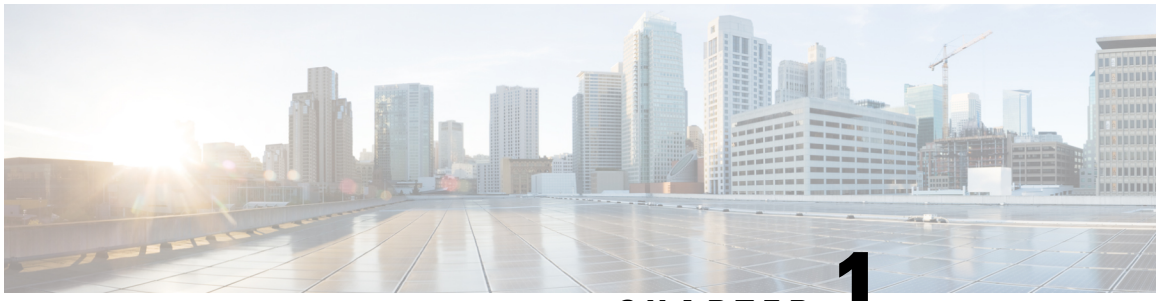
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.

- To get the business results you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

New and Changed Information for this Release

This chapter contains the following section:

- New and Changed Information, on page 1

New and Changed Information

The following table provides an overview of the significant changes to this guide for the current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New and Changed Information in Cisco UCS Director, 6.9(4.0)

Feature	Description	Where Documented
Windows OS deployment without manual preparation of supporting files	Allows you to perform Windows OS deployment without manually customizing `WinPE.wim` and `install.wim` files.	Automating PXE-based Windows OS Deployment

Table 2: New and Changed Information in Cisco UCS Director, 6.9(3.0)

Feature	Description	Where Documented
vMedia support for provisioning Windows Server 2025 OS	Allows you to provision Windows Server 2025 OS to Dell, HP, and UCSM bare metal servers using vMedia.	Provisioning OS Images through Orchestration Workflow Tasks
Generation of Custom ESXi ISO image	Allows you to generate the Custom ESXi ISO image by uploading ESXi Depot file and Driver zip file.	Generating Custom ESXi ISO Image

Table 3: New and Changed Information in Cisco UCS Director, 6.9(2.0)

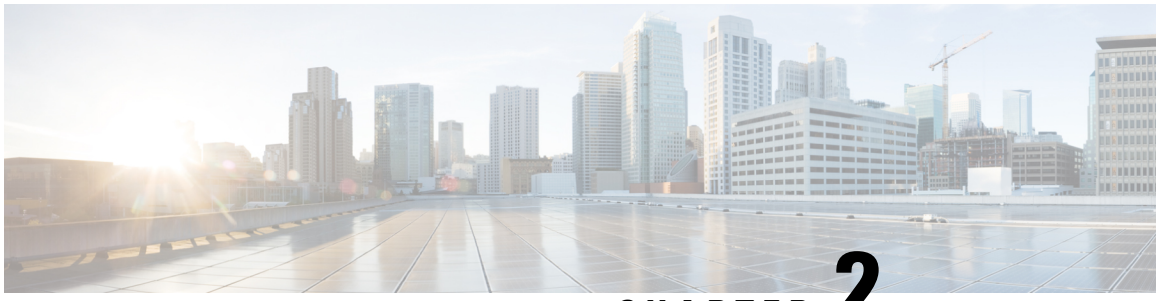
Feature	Description	Where Documented
Deployment of Windows Server 2025 OS through PXE	Allows you to deploy Windows Server 2025 OS on the Dell, HP, and UCSM bare metal servers using PXE boot and installation operations.	Windows Server 2025 x64 Operating System Images
vMedia support for provisioning Windows Server 2022 OS	Allows you to provision Windows Server 2022 OS to Dell, HP, and UCSM bare metal servers using vMedia.	Windows OS Provisioning through vMedia Provisioning OS Images through Orchestration Workflow Tasks
Shelladmin options for bmaadmin user	The root user access is disabled and bmaadmin user is enabled by default. The following shell admin options are introduced: • Manage bmaadmin Access • Login as bmaadmin	Managing bmaadmin Access
Configuring password policy	The new Shell admin option **Configure Password Policy** allows you to define a password policy that must be followed while setting passwords for shelladmin, bmaadmin, and root users.	Configuring Password Policy

Table 4: New and Changed Information in Cisco UCS Director, 6.9(1.0)

Feature	Description	Where Documented
vMedia support for provisioning non-Windows OSs	The Cisco UCS Director enables vMedia support on the Bare Metal Agent. The vMedia supports provisioning of the following OSs for Dell, HP, and UCSM bare metal servers: • ESXi • RHEL	Non-Windows OS Provisioning Through vMedia

Table 5: New and Changed Information in Cisco UCS Director, 6.9(0.0)

Feature	Description	Where Documented
Support for BMA version 6.9(0.0)		



CHAPTER 2

Overview

This chapter contains the following sections:

- Cisco UCS Director Bare Metal Agent, on page 3
- Minimum System Requirements, on page 3
- Guidelines and Limitations, on page 4
- Network Configuration Options, on page 5
- Provisioning Bare Metal Servers through Bare Metal Agent, on page 7
- Upgrade of Bare Metal Agent, on page 7

Cisco UCS Director Bare Metal Agent

Cisco UCS Director Bare Metal Agent (BMA) automates the process of using a Preboot Execution Environment (PXE) to install operating systems on bare metal servers or virtual machines. Bare Metal Agent provides the following services that are required for a functional PXE install environment:

- Dynamic Host Control Protocol (DHCP)
- Hypertext Transfer Protocol (HTTP)
- Trivial File Transfer Protocol (TFTP)

When this environment is operational and Bare Metal Agent and Cisco UCS Director are correctly configured, you can build PXE installation tasks into any Cisco UCS Director infrastructure workflow.

You can access Bare Metal Agent through Secure Shell (SSH). You can also perform services on Bare Metal Agent, such as DHCP configuration and starting and stopping services, through Cisco UCS Director. A single Cisco UCS Director node can support multiple Bare Metal Agent applications.

Minimum System Requirements

For proper installation and operation of Bare Metal Agent, your environment must meet the minimum system requirements.

Minimum Requirements for VMware vSphere

Name	Requirements
VMware vCenter Server	Versions 7.x, 8.x, and 9.x
Minimum reservation in VMware vCenter	Minimum number of CPUs—4 Memory—16 GB Hard disk—100 GB

Minimum Requirements for Microsoft Hyper-V

Name	Requirements
Hyper-V	Windows server 2016, Windows server 2019, Windows server 2022, Windows server 2025
Minimum reservation in Hyper-V	Minimum number of CPUs—4 Memory—16 GB Hard disk—100 GB

Guidelines and Limitations

Before you install Bare Metal Agent, take note of the following guidelines and limitations.

Bare Metal Agent Connections

Each Bare Metal Agent application can connect to only one Cisco UCS Director node.

Network Availability

After installation and configuration, your environment must have the following network availability:

- Bare Metal Agent must be able to reach Cisco UCS Director over the network.
- Cisco UCS Director must be able to reach Bare Metal Agent over the network.
- The bare metal servers (blade or rack) must be able to reach the DHCP network of the Bare Metal Agent during the initial stage of operating system installation over PXE.

DHCP Configuration

If you use DHCP, locate a DHCP server in the same PXE VLAN as Bare Metal Agent. Then configure that DHCP server with the IP address range required by your DHCP server.

VLAN Configuration

When setting up the network configuration, the most common configuration uses one PXE VLAN and one Management VLAN (separate VLANs). However, Bare Metal Agent supports one VLAN for both, if you prefer.

Configure the VLANs end-to-end between Cisco UCS, Cisco UCS Director, and Bare Metal Agent. However, when you configure Bare Metal Agent, do not assume that routing occurs between the PXE_VLAN Layer 2 network and the Management VLAN network.

If you configure Bare Metal Agent to use DHCP, locate and configure the DHCP server in the PXE VLAN and its subnet. This DHCP server serves the transient IP address required for the PXE process. In an environment with two VLANs, the server is allocated an IP address from the subnet of the Management VLAN. An IP address pool managed by Cisco UCS Director assigns this IP address.

If you configure Bare Metal Agent with two VLANs, set up two IP address attributes:

- An IP address for Bare Metal Agent in the PXE VLAN
- A second IP address for Bare Metal Agent in the Management VLAN

TFTP Server

With Bare Metal Agent, use the Cisco UCS Director TFTP server to ensure that configurations such as dynamic variables function properly.

When you add a Bare Metal Agent account, Bare Metal Agent configures the TFTP server when services are started.

Network Configuration Options

You can choose between the following network configuration options for Bare Metal Agent

- Single network for management and Preboot Execution Environment (PXE)
- Separate networks for management and PXE

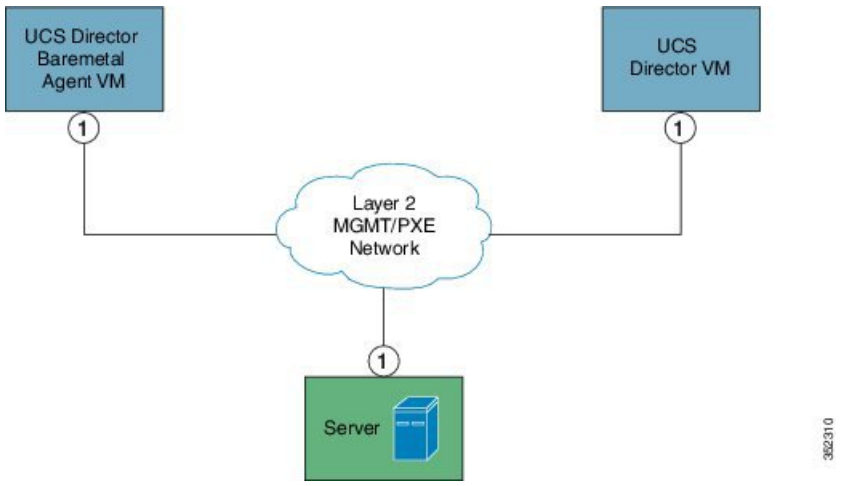
Choose the network configuration option that best meets the requirements of your environment.

Single Network for Management and PXE

We recommend that you choose this network configuration option if your environment permits the following to be hosted on the same VLAN (Layer 2) network (see the following figure):

- Services provided by Bare Metal Agent, such as DHCP, TFTP, and HTTP
- Management traffic between Bare Metal Agent and Cisco UCS Director or other devices and appliances

Figure 1: Sample Topology for a Single Network

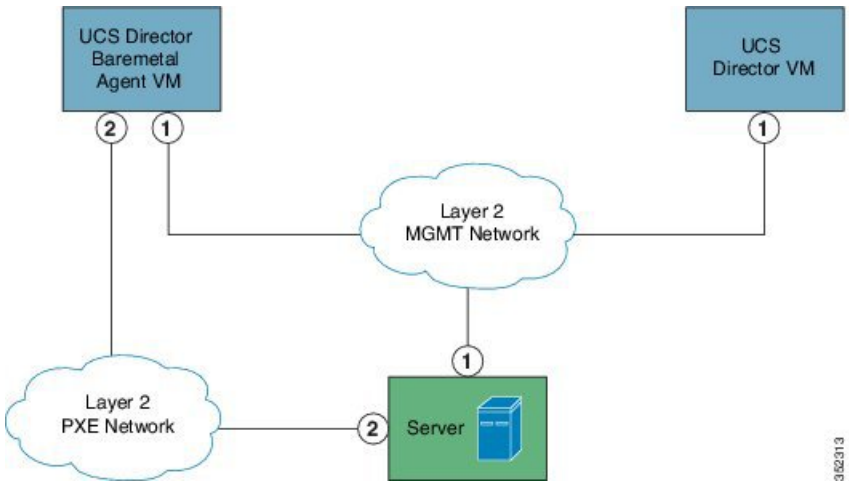


Separate Networks for Management and PXE

We recommend that you choose this network configuration option if your environment does not permit the following to be hosted on the same network interface and Layer 2 network (see the following figure):

- On the PXE network, services provided by Bare Metal Agent, such as DHCP, TFTP, and HTTP
- On the Management network, traffic between Bare Metal Agent and Cisco UCS Director or other devices and appliances

Figure 2: Sample Topology for Separate PXE and Management Networks



Prerequisites and Assumptions for a Network Configuration

Make sure that your environment meets the following prerequisites for Bare Metal Agent network configuration:

- Cisco UCS Director has been installed and the network interface configured, as described in the appropriate Cisco UCS Director installation guide.
- Cisco UCS Director Bare Metal Agent is reachable through a web browser and you can log in.
- Bare Metal Agent has been installed, and no additional configuration has been performed.

- For a single network configuration, make sure that the required single Management and PXE VLAN is provisioned and available as a virtual port group or port profile that virtual machines (VMs) can be attached to or leveraged.
- For a separate network configuration, make sure that the following networks are provisioned and available as a virtual port group or port profile that VMs can be attached to or leveraged:
  - Management (MGMT) network—Used for traffic between Bare Metal Agent and Cisco UCS Director
  - PXE network—Used for PXE services traffic, such as DHCP, HTTP, and TFTP

Provisioning Bare Metal Servers through Bare Metal Agent

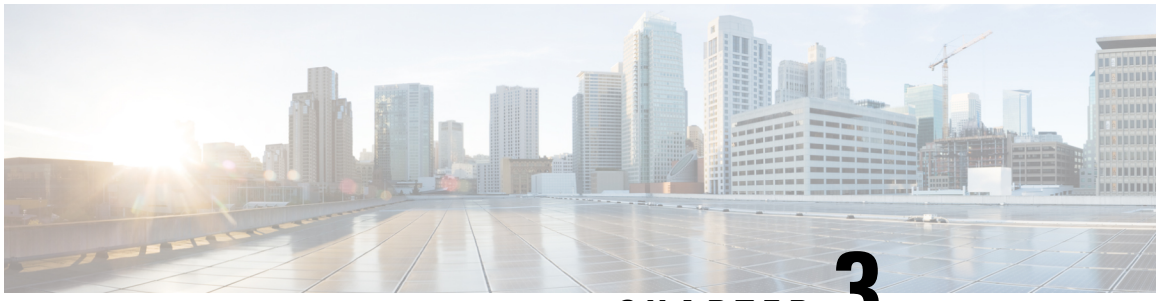
The process involved in installing operating systems on bare metal servers through Bare Metal Agent is as follows:

- Install Bare Metal Agent. See Installing Cisco UCS Director Bare Metal Agent, on page 9.
- Configure Bare Metal Agent. See Configuring Cisco UCS Director Bare Metal Agent, on page 13.
- Add OS images in Bare Metal Agent. See Adding Windows OS Images, on page 51 or Adding Non-Windows OS Images, on page 47.
- Deploy OS images on bare metal servers through workflow tasks. See Provisioning OS Images through Orchestration Workflow Tasks, on page 115.

For managing Bare Metal Agent operations through Cisco UCS Director, see Managing Bare Metal Agent, on page 25.

Upgrade of Bare Metal Agent

For detailed information on upgrading Bare Metal Agent, see the Cisco UCS Director Upgrade Guide.



CHAPTER 3

Installing Cisco UCS Director Bare Metal Agent

This chapter contains the following sections:

- Installing Cisco UCS Director Bare Metal Agent on VMware vSphere, on page 9
- Installing Cisco UCS Director Bare Metal Agent on Microsoft Hyper-V, on page 11

Installing Cisco UCS Director Bare Metal Agent on VMware vSphere

Before you begin

- You must have system administrator privileges for VMware vSphere or vCenter.
- If you want to use a static IP address rather than DHCP, you must know the following information:
  - IP address
  - Subnet mask
  - Default gateway

Procedure

Step 1 On the Cisco.com download site for Cisco UCS Director, download Cisco UCS Director Bare Metal Agent and unzip the OVF file.

Step 2 Log in to VMware vSphere Client.

Step 3 In the **Navigation** pane, click the vSphere host on which you want to deploy Cisco UCS Director Bare Metal Agent.

Step 4 Choose **File** > **Deploy OVF Template**.

Step 5 On the **Source** screen of the **Deploy OVF Template** window, do one of the following to choose your OVF source location and then click **Next**:

- If the OVF file is stored on your local computer, browse to the location, choose the file, and click **Open**.
- If the OVF file is stored on a server on your local area network, enter the location of the file including the IP address or fully qualified domain name of the server.

Step 6 On the **OVF Template Details** screen, verify the details and click **Next**.

Step 7 On the **End User License Agreement** screen, review the license agreement and click **Accept**.

Step 8 On the **Name and Location** screen, do the following:

a) In the **Name** field, enter a unique name for the VM.
b) In the **Inventory Location** area, choose the location where you want the VM to reside.
c) Click **Next**.

Step 9 On the **Storage** screen, choose the storage location for the VM and click **Next**.

Step 10 On the **Disk Format** screen, click **Next** to accept the default radio button for **Thick Provision (Lazy Zeroed)** format.

Step 11 On the **Network Mapping** screen, choose the network for the VM and click **Next**.

Step 12 On the **Properties** screen, do the following:

a) Configure the IP addresses for both the NICs (ens192 and ens224) that you want to assign, as follows:

- To use DHCP to assign the IP addresses, leave the default of 0.0.0.0 in the IP address fields.
- To use static IP addresses, enter the desired IP addresses in the IP address fields. If you only want to configure one NIC, only complete one set of IP addresses and leave the second set at the default.

b) Check the **Enable BMA Migration** check box to enable the BMA migration process.

By default, **Enable BMA Migration** check box is enabled. For new OVF deployment, you can uncheck the **Enable BMA Migration** check box to disable the BMA migration process.

Note You can also log on to the Bare Metal Agent VM using SSH client as 'shelladmin' user and choose the **BMA Migration** option and press **Enter**.

c) Specify the existing BareMetal Agent (6.7.4.2 / 6.8.x.x) IP address, if you have checked the **Enable BMA Migration** check box. Otherwise, enter the IP address as 0.0.0.0.
d) In the **Existing BareMetal Agent (6.7.4.2 / 6.8.x.x) Root Password** section, enter the password in the **Enter password** and **Confirm password** fields.
e) Click **Next**.

Step 13 On the **Ready to Complete** screen, verify the settings and click **Finish**.

A message appears to indicate that Cisco UCS Director Bare Metal Agent is being deployed.

Step 14 On the **Navigation** pane, right-click the VM host and choose **Edit Settings**.

Step 15 Make sure that the VM host has sufficient resources to power on.

For more information about the required resources, see Minimum System Requirements, on page 3.

Step 16 Power on the VM.

Note Make sure that Cisco UCS Director is successfully migrated to version 6.8.0.0.

Important During the migration process, `dhcpd.conf` file of Bare Metal Agent (6.7.4.2 / 6.8.x.x) appliance is copied into the new Bare Metal Agent (6.9.0.0) appliance in the `/etc/dhcp` path. You can check the migration status using the **Migration Status** option. For more information, see Viewing the Bare Metal Agent Migration Status, on page 45. When the migration status is displayed as completed, you can login to the Bare Metal Agent (6.9.0.0) appliance and navigate to the path `/etc/dhcp` and perform the following:

- Execute **cp legacy_bma_dhcpd.conf_bak /etc/dhcpd.conf**.
- Restart the DHCPD services using **service dhcpd restart** command.

Installing Cisco UCS Director Bare Metal Agent on Microsoft Hyper-V

Note We recommend that you deploy Cisco UCS Director Bare Metal Agent on the Hyper-V Manager host, rather than the Microsoft System Center Virtual Machine Manager (SCVMM) console.

Before you begin

- You must have system administrator privileges for Microsoft Hyper-V.
- If you want to use a static IP address rather than DHCP, you must know the following information:
  - IP address
  - Subnet mask
  - Default gateway

Procedure

Step 1 On the Cisco.com download site for Cisco UCS Director, download Cisco UCS Director Bare Metal Agent and unzip the *.vhd file into a folder.

Step 2 Log into the Hyper-V host.

Step 3 Choose **Start** > **Administrative Tools** to open Hyper-V Manager.

Step 4 On the **Hyper-V Manager** screen, choose **Action** > **New Virtual Machine**.

Step 5 In the **Before You Begin** pane, click **Next** to accept the custom configuration option.

Step 6 In the **Specify Name and Location** pane, enter a unique name for the virtual machine (VM) name in the **Name** field.

Step 7 In the **Name and Location** pane, do the following:

a) Check the **Store the virtual machine in a different location** check box.
b) Enter the alternate location.
c) Click **Next**.

Step 8 In the **Select Generation** pane, choose **Generation 2**.

With Generation 2, the virtual machine provides the same virtual hardware to the virtual machine as in previous versions of Hyper-V.

Step 9 In the **Assign Memory** pane, enter the amount of memory to allocate to this VM (3 GB minimum) and click **Next**.

Step 10 In the **Configure Networking** pane, in the **Connection** field, click **Next** to accept the **Not Connected** default option.

Step 11 In the **Connect Virtual Hard Disk** pane, click **Next** to accept the **Attach a virtual disk later** default option.

Step 12 In the **Completing the New Virtual Machine Wizard** pane, verify the settings and click **Finish**.

Step 13 In the left pane, right-click the VM and choose **Edit Settings**.

Step 14 Delete the existing network adapter and click **Apply**.

Step 15 In the **Security** pane, select the **Enable Secure Boot** check box and choose the template **Microsoft UEFI Certificate Authority**.

Step 16 In the **Navigation** pane, click **Processor**.

Step 17 In the **Number of virtual processors** field, enter **2 vCPU**.

Step 18 In the **Navigation** pane, click **Add Hardware**.

Step 19 In the **Add Hardware** pane, choose the **Legacy Network Adapter** and click **OK**.

Step 20 In the **Legacy Network Adapter** pane, in the **Virtual Switch** drop-down list, choose the virtual network device.

Step 21 In the **Navigation** pane, click **SCSI Controller**.

Step 22 In the **SCSI Controller** pane, choose **Hard Drive** and click **Add**.

Step 23 Browse to the .vhd file and choose it.

Step 24 Click **Apply**, and then click **OK**.

Step 25 Power on the VM to configure network properties.

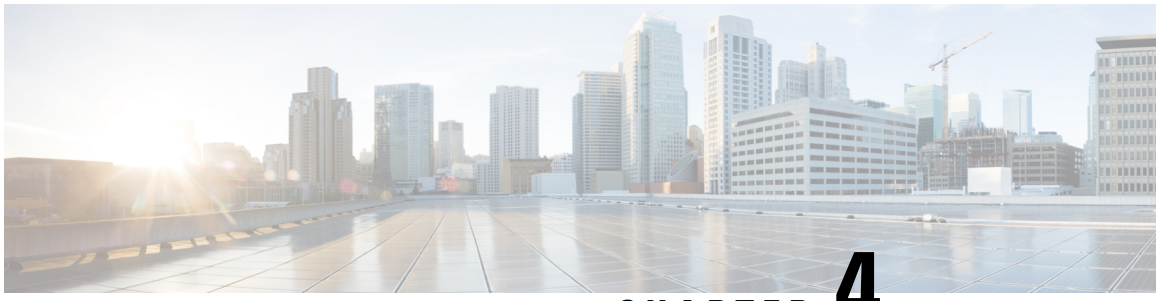
Optionally, you can configure network properties from the Shell Admin.



Note Only when a BMA appliance is associated with a Cisco UCS Director, the dbkeys and dbcreds files are copied to a specific location in the BMA appliance to establish successful connectivity to the Cisco UCS Director. After installing the BMA, you need to add the BMA appliance to Cisco UCS Director.

What to do next

After Cisco UCS Director Bare Metal Agent has started, configure DHCP or a static IP address.



CHAPTER 4

Configuring Cisco UCS Director Bare Metal Agent

This chapter contains the following sections:

- Adding a Bare Metal Agent Account, on page 13
- Configuring the DHCP Server for a Bare Metal Agent Account, on page 15
- Associating a Bare Metal Agent to Cisco UCS Director, on page 17
- Configuring the Interface for the PXE Network, on page 17
- Adding an NFS Mount Point, on page 18
- Uploading an OS Image File, on page 18
- Viewing and Editing the OS Configuration File Details, on page 21
- Cloning an OS Configuration File, on page 22
- Swapping the OS Configuration File Details, on page 23
- Provisioning an OS Image, on page 23

Adding a Bare Metal Agent Account

Before you begin

Important From the Bare Metal Agent release 6.9(2.0), the root user is disabled and 'bmaadmin' is enabled by default.

Before you add a Bare Metal Agent account, do the following:

- Make sure that the Bare Metal Agent is installed.
- Make sure that the Bare Metal Agent VM is completely booted up, login to Bare Metal Agent VM Console to view the Management IP address.
- Log in to Bare Metal Agent through VM Console or SSH client to access the CLI and change the default bmaadmin password using the BMA Shell option **Manage bmaadmin Access**.
- Set up the environment required to support a single or separate PXE and Management network configuration, with the appropriate VLANs.
- To provide required DHCP services, ensure that the PXE interface of the Bare Metal Agent is connected to PXE VLAN network and configure DHCP service with an appropriate IP address range.

- Ensure to use the same Samba password of the legacy BMA (version 6.7.4.2 / 6.8.x.x) in the Samba Password and Confirm Samba Password fields in the migrated BMA (version 6.9.x.x), if the Samba Service for Windows PXE check box is enabled.
- Log into Bare Metal Agent VM using SSH client and update WinPE.wim with eth1 IP address details of the migrated BMA (version 6.9.x.x), if the legacy BMA (version 6.7.4.2 / 6.8.x.x) and migrated BMA (version 6.9.x.x) are deployed with different PXE IP addresses.
- Log into Cisco UCS Manager and update the service profile with PXE VLAN details of the migrated BMA (version 6.9.x.x), reset the server, and then resubmit the service request in Cisco UCS Director appliance, if the legacy BMA (version 6.7.4.2 / 6.8.x.x) and migrated BMA (version 6.9.X.X) are deployed with different PXEVLAN ID or a failed service request is available in the migrated Cisco UCS Director appliance (version 6.9.x.x).

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 On the **Add Bare Metal Agent Appliance** screen, complete the following fields:

Name	Description
Account Name field	The name you assign to this Bare Metal Agent account.
Description field	(Optional) A description of this Bare Metal Agent.
Bare Metal Agent uses different interfaces for management and PXE traffic check box	Select this check box if your configuration uses separate networks for the PXE server and the management network that hosts the traffic manager.
Management/PXE Address field	The IP address assigned to the Management network for Bare Metal Agent. If your configuration uses a single network for the Management and PXE networks, this IP address is automatically assigned as the PXE address. **Note** This address must be reachable from Cisco UCS Director.
PXE Interface Address field	The IP address for the Bare Metal Agent PXE network, if your configuration uses separate networks. **Note** This field appears only if the **Bare Metal Agent uses Different Interfaces for Management and PXE Traffic** check box is selected.

Name	Description
Login ID field	Enter 'bmaadmin'. This account provides the administrative privileges for Bare Metal Agent. As 'bmaadmin' is the default user from the Bare Metal Agent release 6.9(2.0), it is necessary to link Cisco UCS Director with Bare Metal Agent using 'bmaadmin' account.
Password field	Enter the password created for the 'bmaadmin' account.
Enable Samba service for Windows PXE check box	Samba is used for Bare Metal Agent to install Windows Operating Systems. Select this check box if you want to install Windows Operating Systems. In Cisco UCS Director, Release 6.9, ensure to use the same Samba password of the legacy BMA (version 6.7.4.2 / 6.8.x.x) in the Samba Password and Confirm Samba Password fields in the migrated BMA (version 6.9.x.x), if this check box is enabled.
Samba Password field	Enter the password for the Samba service.
Confirm Samba Password field	Confirm the password for the Samba service.
Location field	(Optional) The location of the Bare Metal Agent.
Database Address drop-down list	The Bare Metal Agent requires access to the Cisco UCS Director database. Choose the IP address of Cisco UCS Director which is on the same Management network as the Bare Metal Agent. **Note** If you are configuring the Bare Metal Agent for the Cisco UCS Director multi-node deployment, choose the IP address of the Inventory Database node.

Step 4 Click **Submit**.

What to do next

Configure the DHCP Server for Bare Metal Agent.

Configuring the DHCP Server for a Bare Metal Agent Account

Note For a multi-home DHCP configuration, use this procedure to configure the first subnet for the DHCP server. For the remaining subnets, you must manually edit the DHCP configuration file (`/etc/dhcpd.conf`).

Before you begin

To provide required DHCP services, ensure that at least one DHCP server is located in the same PXE VLAN as Bare Metal Agent. Configure the DHCP server with an appropriate IP address range. The DHCP server, together with the TFTP server, is used to communicate with a PXE server.

Procedure

Step 1 Log in to the Cisco UCS Director server with the following credentials:
a) User—**admin**
b) Password—**admin**

Step 2 Choose **Administration** > **Physical Accounts**.

Step 3 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 4 Click the row for the Bare Metal Agent account for which you want to configure the DHCP server.

Step 5 Click **Service Status** to verify that services for the Bare Metal Agent account are stopped.

Step 6 Click **Configure DHCP**.

Step 7 On the **Configure DHCP** screen, complete the following fields and click **Submit**.

- **DHCP Subnet**
- **DHCP Netmask**
- **DHCP Start IP**
- **DHCP End IP**
- **Router IP Address**

The DHCP IP address assignments are updated, and the DHCP service is restarted.

Step 8 Click the row for the Bare Metal Agent account and click **Start Services**.

Step 9 After the services have started, do the following:

- Verify that the status of the account in the **Status** column is Active.
- Verify that the **Enabled Services** column shows that all services are running. If this status indicates that one or more services are stopped, verify the configuration of your DHCP server and try again.
- Click **Service Status** to verify that the status of all expected services is up:
  - Network Services status in the Bare Metal Agent appliance
  - Database connectivity status from the Bare Metal Agent appliance

What to do next

Set up PXE boot requests.

Associating a Bare Metal Agent to Cisco UCS Director

To establish a connection between the Bare Metal Agent and Cisco UCS Director, you need to associate the Bare Metal Agent to Cisco UCS Director.

Procedure

Step 1 Log in to Cisco UCS Director deployed with the compatible version of the Bare Metal Agent.

Step 2 Choose **Administration** > **Physical Accounts**.

Step 3 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 4 Add a Bare Metal Agent account. See Adding a Bare Metal Agent Account, on page 13.

Step 5 Click the row for the Bare Metal Agent account and click **Start Services**. It might take around two minutes for the services to start.

Step 6 After the services have started, verify that the status of the account in the **Status** column is Active. It might take two minutes for the status to reflect as Active. When status of the BMA service is active, the BMA is ready for use.

Note Only when the BMA services are started from the Cisco UCS Director UI, the dbkeys and dbcreds files are copied to a specific location in the BMA appliance to establish successful connectivity to the Cisco UCS Director.

Configuring the Interface for the PXE Network

You can use this to change or add an IP address for the PXE network used by Bare Metal Agent.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to configure the interface for the PXE network.

Step 4 Click **Configure Interface**.

Step 5 On the **Configure PXE Interface** screen, complete the following fields:

a) From the **Interface Name** drop-down list, choose the interface that you want to use for the PXE network.

b) Enter the IP address and subnet mask for the PXE network.

c) Click **Submit**.

Adding an NFS Mount Point

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to view PXE service requests.

Step 4 Click **View Details**.

Step 5 Click **NFS Mount Point**.

Step 6 Click **Add**.

Step 7 On the **Add NFS Mount Point** screen, do the following:

a) In the **NFS Server IP Address** field, enter the IP address of the NFS server where you plan to store the OS images for Bare Metal Agent to use.

b) In the **NFS Server Path** field, enter the location on the NFS server where the OS images are stored.

c) Click **Submit**.

After you add the NFS mount point, all content in the `imageRepository` folder in the NFS server is available under the `/mnt/external` folder. You include this path in the `isoExtractor.sh` file when you create a non-Windows image template.

Uploading an OS Image File

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to upload the OS image.

Step 4 From the **More Actions** drop-down list, click **View Details**.

Step 5 Click **Image Repository**.

Step 6 Click **Upload Image**.

Step 7 On the **Image Upload** screen, complete the following fields:

Name	Description
Image Name field	The name of the OS image.
OS Type drop-down list	Choose the OS image type that you want to install on the server. The drop-down list includes all OS types supported by the Bare Metal Agent.

Name	Description
Upload Type drop-down list	Choose one of the following: • Desktop File - To select the file from your local. • Web Server Path - To select the file from a remote server that is reachable by the Cisco UCS Director Bare Metal Agent.
Local File Path field	This field is displayed when you choose the Desktop File option in the **Upload Type** drop-down list. To upload the file, you can either drag and drop the required file or click **Select** and click **Submit**.
Web URL field	This field is displayed when you choose the Web Server Path option in the **Upload Type** drop-down list. Enter the web server path where the ISO images are stored and click **Submit**.
MD5 Checksum field	This field is displayed when you choose the Web Server Path option in the **Upload Type** drop-down list. (Optional) Enter the MD5 checksum value of the downloaded ISO file which is used to verify the data integrity.

Step 8 Click **Submit**. The details of the uploaded image is displayed.

Step 9 Under **Image Repository** menu, select the row for the OS image for which you want to view the upload status and log details.

The **Upload Status** is updated to **Upload Succeeded**, and the corresponding log message is displayed under the **Upload Log** column.

Generating Custom ESXi ISO Image

From the Cisco UCS Director Bare Metal Agent, release 6.9(3.0), you can have the system generate the required ISO image for the ESXi OS by uploading the ESXi Depot file and the Driver zip file.

Before you begin

- Ensure that the Cisco UCS Director Bare Metal Agent is well connected to the internet so that the system can download the VMware PowerCLI software from the Broadcom website, as this software is essential for the successful generation of Custom ESXi ISO image.
- ESXi Depot File—You must have downloaded the ESXi base image from the VMware website. For example, `VMware-ESXi-9.0.0.0.24580437-depot.zip`.
- Driver File—You must have downloaded or created a driver ZIP file containing all the required async drivers to be integrated into the Custom ESXi ISO image. The required files can be downloaded from the Cisco website.
- If the Cisco UCS Director Bare Metal Agent does not have direct internet access and must use a proxy, configure the proxy before generating a custom ESXi ISO. Run the following commands once in the

BMA SSH session after upgrading to Cisco UCS Director Release 6.9(2.0) or later. This enables connectivity to the Broadcom CDN. You do not need to run the commands before every custom ESXi ISO generation. Repeat the setup only if the proxy settings change.

```
sudo pwsh
sudo pwsh -Command '
$line = "[System.Net.Http.HttpClient]::DefaultProxy = New-Object
System.Net.WebProxy("http://<PROXY_SERVER>:<PORT_NUMBER>")"
$p = Join-Path $PSHOME "profile.ps1"
if (-not (Test-Path $p)) { New-Item -ItemType File -Path $p -Force | Out-Null }
if (-not (Select-String -Path $p -SimpleMatch "DefaultProxy" -Quiet)) { Add-Content
-Path $p -Value $line }
Write-Host "Updated: $p"
'
exit
```

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 From the list of Bare Metal Agent accounts, select the required Bare Metal Agent account for which you want to upload the Custom ESXi ISO image.

Step 4 From the top menu, select **Image Repository**.

Step 5 Click the **Upload Image** icon.

Step 6 On the **Image Upload** screen, complete the following fields:

Name	Description
Image Name field	The name of the Custom ESXi ISO image.
OS Type drop-down list	Select **Custom-ESXi**.
Upload Type drop-down list	Choose one of the following: • Desktop File—To select the files from your local. • Web Server Path—To select the files from a remote server. **Important** When you upload incompatible files or files with unsupported or invalid file formats, the upload will not succeed, and the OS image entry added under the **Image Repository** area will be removed after validation.
ESXi Depot File Path field	This field is displayed when you choose the Desktop File option in the **Upload Type** drop-down list. To upload the file, you can either drag and drop the required file or click **Select a File** to browse and choose the file from your local system.

Name	Description
Driver File Path field	This field is displayed when you choose the Desktop File option in the **Upload Type** drop-down list. To upload the file, you can either drag and drop the required file or click **Select a File** to browse and choose the file from your local system.
ESXi Depot File Web URL field	This field is displayed when you choose the Web Server Path option in the **Upload Type** drop-down list. Enter the web server path where the ESXi Depot file is stored.
Driver File Web URL field	This field is displayed when you choose the Web Server Path option in the **Upload Type** drop-down list. Enter the web server path where the Driver file is stored.

Step 7 Click **Submit**.

The system will take some time to prepare the Custom ESXi ISO image.

Step 8 Under the **Image Repository** menu, select the row for the OS image for which you want to view the upload status and log details.

The **Upload Status** is updated to **Upload Succeeded** upon successful completion of the Custom ESXi ISO image generation, and the corresponding log message is displayed under the **Upload Log** column.

What to do next

Deploy the Custom ESXi OS on the Cisco UCS Manager-based bare metal servers using the provisioning processes. For more information, refer Provisioning OS Images through Orchestration Workflow Tasks.

Note The Custom ESXi OS deployment is not applicable for the third party servers.

Viewing and Editing the OS Configuration File Details

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account.

Step 4 From the **More Actions** drop-down list, click **View Details**.

Step 5 Click **OS Catalogs**.

Step 6 Click the row for the OS catalog for which you want to view the configuration details.

Step 7 Click **View Configuration Files**.

Step 8 On the **View Configuration Files** screen, choose a file. The configuration details for the file are displayed.

Step 9 Click the row for the OS catalog for which you want to edit the configuration details and click **Edit Configuration Files**.

Step 10 On the **Modify Configuration Files** screen, choose the required file from the **Select the file** drop-down list and make the necessary changes.



Important For provisioning of ESXi and RHEL OS to HP, Dell, and UCSM bare metal servers through vMedia, as a prerequisite, the following files must be edited:

OS	Configuration Files
ESXi	boot.cfg boot-uefi.cfg
RHEL	ks.cfg ks-uefi.cfg

Step 11 Click **Submit**.

You can delete the configuration details by clicking **Delete Configuration Files**.

Cloning an OS Configuration File

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account.

Step 4 From the **More Actions** drop-down list, click **View Details**.

Step 5 Click **OS Catalogs**.

Step 6 Click the row for the OS catalog for which you want to clone the configuration details.

Step 7 Click **Clone Configuration Files**.

Step 8 On the **Clone Configuration Files** screen, do the following:

a) Choose a file from the **Select the file** drop-down list.
b) Enter a unique name for the file.
c) Click **Submit**.

Swapping the OS Configuration File Details

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.
Step 3 Click the row for the Bare Metal Agent account.
Step 4 From the **More Actions** drop-down list, click **View Details**.
Step 5 Click **OS Catalogs**.
Step 6 Click the row for the OS catalog for which you want to swap the configuration details.
Step 7 Click **Swap Configuration Files**.
Step 8 On the **Swap Configuration Files** screen, choose the files whose details need to be swapped.
Step 9 Click **Submit**.

Provisioning an OS Image

Procedure

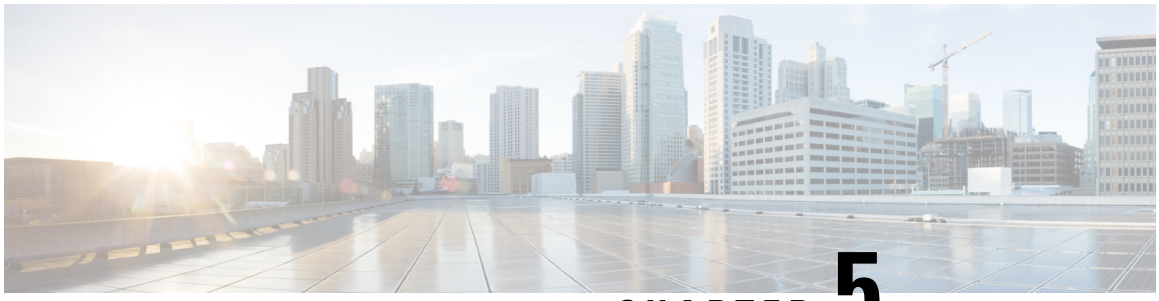
Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.
Step 3 Click the row for the Bare Metal Agent account for which you want to upload the OS image.
Step 4 From the **More Actions** drop-down list, click **View Details**.
Step 5 Click **Image Repository**.
Step 6 Click the row for the OS image that you want to provision.
Step 7 Click **Provision Image**.
Step 8 On the **Provision Image Catalog** screen, complete the following fields:

Name	Description
OS Type drop-down list	Choose the OS image type that needs to be provisioned in the Bare Metal Agent. The drop-down list includes all the available OS types with details such as version and update number.
Catalog Name field	Enter the catalog name. **Important** While provisioning ESXi and RHEL OS to Dell, HP, and UCSM bare metal servers, make a note of the catalog name as it is used as an input for a workflow.

Step 9 Click **Provision Image**.



Note For provisioning of ESXi and RHEL OS for HP, Dell, and UCSM bare metal servers, some prerequisites must be met. For more information, see Provisioning OS Images through Orchestration Workflow Tasks.



CHAPTER 5

Managing Bare Metal Agent

This chapter contains the following sections:

- Managing bmaadmin Access, on page 25
- Password Management, on page 29
- Changing the Default Bare Metal Agent Account, on page 29
- Starting and Stopping Bare Metal Agent Services, on page 30
- Checking the Status of a Bare Metal Agent, on page 30
- Viewing the DHCP Configuration for a Bare Metal Agent Account, on page 31
- Using External DHCP Server and Bare Metal Agent, on page 31
- Viewing the DHCP Logs for a Bare Metal Agent Account, on page 37
- Viewing the Logs for a Bare Metal Agent Account, on page 38
- Viewing Operating System Images, on page 38
- Viewing PXE Service Requests, on page 38
- Viewing the Network Interface Details for a Bare Metal Agent Account, on page 39
- Shelladmin Script for Bare Metal Agent, on page 39
- Bare Metal Agent Migration Using Shelladmin Script, on page 40
- Viewing the Bare Metal Agent Migration Status, on page 45
- Setting Up UEFI as Network Boot Manager, on page 45

Managing bmaadmin Access

From the Cisco UCS Director Bare Metal Agent release 6.9(2.0), root user access is disabled by default to prevent the use of root privileges for regular management operations. Instead, 'bmaadmin' user account is enabled by default to enhance security. Therefore, it is recommended to access the Cisco UCS Director Bare Metal Agent using the 'bmaadmin' account.

To provide administrative privileges, the following BMA Shell options are introduced:

- **Manage bmaadmin Access**
- **Login as bmaadmin**

Logging in as bmaadmin User

Note As the 'root' user access is disabled and 'bmaadmin' user access is enabled by default, you must log in as bmaadmin user with **bmaadmin** as the password.

Procedure

Step 1 From the BMA Shell menu, choose **Login as bmaadmin** and press **Enter**.

The following information is displayed:

```
Do you want to Login As bmaadmin [y/n]?
```

Step 2 Enter **y** and press **Enter**.
The following information is displayed:

```
Logging in as bmaadmin
Password:
```

Step 3 Enter the password and press **Enter**.

Note The first time you enter the default password **bmaadmin**, you will be prompted to change the password in accordance with the password policy.

The BMA shell options are displayed.

Enabling bmaadmin Access

Procedure

Step 1 From the BMA Shell menu, choose the **Manage bmaadmin Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (bmaadmin privilege) [e/d/c]:
```

Step 2 Enter **e** and press **Enter**.
The following information is displayed:

```
Do you want to Enable bmaadmin Access [y/n]?
```

Step 3 Enter **y** and press **Enter**.
The following information is displayed:

```
Enabling bmaadmin access...
Unlocking password for user bmaadmin.
passwd: Success
bmaadmin access enabled successfully
Press return to continue ...
```

Step 4 Press **Enter** to complete the process.

Disabling bmaadmin Access



Note As the 'root' user access is disabled and 'bmaadmin' user access is enabled by default to enhance security, it is not recommended to disable the **bmaadmin** access.

Procedure

Step 1 From the BMA Shell menu, choose the **Manage bmaadmin Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (bmaadmin privilege) [e/d/c]:
```

Step 2 Enter **d** and press **Enter**.

The following information is displayed:

```
Warning: All active terminal sessions of the bmaadmin user will be terminated.
Do you want to Disable bmaadmin Access [y/n]?
```

Step 3 Enter **y** and press **Enter**.

The following information is displayed:

```
Disabling bmaadmin access...
Locking password for user bmaadmin.
passwd: Success
bmaadmin access disabled successfully
All active bmaadmin sessions have been terminated.
Press return to continue ...
```

Step 4 Press **Enter** to complete the process.

Configuring bmaadmin Access

Procedure

Step 1 Log in to BMA CLI using an SSH client.

Step 2 From the BMA Shell menu, choose the **Manage bmaadmin Access** option and press **Enter**.

The following information is displayed:

```
Enable/Disable/Configure (bmaadmin privilege) [e/d/c]:
```

Step 3 Enter **c** and press **Enter**.

The following information is displayed:

```
Warning: If the bmaadmin user account is disabled, it will be enabled during the password reset
process.
Do you want to Configure/Set bmaadmin Privilege/Password [y/n]?
```

Step 4 Enter **y** and press **Enter**.

The following information is displayed:

```
Changing password for user bmadadmin.
New password:
```

Step 5 Enter the password and press **Enter**.

The following information is displayed:

```
Retype new password:
```

Step 6 Enter the password again for confirmation and press **Enter**.

The following information is displayed:

```
passwd: all authentication tokens updated successfully.
bmaadmin password changed successfully and bmaadmin account has been enabled.
Press return to continue...
```

Step 7 Press **Enter** to complete the process.

Configuring Password Policy

The Shell admin console allows you to configure a password policy for users such as shelladmin, bmaadmin, and root. This configuration enforces strong password requirements to ensure the security of the Cisco UCS Director Bare Metal Agent.

Procedure

Step 1 From the BMA Shell menu, choose **Configure Password Policy** and press **Enter**.

The password policy criteria is displayed.

Criteria	Minimum Range	Maximum Range	Default Value
Minimum Password Length	6	80	8
Minimum Character Classes	0	4	4
Minimum Lowercase Letters	–5	0	–1
Minimum Uppercase Letters	–5	0	–1
Minimum Digits	–5	0	–2

Criteria	Minimum Range	Maximum Range	Default Value
Minimum Special Characters	–5	0	–1
Minimum Unique Characters from Old Password	0	5	2
Maximum Sequential Identical Characters Allowed	0	5	3
Maximum Retry Attempts	0	5	5
Number of Old Passwords Remembered	0	15	10
Enforce Policy for root	Yes/No		Yes

Step 2 Press **Enter** to keep the default values or enter a new value within the given range and press **Enter**.

The following information is displayed:

```
Password policy updated successfully in /etc/security/pwquality.conf and /etc/security/pwhistory.conf
Press return to continue ...
```

Note When a shelladmin, bmaadmin, or root user attempts to set a new password, the user must adhere to the configured password policy.

Password Management

The default password for Bare Metal Agent is 'bmaadmin'. When you log in to the Bare Metal Agent for the first time, you will be prompted to reset the default password according to the password policy. For more information, see Managing BMA Admin Access.

Changing the Default Bare Metal Agent Account

The first Bare Metal Agent account that you create is designated as the default account. This account is used by default in legacy workflows. To use a different account in the legacy workflows, you must designate that Bare Metal Agent account as the default.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account that you want designate as the default.

Step 4 Click **Set Default BMA**.

Starting and Stopping Bare Metal Agent Services

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account whose services you want to start or stop.

Step 4 Click one of the following:

- **Start Services**
- **Stop Services**

Step 5 Click **Service Status** and check the status displayed in the **Enabled Services** column to ensure that services have started or stopped as desired.

If services do not start, check the status displayed in the **Enabled Services** column. If this status indicates that services are not enabled, verify the configuration of your DHCP server and try again.

Checking the Status of a Bare Metal Agent

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account whose status you want to check.

Step 4 To see if services for the Bare Metal Agent account are Active or Inactive, check the **Status** column.

Step 5 To check the status of the services, click **Service Status**.

Step 6 To view the SSH-based test connection status, check the **Reachable** column.

Viewing the DHCP Configuration for a Bare Metal Agent Account

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to view the DHCP configuration.

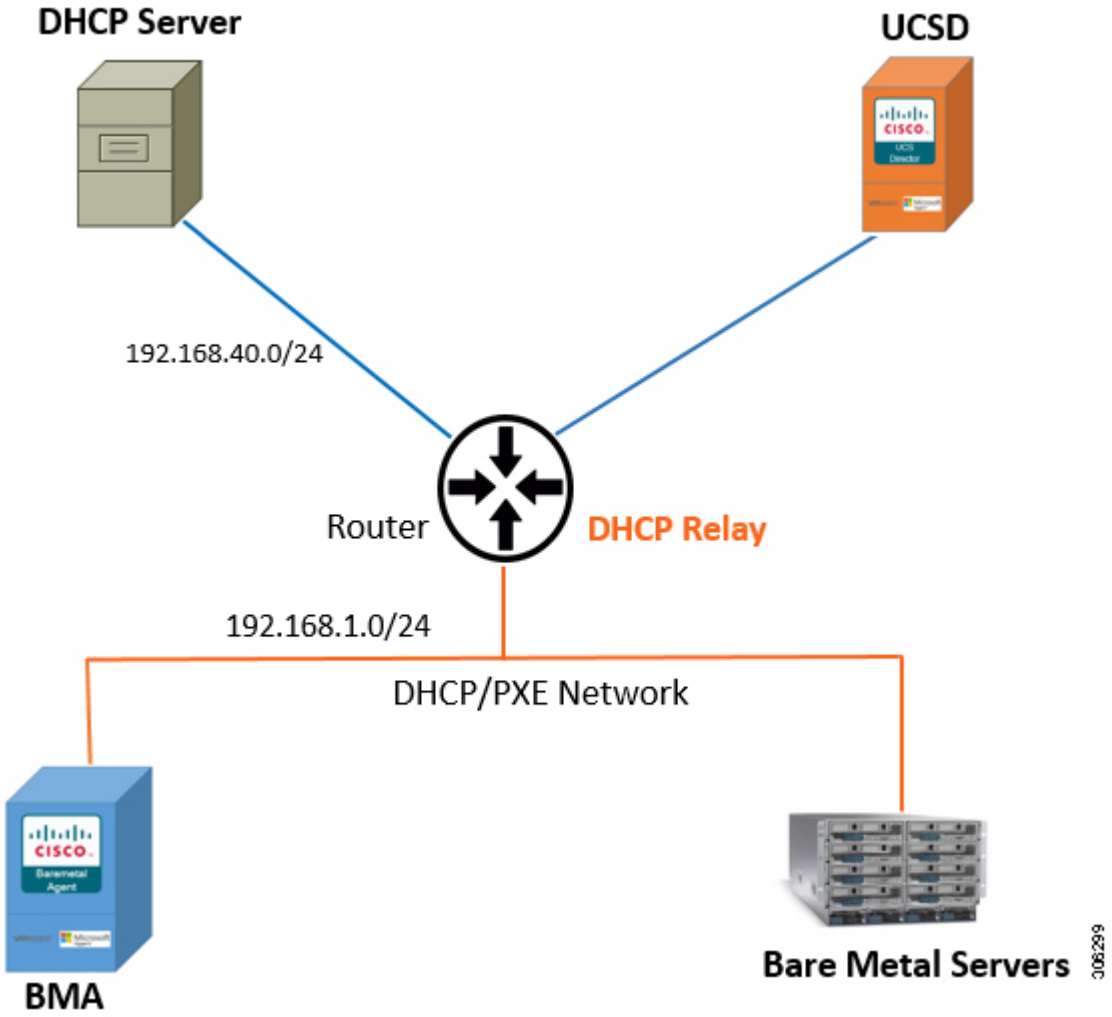
Step 4 Click **View DHCP Configuration**.

You might need to click the Down arrow at the end of the button bar to access the **View DHCP Configuration** option.

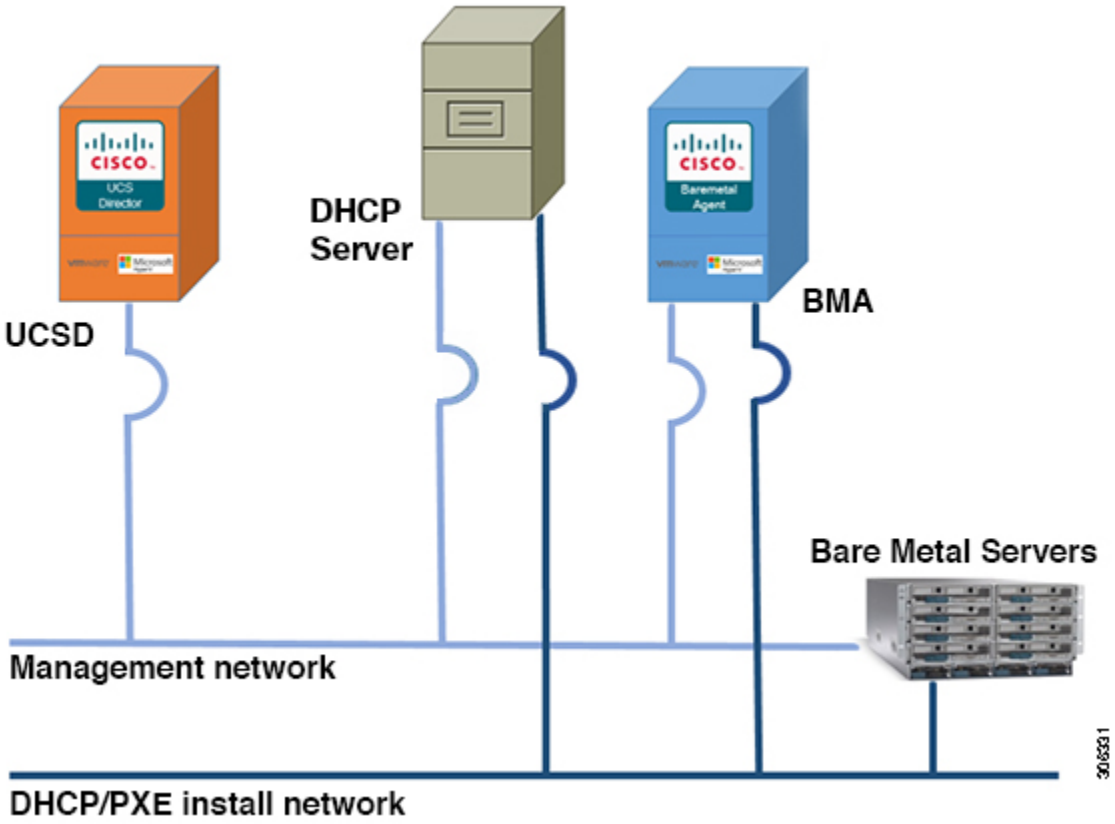
The **View DHCP Server Configuration** window displays the contents of the DHCP server configuration file for the account.

Using External DHCP Server and Bare Metal Agent

The following figure shows the sample topology for OS deployment over PXE from Cisco UCS Director using an external DHCP server, Bare Metal Agent, and bare metal servers in different subnets.



The following figure shows the sample topology for OS deployment over PXE from Cisco UCS Director using an external DHCP server, Bare Metal Agent, and bare metal servers in the same subnet.



Configuring the DHCP Server on Linux OS

Procedure

Step 1 Disable the DHCP services on the BMA. Perform the following:

a) Log on to the Bare Metal Agent VM using SSH client as 'shelladmin' user. See, Shelladmin Script for Bare Metal Agent, on page 39.

b) Choose the **Disable DHCP Service** option to stop the DHCP service.

Note In future, if you want to use the DHCP service on the same BMA, you can choose the **Enable DHCP Service** option to start the DHCP service.

Step 2 Perform the following in the router:

a) Enable routing between the BMA or the Bare Metal server subnet and the DHCP server subnet.

b) Enable the DHCP functionality on the router.

c) Configure DHCP relay agent such that the DHCP relay address points to the DHCP server IP address.

Step 3 Perform the following on the Linux server to configure the DHCP server:

a) Copy the network details of the BMA or the Bare Metal server subnet to `/etc/dhcpd.conf` file.
b) Configure the DHCP configuration file having the 'next-server' IP with the BMA PXE interface IP address.



Note DHCP relay configuration is only needed when the DHCP server and the target bare metal servers on the different subnet.

c) Configure the PXE binary.

```
if substring (option vendor-class-identifier, 15,5) = "00000" {
filename "/ipxelinux.0";
}else{
filename "ipxe.efi";
}
```

The following is a sample of the DHCP configuration file on the Linux OS which is catering DHCP services to two subnets. You can customize the DHCP configuration based on your requirements.

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style interim;
ignore client-updates;
subnet 192.168.4.0  netmask 255.255.255.0 {
         option routers                  192.168.4.1;
#        option subnet-mask              255.255.255.0;
#        option nis-domain               "domain.org";
#        option domain-name              "domain.org";
#        option domain-name-servers      192.168.55.1;
        option time-offset              -18000; # Eastern Standard Time
        range dynamic-bootp 192.168.4.100 192.168.4.200;
        default-lease-time 21600;
        max-lease-time 43200;
        allow booting;
        allow bootp;
        next-server 192.168.4.20; # IP of the BMA server
        if substring (option vendor-class-identifier, 15, 5) = "00000" {
                filename "/ipxelinux.0";
        }else{
                filename "/ipxe.efi";
        }
}



subnet 192.168.1.0  netmask 255.255.255.0 {
         option routers                  192.168.1.1;
#        option subnet-mask              255.255.255.0;
#        option nis-domain               "domain.org";
#        option domain-name              "domain.org";
#        option domain-name-servers      192.168.55.1;
        option time-offset              -18000; # Eastern Standard Time
        range dynamic-bootp 192.168.1.100 192.168.1.220;
        default-lease-time 21600;
        max-lease-time 43200;
        allow booting;
        allow bootp;
        next-server 192.168.1.60; # IP of my PXE server
        if substring (option vendor-class-identifier, 15, 5) = "00000" {
                filename "/ipxelinux.0";
```

```
        }else{
                filename "/ipxe.efi";
        }
}
```

Configuring the DHCP Server on Windows OS

Procedure

Step 1 Disable the DHCP services on the BMA. Perform the following:

a) Log on to the Bare Metal Agent VM using SSH client as 'shelladmin' user. See, Shelladmin Script for Bare Metal Agent, on page 39.

b) Choose the **Disable DHCP Service** option to stop the DHCP service.

Note In future, if you want to use the DHCP service on the same BMA, you can choose the **Enable DHCP Service** option to start the DHCP service.

Step 2 Perform the following in the router:

a) Enable routing between the BMA or the Bare Metal server subnet and the DHCP server subnet.

b) Enable the DHCP functionality on the router.

c) Configure DHCP relay agent such that the DHCP relay address points to the DHCP server IP address.

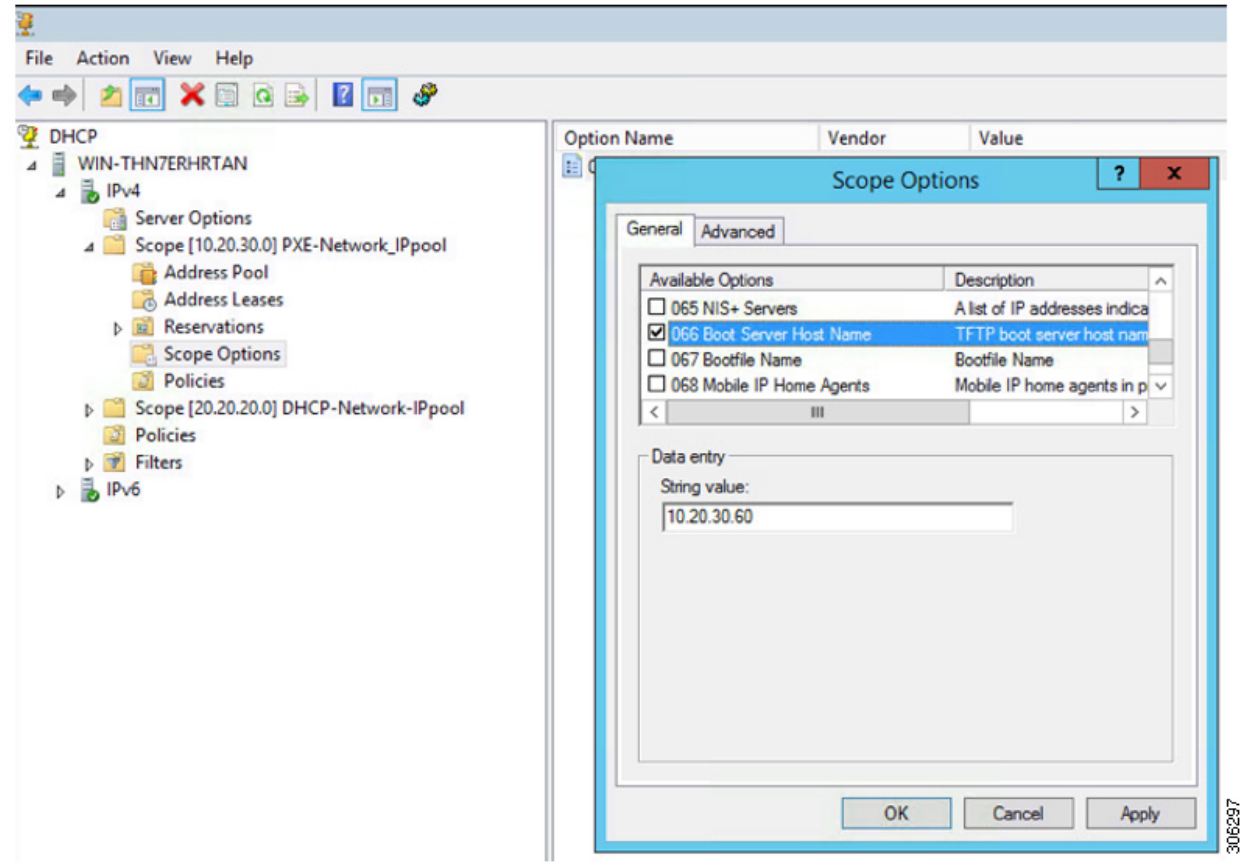
Note DHCP relay configuration is only needed when the DHCP server and the target bare metal servers on the different subnet.

Step 3 Perform the following on the Windows server to configure the DHCP server:

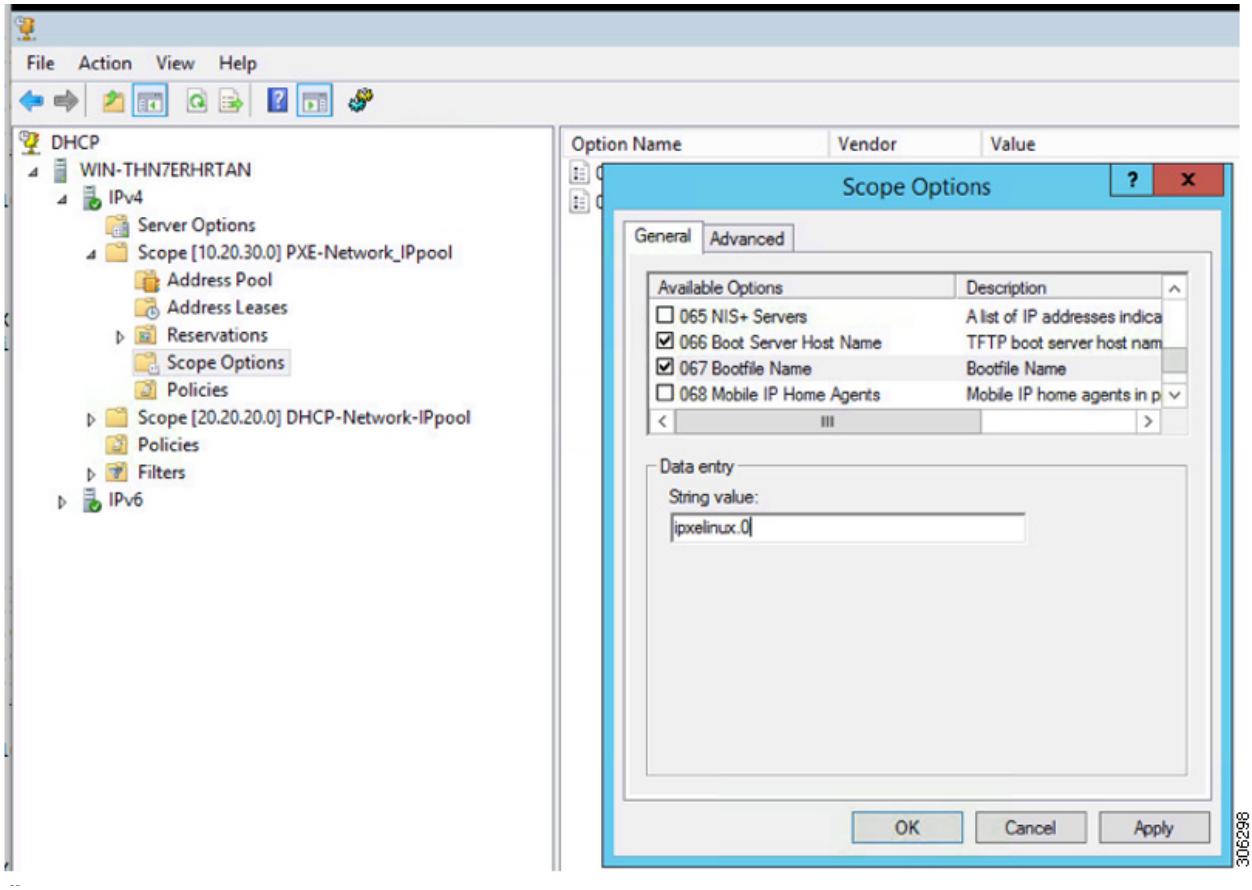
a) Configure the firewall rules on the Windows server to allow the DHCP requests.

b) Configure the DHCP scope options with the network details of the BMA or the Bare Metal server subnet.

c) Choose the **066-Boot Server Host Name** option and specify the BMA PXE interface IP address in the **Data entry**



d) Choose the **067-Bootfile Name** option and enter `ipxelinux.0` in the **Data entry**



Viewing the DHCP Logs for a Bare Metal Agent Account

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to view the DHCP logs.

Step 4 Click the down arrow at the end of the button bar and choose **View DHCP Logs**.

The **View Bare Metal Agent DHCP Log** window displays the contents of the DHCP server logs for the account.

Viewing the Logs for a Bare Metal Agent Account

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to view the logs.

Step 4 Click the down arrow at the end of the button bar and choose **View BMA Logs**.

The **View Bare Metal Agent Log** window displays the logs for the account.

Viewing Operating System Images

You can view a list of the operating system (OS) images that have been created and are available for a Bare Metal Agent account.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account for which you want to view OS images.

Step 4 Click **View Details**.

Step 5 Click **BMA OS List**.

Viewing PXE Service Requests

You can view information about PXE requests made through a workflow that have an associated service request. You cannot view details of PXE requests that are not made through a workflow, as those requests are not associated with a service request.

The information provided about each PXE request includes the following:

- Service request ID
- Request type
- User who initiated the request
- Name of the catalog or workflow that was used to create the request

- Any comments provided by the user who initiated the request
- Time of the request
- Status of the request
- Rollback type, if applicable

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.
Step 3 Click the row for the Bare Metal Agent account for which you want to view PXE service requests.
Step 4 Click **View Details**.
Step 5 Click **PXE Service Requests**.

Viewing the Network Interface Details for a Bare Metal Agent Account

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.
Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.
Step 3 Click the row for the Bare Metal Agent account for which you want to view the network interface details.
Step 4 Click the down arrow at the end of the button bar and choose **View Details**.
Step 5 Click **Network Interface Summary**. The network interface details are displayed.

Shelladmin Script for Bare Metal Agent

Procedure

Step 1 Log in to the Bare Metal Agent VM using SSH client as 'shelladmin' user.

Example:

The following list of services appears:

```
BMA | Version:6.8.0.0 | UpTime:  03:34:47 up 10 days,  2:38

0)  Quit
1)  Display Services Status
2)  Stop Services
3)  Start Services
4)  Display Samba Service
5)  Stop Samba Service
6)  Start Samba Service
7)  Change Samba Password
8)  Disable DHCP Service
9)  Enable DHCP Service
10) Time Sync
11) Ping Hostname/IP Address
12) Show Version
13) Configure Network Interface
14) Display Network Details
15) Add DNS Server
16) Tail Network Services Logs
17) Tail DHCP Logs
18) Change DHCP Configuration
19) Run IsoExtractor Script
20) Apply Patch
21) Apply Signed Patch
22) Shutdown Appliance
23) Reboot Appliance
24) Change Root Password
25) Change ShellAdmin Password
26) Login as Root
27) Show UCSD appliance host name
28) BMA Migration
29) Migration Status
30) Manage Root Access
31) Manage bmaadmin Access
32) Login as bmaadmin
33) Configure Password Policy
```

Step 2 Choose the required option and press **Enter**.

Bare Metal Agent Migration Using Shelladmin Script

Online Migration

Procedure

Step 1 Log on to the Bare Metal Agent VM using SSH client as **shelladmin** user.

The following list of services appears:

```
Cisco UCS BareMetal Agent Shell Menu
BMA | Version:6.9.0.0 | UpTime:  10:17:03 up 33 min,  1 user

0)  Quit
```

```
1)  Display Services Status
2)  Stop Services
3)  Start Services
4)  Display Samba Service
5)  Stop Samba Service
6)  Start Samba Service
7)  Change Samba Password
8)  Disable DHCP Service
9)  Enable DHCP Service
10) Time Sync
11) Ping Hostname/IP Address
12) Show Version
13) Configure Network Interface
14) Display Network Details
15) Add DNS Server
16) Tail Network Services Logs
17) Tail DHCP Logs
18) Change DHCP Configuration
19) Run IsoExtractor Script
20) Apply Patch
21) Apply Signed Patch
22) Shutdown Appliance
23) Reboot Appliance
24) Change Root Password
25) Change ShellAdmin Password
26) Login as Root
27) Show UCSD appliance host name
28) BMA Migration
29) Migration Status
30) Manage Root Access
31) Manage bmaadmin Access
32) Login as bmaadmin
33) Configure Password Policy
```

Step 2 From the Bare Metal Agent Shell menu, choose the **BMA Migration** option and press **Enter**.

The following information displays:

```
*********************************************************************************
*****************************    BMA migration     ********************************
*********************************************************************************

Current BMA Version : 6.9.0.0
Stopping BMA services , before Starting migration ..........
Enter existing Baremetal Agent Appliance Address   : 10.193.47.218
```

Step 3 Enter the existing address of the BMA appliance and press **Enter**.

The following information is displayed:

```
Enter root password   of xxxxxx       :
```

Step 4 Enter the root password and press **Enter**.

The following information is displayed:

```
Enter the root password and press Enter.
The following information is displayed:
Existing Baremetal Agent Appliance Address   : XX.XX.XX.XX

*****************   STARTING BMA MIGRATION STEP (1/2)   **************************

Required disk space : 2638 MB
Available free disk space : 86650 MB
Stop BMA service for 10.193.47.218
```

```
******************   COMPLETED BMA MIGRATION STEP (1/2)  *************************
******************   STARTING BMA MIGRATION STEP (2/2)   *************************

Copying ipconfig files of Legacy BMA
Warning: Permanently added '10.193.47.218' (ED25519) to the list of known hosts.
Copying the version information from existing appliance...
Copying dhcpd.conf file from the existing BMA...
Copying provisioned image files from the existing BMA. This may take some time depending on the number
 of images provisioned d the network speed
Copying image templates from the existing BMA...
Copying osImagesRepository from the existing BMA...
Copying pxelinux configuration files from the existing BMA...
Copying bma-sw-rep folder and its softlinks  from existing BMA...
Copying image softlinks from existing BMA...
Copying windows  Win2k12R2x64 image...
Copying windows  Win2k12x64 image...
Copying windows  Win2k8R2x64 image...
Copying windows  Win2k16x64 image...
Copying windows  Win2k19x64 image...
Copying windows  Win2k22x64 image...
Copying as-repository folder...
Copying Boot folder for Windows PXE.
Copying web folder...
Validating Legacy hostname
Changing Hostname for BMA 10.193.47.219 from localhost.localdomain to localhost.localdomain
Changed Hostname Successfully
Hosts file updated successfully with localhost.localdomain

******************   COMPLETED BMA MIGRATION STEP (2/2)  *************************

Starting BMA services , after migration ..........
Completed the Baremetal Agent Migration process successfully.
Generated migration log file at /var/log/bmaMigrationLogs.txt
Migrated BMA successfully
Press return to continue:
```

Step 5 Press **Enter** to return to complete the process.

Offline Migration

Procedure

Step 1 Login to BMA 6.9.0.0 with root credentials.

Step 2 Navigate to the migration folder using the following command.

```
cd /opt/infra/migration and execute ./performBMAMigration.sh offline copyMigrationScript
********************************************************************************
****************************    BMA migration     ******************************
********************************************************************************
Current BMA Version : 6.9.0.0
```

Step 3 Specify the IP address and root password details of BMA 6.7.4.2 / 6.8.x.x appliance.

```
Enter Baremetal Agent 6.7.4.2/6.8.x.x appliance IP address : XX.XX.XX.XX
Enter root password for XX.XX.XX.XX :
```

```
Transfer AlmaLinux9 BMA migration script into a Remote mechine(XX.XX.XX.XX)
****************** STARTING BMA MIGRATION STEP (1/1) *************************

Move migration script files into XX.XX.XX.XX
file Moved successfully..
Transferred AlmaLinux9 BMA migration files successfully.

****************** COMPLETED BMA MIGRATION STEP (1/1) *************************
[root@localhost migration]#
```

Step 4 Login to BMA 6.7.4.2 / 6.8.x.x appliance with root credentials and execute the command below to backup the data.

```
[root@localhost migration]# ./performBMAMigration.sh offline backup
*******************************************************************************
****************************    BMA migration     *****************************
*******************************************************************************
Current BMA Version : 6.8.8.0
Required disk space : 2638 MB
Available free disk space : 82719 MB
Services will be stopped before migration starts. Do you want to continue [y/n]? y

******************   STARTING BMA MIGRATION STEP (1/2)   *************************

Stopping services..........
Capturing Source BMA IP Details
Copying the version information from existing appliance...
Copying dhcpd.conf file from source appliance
Copying provisioned image files from the existing BMA. This may take some time depending on the number
 of images provisioned d the network speed
..
Copying image templates from the existing BMA...
Copying osImagesRepository from the existing BMA...
Copying pxelinux configuration files from the existing BMA...
Copying bma-sw-rep folder from the existing BMA...
Copying image softlinks from existing BMA...
Copying windows images...
Copying Boot folder for Windows PXE.
Copying web folder...
Skipping Bigdata specific migration as the existing BMA doesn't have Bigdata files.
generating tar files...
.............................................................
Generated /opt/infra/migration/backup-bma/backup-bma.tar.gz file with the backup contents.

******************   COMPLETED BMA MIGRATION STEP (1/2)  *************************
******************   STARTING BMA MIGRATION STEP (2/2)   *************************

Do you want to copy BMA backup file to a remote location [y/n]? : y

Specify the Transfer mode [FTP/SFTP/SCP]: sftp

Specify the necessary login credentials

Server IP Address: 10.193.47.218
Server Login: root
Server Password:
Sub-directory (from Home directory) to store the file. Press enter to select the Home directory
itself: /tmp
File is copied successfully

******************   COMPLETED BMA MIGRATION STEP (2/2)  *************************
```

Step 5 Login into BMA 6.9.0.0 with root Credentials and navigate to **/opt/infra/migration** directory.

Step 6 Initiate restore operation using the following command.

```
[root@localhost migration]# ./performBMAMigration.sh offline restore
********************************************************************************
*****************************    BMA migration     *****************************
********************************************************************************
Current BMA Version : 6.9.0.0
Stopping BMA services , before Starting migration ..........

******************   STARTING BMA MIGRATION STEP (1/2)   **************************

Do you want to copy BMA backup file from a remote location [y/n]? : y
```

Step 7 Enter **y** and press **Enter**.

Step 8 Specify the transfer mode and press **Enter**.

```
Specify the Transfer mode [FTP/SFTP/SCP]: SFTP
```

Step 9 Specify the IP and login credentials, and press **Enter**.

The following output is displayed.

```
Specify the necessary login credentials

Server IP Address: XX.XX.XX.XX
Server Login: root
Server Password:
Remote Backup File (Absolute Path to File backup-bma.tar.gz ):
/opt/infra/migration/backup-bma/backup-bma.tar.gz

File is fetched successfully.

******************   COMPLETED BMA MIGRATION STEP (1/2)  **************************
******************   STARTING BMA MIGRATION STEP (2/2)   **************************

Extracting the backup archive file...
..........
Moving the version information from existing appliance
Moving resolv.conf file from source appliance
Moving dhcpd.conf file from source appliance
Updating Migration Properties File
Done Updating Migration Properties File
Moving provisioned image files from the existing BMA. This may take some time depending on the number
 of images provisioned and the network speed
Moving image templates from the existing BMA.
Moving osImagesRepository from the existing BMA...
Moving pxelinux configuration files from the existing BMA...
Moving bma-sw-rep folder from the existing BMA...
Moving image softlinks from existing BMA
Moving windows image.
Moving Boot folder for Windows PXE.
Moving web folder...
Skipping Bigdata specific migration as the existing BMA doesn't have Bigdata files.

******************   COMPLETED BMA MIGRATION STEP (2/2)  **************************

Starting BMA services , after migration ..........
Completed the Baremetal Agent Migration process successfully.
Generated migration log file at /var/log/bmaMigrationLogs.txt         ...
```

Viewing the Bare Metal Agent Migration Status

Procedure

From the Bare Metal Agent Shell menu, choose the **Migration Status** option and press **Enter**.

The following information displays:

```
Migration Status : Completed
Successfully completed the BMA migration.
Press return to continue:
```

Note The BMA migration status can be one of the following:

- Completed

  Note When the migration status is displayed as **Completed**, log in to Cisco UCS Director, Release 6.9 and choose **Administration > Physical Accounts** and click **Bare Metal Agent**. On the **Add Bare Metal Agent Appliance** screen, delete the BMA account (specific to version 6.7.4.2 / 6.8.x.x) and add the BMA account (migrated BMA, version 6.9.0.0) to Cisco UCS Director, Release 6.9.

- In Progress
- Failed
- Not Triggered

Setting Up UEFI as Network Boot Manager

The following are the list of operating system supported for UEFI booting:

- Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2022, and Windows Server 2025.
- ESXi 6.5, ESXi 6.7, and ESXi 8.0
- Centos 7.x and Centos 8.x
- RHEL 7.x and RHEL 9.x
- SLES 12 and above

For more information, see Cisco UCS Director Compatibility Matrix, Release 6.9.

Note RHEL 7.3 and Centos 7.3 installation are not supported for UEFI booting. OS kernels which are not compiled with EFI stub are also not supported.

Procedure

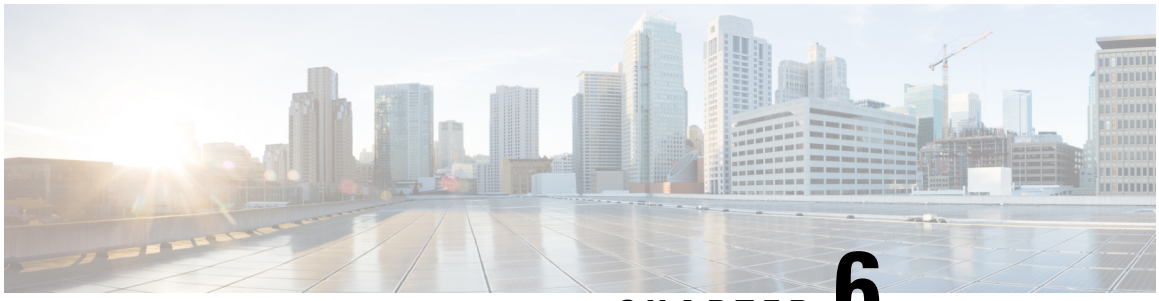
Step 1 Create a catalog from the Bare Metal Agent 6.9.

Note For Non-Windows operating system, provision the OS image from the Cisco UCS Director UI or run **isoExtractor.sh** available in `/opt/infra` folder. See Configuring Cisco UCS Director Bare Metal Agent, on page 13. However, for Windows operating system, ensure that `ipxe-uefi.cfg` and `autounattend-uefi.xml` files are available in the catalog.

Step 2 Choose **iPXE-UEFI** as the network boot manager. See, Provisioning OS Images through Orchestration Workflow Tasks, on page 115.

Note iPXE-UEFI supports TFTP protocol by default. However, you can modify the `ipxe-uefi.cfg` with the following details to support the HTTP protocol. HTTP protocol with UEFI does not work on all servers.

```
#!ipxe
initrd  http://$PXE_NATIVE_WEBSERVER/$PXE_OS/isolinux/initrd.img
kernel  http://$PXE_NATIVE_WEBSERVER/$PXE_OS/isolinux/vmlinuz initrd=initrd.img ks=$PXE_KS_URL
 net.ifnames=0 biosdevname=0
initrd  http://$PXE_NATIVE_WEBSERVER/$PXE_OS/isolinux/initrd.img
boot
```



CHAPTER 6

Adding Non-Windows OS Images

This chapter contains the following sections:

- Adding a Non-Windows OS Image in Bare Metal Agent, on page 47
- Non-Windows OS Provisioning through vMedia, on page 48
- Downloading Cisco UCS Storage Drivers, on page 48

Adding a Non-Windows OS Image in Bare Metal Agent

This procedure creates a Non-Windows OS image template in Bare Metal Agent. You must add the OS image template before you can request a PXE boot for the OS image.

Note You cannot use this procedure to create supported Windows operating systems images. For more information about how to set up Windows OS images, see Adding Windows OS Images, on page 51.

Before you begin

You must have all resources and requirements in place for each operating system image that you want to install through a Bare Metal Agent PXE boot request.

Procedure

Step 1 Upload the Non-Windows OS image file. For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Non-Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Navigate to `/opt/cnsaroot/templates/catalogname` and confirm that the PXE configuration templates are available in that location.

Step 4 To verify that the OS image is created, do the following:

a) In Cisco UCS Director, choose **Physical** > **Compute**.

b) In the left pane, navigate to the pod that contains the Bare Metal Agent.

c) In the right pane, click **PXE Boot Requests**.

d) Click **Add PXE Boot Request** and verify that the OS image is included in the **OS Type** drop-down list.

Non-Windows OS Provisioning through vMedia

The Cisco UCS Director allows non-windows OS deployment to be performed on the bare metal servers with the automation of vMedia as the vMedia support is enabled on the Bare Metal Agent. The ISO files are located in the Bare Metal Agent. During execution of a provisioning workflow, the vMedia is connected to a CD/DVD drive of the Dell, HP, and UCSM bare metal servers using the ISO file. The Cisco UCS Director supports deployment of the following OSs through the vMedia:

- ESXi
- RHEL

Each of the above OS can be deployed on the Dell, HP, and UCSM bare metal servers when the respective OS provisioning workflows are executed. Some prerequisites must be met before executing OS provisioning workflows. For more information, see prerequisites sections in Provisioning OS Images through Orchestration Workflow Tasks.

Downloading Cisco UCS Storage Drivers

We recommend you to download the relevant drivers using the UCS Hardware and Software Compatibility tool.

Procedure

Step 1 Go to UCS Hardware and Software Compatibility tool.

`https://ucshcltool.cloudapps.cisco.com/public/`

Step 2 Click **Search**.

Step 3 Click the required radio button. For example, click the **Server** radio button to identify the compatible software for the Cisco UCS server.

Step 4 On the **Search Options** section, choose the required **Server Type**, **Server Model**, **Processor Version**, **Operating System**, and **Operating System Version** from the drop-down menus.

Step 5 On the **Search Results** section, refine the search results by checking or unchecking checkboxes next to **Product Category** (Adapters) and **UCS Server Firmware** version number

Step 6 Click **Driver ISO** under **Details** section.



Note By clicking the **View Notes** and **Install & Upgrade Guides** links under **Documents**, you can view the note details and install and upgrade details.

Step 7 Download a compatible Driver ISO file from the **Software Download** window.

Step 8 Extract the Storage ISO files.



Note To extract the ISO files, navigate to `Storage > Intel > C600 > RHEL` or `Storage > LSI > C600 > RHEL` and choose the required OS. For example, `Storage > Intel > C600 > RHEL > RHEL8.0 > megasr-18.0*.iso` for M.2 servers.

Step 9 Login to Bare Metal Agent through VM Console or SSH client to access the CLI.

Step 10 Create the `/opt/cnsaroot/bma-sw-rep` directory.

Step 11 Create directories for the operating system in the `/opt/cnsaroot/bma-sw-rep` directory of the Bare Metal Agent VM.

mkdir /opt/cnsaroot/bma-sw-rep/*RHEL8.0_MEGASR_DRIVERS*



Note We recommend that you make the directory name descriptive enough that you can identify the operating system of the images within it. For example, we recommend that you name the directory `RHEL8.0_MEGASR_DRIVERS`, where RHEL8.0 is the catalog name used during OS provisioning.

Step 12 Navigate to **cd /opt/cnsaroot/bma-sw-rep/***RHEL8.0_MEGASR_DRIVERS* and copy the *RHEL8.0_MEGASR_DRIVERS* file to this location.

Step 13 Execute ln -s <<path of the original iso file>> <<target link name>> to provide links to the ISO images.

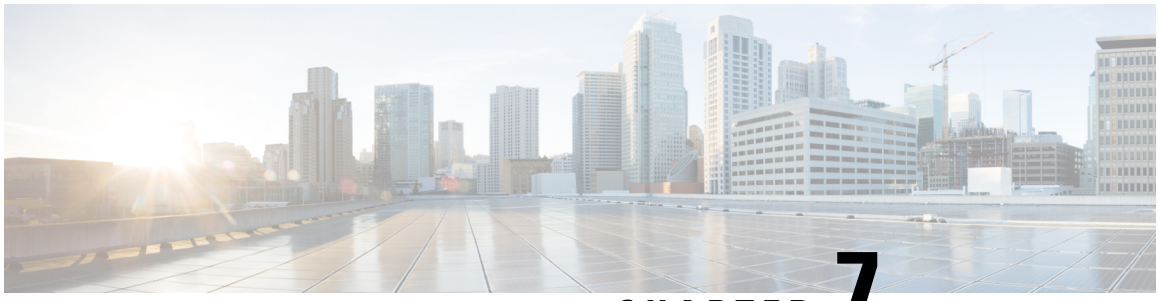
For example, ln -s /opt/cnsaroot/bma-sw-rep/RHEL8.0_MEGASR_DRIVERS/megasr-18.01.2019.0524-1-rhel8-x86_64.iso megasr_drivers_softlink_to_original.iso.



Note The links to the RHEL8.0_MEGASR_DRIVERS should refer to the iso files.



Note We recommend that you make the directory name based on the operating system used for the OS deployment. For example, CentOS7.5_MEGASR_DRIVERS directory is used to store the operating system driver image file. You use the same set of RHEL drivers for CentOS as well.



CHAPTER 7

Adding Windows OS Images

This chapter contains the following sections:

- Windows OS Provisioning through vMedia, on page 51
- Windows Operating Systems Supported for Cisco UCS Director Bare Metal Agent, on page 52
- Guidelines and Limitations for Windows Operating System Images, on page 52
- Windows Server 2008 R2 x64 Operating System Images, on page 53
- Windows Server 2012 x64 and 2012 R2 x64 Operating System Images, on page 63
- Windows Server 2016 x64 Operating System Images, on page 76
- Windows Server 2019 x64 Operating System Images, on page 84
- Windows Server 2022 x64 Operating System Images, on page 92
- Windows Server 2025 x64 Operating System Images, on page 100
- Using MEMDISK for Deploying Multiple Versions of Windows Simultaneously, on page 108
- Automating PXE-based Windows OS Deployment, on page 110

Windows OS Provisioning through vMedia

Note Starting with Cisco UCS Director 6.9(2.0), you can perform Windows Server 2022 OS deployment on bare metal servers.

The Cisco UCS Director allows Windows OS deployment through the automation of vMedia, enabling you to store ISO files on the Bare Metal Agent. During the execution of a Windows OS provisioning workflow, the vMedia is connected to the CD/DVD drive of Dell, HP, and UCSM bare metal servers using the ISO file, facilitating the Windows OS deployment.

Some prerequisites must be met before executing Windows OS provisioning workflows. For more information, see Provisioning OS Images through Orchestration Workflow Tasks.

Windows Operating Systems Supported for Cisco UCS Director Bare Metal Agent

Cisco UCS Director Bare Metal Agent (Bare Metal Agent) supports the following Windows operating system (OS) images and the automated creation of their required answer files:

- Windows Server 2008 R2 x64
- Windows Server 2012 x64
- Windows Server 2012 R2 x64
- Windows Server 2016 x64
- Windows Server 2019 x64
- Windows Server 2022 x64
- Windows Server 2025 x64

You can set up all OS images in Bare Metal Agent. You can use the same answer file for both local boot and SAN boot.

The procedure for setting up a Windows OS image depend upon the operating system. Make sure you use the appropriate procedure for the OS image that you are setting up.



Note After adding Bare Metal Agent to Cisco UCS Director and running inventory, Cisco UCS Director shows as if Windows images are added by default. But no Windows images are added. Install Windows images manually.

Guidelines and Limitations for Windows Operating System Images

Consider the following guidelines and limitations when you set up Windows Server OS images for provisioning:

Follow a Strict Naming Convention

You must follow a strict naming convention when you configure the files for Windows OS images. The paths and file names are case sensitive.



Note Mistakes in naming will require you to modify the names throughout the Bare Metal Agent data infrastructure.

Ensure That File Names, Drive Letters, and Other Information Match in All Files

If you use the automatically generated answer file, Bare Metal Agent ensures that the file names, drive letters and other information match.

However, if you manually edit the answer file, you must ensure that the drive letter in the `WinPE.wim` matches the drive letter provided in the answer file. With this configuration you are defining `WinPE.wim` such that it installs Windows from a particular location by using an answer file setup option. The static names, paths, IP addresses, drive letters, answer file name, and user name credentials must be correct.

File and folder names are case sensitive: `WinPE.wim` names must exactly match entries in the Boot Configuration Data (BCD) store.

Use Single Path Workflow for SAN Boot

Warning Because the Windows installation does not support multi-path SAN boot, you must use the single path workflow to achieve SAN boot.

Windows Server 2008 R2 x64 Operating System Images

The Windows Server 2008 R2 x64 OS (Windows 2008 OS) supports PXE boot and installation operations. You can use this OS image in bare metal provisioning workflows.

Prerequisites for Setting Up Windows Server 2008 R2 x64 Operating System Images

To install and set up the environment and files that are required for the setup of Windows Server 2008 R2 x64 OS images, you must first download the following:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK). See https://www.microsoft.com/en-us/download/details.aspx?id=30652. The Windows ADK enables you to generate a customized WinPE. Make sure Windows ADK is compatible with Windows Server 2008 R2 version.
- Windows Server 2008 R2 x64 ISO version.

Note You need not manually create a Windows answer file when setting up the Windows OS images. Bare Metal Agent builds the Windows answer file necessary to support your PXE Boot request, based on the information you provide when you create the PXE boot request.

Before installing the Windows 2008 R2 operating system using the Bare Metal Agent VM, set up and configure the following prerequisites:

- A customized Windows Pre-installation Environment (WinPE)
- Boot Configuration Data (BCD) file (optional)
- Windows installation files (the files extracted from the ISO image file)

Tip We recommend that you use the Windows 2008 R2 OS ISO image file, which contains all editions, including Standard, Enterprise, Datacenter, and Web. You can typically remove all editions except for Standard and Datacenter.

After customizing the WinPE image and creating the BCD file, you must do the following:

- Set up WinPE and copy the supporting files to the Bare Metal Agent VM for the PXE boot.
- Extract the Windows 2008 R2 OS ISO image files into the appropriate image repository directory.

Creating a Customized WinPE

You need to create and customize the Windows Preinstallation Environment (WinPE) for Windows 2008 R2 x64. The initial WinPE includes the minimum boot image necessary to load kernel and default device drivers supported by the Windows OS. Most servers require additional drivers, such as network interface cards and storage controllers that enable Windows OS to detect the network and disks during installation. You must add these drivers to the WinPE.wim image.

Add the device drivers to the WinPE image by using the Deployment Image Servicing and Management (DISM.exe) command tool, which is installed with the Windows ADK. Make sure that you download the required device drivers before you execute the associated DISM commands.

Important The following procedure includes a sample configuration that is for reference only. The sample configuration might or might not work in your environment. For information about adding device drivers to the WinPE image through DISM.exe, see the documentation provided by Microsoft.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2008 R2 x64 Operating System Images, on page 53.

Download the following:

- Windows Assessment and Deployment Kit (Windows ADK) specifically for Windows 2008 R2 x64.
- Required device drivers to be added to the `WinPE.wim` image.

Procedure

Step 1 Launch the command prompt (click **Start** > **All Programs** > **Accessories** > **Command Prompt**).

Step 2 Change the directory to Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment
```

Here, `C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation Environment` is the directory where Windows ADK has been installed.

Step 3 Create a new WinPE environment folder using 'copype.cmd' command.

```
copype.cmd amd64 c:\win2k8r2x64
```

Here, `c:\win2k8r2x64` is the directory where the new WinPE environment is created.

Step 4 Extract the device drivers to a folder. For example, `c:\cisco\drivers`.

Step 5 Add the device drivers to the WinPE image by using the DISM.exe command.

- Mount the WinPE.wim image:

```
DISM.exe /mount-wim /wimfile:c:\win2k8r2x64\WinPE.wim /index:1 mountdir:c:\win2k8r2x64\mount
```

- Add the device drivers to WinPE.wim image by using the individual driver's absolute path:

```
DISM.exe /image:c:\win2k8r2x64\mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

- Alternatively, add the device drivers to the WinPE.wim image by automatically searching through all the subfolders of the device drivers directory:

```
DISM.exe /image:c:\win2k8r2x64\mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 6 Unmount the WinPE.wim image and commit the changes:

```
DISM.exe /unmount-wim /mountdir:c:\win2k8r2x64\mount /commit
```

When all the device drivers have been added, the WinPE.wim image is ready to be used.

Preparing Windows Server 2008 R2 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2008 R2 operating system
- Windows 2008 R2 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2008 R2 ISO image installation files to the folder.

```
mkdir c:\win2k8r2x64-iso
```

Step 3 Take a backup copy of the install.wim file.

```
cd c:\win2k8r2x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2008 R2 operating system.

Step 4 Create a folder to mount the `c:\win2k8r2x64-iso\sources\install.wim` file.

```
mkdir c:\win2k8r2x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 Add the device drivers to the install.wim image by using the DISM.exe command from the Windows ADK installation directory.

Step 7 List the supported Windows 2008 R2 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k8r2x64-iso\sources\install.wim
```

The supported Windows 2008 R2 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2008 R2 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2008 R2 SERVERSTANDARD
Description : Windows Server 2008 R2 SERVERSTANDARD
Size : 10,510,509,480 bytes

Index : 2
Name : Windows Server 2008 R2 SERVERSTANDARDCORE
Description : Windows Server 2008 R2 SERVERSTANDARDCORE
Size : 3,563,998,339 bytes

Index : 3
Name : Windows Server 2008 R2 SERVERENTERPRISE
Description : Windows Server 2008 R2 SERVERENTERPRISE
Size : 10,510,890,698 bytes

Index : 4
Name : Windows Server 2008 R2 SERVERENTERPRISECORE
Description : Windows Server 2008 R2 SERVERENTERPRISECORE
Size : 3,563,972,455 bytes

Index : 5
Name : Windows Server 2008 R2 SERVERDATACENTER
Description : Windows Server 2008 R2 SERVERDATACENTER
Size : 10,510,997,874 bytes

Index : 6
Name : Windows Server 2008 R2 SERVERDATACENTERCORE
Description : Windows Server 2008 R2 SERVERDATACENTERCORE
Size : 3,564,010,572 bytes

Index : 7
Name : Windows Server 2008 R2 SERVERWEB
Description : Windows Server 2008 R2 SERVERWEB
Size : 10,520,088,768 bytes

Index : 8
Name : Windows Server 2008 R2 SERVERWEBCORE
```

```
Description : Windows Server 2008 R2 SERVERWEBCORE
Size : 3,562,616,654 bytes
```

Step 8 Mount the install.wim image with Index ID 5 to install Windows 2008 R2 Datacenter Edition.

```
DISM.exe /mount-wim /wimfile:c:\win2k8r2x64-iso\sources\install.wim /index:5
mountdir:c:\win2k8r2x64-mount
```

Step 9 Add device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k8r2x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k8r2x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the install.wim image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k8r2x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Creating a Boot Configuration Data File

The Boot Configuration Data (BCD) file contains the boot configuration parameters. It controls how the operating system is started in Windows and is used to load the base kernel (WinPE.wim) from the PXE server. Creating a new BCD file is optional. The Bare Metal Agent provides a BCD file with default configuration out of the box. The absolute location path of the BCD file is `/opt/cnsaroot/Boot/BCD`. The default BCD file can be used to install any Windows OS version, unless it is required to be customized for a specific version of Windows.

By default, the BCD file points to `/opt/cnsaroot/Boot/WinPE.wim` and `/opt/cnsaroot/Boot/boot.sdi` files. These filenames are case sensitive.

The new BCD file can be created through the BCDEdit command-line tool. This tool is commonly available in the Windows operating system under root directory, `C:\Windows\system32`.

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new working directory to create a new BCD file. (At the command prompt, type `C:\> mkdir C:\NewBCDStore`)

Step 3 Change the directory to `C:\NewBCDStore`. (At the command prompt, type `C:\> cd C:\NewBCDStore`)

Step 4 Run the below sequence of commands to create a new BCD file:

```
C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /createstore BCD

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /create {ramdiskoptions} /d "Ramdisk
options"

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdidevice
boot

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdipath
\Boot\boot.sdi

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /create /d "My WinPE Boot Image" /application
 osloader
```

Running the above command generates and displays a new GUID as the command output.

Step 5 Run the following commands. When you run these commands, replace the GUID (for example: *{a20f8db8-7459-11e2-8ec3-00155d37efa7}*) with the GUID generated from your system:

```
C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {a20f8db8-7459-11e2-8ec3-00155d37efa7}
 systemroot \Windows

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {a20f8db8-7459-11e2-8ec3-00155d37efa7}
 detecthal Yes

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {a20f8db8-7459-11e2-8ec3-00155d37efa7}
 winpe Yes

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {a20f8db8-7459-11e2-8ec3-00155d37efa7}
 osdevice ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {a20f8db8-7459-11e2-8ec3-00155d37efa7}
 device ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2008r2
BootManager"

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /set {bootmgr} timeout 30

C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /displayorder
{a20f8db8-7459-11e2-8ec3-00155d37efa7}
```

Use the following command to verify that the configurations are correct:

```
C:\NewBCDStore> C:\Windows\System32\bcdedit.exe /store BCD /enum all
```

What to do next

Verify that you have appropriate Windows 2008 R2 OS installation files inside the ISO image.

Verifying the Installation files For All Editions of Windows 2008 R2

Before you begin

Mount or extract the Windows 2008 R2 ISO image.

Procedure

Verify that you have the following CLG files under the SOURCE folder of mounted or extracted Windows 2008 R2 ISO image:

- install_Windows Server 2008 R2 SERVERDATACENTER.clg
- install_Windows Server 2008 R2 SERVERDATACENTERCORE.clg
- install_Windows Server 2008 R2 SERVERENTERPRISE.clg
- install_Windows Server 2008 R2 SERVERENTERPRISECORE.clg
- install_Windows Server 2008 R2 SERVERSTANDARD.clg
- install_Windows Server 2008 R2 SERVERSTANDARDCORE.clg
- install_Windows Server 2008 R2 SERVERDATAWEB.clg
- install_Windows Server 2008 R2 SERVERDATAWEBCORE.clg

What to do next

Edit the WinPE.wim image file to add PowerShell packages and modify the startnet.cmd file with PXE install commands and parameters as described in Customizing and Copying the WinPE.wim and PXE Boot Files for Windows 2008 R2, on page 59.

Customizing and Copying the WinPE.wim and PXE Boot Files for Windows 2008 R2

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Change the directory to WinPE environment that was created.

```
cd c:\win2k8r2x64
```

Step 3 Mount WinPE.wim image to a folder called 'mount' under the `c:\win2k8r2x64` directory.

```
DISM.exe /mount-wim /wimfile:c:\win2k8r2x64\WinPE.wim /index:1 /mountdir:c:\win2k8r2x64\mount
```

Step 4 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.

Note The Powershell package files shown below are provided for your reference only. The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent upon the version of Windows and `WinPE.wim`.To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page.

```
Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k8r2x64\mount" /PackagePath:"C:\Program Files (x86)\Windows
Kits\8.0\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 5 Navigate to the mount folder (`c:\win2k8r2x64\mount` in the code example above) and verify that you can see the data inside the mount folder.

Step 6 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the IP address and other details as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:user_id password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```



Note

- Use the drvload command when a driver has failed to be installed. For example, include the following line in the `startnet.cmd` file to install a fnic driver:

  ```
  drvload <ipaddress of share>:\\<the_fnic.inf>
  ```

  Use the drvload command only when you face issues in installing drivers. Otherwise, follow the standard process to inject a driver to WinPE.

- Make sure that you modify the IP address in all the entries so that they point to the Bare Metal Agent IP address.

- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 7 Save the `startnet.cmd` file.

Step 8 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k8r2x64\mount /commit
```



Caution Do not leave any files open that are located in the mounted directory when you unmount `WinPE.wim`. If you have any files open, the unmount process might fail.

What to do next

Copy the customized Windows installation files to the Bare Metal Agent VM.

Copying the Customized Windows Installation Files to the Bare Metal Agent VM

Before you begin

You must have the following in place:

- Customized WinPE.wim image file
- Customized install.wim image file
- Customized BCD file (optional)
- Windows 2008 R2 ISO image

Procedure

Step 1 Upload the Windows OS image file, customized WinPE.wim file, and customized BCD file (optional). For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Customize install.wim image file from `c:\win2k8r2x64-iso\sources` to `/tmp` folder.

Step 4 Move the install.wim image file from `/tmp` to `/samba/Win2k8R2x64/sources` folder.

```
mv /tmp/install.wim /samba/Win2k8R2x64/sources/
```

Step 5 Open the `/samba/notifications/notify.ps1` file and verify that the IP address in the file matches that of the PXE IP address of Bare Metal Agent.

Note Do not change the folder paths, filenames, or folder names.

The following is a sample of the contents of a `Win2k8R2x64` folder:

```
boot
efi
sources
support
autorun.inf
bootmgr.efi
setup.exe
```

Windows Server 2012 x64 and 2012 R2 x64 Operating System Images

Cisco UCS Director Bare Metal Agent supports PXE boot and installation operations for Windows 2012 x64 or 2012 R2 x64 OS images and PXE boot tasks used in bare metal provisioning workflows.

Note If you need to support both Windows 2012 and 2012 R2, you must perform the image setup process twice, once for each OS. Although it is possible to set up a single WinPE file that supports multiple Windows OS versions, we recommend that you set up a separate `WinPE` file for each OS.

Prerequisites for Setting Up Windows Server 2012 x64 and 2012 R2 x64 Operating System Images

Before you can install a Windows 2012 or 2012 R2 OS image in the `/opt/cnsaroot/Boot` directory of the Bare Metal Agent VM, you must install and set up the following prerequisites:

- Windows Assessment and Deployment Kit (Windows ADK, version 8.0 or later recommended, depending on the Windows version compatibilities with respect to the `WinPE.wim` file)
- A customized Windows Preinstallation Environment (`WinPE.wim`) and PXE supporting files
- Boot Configuration Data (BCD) file
- Windows installation files (the files extracted from the ISO)

Note You do not need to manually create a Windows answer file when setting up Windows OS images. Bare Metal Agent builds the Windows answer file necessary to support your PXE Boot request, based on the information you provide when you create the PXE boot request.

To install and set up the images, download the following:

- Windows Assessment and Deployment Kit that supports Windows Server 2012 and Windows Server 2012 R2. For more information, see http://technet.microsoft.com/en-us/library/dn613859.aspx.
- Windows Server 2012 x64 and/or 2012 R2 x64 (Standard and Datacenter editions are required).

Tip We recommend that you use the ISO download file, which contains all editions, including Standard, Enterprise, Datacenter, and Web. You can typically remove all editions except for Standard and Datacenter.

After the system image is in place, perform the following additional procedures:

- Set up WinPE and copy the supporting files to the Network Service Agent server for the PXE boot.

- Copy the Windows installation files to the server path.

Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2012

Note The `/opt/cnsaroot/Boot` folder is static, and each Bare Metal Agent can have only one boot folder.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2012 x64 and 2012 R2 x64 Operating System Images, on page 63.

Procedure

Step 1 Download an ADK version that supports Windows 2012 and install it on a Windows 2012 machine.

Note When you specify the features to include in the download, you must include the Windows PE and Deployment Tools.

Step 2 Navigate to the Windows Pre-installation Environment folder in the ADK tools and execute **copype.cmd** to create the files that WinPE requires.

```
Copype.cmd amd64 C:\WinPE_amd64
```

The target directory contains the `WinPE.wim` file. The latest ADK versions create a `boot.wim` file, which needs to be renamed to `WinPE.wim`.

Step 3 In the Windows machine that has the ADK tools installed, create a directory. Copy the `WinPE.wim` file from `/opt/cnsaroot/Boot` to the directory you have created.

Step 4 At the command line, navigate to the ADK installed folder.

Step 5 Add the drivers from their folder locations to the WinPE image.

Use the following `DISM.exe` command when you know the paths to the drivers that you want to add.

```
// The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k12x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k12x64\WinPE.wim /index:1 /mountdir:c:\win2k12x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k12x64\mount /Add-Driver /driver:C:\test\drivers\1.inf
/driver:C:\test\drivers\2.inf /driver:C:\test\drivers\3.inf
```

Use the following `DISM.exe` command when you do not know the paths to the drivers that you want to add and need to query all subfolders.

```
 // The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k12x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k12x64\WinPE.wim /index:1 /mountdir:c:\win2k12x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k12x64\mount /Add-Driver /driver:c:\test\drivers /Recurse
```

Step 6 Mount `WinPE.wim` to a folder.

Step 7 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.



Note The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent upon the version of Windows and `WinPE.wim`.To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page. The PowerShell package files shown below are provided for reference and will vary depending on the version of Windows and WinPE.wim.

```
\\ Sample PowerShell package files.
\\ The PowerShell packages and file names that you need to add to WinPE.wim vary depending on the
version of Windows and WinPE.wim.

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
```

```
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k12x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 8 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the password for samba service and the PXE interface IP address for Bare Metal Agent as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:smbuser password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```

Note

- Do not change any information in the `startnet.cmd` file, except for the password for samba service and the PXE interface IP address of the Bare Metal Agent.
- Make sure that you modify the IP addresses in all the entries so that they point to the Bare Metal Agent IP address.
- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 9 Save the `startnet.cmd` file.

Step 10 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k12x64\mount /commit
```

What to do next

Install and set up (as necessary) the Boot Configuration Data (BCD) file.

Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2012 R2

For Windows Server 2012 R2 x64, Bare Metal Agent provides the WinPE and supported PXE files. You need only add any required drivers to the `WinPE.wim` file, and then edit the `WinPE.wim` file to change the IP address in the `startnet.cmd` file to the PXE IP address for your Bare Metal Agent.

Note The `/opt/cnsaroot/Boot` folder is static, and each Bare Metal Agent can have only one boot folder.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2012 x64 and 2012 R2 x64 Operating System Images, on page 63.

Procedure

Step 1 Download an ADK version that supports Windows 2012 R2 and install it on a Windows 2012 R2 machine.

Note When you specify the features to include in the download, you must include the Windows PE and Deployment Tools.

Step 2 In the Windows machine that has the ADK tools installed, create a directory. Copy the `WinPE.wim` file from `/opt/cnsaroot/Boot` to the directory you created.

Step 3 At the command line, navigate to the ADK installed folder.

Step 4 Add the drivers from their folder locations to the WinPE image.

Use the following `DISM.exe` command when you know the paths to the drivers that you want to add.

```
// The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k12r2x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k12r2x64\WinPE.wim /index:1 /mountdir:c:\win2k12r2x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k12r2x64\mount /Add-Driver /driver:C:\test\drivers\1.inf
/driver:C:\test\drivers\2.inf /driver:C:\test\drivers\3.inf
```

Use the following `DISM.exe` command when you do not know the paths to the drivers that you want to add and need to query all subfolders.

```
 // The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k12r2x64 directory and the \mount subdirectory have been created before
```

```
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k12r2x64\WinPE.wim /index:1 /mountdir:c:\win2k12r2x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k12r2x64\mount /Add-Driver /driver:c:\test\drivers /Recurse
```

Step 5 Mount `winPE.wim` to a folder.

Step 6 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.



Note The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent on the version of Windows and `WinPE.wim`. To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page. The PowerShell package files shown below are provided for reference and will vary depending on the version of Windows and WinPE.wim.

```
\\ Sample PowerShell package files.
\\ The PowerShell packages and file names that you need to add to WinPE.wim vary depending on the
version of Windows and WinPE.wim.

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
```

```
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k12r2x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\8.1\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 7 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the password for samba service and the PXE interface IP address for Bare Metal Agent as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:smbuser password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```

Note

- Do not change any information in the `startnet.cmd` file, except for the password for samba service and the PXE interface IP address of the Bare Metal Agent.
- Make sure that you modify the IP addresses in all the entries so that they point to the Bare Metal Agent IP address.
- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 8 Save the `startnet.cmd` file.

Step 9 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k12r2x64\mount /commit
```

What to do next

Install and set up (as necessary) the Boot Configuration Data (BCD) file.

Preparing Windows Server 2012 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2012 operating system
- Windows 2012 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2012 ISO image installation files to the folder.

```
mkdir c:\win2k12x64-iso
```

Step 3 Take a backup copy of the install.wim file.

```
cd c:\win2k12x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2012 operating system.

Step 4 Create a folder to mount the `c:\win2k12x64-iso\sources\install.wim` file.

```
mkdir c:\win2k12x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 Add the device drivers to the install.wim image by using the DISM.exe command from the Windows ADK installation directory.

Step 7 List the supported Windows 2012 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k12x64-iso\sources\install.wim
```

The supported Windows 2012 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2012 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2012 SERVERSTANDARD
Description : Windows Server 2012 SERVERSTANDARD
Size : 10,510,509,480 bytes

Index : 2
Name : Windows Server 2012 SERVERSTANDARDCORE
Description : Windows Server 2012 SERVERSTANDARDCORE
Size : 3,563,998,339 bytes

Index : 3
```

```
Name : Windows Server 2012 SERVERENTERPRISE
Description : Windows Server 2012 SERVERENTERPRISE
Size : 10,510,890,698 bytes

Index : 4
Name : Windows Server 2012 SERVERENTERPRISECORE
Description : Windows Server 2012 SERVERENTERPRISECORE
Size : 3,563,972,455 bytes

Index : 5
Name : Windows Server 2012 SERVERDATACENTER
Description : Windows Server 2012 SERVERDATACENTER
Size : 10,510,997,874 bytes

Index : 6
Name : Windows Server 2012 SERVERDATACENTERCORE
Description : Windows Server 2012 SERVERDATACENTERCORE
Size : 3,564,010,572 bytes

Index : 7
Name : Windows Server 2012 SERVERWEB
Description : Windows Server 2012 SERVERWEB
Size : 10,520,088,768 bytes

Index : 8
Name : Windows Server 2012 SERVERWEBCORE
Description : Windows Server 2012 SERVERWEBCORE
Size : 3,562,616,654 bytes
```

Step 8 Mount the install.wim image with Index ID 5 to install Windows 2012 Datacenter Edition.

```
DISM.exe /mount-wim /wimfile:c:\win2k12x64-iso\sources\install.wim /index:5
mountdir:c:\win2k12x64-mount
```

Step 9 Add device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k12x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k12x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the install.wim image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k12x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Preparing Windows Server 2012 R2 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2012 R2 operating system
- Windows 2012 R2 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2012 R2 ISO image installation files to the folder.

```
mkdir c:\win2k12r2x64-iso
```

Step 3 Take a backup copy of the install.wim file.

```
cd c:\win2k12r2x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2012 R2 operating system.

Step 4 Create a folder to mount the `c:\win2k12r2x64-iso\sources\install.wim` file.

```
mkdir c:\win2k12r2x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\8.0\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 Add the device drivers to the install.wim image by using the DISM.exe command from the Windows ADK installation directory.

Step 7 List the supported Windows 2012 R2 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k12r2x64-iso\sources\install.wim
```

The supported Windows 2012 R2 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2012 R2 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2012 R2 SERVERSTANDARD
Description : Windows Server 2012 R2 SERVERSTANDARD
Size : 10,510,509,480 bytes

Index : 2
Name : Windows Server 2012 R2 SERVERSTANDARDCORE
Description : Windows Server 2012 R2 SERVERSTANDARDCORE
Size : 3,563,998,339 bytes

Index : 3
```

```
Name : Windows Server 2012 R2 SERVERENTERPRISE
Description : Windows Server 2012 R2 SERVERENTERPRISE
Size : 10,510,890,698 bytes

Index : 4
Name : Windows Server 2012 R2 SERVERENTERPRISECORE
Description : Windows Server 2012 R2 SERVERENTERPRISECORE
Size : 3,563,972,455 bytes

Index : 5
Name : Windows Server 2012 R2 SERVERDATACENTER
Description : Windows Server 2012 R2 SERVERDATACENTER
Size : 10,510,997,874 bytes

Index : 6
Name : Windows Server 2012 R2 SERVERDATACENTERCORE
Description : Windows Server 2012 R2 SERVERDATACENTERCORE
Size : 3,564,010,572 bytes

Index : 7
Name : Windows Server 2012 R2 SERVERWEB
Description : Windows Server 2012 R2 SERVERWEB
Size : 10,520,088,768 bytes

Index : 8
Name : Windows Server 2012 R2 SERVERWEBCORE
Description : Windows Server 2012 R2 SERVERWEBCORE
Size : 3,562,616,654 bytes
```

Step 8 Mount the install.wim image with Index ID 5 to install Windows 2012 R2 Datacenter Edition.

```
DISM.exe /mount-wim /wimfile:c:\win2k12r2x64-iso\sources\install.wim /index:5
mountdir:c:\win2k12r2x64-mount
```

Step 9 Add device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k12r2x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k12r2x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the install.wim image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k12r2x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Installing and Setting Up the Boot Configuration Data File

The Boot Configuration Data (BCD) file contains the boot configuration parameters. It controls how the operating system is started in Windows and is used to load the base kernel (WinPE.wim) from the PXE server. You do not need to create a BCD file. Bare Metal Agent provides a BCD file with default paths that you can use.

By default, the BCD file points to the `/Boot/WinPE.wim` and `boot.sdi` files. These filenames are case sensitive.



Note We recommend that you use a set of standard names for Bare Metal Agent configuration purposes. The folder name should be Boot. The winpe file name should be WinPE.wim. Use corresponding filenames such as boot.sdi. The created BCD file should be in uppercase, and this file will not have any file extension. Bare Metal Agent delivers the BCD file to `/opt/cnsaroot/Boot`, which contains a default path pointing to `/opt/cnsaroot/Boot/WinPE.wim`. This file can be used by any Windows OS version, unless you change the path names.

The command **bcdedit.exe** used to create BCD files is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Before you begin

Create a custom WinPE and copy the PXE supported files

Procedure

Step 1 Navigate to the directory that contains the **bcdedit.exe** command and run the following sequence of commands to create the BCD file.

The **bcdedit.exe** command is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Step 2 **bcdedit.exe /createstore BCD**

Step 3 **bcdedit.exe /store BCD /create {ramdiskoptions} /d "Ramdisk options"**

Step 4 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdidevice boot**

Step 5 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdipath \Boot\boot.sdi**

Step 6 **bcdedit.exe /store BCD /create /d** *"My WinPE Boot Image"* **/application osloader**

At this point, the GUID is displayed. Replace *`{a20f8db8-7459-11e2-8ec3-00155d37efa7}`* in the following steps with the GUID from your system.

Step 7 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **systemroot \Windows**

Step 8 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **detecthal Yes**

Step 9 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **winpe Yes**

Step 10 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **osdevice ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 11 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **device ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 12 One of the following:

- **bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2012r2 BootManager"**
- **bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2012 BootManager"**

Step 13 **bcdedit.exe /store BCD /set {bootmgr} timeout 30**

Step 14 **bcdedit.exe /store BCD /displayorder** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}*

Step 15 Use the following command to verify that the configuration names are correct: **bcdedit.exe /store BCD /enum all**

What to do next

Copy the Windows installation ISO image to the server folder.

Copying the Windows Installation Files to the Server Folder

Before you begin

You must have the following in place:

- Customized `winPE.wim` and PXE boot files in the `opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Configured BCD file in the `/opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Windows installation files (ISO version).

Procedure

Step 1 Upload the Windows OS image file, customized WinPE.wim file, and customized BCD file (optional). For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Customize install.wim image file from:

- `c:\Win2k12R2x64-iso\sources` (for Windows 2012 R2) to `/tmp` folder
- `c:\Win2k12x64-iso\sources` (for Windows 2012) to `/tmp` folder

Step 4 Move the install.wim image file from `/tmp` to:

- `/samba/Win2k12R2x64/sources` folder (for Windows 2012 R2)
- `/samba/Win2k12x64/sources` folder (for Windows 2012).

Following is the sample content.

```
mv /tmp/install.wim /samba/Win2k12R2x64/sources/
mv /tmp/install.wim /samba/Win2k12x64/sources/
```

Step 5 Open the `/samba/notifications/notify.ps1` file and verify that the IP address matches the PXE IP address of Bare Metal Agent.

Note Do not change the folder paths, filenames, or folder names.

The following is a sample of the contents of a `Win2k12x64` folder:

```
boot
efi
sources
support
autorun.inf
bootmgr.efi
setup.exe
```

Windows Server 2016 x64 Operating System Images

Cisco UCS Director Bare Metal Agent supports PXE boot and installation operations for Windows 2016 x64 OS images and PXE boot tasks used in bare metal provisioning workflows.

Prerequisites for Setting Up Windows Server 2016 x64 Operating System Images

Before you can install a Windows 2016 OS image in the `/opt/cnsaroot/Boot` directory of the Bare Metal Agent VM, you must install and set up the following prerequisites:

- Windows Assessment and Deployment Kit (Windows ADK, version 8.0 or later recommended, depending on the Windows version compatibilities with respect to the `WinPE.wim` file)
- A customized Windows Preinstallation Environment (`WinPE.wim`) and PXE supporting files
- Boot Configuration Data (BCD) file
- Windows installation files (the files extracted from the ISO)

Note You do not need to manually create a Windows answer file when setting up Windows OS images. Bare Metal Agent builds the Windows answer file necessary to support your PXE Boot request, based on the information you provide when you create the PXE boot request.

To install and set up the images, download the following:

- Windows Assessment and Deployment Kit that supports Windows Server 2016. For more information, see http://technet.microsoft.com/en-us/library/dn613859.aspx.
- Windows Server 2016 x64.

Tip We recommend that you use the ISO download file, which contains all editions, including Standard, Enterprise, Datacenter, and Web. You can typically remove all editions except for Standard and Datacenter.

After the system image is in place, perform the following additional procedures:

- Set up WinPE and copy the supporting files to the Network Service Agent server for the PXE boot.
- Copy the Windows installation files to the server path.

Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2016

Note The `/opt/cnsaroot/Boot` folder is static, and each Bare Metal Agent can have only one boot folder.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2016 x64 Operating System Images, on page 76.

Procedure

Step 1 Download an ADK version that supports Windows 2016 and install it on a Windows 2016 machine.

Note When you specify the features to include in the download, you must include the Windows PE and Deployment Tools.

Step 2 Navigate to the Windows Pre-installation Environment folder in the ADK tools and execute **copype.cmd** to create the files that WinPE requires.

```
Copype.cmd amd64 C:\WinPE_amd64
```

The target directory contains the `WinPE.wim` file. The latest ADK versions create a `boot.wim` file, which needs to be renamed to `WinPE.wim`.

Step 3 In the Windows machine that has the ADK tools installed, create a directory. Copy the `WinPE.wim` file from `/opt/cnsaroot/Boot` to the directory you have created.

Step 4 At the command line, navigate to the ADK installed folder.

Step 5 Add the drivers from their folder locations to the WinPE image.

Use the following `DISM.exe` command when you know the paths to the drivers that you want to add.

```
// The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k16x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k16x64\WinPE.wim /index:1 /mountdir:c:\win2k16x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k16x64\mount /Add-Driver /driver:C:\test\drivers\1.inf
/driver:C:\test\drivers\2.inf /driver:C:\test\drivers\3.inf
```

Use the following `DISM.exe` command when you do not know the paths to the drivers that you want to add and need to query all subfolders.

```
 // The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k16x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k16x64\WinPE.wim /index:1 /mountdir:c:\win2k16x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k16x64\mount /Add-Driver /driver:c:\test\drivers /Recurse
```

Step 6 Mount `WinPE.wim` to a folder.

Step 7 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.

Note The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent upon the version of Windows and `WinPE.wim`.To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page. The PowerShell package files shown below are provided for reference and will vary depending on the version of Windows and WinPE.wim.

```
\\ Sample PowerShell package files.
\\ The PowerShell packages and file names that you need to add to WinPE.wim vary depending on the
version of Windows and WinPE.wim.

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"
```

```
Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k16x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 8 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the password for samba service and the PXE interface IP address for Bare Metal Agent as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:smbuser password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```



Note

- Do not change any information in the `startnet.cmd` file, except for the password for samba service and the PXE interface IP address of the Bare Metal Agent.
- Make sure that you modify the IP addresses in all the entries so that they point to the Bare Metal Agent IP address.
- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 9 Save the `startnet.cmd` file.

Step 10 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k16x64\mount /commit
```

What to do next

Install and set up (as necessary) the Boot Configuration Data (BCD) file.

Preparing Windows Server 2016 R2 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2016 R2 operating system
- Windows 2016 R2 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2016 R2 ISO image installation files to the folder.

```
mkdir c:\win2k16r2x64-iso
```

Step 3 Take a backup copy of the install.wim file.

```
cd c:\win2k16r2x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2016 R2 operating system.

Step 4 Create a folder to mount the `c:\win2k16r2x64-iso\sources\install.wim` file.

```
mkdir c:\win2k16r2x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 Add the device drivers to the install.wim image by using the DISM.exe command from the Windows ADK installation directory.

Step 7 List the supported Windows 2016 R2 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k16r2x64-iso\sources\install.wim
```

The supported Windows 2016 R2 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2016 R2 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2016 R2 SERVERSTANDARD
Description : Windows Server 2016 R2 SERVERSTANDARD
Size : 10,510,509,480 bytes

Index : 2
Name : Windows Server 2016 R2 SERVERSTANDARDCORE
Description : Windows Server 2016 R2 SERVERSTANDARDCORE
Size : 3,563,998,339 bytes

Index : 3
Name : Windows Server 2016 R2 SERVERENTERPRISE
Description : Windows Server 2016 R2 SERVERENTERPRISE
Size : 10,510,890,698 bytes

Index : 4
Name : Windows Server 2016 R2 SERVERENTERPRISECORE
Description : Windows Server 2016 R2 SERVERENTERPRISECORE
Size : 3,563,972,455 bytes

Index : 5
Name : Windows Server 2016 R2 SERVERDATACENTER
Description : Windows Server 2016 R2 SERVERDATACENTER
Size : 10,510,997,874 bytes

Index : 6
Name : Windows Server 2016 R2 SERVERDATACENTERCORE
Description : Windows Server 2016 R2 SERVERDATACENTERCORE
Size : 3,564,010,572 bytes

Index : 7
Name : Windows Server 2016 R2 SERVERWEB
Description : Windows Server 2016 R2 SERVERWEB
Size : 10,520,088,768 bytes

Index : 8
Name : Windows Server 2016 R2 SERVERWEBCORE
Description : Windows Server 2016 R2 SERVERWEBCORE
Size : 3,562,616,654 bytes
```

Step 8 Mount the install.wim image with Index ID 5 to install Windows 2016 R2 Datacenter Edition.

```
DISM.exe /mount-wim /wimfile:c:\win2k16r2x64-iso\sources\install.wim /index:5
mountdir:c:\win2k16r2x64-mount
```

Step 9 Add device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k16r2x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k16r2x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the install.wim image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k16r2x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Installing and Setting Up the Boot Configuration Data File

The Boot Configuration Data (BCD) file contains the boot configuration parameters. It controls how the operating system is started in Windows and is used to load the base kernel (WinPE.wim) from the PXE server. You do not need to create a BCD file. Bare Metal Agent provides a BCD file with default paths that you can use.

By default, the BCD file points to the `/Boot/WinPE.wim` and `boot.sdi` files. These filenames are case sensitive.

Note We recommend that you use a set of standard names for Bare Metal Agent configuration purposes. The folder name should be Boot. The winpe file name should be WinPE.wim. Use corresponding filenames such as boot.sdi. The created BCD file should be in uppercase, and this file will not have any file extension. Bare Metal Agent delivers the BCD file to `/opt/cnsaroot/Boot`, which contains a default path pointing to `/opt/cnsaroot/Boot/WinPE.wim`. This file can be used by any Windows OS version, unless you change the path names.

The command **bcdedit.exe** used to create BCD files is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Before you begin

Create a custom WinPE and copy the PXE supported files

Procedure

Step 1 Navigate to the directory that contains the **bcdedit.exe** command and run the following sequence of commands to create the BCD file.

The **bcdedit.exe** command is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Step 2 **bcdedit.exe /createstore BCD**

Step 3 **bcdedit.exe /store BCD /create {ramdiskoptions} /d "Ramdisk options"**

Step 4 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdidevice boot**

Step 5 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdipath \Boot\boot.sdi**

Step 6 **bcdedit.exe /store BCD /create /d** *"My WinPE Boot Image"* **/application osloader**

At this point, the GUID is displayed. Replace *`{a20f8db8-7459-11e2-8ec3-00155d37efa7}`* in the following steps with the GUID from your system.

Step 7 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **systemroot \Windows**

Step 8 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **detecthal Yes**

Step 9 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **winpe Yes**

Step 10 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **osdevice ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 11 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **device ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 12 **bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2016 BootManager"**

Step 13 **bcdedit.exe /store BCD /set {bootmgr} timeout 30**

Step 14 **bcdedit.exe /store BCD /displayorder** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}*

Step 15 Use the following command to verify that the configuration names are correct: **bcdedit.exe /store BCD /enum all**

What to do next

Copy the Windows installation ISO image to the server folder.

Copying the Windows Installation Files to the Server Folder

Before you begin

You must have the following in place:

- Customized `winPE.wim` and PXE boot files in the `opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Configured BCD file in the `/opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Windows installation files (ISO version).

Procedure

Step 1 Upload the Windows OS image file, customized WinPE.wim file, and customized BCD file (optional). For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Customize install.wim image file from `c:\Win2k16x64-iso\sources` to `/tmp` folder.

Step 4 Move the install.wim image file from `/tmp` to `/samba/Win2k16x64/sources` folder.

```
mv /tmp/install.wim /samba/Win2k16x64/sources/
```

Step 5 Open the `/samba/notifications/notify.ps1` file and verify that the IP address in the file matches that of the PXE IP address of Bare Metal Agent.

Note Do not change the folder paths, filenames, or folder names.

The following is a sample of the contents of a `Win2k16x64` folder:

```
boot
efi
sources
support
autorun.inf
bootmgr.efi
setup.exe
```

Windows Server 2019 x64 Operating System Images

Cisco UCS Director Bare Metal Agent supports PXE boot and installation operations for Windows 2019 x64 OS images and PXE boot tasks used in bare metal provisioning workflows.

Important For provisioning Windows 2019, after upgrading the Cisco Bare Metal Agent Connector Pack to the latest version, you should reset Samba password if the samba services are already enabled and running.

Prerequisites for Setting Up Windows Server 2019 x64 Operating System Images

Before you install a Windows 2019 OS image in the `/opt/cnsaroot/Boot` directory of the Bare Metal Agent VM, you must install and set up the following prerequisites:

- Windows Assessment and Deployment Kit (Windows ADK, version 8.0 or later recommended, depending on the Windows version compatibilities with respect to the `WinPE.wim` file)
- A customized Windows Preinstallation Environment (`WinPE.wim`) and PXE supporting files
- Boot Configuration Data (BCD) file
- Windows installation files (the files extracted from the ISO)

Note You do not need to manually create a Windows answer file when setting up Windows OS images. Bare Metal Agent builds the Windows answer file necessary to support your PXE Boot request, based on the information you provide when you create the PXE boot request.

To install and set up the images, download the following:

- Windows Assessment and Deployment Kit that supports Windows Server 2019. For more information, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn613859(v=win.10)?redirectedfrom=MSDN.
- Windows Server 2019 x64.

Tip We recommend that you use the ISO download file, which contains all editions, including Standard, Enterprise, Datacenter, and Web. You can typically remove all editions except for Standard and Datacenter.

After the system image is in place, perform the following additional procedures:

- Set up WinPE and copy the supporting files to the Network Service Agent server for the PXE boot.
- Copy the Windows installation files to the server path.

Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2019

Note The `/opt/cnsaroot/Boot` folder is static, and each Bare Metal Agent can have only one boot folder.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2019 x64 Operating System Images, on page 84.

Procedure

Step 1 Download an ADK version that supports Windows 2019 and install it on a Windows 2019 machine.

Note When you specify the features to include in the download, you must include the Windows PE and Deployment Tools.

Step 2 Navigate to the Windows Pre-installation Environment folder in the ADK tools and execute **copype.cmd** to create the files that WinPE requires.

```
Copype.cmd amd64 C:\WinPE_amd64
```

The target directory contains the `WinPE.wim` file. The latest ADK versions create a `boot.wim` file, which needs to be renamed to `WinPE.wim`.

Step 3 In the Windows machine that has the ADK tools installed, create a directory. Copy the `WinPE.wim` file from `C:\WinPE_amd64/media/sources` to the directory you have created.

Step 4 At the command line, navigate to the ADK installed folder.

Step 5 Mount `WinPE.wim` to a folder.

Step 6 Add the drivers from their folder locations to the WinPE image.

Use the following `DISM.exe` command when you know the paths to the drivers that you want to add.

```
// The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k19x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k19x64\WinPE.wim /index:1 /mountdir:c:\win2k19x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k19x64\mount /Add-Driver /driver:C:\test\drivers\1.inf
/driver:C:\test\drivers\2.inf /driver:C:\test\drivers\3.inf
```

Use the following `DISM.exe` command when you do not know the paths to the drivers that you want to add and need to query all subfolders.

```
 // The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k19x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k19x64\WinPE.wim /index:1 /mountdir:c:\win2k19x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k19x64\mount /Add-Driver /driver:c:\test\drivers /Recurse
```

Step 7 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.

Note The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent upon the version of Windows and `WinPE.wim`.To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page. The PowerShell package files shown below are provided for reference and will vary depending on the version of Windows and WinPE.wim.

```
\\ Sample PowerShell package files.
\\ The PowerShell packages and file names that you need to add to WinPE.wim vary depending on the
version of Windows and WinPE.wim.

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
```

```
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k19x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 8 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the password for samba service and the PXE interface IP address for Bare Metal Agent as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:smbuser password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```


Note

- Do not change any information in the `startnet.cmd` file, except for the password for samba service and the PXE interface IP address of the Bare Metal Agent.
- Make sure that you modify the IP addresses in all the entries so that they point to the Bare Metal Agent IP address.
- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 9 Save the `startnet.cmd` file.

Step 10 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k19x64\mount /commit
```



Caution Do not leave any files open that are located in the mounted directory when you unmount `WinPE.wim`. If you have any files open, the unmount process might fail.

What to do next

Install and set up (as necessary) the Boot Configuration Data (BCD) file.

Preparing Windows Server 2019 x64 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2019 x64 operating system
- Windows 2019 x64 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2019 x64 ISO image installation files to the folder.

```
mkdir c:\win2k19x64-iso
```

Step 3 Take a backup copy of the install.wim file.

```
cd c:\win2k19x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2019 x64 operating system.

Step 4 Create a folder to mount the `c:\win2k19x64-iso\sources\install.wim` file.

```
mkdir c:\win2k19x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 List the supported Windows 2019 x64 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k19x64-iso\sources\install.wim
```

The supported Windows 2019 x64 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2019 x64 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2019 x64 SERVERSTANDARD
Description : Windows Server 2019 x64 SERVERSTANDARD
Size : 10,510,509,480 bytes

Index : 2
Name : Windows Server 2019 x64 SERVERSTANDARDCORE
Description : Windows Server 2019 x64 SERVERSTANDARDCORE
Size : 3,563,998,339 bytes

Index : 3
Name : Windows Server 2019 x64 SERVERENTERPRISE
Description : Windows Server 2019 x64 SERVERENTERPRISE
Size : 10,510,890,698 bytes

Index : 4
Name : Windows Server 2019 x64 SERVERENTERPRISECORE
Description : Windows Server 2019 x64 SERVERENTERPRISECORE
Size : 3,563,972,455 bytes

Index : 5
Name : Windows Server 2019 x64 SERVERDATACENTER
Description : Windows Server 2019 x64 SERVERDATACENTER
Size : 10,510,997,874 bytes

Index : 6
Name : Windows Server 2019 x64 SERVERDATACENTERCORE
Description : Windows Server 2019 x64 SERVERDATACENTERCORE
Size : 3,564,010,572 bytes

Index : 7
Name : Windows Server 2019 x64 SERVERWEB
Description : Windows Server 2019 x64 SERVERWEB
Size : 10,520,088,768 bytes

Index : 8
Name : Windows Server 2019 x64 SERVERWEBCORE
Description : Windows Server 2019 x64 SERVERWEBCORE
Size : 3,562,616,654 bytes
```

Step 7 Mount the install.wim image with Index ID 5 to install Windows 2019 x64 Datacenter Edition.

```
DISM.exe /mount-wim /wimfile:c:\win2k19x64-iso\sources\install.wim /index:5
mountdir:c:\win2k19x64-mount
```

Step 8 Add the device drivers to the install.wim image by using the DISM.exe command from the Windows ADK installation directory.

Step 9 Add the device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k19x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k19x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the install.wim image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k19x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Installing and Setting Up the Boot Configuration Data File

The Boot Configuration Data (BCD) file contains the boot configuration parameters. It controls how the operating system is started in Windows and is used to load the base kernel (WinPE.wim) from the PXE server. You do not need to create a BCD file. Bare Metal Agent provides a BCD file with default paths that you can use.

By default, the BCD file points to the `/Boot/WinPE.wim` and `boot.sdi` files. These filenames are case sensitive.

Note We recommend that you use a set of standard names for Bare Metal Agent configuration purposes. The folder name should be Boot. The winpe file name should be WinPE.wim. Use corresponding filenames such as boot.sdi. The created BCD file should be in uppercase, and this file will not have any file extension. Bare Metal Agent delivers the BCD file to `/opt/cnsaroot/Boot`, which contains a default path pointing to `/opt/cnsaroot/Boot/WinPE.wim`. This file can be used by any Windows OS version, unless you change the path names.

The command **bcdedit.exe** used to create BCD files is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Before you begin

Create a custom WinPE and copy the PXE supported files

Procedure

Step 1 Navigate to the directory that contains the **bcdedit.exe** command and run the following sequence of commands to create the BCD file.

The **bcdedit.exe** command is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Step 2 **bcdedit.exe /createstore BCD**

Step 3 **bcdedit.exe /store BCD /create {ramdiskoptions} /d "Ramdisk options"**

Step 4 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdidevice boot**

Step 5 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdipath \Boot\boot.sdi**

Step 6 **bcdedit.exe /store BCD /create /d** *"My WinPE Boot Image"* **/application osloader**

At this point, the GUID is displayed. Replace `{a20f8db8-7459-11e2-8ec3-00155d37efa7}` in the following steps with the GUID from your system.

Step 7 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **systemroot \Windows**

Step 8 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **detecthal Yes**

Step 9 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **winpe Yes**

Step 10 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **osdevice ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 11 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **device ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 12 **bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2019 BootManager"**

Step 13 **bcdedit.exe /store BCD /set {bootmgr} timeout 30**

Step 14 **bcdedit.exe /store BCD /displayorder** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}*

Step 15 Use the following command to verify that the configuration names are correct: **bcdedit.exe /store BCD /enum all**

What to do next

Copy the Windows installation ISO image to the server folder.

Copying the Windows Installation Files to the Server Folder

Before you begin

You must have the following in place:

- Customized `winPE.wim` and PXE boot files in the `opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Configured BCD file in the `/opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Windows installation files (ISO version).

Procedure

Step 1 Upload the Windows OS image file, customized WinPE.wim file, and customized BCD file (optional). For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Customize install.wim image file from `c:\Win2k19x64-iso\sources` to `/tmp` folder.

Step 4 Move the install.wim image file from `/tmp` to `/samba/Win2k19x64/sources` folder.

```
mv /tmp/install.wim /samba/Win2k19x64/sources/
```

Step 5 Open the `/samba/notifications/notify.ps1` file and verify that the IP address matches the PXE IP address of Bare Metal Agent.

Note Do not change the folder paths, filenames, or folder names.

The following is a sample of the contents of a `Win2k19x64` folder:

```
boot
efi
sources
support
autorun.inf
bootmgr.efi
setup.exe
```

Windows Server 2022 x64 Operating System Images

Cisco UCS Director Bare Metal Agent supports PXE boot and installation operations for Windows 2022 x64 OS images and PXE boot tasks used in bare metal provisioning workflows.

Prerequisites for Setting Up Windows Server 2022 x64 Operating System Images

Before you install a Windows 2022 OS image in the `/opt/cnsaroot/Boot` directory of the Bare Metal Agent VM, you must install and set up the following prerequisites:

- Windows Assessment and Deployment Kit (Windows ADK, version 8.0 or later recommended, depending on the Windows version compatibilities with respect to the `WinPE.wim` file)
- A customized Windows Preinstallation Environment (`WinPE.wim`) and PXE supporting files
- Boot Configuration Data (BCD) file
- Windows installation files (the files extracted from the ISO)

Note You do not need to manually create a Windows answer file when setting up Windows OS images. Bare Metal Agent builds the Windows answer file necessary to support your PXE Boot request, based on the information you provide when you create the PXE boot request.

To install and set up the images, download the following:

- Windows Assessment and Deployment Kit that supports Windows Server 2022. For more information, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn613859(v=win.10)?redirectedfrom=MSDN.

- Windows Server 2022 x64.

Tip We recommend that you use the ISO download file, which contains all editions, including Standard, Enterprise, Datacenter, and Web. You can typically remove all editions except for Standard and Datacenter.

After the system image is in place, perform the following additional procedures:

- Set up WinPE and copy the supporting files to the Network Service Agent server for the PXE boot.
- Copy the Windows installation files to the server path.

Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2022

Note The `/opt/cnsaroot/Boot` folder is static, and each Bare Metal Agent can have only one boot folder.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2022 x64 Operating System Images, on page 92.

Procedure

Step 1 Download an ADK version that supports Windows 2022 and install it on a Windows 2022 machine.

Note When you specify the features to include in the download, you must include the Windows PE and Deployment Tools.

Step 2 Navigate to the Windows Pre-installation Environment folder in the ADK tools and execute **copype.cmd** to create the files that WinPE requires.

```
Copype.cmd amd64 C:\WinPE_amd64
```

The target directory contains the `WinPE.wim` file. The latest ADK versions create a `boot.wim` file, which needs to be renamed to `WinPE.wim`.

Step 3 In the Windows machine that has the ADK tools installed, create a directory. Copy the `WinPE.wim` file from `C:\WinPE_amd64/media/sources` to the directory you have created.

Step 4 At the command line, navigate to the ADK installed folder.

Step 5 Mount `WinPE.wim` to a folder.

Step 6 Add the drivers from their folder locations to the WinPE image.

Use the following `DISM.exe` command when you know the paths to the drivers that you want to add.

```
// The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k22x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k22x64\WinPE.wim /index:1 /mountdir:c:\win2k22x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k22x64\mount /Add-Driver /driver:C:\test\drivers\1.inf
/driver:C:\test\drivers\2.inf /driver:C:\test\drivers\3.inf
```

Use the following `DISM.exe` command when you do not know the paths to the drivers that you want to add and need to query all subfolders.

```
 // The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k22x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k22x64\WinPE.wim /index:1 /mountdir:c:\win2k22x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k22x64\mount /Add-Driver /driver:c:\test\drivers /Recurse
```

Step 7 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.

Note The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent upon the version of Windows and `WinPE.wim`.To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page. The PowerShell package files shown below are provided for reference and will vary depending on the version of Windows and WinPE.wim.

```
\\ Sample PowerShell package files.
\\ The PowerShell packages and file names that you need to add to WinPE.wim vary depending on the
version of Windows and WinPE.wim.

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
```

```
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k22x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 8 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the password for samba service and the PXE interface IP address for Bare Metal Agent as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:smbuser password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```



Note

- Do not change any information in the `startnet.cmd` file, except for the password for samba service and the PXE interface IP address of the Bare Metal Agent.
- Make sure that you modify the IP addresses in all the entries so that they point to the Bare Metal Agent IP address.
- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 9 Save the `startnet.cmd` file.

Step 10 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k22x64\mount /commit
```



Caution Do not leave any files open that are located in the mounted directory when you unmount `WinPE.wim`. If you have any files open, the unmount process might fail.

What to do next

Install and set up (as necessary) the Boot Configuration Data (BCD) file.

Preparing Windows Server 2022 x64 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2022 x64 operating system
- Windows 2022 x64 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2022 x64 ISO image installation files to the folder.

```
mkdir c:\win2k22x64-iso
```

Step 3 Take a backup copy of the install.wim file.

```
cd c:\win2k22x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2022 x64 operating system.

Step 4 Create a folder to mount the `c:\win2k22x64-iso\sources\install.wim` file.

```
mkdir c:\win2k22x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 List the supported Windows 2022 x64 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k22x64-iso\sources\install.wim
```

The supported Windows 2022 x64 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2022 x64 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2022 x64 SERVERSTANDARD
Description : Windows Server 2022 x64 SERVERSTANDARD
Size : 10,510,509,480 bytes

Index : 2
Name : Windows Server 2022 x64 SERVERSTANDARDCORE
Description : Windows Server 2022 x64 SERVERSTANDARDCORE
Size : 3,563,998,339 bytes

Index : 3
Name : Windows Server 2022 x64 SERVERENTERPRISE
Description : Windows Server 2022 x64 SERVERENTERPRISE
Size : 10,510,890,698 bytes

Index : 4
Name : Windows Server 2022 x64 SERVERENTERPRISECORE
Description : Windows Server 2022 x64 SERVERENTERPRISECORE
Size : 3,563,972,455 bytes

Index : 5
Name : Windows Server 2022 x64 SERVERDATACENTER
Description : Windows Server 2022 x64 SERVERDATACENTER
Size : 10,510,997,874 bytes

Index : 6
Name : Windows Server 2022 x64 SERVERDATACENTERCORE
Description : Windows Server 2022 x64 SERVERDATACENTERCORE
Size : 3,564,010,572 bytes

Index : 7
Name : Windows Server 2022 x64 SERVERWEB
Description : Windows Server 2022 x64 SERVERWEB
Size : 10,520,088,768 bytes

Index : 8
Name : Windows Server 2022 x64 SERVERWEBCORE
Description : Windows Server 2022 x64 SERVERWEBCORE
Size : 3,562,616,654 bytes
```

Step 7 Mount the install.wim image with Index ID 5 to install Windows 2022 x64 Datacenter Edition.

```
DISM.exe /mount-wim /wimfile:c:\win2k22x64-iso\sources\install.wim /index:5
mountdir:c:\win2k22x64-mount
```

Step 8 Add the device drivers to the install.wim image by using the DISM.exe command from the Windows ADK installation directory.

Step 9 Add the device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k22x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k22x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the install.wim image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k22x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Installing and Setting Up the Boot Configuration Data File

The Boot Configuration Data (BCD) file contains the boot configuration parameters. It controls how the operating system is started in Windows and is used to load the base kernel (WinPE.wim) from the PXE server. You do not need to create a BCD file. Bare Metal Agent provides a BCD file with default paths that you can use.

By default, the BCD file points to the `/Boot/WinPE.wim` and `boot.sdi` files. These filenames are case sensitive.

Note We recommend that you use a set of standard names for Bare Metal Agent configuration purposes. The folder name should be Boot. The winpe file name should be WinPE.wim. Use corresponding filenames such as boot.sdi. The created BCD file should be in uppercase, and this file will not have any file extension. Bare Metal Agent delivers the BCD file to `/opt/cnsaroot/Boot`, which contains a default path pointing to `/opt/cnsaroot/Boot/WinPE.wim`. This file can be used by any Windows OS version, unless you change the path names.

The command **bcdedit.exe** used to create BCD files is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Before you begin

Create a custom WinPE and copy the PXE supported files

Procedure

Step 1 Navigate to the directory that contains the **bcdedit.exe** command and run the following sequence of commands to create the BCD file.

The **bcdedit.exe** command is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Step 2 **bcdedit.exe /createstore BCD**

Step 3 **bcdedit.exe /store BCD /create {ramdiskoptions} /d "Ramdisk options"**

Step 4 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdidevice boot**

Step 5 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdipath \Boot\boot.sdi**

Step 6 **bcdedit.exe /store BCD /create /d** *"My WinPE Boot Image"* **/application osloader**

At this point, the GUID is displayed. Replace `{a20f8db8-7459-11e2-8ec3-00155d37efa7}` in the following steps with the GUID from your system.

Step 7 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **systemroot \Windows**

Step 8 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **detecthal Yes**

Step 9 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **winpe Yes**

Step 10 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **osdevice ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 11 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **device ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 12 **bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2022 BootManager"**

Step 13 **bcdedit.exe /store BCD /set {bootmgr} timeout 30**

Step 14 **bcdedit.exe /store BCD /displayorder** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}*

Step 15 Use the following command to verify that the configuration names are correct: **bcdedit.exe /store BCD /enum all**

What to do next

Copy the Windows installation ISO image to the server folder.

Copying the Windows Installation Files to the Server Folder

Before you begin

You must have the following in place:

- Customized `winPE.wim` and PXE boot files in the `opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Configured BCD file in the `/opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Windows installation files (ISO version).

Procedure

Step 1 Upload the Windows OS image file, customized WinPE.wim file, and customized BCD file (optional). For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Customize install.wim image file from `c:\Win2k22x64-iso\sources` to `/tmp` folder.

Step 4 Move the install.wim image file from `/tmp` to `/samba/Win2k22x64/sources` folder.

```
mv /tmp/install.wim /samba/Win2k22x64/sources/
```

Step 5 Open the `/samba/notifications/notify.ps1` file and verify that the IP address matches the PXE IP address of Bare Metal Agent.

Note Do not change the folder paths, filenames, or folder names.

The following is a sample of the contents of a `Win2k22x64` folder:

```
boot
efi
sources
support
autorun.inf
bootmgr.efi
setup.exe
```

Windows Server 2025 x64 Operating System Images

Cisco UCS Director Bare Metal Agent supports PXE boot and installation operations for Windows 2025 x64 OS images and PXE boot tasks used in bare metal provisioning workflows.

Prerequisites for Setting Up Windows Server 2025 x64 Operating System Images

Before you install a Windows 2025 OS image in the `/opt/cnsaroot/Boot` directory of the Bare Metal Agent VM, you must install and set up the following prerequisites:

- Windows Assessment and Deployment Kit (Windows ADK) version 10.1.26100.2454 and later depending on the Windows version compatibilities with respect to the `WinPE.wim` file
- A customized Windows Preinstallation Environment (`WinPE.wim`) and PXE supporting files
- Boot Configuration Data (BCD) file
- Windows installation files (the files extracted from the ISO)

Note You do not need to manually create a Windows answer file when setting up Windows OS images. Bare Metal Agent builds the Windows answer file necessary to support your PXE Boot request, based on the information you provide when you create the PXE boot request.

To install and set up the images, download the following:

- Windows ADK that supports Windows Server 2025. For more information, see Download and install the Windows ADK.
- Windows Server 2025 x64.

Tip We recommend that you use the ISO download file, which contains all editions, including Standard, Enterprise, Datacenter, and Web. You can typically remove all editions except for Standard and Datacenter.

After the system image is in place, perform the following additional procedures:

- Set up WinPE and copy the supporting files to the Network Service Agent server for the PXE boot.
- Copy the Windows installation files to the server path.

Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2025

Note The `/opt/cnsaroot/Boot` folder is static, and each Bare Metal Agent can have only one boot folder.

Before you begin

Complete the prerequisites listed in Prerequisites for Setting Up Windows Server 2025 x64 Operating System Images.

Procedure

Step 1 Download an ADK version that supports Windows 2025 and install it on a Windows 2025 machine.

Note When you specify the features to include in the download, you must include the Windows PE and Deployment Tools.

Step 2 Navigate to the Windows Pre-installation Environment folder in the ADK tools and execute **copype.cmd** to create the files that WinPE requires.

```
Copype.cmd amd64 C:\WinPE_amd64
```

The target directory contains the `WinPE.wim` file. The latest ADK versions create a `boot.wim` file, which needs to be renamed to `WinPE.wim`.

Step 3 In the Windows machine that has the ADK tools installed, create a directory. Copy the `WinPE.wim` file from `C:\WinPE_amd64/media/sources` to the directory you have created.

Step 4 At the command line, navigate to the ADK installed folder.

Step 5 Mount `WinPE.wim` to a folder.

Step 6 Add the drivers from their folder locations to the WinPE image.

Use the following `DISM.exe` command when you know the paths to the drivers that you want to add.

```
// The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k25x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k25x64\WinPE.wim /index:1 /mountdir:c:\win2k25x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k25x64\mount /Add-Driver /driver:C:\test\drivers\1.inf
/driver:C:\test\drivers\2.inf /driver:C:\test\drivers\3.inf
```

Use the following `DISM.exe` command when you do not know the paths to the drivers that you want to add and need to query all sub folders.

```
 // The DISM.exe command mounts the WinPE to a folder.
// In this example, the c:\win2k25x64 directory and the \mount subdirectory have been created before
 running the command.
DISM.exe /mount-wim /wimfile:c:\win2k25x64\WinPE.wim /index:1 /mountdir:c:\win2k25x64\mount

// To add individual driver files to WinPE image, use the following format.
DISM.exe /image:c:\win2k25x64\mount /Add-Driver /driver:c:\test\drivers /Recurse
```

Step 7 In `WinPE.wim`, add the required PowerShell packages and edit the paths in each command with the correct mount point and ADK installation path for your environment.

Note The PowerShell packages and file names that you need to add to `WinPE.wim` are dependent upon the version of Windows and `WinPE.wim`.To determine which PowerShell packages you need to add, see the compliance report on the Microsoft website. For information about the commands to add the necessary packages for PowerShell, see the WinPE: Adding PowerShell support to Windows PE Technet Page. The PowerShell package files shown below are provided for reference and will vary depending on the version of Windows and WinPE.wim.

```
\\ Sample PowerShell package files.
\\ The PowerShell packages and file names that you need to add to WinPE.wim vary depending on the
version of Windows and WinPE.wim.

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-WMI.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-WMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-NetFX.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-NetFX_en-us.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
```

```
Environment\amd64\WinPE_OCs\WinPE-Scripting.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-Scripting_en-us.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-PowerShell.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-PowerShell_en-us.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-StorageWMI.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-StorageWMI_en-us.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\WinPE-DismCmdlets.cab"

Dism /Add-Package /Image:"C:\win2k25x64\mount" /PackagePath:"C:\Program Files\Windows
Kits\10\Assessment and Deployment Kit\Windows Preinstallation
Environment\amd64\WinPE_OCs\en-us\WinPE-DismCmdlets_en-us.cab"
```

Step 8 Navigate to `\windows\system32` in the mount folder and do the following:

a) Edit `startnet.cmd`.

b) Paste the following entries into the file in the order shown, to update the password for samba service and the PXE interface IP address for Bare Metal Agent as required for your environment:

```
wpeinit
wpeutil.exe InitializeNetwork
wpeutil.exe disablefirewall
ECHO OFF
net use R: \\Baremetal_Agent_PXE_IP_Address\bits /user:smbuser password
ECHO ON
R:
Powershell.exe -NonInteractive -NoLogo -ExecutionPolicy bypass -command R:\enroute.ps1
```


Note

- Do not change any information in the `startnet.cmd` file, except for the password for samba service and the PXE interface IP address of the Bare Metal Agent.
- Make sure that you modify the IP addresses in all the entries so that they point to the Bare Metal Agent IP address.
- All drive letter references (such as the reference to an R: drive) must match in both the `startnet.cmd` file and the Windows answer file. By default, Bare Metal Agent comes with an R: drive letter assignment.

Step 9 Save the `startnet.cmd` file.

Step 10 After you have confirmed that the `startnet.cmd` is updated correctly, unmount `WinPE.wim` with the DISM Unmount command and use the /**commit** option to save the modified `startnet.cmd` file.

```
DISM.exe /Unmount-Wim /Mountdir:c:\win2k25x64\mount /commit
```



Caution Do not leave any files open that are located in the mounted directory when you unmount `WinPE.wim`. If you have any files open, the unmount process might fail.

What to do next

Install and set up (as necessary) the Boot Configuration Data (BCD) file.

Preparing Windows Server 2025 x64 Installation Files

Before you begin

You must have the following in place:

- Windows Assessment and Deployment Kit (ADK, sometimes called as Windows ADK) that is compatible with the Windows 2025 x64 operating system
- Windows 2025 x64 ISO image

Procedure

Step 1 Launch the command prompt (click **Start > All Programs > Accessories > Command Prompt**).

Step 2 Create a new folder and extract the Windows 2025 x64 ISO image installation files to the folder.

```
mkdir c:\win2k25x64-iso
```

Step 3 Take a backup copy of the `install.wim` file.

```
cd c:\win2k25x64-iso\sources
copy install.wim install.wim.backup
```

The backup is recommended as device drivers will be added to the install.wim file in the subsequent steps. The device drivers are used during the installation of the Windows 2025 x64 operating system.

Step 4 Create a folder to mount the `c:\win2k25x64-iso\sources\install.wim` file.

```
mkdir c:\win2k25x64-mount
```

Step 5 Change the directory to the Windows ADK installation directory.

```
cd C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Deployment Tools\amd64\DISM
```

Step 6 List the supported Windows 2025 x64 Editions.

```
dism.exe /Get-ImageInfo /imagefile:c:\win2k25x64-iso\sources\install.wim
```

The supported Windows 2025 x64 editions are listed, with each edition represented by an Index ID. Choose the corresponding Index ID of the Windows 2025 x64 Edition that you want to install through PXE.

```
Index : 1
Name : Windows Server 2025 Standard
Description : (Recommended) This option omits most of the Windows graphical environment. Manage
with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.
Size : 10,706,668,594 bytes

Index : 2
Name : Windows Server 2025 Standard (Desktop Experience)
Description : This option installs the full Windows graphical environment, consuming extra drive
space. It can be useful if you want to use the Windows desktop or have an app that requires it.
Size : 23,309,091,550 bytes

Index : 3
Name : Windows Server 2025 Datacenter
Description : (Recommended) This option omits most of the Windows graphical environment. Manage
with a command prompt and PowerShell, or remotely with Windows Admin Center or other tools.
Size : 10,709,582,325 bytes

Index : 4
Name : Windows Server 2025 Datacenter (Desktop Experience)
Description : This option installs the full Windows graphical environment, consuming extra drive
space. It can be useful if you want to use the Windows desktop or have an app that requires it.
Size : 23,375,974,482 bytes
```

Step 7 Mount the install.wim image with Index ID 2 to install Windows Server 2025 Standard (Desktop Experience).

```
DISM.exe /mount-wim /wimfile:c:\win2k25x64-iso\sources\install.wim /index:5
mountdir:c:\win2k25x64-mount
```

Step 8 Add the device drivers to the install.wim image by using the `DISM.exe` command from the Windows ADK installation directory.

Step 9 Add the device drivers to the install.wim image by using the individual driver's absolute path.

```
DISM.exe /image:c:\win2k25x64-mount /Add-Driver /driver:C:\cisco\drivers\1.inf
/driver:C:\cisco\drivers\2.inf /driver:C:\cisco\drivers\3.inf
```

Alternatively, you can add the device drivers to the install.wim image by automatically searching through all the subfolders of the device drivers directory.

```
DISM.exe /image:c:\win2k25x64-mount /Add-Driver /driver:C:\cisco\drivers /Recurse
```

Step 10 Unmount the `install.wim` image and commit the changes.

```
DISM.exe /unmount-wim /mountdir:c:\win2k25x64-mount /commit
```

Note When all the device drivers have been added, the install.wim image is ready to be used.

Installing and Setting Up the Boot Configuration Data File

The Boot Configuration Data (BCD) file contains the boot configuration parameters. It controls how the operating system is started in Windows and is used to load the base kernel (WinPE.wim) from the PXE server. You do not need to create a BCD file. Bare Metal Agent provides a BCD file with default paths that you can use.

By default, the BCD file points to the `/Boot/WinPE.wim` and `boot.sdi` files. These filenames are case sensitive.



Note We recommend that you use a set of standard names for Bare Metal Agent configuration purposes. The folder name should be Boot. The winpe file name should be WinPE.wim. Use corresponding filenames such as boot.sdi. The created BCD file should be in uppercase, and this file will not have any file extension. Bare Metal Agent delivers the BCD file to `/opt/cnsaroot/Boot`, which contains a default path pointing to `/opt/cnsaroot/Boot/WinPE.wim`. This file can be used by any Windows OS version, unless you change the path names.

The command **bcdedit.exe** used to create BCD files is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Before you begin

Create a custom WinPE and copy the PXE supported files

Procedure

Step 1 Navigate to the directory that contains the **bcdedit.exe** command and run the following sequence of commands to create the BCD file.

The **bcdedit.exe** command is commonly available in the Windows operating systems root directory: `c:\windows\system32`.

Step 2 **bcdedit.exe /createstore BCD**

Step 3 **bcdedit.exe /store BCD /create {ramdiskoptions} /d "Ramdisk options"**

Step 4 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdidevice boot**

Step 5 **bcdedit.exe /store BCD /set {ramdiskoptions} ramdisksdipath \Boot\boot.sdi**

Step 6 **bcdedit.exe /store BCD /create /d** *"My WinPE Boot Image"* **/application osloader**

At this point, the GUID is displayed. Replace *`{a20f8db8-7459-11e2-8ec3-00155d37efa7}`* in the following steps with the GUID from your system.

Step 7 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **systemroot \Windows**

Step 8 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **detecthal Yes**

Step 9 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **winpe Yes**

Step 10 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **osdevice ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 11 **bcdedit.exe /store BCD /set** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}* **device ramdisk=[boot]\Boot\WinPE.wim,{ramdiskoptions}**

Step 12 **bcdedit.exe /store BCD /create {bootmgr} /d "Windows 2025 BootManager"**

Step 13 **bcdedit.exe /store BCD /set {bootmgr} timeout 30**

Step 14 **bcdedit.exe /store BCD /displayorder** *{a20f8db8-7459-11e2-8ec3-00155d37efa7}*

Step 15 Use the following command to verify that the configuration names are correct: **bcdedit.exe /store BCD /enum all**

What to do next

Copy the Windows installation ISO image to the server folder.

Copying the Windows Installation Files to the Server Folder

Before you begin

You must have the following in place:

- Customized `winPE.wim` and PXE boot files in the `opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Configured BCD file in the `/opt/cnsaroot/Boot` directory in the Bare Metal Agent VM.
- Windows installation files (ISO version).

Procedure

Step 1 Upload the Windows OS image file, customized WinPE.wim file, and customized BCD file (optional). For more information, see Uploading an OS Image File, on page 18.

Step 2 Provision the Windows OS image. For more information, see Provisioning an OS Image, on page 23.

Step 3 Customize install.wim image file from `c:\Win2k25x64-iso\sources` to `/tmp` folder.

Step 4 Move the install.wim image file from `/tmp` to `/samba/Win2k25x64/sources` folder.

```
mv /tmp/install.wim /samba/Win2k25x64/sources/
```

Step 5 Open the `/samba/notifications/notify.ps1` file and verify that the IP address matches the PXE IP address of Bare Metal Agent.

Note Do not change the folder paths, filenames, or folder names.

The following is a sample of the contents of a `Win2k25x64` folder:

```
boot
efi
sources
support
autorun.inf
```

```
bootmgr.efi
setup.exe
```

Using MEMDISK for Deploying Multiple Versions of Windows Simultaneously

Currently, Bare Metal Agent adopts the Microsoft Windows PXE boot process, which expects WinPE.wim to be placed in the **/tftproot/Boot** folder. This process results in maintaining a single WinPE for deploying multiple versions of Windows simultaneously from Bare Metal Agent. To use different WinPE files for deploying different versions of Windows simultaneously, you have to rename each WinPE.wim file manually according to the BCD file. To overcome this limitation, you can use MEMDISK to boot the ISO file. The MEMDISK file is available in the **/opt/cnsaroot** folder in Bare Metal Agent, as part of syslinux. When you use MEMDISK , the ISO file can be placed anywhere in the TFTP root directory in Bare Metal Agent.

Requirements for Using MEMDISK

To use MEMDISK in Bare Metal Agent, create a bootable WINPE ISO file and then modify the MAC file template.

Creating Bootable WINPE File for Windows Server 2008 R2, 2012, 2012 R2, or 2016

Before you begin

Install Windows Assessment and Deployment Kit (Windows ADK) that is compatible with the Windows Server version you want to deploy.

Procedure

Step 1 Launch the Deployment and Imaging Tools Environment.

Step 2 Create a new WinPE environment folder:

```
Copype.cmd amd64 C:\WinPE_amd64
```

The ‘copype.cmd’ command creates a "WinPE_amd64" folder with three subfolders: fwfiles, media and mount. The folders created are based on the ADK version.

Step 3 Delete bootfix.bin from `/media/Boot folder`.

Deleting bootfix.bin helps you avoid pressing a key to boot the ISO if any partition is detected on the hard disk drive.

Step 4 Create the customized WinPE.wim (available in the `/media/Sources` folder) by making the following changes:

a) Inject PowerShell packages.
b) Inject drivers (if any)
c) Edit Startnet.cmd.

For injecting PowerShell packages and editing Startnet.cmd for the Windows Server version you are deploying, see

- Customizing and Copying the WinPE.wim and PXE Boot Files for Windows 2008 R2, on page 59
- Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2012, on page 64
- Creating a Custom WinPE and Copying the PXE Supported Files for Windows 2012 R2, on page 67

Step 5 Execute the following command from the terminal to create the bootable WINPE ISO file:

```
Makewinpemedia.cmd /iso C:\WinPE_amd64 C:\WinPE_amd64.iso
```

Modifying MAC File Template

To support the MEMDISK boot process in Bare Metal Agent, the MAC file template has to be modified. The `/opt/cnsaroot/templates` folder in Bare Metal Agent has the configuration files templates for all the three versions of Windows.



Note As the MAC template file is static, you can either implement the Windows PXE boot process or the MEMDISK boot process. You cannot implement both of them.

Procedure

Step 1 After creating the bootable WINPE ISO file, create a folder called 'windows' under `/opt/cnsaroot` (folder name is not static) in the BMA tftp root directory.

Step 2 Copy the working bootable WINPE ISO file to the windows folder.

Step 3 When the MEMDISK module is loaded, it adds the ISO image to the memory (specified as INITRD in the MAC File).

Step 4 Pass the two parameters, iso and raw, to MEMDISK using APPEND. (This instructs MEMDISK to load an ISO image and enter in protected mode directly).

Example:

For example, if you want to boot Windows Server 2012 R2 using MEMDISK, make the following changes in pxe.cfg available in the Win2k12R2x64 folder:

```
default 1
timeout 100
prompt 1
label 1
KERNEL memdisk
INITRD /windows/WinPE.iso
APPEND iso raw
```

Automating PXE-based Windows OS Deployment

From the release of Cisco UCS Director 6.9(4.0), you can automate the Windows OS deployment on Cisco UCS and third party servers without manual preparation of `WinPE.wim` and `install.wim` files.

Note This process can be used for any versions of Windows server OS images.

Before you begin

The following prerequisites must be met:

- Download the required Windows server OS ISO file.
- Download the required driver files from the specific site, extract them, and compress them into a file in **.zip** format. The Cisco UCS server driver files can be downloaded from ucshcltool.cloudapps.cisco.com/public or ucshcltool.cisco.com/public.

Important Ensure that you select the driver file specific to the UCSM version you are using.

Specifying Windows OS Variant to be Deployed

Important This section is applicable only if you want to select a specific Windows server OS variant before provisioning the Windows OS image. If you are fine with the default Windows server OS variant, skip this section and follow the instructions in the section Automating PXE-based Windows OS Deployment.

Any Windows Server OS includes different variants. For example, the Windows Server 2022 OS includes the following variants:

- Standard
- Datacenter
- Datacenter: Azure Edition

The system identifies the variant to be installed based on the index value defined in the `customize_winpe_install_wim.sh` file in the `/opt/infra/bin` directory. The PXE-based Windows OS automation process enables the default Windows server variant to be installed by looking for the index value mentioned by default.

To specify the required Windows server variant, perform the following steps first after uploading the Windows OS and driver files and before provisioning the Windows OS image:

Before you begin

The specific Windows ISO and Windows Driver.zip files must be uploaded for the selected bare metal agent account.

Procedure

Step 1 Login to Cisco UCS Director Bare Metal Agent through a SSH client.

Step 2 To know the index value corresponding to the Windows server OS variant, perform the following:

a. Open the samba sources folder for the required Windows server OS main version, for example `cd /samba/Win2k25x64/sources/`.

b. Run the command `wimlib-imagex info install.wim` or `wiminfo install.wim`.

The related information is displayed for each index.

Step 3 Navigate to the `/opt/infra/bin` directory.

Step 4 Open the `customize_winpe_install_wim.sh` file, and edit the index value in the `INSTALL_INDEX` field.

What to do next

In the **Provision Image** catalog screen, select the required Windows version from the **OS Type** drop-down list and proceed further. For more information, see Automating PXE-based Windows OS Deployment.

Provisioning Windows OS Image

Procedure

Step 1 Go to **Administration** > **Physical Accounts**.

Step 2 Select **Physical Accounts**.

Step 3 Click **Add** icon to add an account. See **Adding a Physical Account** section in Cisco UCS Director Administration Guide.

Step 4 Select **Bare Metal Agents**.

Step 5 Add a Bare metal agent account. See Adding a Bare Metal Agent Account.

Step 6 Select a Bare metal agent account.

Step 7 On the **Bare Metal Account** screen, select **Image Repository**.

Step 8 Click **Upload Image** to upload Windows ISO and driver zip files.

Step 9 On the **Image Upload** screen, complete the following fields:

Name	Description
Image Name field	The name of the OS image.

Name	Description
OS Type drop-down list	The drop-down list includes all OS types supported by the Bare Metal Agent. Select **WINDOWS** as the OS Type first to upload the `Windows OS ISO` file, proceed through the following fields, and then select **Windows-Driver** as the OS type to upload the prepared `Windows Driver.zip` file and complete the same fields again.
Upload Type drop-down list	Choose one of the following: • Desktop File - To select the file from your local. • Web Server Path - To select the file from a remote server that is reachable by the Cisco UCS Director Bare Metal Agent.
Local File Path field	This field appears when you choose the Desktop File option in the **Upload Type** drop-down list. To upload the file, you can either drag and drop the required file or click **Select** and click **Submit**.
Web URL field	This field appears when you choose the Web Server Path option in the **Upload Type** drop-down list. Enter the web server path where the ISO images are stored and click **Submit**.
MD5 Checksum field	This field appears when you choose the Web Server Path option in the **Upload Type** drop-down list. (Optional) Enter the MD5 checksum value of the downloaded ISO file which is used to verify the data integrity.



Important Make sure to bundle only the required drivers in the `Windows Driver.zip` file, as a file size equal to or greater than 1.5 GB may lead to system timeouts and disrupt the ongoing Windows OS provisioning process when attempted via a GUI action. If the file size exceeds 1.5 GB, you can perform the Windows OS provisioning process using the **BMA OS Image Provision** workflow task, or **Upload Image** and **Provision OS Image** REST APIs.

Step 10 Click **Submit**. The details of the uploaded image is displayed.

Step 11 Under **Image Repository** menu, select the row for the OS image for which you want to view the upload status and log details.

The **Upload Status** is updated to **Upload Succeeded**, and the corresponding log message is displayed under the **Upload Log** column.

Step 12 (Optional) If you want to know and deploy the specific Windows server OS variant, see Specifying Windows Server OS Variant to be Deployed.

Step 13 Under **Image Repository**, select the Windows image, and then select **Provision Image**.

Step 14 In the **Provision Image catalog** screen, select the required Windows version from the **OS Type** drop-down list.

Step 15 Select the driver file from the **Windows Driver** drop-down list.

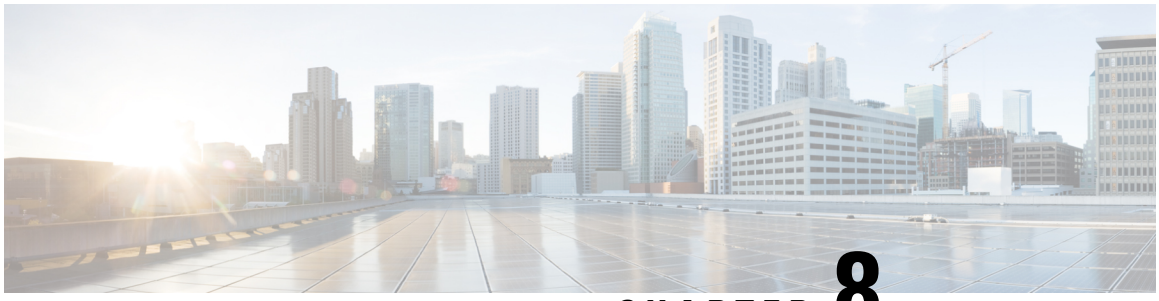
Note As part of the automation of Windows OS deployment process, the `startnet.cmd` file will be generated dynamically and injected into the `WinPE.wim` file based on Bare metal agent topology. The driver files from the selected `Windows Driver.zip` file will be injected into both `WinPE.wim` and `install.wim` files.

Step 16 Click **Provision Image**.
The following message is displayed:

OS Image provisioned successfully.

Note If you get a page or GUI action timeout error message on screen due to large `Windows Driver.zip` file size, perform the provisioning process using the **BMA OS Image Provision** workflow task, or **Upload Image** and **Provision OS Image** REST APIs.

Step 17 Execute the required Windows OS deployment workflow.



CHAPTER 8

Provisioning OS Images through Orchestration Workflow Tasks

This chapter contains the following sections:

- Orchestration Workflow Tasks for PXE/vMedia Boot, on page 115
- Prerequisites for Workflows with PXE/vMedia Boot Tasks, on page 116
- Execution of the Setup PXE/vMedia Boot Tasks , on page 117
- Determining the Windows OS Edition, on page 118
- Inputs for the Setup PXE/vMedia Boot Task, on page 119
- Inputs for the Setup PXE/vMedia Boot with BMA Selection Task, on page 122
- Inputs for the Setup Windows PXE/vMedia Boot Task, on page 125
- Outputs from the Setup PXE/vMedia Boot Task and Setup Windows PXE/vMedia Boot Task, on page 128
- Creating a PXE Boot Request in Cisco UCS Director, on page 129
- Viewing the PXE Request Configuration Files, on page 132
- PXE Boot States, on page 132
- Monitor PXE/vMedia Boot Setup Task, on page 133
- Remove PXE/vMedia Boot Setup Task, on page 133
- Injecting Drivers When Installing RHEL 7 or CentOS 7 on UCS Modular Servers, on page 134
- Simultaneous Provisioning of Windows Server Operating Systems, on page 135
- Prerequisites for Provisioning ESXi OS to Dell, HP, and UCSM Bare Metal Servers through vMedia, on page 139
- Prerequisites for Provisioning RHEL OS to Dell, HP, and UCSM Bare Metal Servers through vMedia, on page 139
- Prerequisites for Provisioning Windows OS to Dell Bare Metal Servers through vMedia, on page 142
- Prerequisites for Provisioning Windows OS to HP Bare Metal Servers through vMedia, on page 143
- Prerequisites for Provisioning Windows OS to UCSM Bare Metal Servers through vMedia, on page 144

Orchestration Workflow Tasks for PXE/vMedia Boot

The orchestration workflow tasks for PXE/vMedia boot enable you to create workflows within Cisco UCS Director that use the functionality of Cisco UCS Director Bare Metal Agent.

When you include any of the PXE/vMedia boot tasks in an orchestration workflow, the task prepares the Bare Metal Agent environment to receive a PXE install request for a physical or virtual machine.

The values for each input required within the task can be supplied in one of the following ways:

- As user inputs by the user who executes the workflow
- Through outputs from a previous task in the workflow
- Through admin inputs that are assigned by the Cisco UCS Director user who creates the workflow

The following orchestration workflow tasks are available:

- Setup PXE/vMedia Boot task
- Setup PXE/vMedia Boot with BMA Selection task
- Setup Windows PXE/vMedia Boot task
- Monitor PXE/vMedia Boot task
- Remove PXE/vMedia Boot Setup task



Note To set up a PXE/vMedia boot for a Windows Server operating system, you must use the PXE/vMedia boot setup task that is defined specifically for Windows. To set up a PXE/vMedia boot for all other supported operating systems, use the Setup PXE/vMedia Boot task or the Setup PXE/vMedia Boot with BMA Selection task.

You can access these workflow tasks in the **Network Services** area of the Cisco UCS Director Workflow Designer Task Library.

Most inputs and outputs are the same for the Setup PXE/vMedia Boot task, the Setup PXE/vMedia Boot with BMA Selection task, and the Setup Windows PXE/vMedia Boot task, with the following notable exceptions:

- The Setup PXE/vMedia Boot with BMA Selection task has an input field for selecting the target Bare Metal Agent.
- The Setup PXE/vMedia Boot task does not have an option to select the target Bare Metal Agent. This legacy workflow task uses the default Bare Metal Agent as the target Bare Metal Agent.
- The Setup Windows PXE/vMedia boot task has an input field for selecting the target Bare Metal Agent.



Tip For the legacy Setup PXE/vMedia Boot task, the default Bare Metal Agent is the first Bare Metal Agent added. However, you can change the default Bare Metal Agent. See Changing the Default Bare Metal Agent Account, on page 29.

Prerequisites for Workflows with PXE/vMedia Boot Tasks

If you plan to create orchestration workflows that include one or more of the PXE/vMedia boot tasks, your Cisco UCS Director and Cisco UCS Director Bare Metal Agent environment must meet the following prerequisites:

- Cisco UCS Director has been installed and the network interface configured as described in the appropriate Cisco UCS Director installation guide.
- Cisco UCS Director is reachable through a web browser and you can log in.
- Cisco UCS Director Bare Metal Agent has been installed as described in Installing Cisco UCS Director Bare Metal Agent, on page 9.
- The required network/VLAN has been configured as the native, or default, VLAN on the server. For example, for a Cisco UCS server, edit the vNIC template associated with the server and choose the PXE network/VLAN as the native VLAN. You can perform this configuration through an orchestration workflow.
- Each Bare Metal Agent account that you want to use in a workflow has been set up, is active, has a tested connection, and has services that have been enabled and started.

Execution of the Setup PXE/vMedia Boot Tasks

The following Setup PXE/vMedia Boot tasks are available for use in workflows:

- Setup PXE/vMedia Boot task
- Setup PXE/vMedia Boot with BMA Selection task
- Setup Windows PXE/vMedia Boot task

Each time that one of these tasks is executed within a workflow, Cisco UCS Director uses the following values for the inputs to complete a set of configuration files for that particular PXE request:

- Dynamic values received from previous tasks in the workflow or from the user at run-time.
- Static values that you enter when you create the workflow.
- Template configuration files—the ks.cfg Kickstart files—that were created when the chosen operating system was added to Bare Metal Agent. For more information about these files, see Sample Operating System Configuration Template Files, on page 145.

When the workflow is executed, Bare Metal Agent and Cisco UCS Director use the values gathered through the task and perform the following steps to prepare for a PXE installation request on the specified server:

Step	Action	Notes
1	Creates a new directory in the Cisco UCS Director Bare Metal Agent VM that corresponds to the PXE ID request in the `/opt/cnsaroot/web/ks-repository/` directory.	You can view these PXE requests and PXE IDs on the **PXE Boot Requests** tab for a pod in Cisco UCS Director.

Step	Action	Notes
2	Adds the required unique configuration files to the `/opt/cnsaroot/web/ks-repository/`*`PXE_ID`* directory for the PXE installation specific to this request, including the `ks.cfg`, or Kickstart Configuration, file. Depending upon the operating system, other configuration files might be added to this directory, such as the `boot.cfg` file required for an ESXi installation.	For example, to create the customized `ks.cfg` file for the PXE installation,Cisco UCS Director takes the template `ks.cfg` file from the `/opt/cnsaroot/templates/`*`Operating_System`*`/` directory and fills in the variables provided in the Setup PXE/vMedia Boot task. This customized `ks.cfg` file is saved in a directory that corresponds to the PXE ID, such as `/opt/cnsaroot/web/ks-repository/`*`PXE_ID`*.
3	Creates a file corresponding to the MAC address of the server in the `/opt/cnsaroot/pxelinux.cfg/` directory in the Bare Metal Agent VM.	The workflow appends "01-" to the MAC address of the server to create the filename. This file includes information about where the image files are located and is generated through the `pxe.cfg` file in the `/opt/cnsaroot/templates/`*`Operating_System`*`/` directory.

Note Bare Metal Agent automatically creates Windows answer files for the supported operating systems. The same answer file is used for local boot and SAN boot. The Windows installation does not support multi-path SAN boot, but you can use a single path workflow to achieve SAN boot.

Determining the Windows OS Edition

The exact Windows OS edition is required for successful PXE boot of a Windows Server image. You must enter the exact character string used by Windows PE (WinPE). This string is case sensitive. The Windows OS edition follows a consistent naming convention. Some examples of OS editions are as follows:

```
Windows Server 2008 R2 SERVERSTANDARD
Windows Server 2008 R2 SERVERSTANDARDCORE
Windows Server 2008 R2 SERVERENTERPRISE
Windows Server 2008 R2 SERVERENTERPRISECORE
Windows Server 2008 R2 SERVERDATACENTER
Windows Server 2008 R2 SERVERDATACENTERCORE
Windows Server 2008 R2 SERVERWEB
Windows Server 2008 R2 SERVERWEBCORE
Windows Server 2012 SERVERSTANDARD
Windows Server 2012 SERVERSTANDARDCORE
Windows Server 2012 R2 SERVERSTANDARD
Windows Server 2012 R2 SERVERSTANDARDCORE
Windows Server 2012 R2 SERVERDATACENTER
Windows Server 2012 R2 SERVERDATACENTERCORE
```

Procedure

Step 1 Navigate to the extracted ISO files for the Windows OS image.

Step 2 For a Windows 2012 R2 image, navigate to `C:\win2k12r2\sources\install.wim` and use a PowerShell cmdlet to find the edition.

An example of the use of this cmdlet is as follows:

```
PS C:\Windows\system32> Get-WindowsImage -ImagePath
C:\win2k12r2\sources\install.wim
Index       : 1
Name        : Windows Server 2012 R2 SERVERSTANDARDCORE
Description : Windows Server 2012 R2 SERVERSTANDARDCORE
Size        : 6,653,342,051 bytes
Index       : 2
Name        : Windows Server 2012 R2 SERVERSTANDARD
Description : Windows Server 2012 R2 SERVERSTANDARD
Size        : 11,807,528,410 bytes
Index       : 3
Name        : Windows Server 2012 R2 SERVERDATACENTERCORE
Description : Windows Server 2012 R2 SERVERDATACENTERCORE
Size        : 6,653,031,430 bytes
<etcetera>
```

Step 3 For a Windows 2008 image, use the DISM.EXE syntax from the computer on which you installed the WAIK tools.

An example of the use of this syntax is as follows:

```
C:\Program Files\Windows AIK\Tools\>dism
/get-wiminfo /wimfile:e:\\Win2k8r2x64\sources\install.wim
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Details for image : e:\Username_Windowsbits\Win2k8r2x64\sources\install.wim
Index : 1
Name : Windows Server 2008 R2 SERVERSTANDARD
Description : Windows Server 2008 R2 SERVERSTANDARD
Size : 10,510,503,883 bytes
Index : 2
Name : Windows Server 2008 R2 SERVERSTANDARDCORE
Description : Windows Server 2008 R2 SERVERSTANDARDCORE
Size : 3,563,695,852 bytes
<etcetera>
```

Inputs for the Setup PXE/vMedia Boot Task

The following table describes the inputs for the Setup PXE/vMedia Boot task. Because the information for one or more of these inputs can be obtained from a previous task or from a user at run-time, the values for these inputs can be dynamic and change with each execution of the workflow.

Note For legacy Setup PXE Boot tasks, the default Bare Metal Agent is the first Bare Metal Agent added. However, you can change the default Bare Metal Agent. See Changing the Default Bare Metal Agent Account, on page 29.

Important The host name specified in the **Server Host Name** field in the task input screen is correctly applied to the ESXi host after successful deployment of ESXi 8 or ESXi 9 OS in the following scenarios:

- When **Secure Boot is disabled**, and the IP Configuration Type is **Static** or **DHCP**.
- When **Secure Boot is enabled**, and the IP Configuration Type is **Static**.

In these cases, the configured host name is successfully passed to the ESXi host and is displayed when you log in to the ESXi host after deployment.

The host name specified in the **Server Host Name** field in the task input screen is not retained to the ESXi host after successful deployment of ESXi 8 or ESXi 9 OS when **Secure Boot** is enabled and **DHCP** is selected as the **IP Configuration Type** in the task input screen. To configure the host name for the ESXi host after a successful ESXi deployment, log in to the specific ESXi host console and execute the following commands:

```
esxcli system hostname set --host=<HOST_NAME>
esxcli system hostname set --fqdn=<HOST_NAME>.domain.org
/etc/init.d/hostd restart
```

Table 6: Setup PXE/vMedia Boot Task Inputs

Input	Description
Network Boot Manager drop-down list	Choose the network boot manager that you want to use. Choose one of the following: • PXE—PXE supports only TFTP protocol • iPXE-BIOS—iPXE-BIOS supports HTTP protocol by default • iPXE-UEFI—iPXE-UEFI supports TFTP protocol by default. However, you can modify the `ipxe-uefi.cfg` to support the HTTP protocol. See Setting Up UEFI as Network Boot Manager. The default option is **PXE**.
OS Type drop-down list	The OS image that you want this PXE or iPXE boot request to install on the server. The drop-down list includes all OS images that have been created and are available for PXE or iPXE installation.
Server MAC Address	The MAC address of the server that requires the PXE or iPXE installation. This input is typically mapped to the MAC address output from the Create UCS Service Profile task.

Input	Description
IP Configuration Type drop-down list	Choose the configuration type. Choose one of the following: • Static • DHCP
Server IP Address field	The IP Address that you want to assign to the server. This IP address is given to the server after the PXE or iPXE installation process is complete, and is the final IP address for the server. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list. This IP address can be on a different network or subnet than the PXE or iPXE network or Management network that you configured for Bare Metal Agent.
Server Net Mask field	The subnet mask that you want to assign to the server after the PXE or iPXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Host Name field	The hostname that you want to assign to the server after the PXE or iPXE installation process is complete.
Server Gateway field	The default gateway IP address that you want to assign to the server after the PXE or iPXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Name Server field	(Optional) The DNS server that you want the server to use. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list. If no DNS server is required, leave this input blank.
Management VLAN field	(Optional) The VLAN ID that you want to assign to the management interface on the server after the PXE or iPXE installation process is complete. This setting is typically used in ESX/ESXi deployments where VLAN tagging is prevalent on the virtual switch. It sets the VLAN ID for tagging on the management vmkernel port.
Root Password field	The password that you want to assign to the root user on the server.
Timezone field	The time zone in which you want to configure the server.

Input	Description

Additional Parameters interface	Interface to add, edit, or delete single-line parameters that are used additionally for the PXE or iPXE boot request. You can add multiple parameters using this interface.
	
	To add an additional parameter, click (+). In the **Add Additional Parameter** box that appears, enter the parameter name and the value for the parameter. Use the **Edit** button to modify the parameter name or its value. Use the **Delete** button to delete a parameter.
	
	For example, you can use an additional parameter to customize the ks.cfg file template and provide a value for the parameter here. The parameter is then updated with the appropriate value in the ks.cfg file template.
	
	Suppose the existing firewall configuration in ks.cfg is as follows:
	
	`# Firewall configuration`
	`firewall --disabled`
	
	You can customize the configuration as following:
	
	`# Firewall configuration`
	`firewall —$FIREWALL_CONFIG`
	
	In the Additional Parameter interface here, you can include `FIREWALL_CONFIG` as the parameter name and provide the value as `disabled`. The value of the parameter can also be mapped to a user input `${variable}`. This parameter is updated with the appropriate value in the ks.cfg file template.
	
	The ks.cfg file templates used by Bare Metal Agent are available in `/opt/cnsaroot/templates/`*`IMAGE_CATALOG_NAME`*`/ks.cfg`. For example, the ks.cfg file for CentOS 6.0 is available in `/opt/cnsaroot/templates/CentOS60/ks.cfg`
	
	Note
	In the template files to retain dollar sign ($) and backslash (\), you must include a backslash (\) before the character.

Inputs for the Setup PXE/vMedia Boot with BMA Selection Task

The following table describes the inputs for the Setup PXE/vMedia Boot with BMA Selection task. Because the information for one or more of these inputs can be obtained from a previous task or from a user at run-time, the values for these inputs can be dynamic and change with each execution of the workflow.

Note The Setup PXE/vMedia Boot with BMA Selection task does not support the Windows OS and does not accept inputs for that OS.



Important The host name specified in the **Server Host Name** field in the task input screen is correctly applied to the ESXi host after successful deployment of ESXi 8 or ESXi 9 OS in the following scenarios:

- When **Secure Boot is disabled**, and the IP Configuration Type is **Static** or **DHCP**.
- When **Secure Boot is enabled**, and the IP Configuration Type is **Static**.

In these cases, the configured host name is successfully passed to the ESXi host and is displayed when you log in to the ESXi host after deployment.

The host name specified in the **Server Host Name** field in the task input screen is not retained to the ESXi host after successful deployment of ESXi 8 or ESXi 9 OS when **Secure Boot** is enabled and **DHCP** is selected as the **IP Configuration Type** in the task input screen. To configure the host name for the ESXi host after a successful ESXi deployment, log in to the specific ESXi host console and execute the following commands:

```
esxcli system hostname set --host=<HOST_NAME>
esxcli system hostname set --fqdn=<HOST_NAME>.domain.org
/etc/init.d/hostd restart
```

Table 7: Setup PXE/vMedia Boot with BMA Selection Task Inputs

Input	Description
Network Boot Manager drop-down list	Choose the network boot manager that you want to use. Choose one of the following: • PXE—PXE supports only TFTP protocol • iPXE-BIOS—iPXE-BIOS supports HTTP protocol by default • iPXE-UEFI—iPXE-UEFI supports TFTP protocol by default. However, you can modify the `ipxe-uefi.cfg` to support the HTTP protocol. See Setting Up UEFI as Network Boot Manager. The default option is **PXE**.
Target BMA field	The Bare Metal Agent accounts that have been added to Cisco UCS Director and are available for use.
OS Type drop-down list	The OS image that you want this PXE or iPXE boot request to install on the server. The drop-down list includes all OS images that have been created and are available for PXE or iPXE installation.
Server MAC Address	The MAC address of the server that requires the PXE or iPXE installation. This input is typically mapped to the MAC address output from the Create UCS Service Profile task.
IP Configuration Type drop-down list	Choose the configuration type. Choose one of the following: • Static • DHCP

Input	Description
Server Address field	The IP Address that you want to assign to the server. This IP address is given to the server after the PXE or iPXE installation process is complete and is the final IP address for the server. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list. This IP address can be on a different network or subnet than the PXE or iPXE network or Management network that you configured for Bare Metal Agent.
Server Net Mask field	The subnet mask that you want to assign to the server after the PXE or iPXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Host Name field	The hostname that you want to assign to the server after the PXE or iPXE installation process is complete.
Server Gateway field	The default gateway IP address that you want to assign to the server after the PXE or iPXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Name Server field	(Optional) The DNS server that you want the server to use. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list. If no DNS server is required, leave this input blank.
Management VLAN field	(Optional) The VLAN ID that you want to assign to the management interface on the server after the PXE or iPXE installation process is complete. This setting is typically used in ESX/ESXi deployments where VLAN tagging is prevalent on the virtual switch. It sets the VLAN ID for tagging on the management vmkernel port.
Root Password field	The password that you want to assign to the root user on the server.
Timezone field	The time zone in which you want to configure the server.

Input	Description

Additional Parameters interface	Interface to add, edit, or delete single-line parameters that are used additionally for the PXE or iPXE boot request. You can add multiple parameters using this interface.
	
	To add an additional parameter, click (+). In the **Add Additional Parameter** box that appears, enter the parameter name and the value for the parameter. Use the **Edit** button to modify the parameter name or its value. Use the **Delete** button to delete a parameter.
	
	For example, you can use an additional parameter to customize the ks.cfg file template and provide a value for the parameter here. The parameter is then updated with the appropriate value in the ks.cfg file template.
	
	Suppose the existing firewall configuration in ks.cfg is as follows:
	
	`# Firewall configuration`
	`firewall --disabled`
	
	You can customize the configuration as following:
	
	`# Firewall configuration`
	`firewall —$FIREWALL_CONFIG`
	
	In the Additional Parameter interface here, you can include `FIREWALL_CONFIG` as the parameter name and provide the value as `disabled`. The value of the parameter can also be mapped to a user input `${variable}`. This parameter is updated with the appropriate value in the ks.cfg file template.
	
	The ks.cfg file templates used by Bare Metal Agent are available in `/opt/cnsaroot/templates/`*`IMAGE_CATALOG_NAME`*`/ks.cfg`. For example, the ks.cfg file for CentOS 6.0 is available in `/opt/cnsaroot/templates/CentOS60/ks.cfg`
	
	Note
	In the template files to retain dollar sign ($) and backslash (\), you must include a backslash (\) before the character.

Inputs for the Setup Windows PXE/vMedia Boot Task

The following table describes the inputs for the Setup Windows PXE/vMedia Boot task. Because the information for one or more of these inputs can be obtained from a previous task or from a user at run-time, the values for these inputs can be dynamic and change with each execution of the workflow.

Note Bare Metal Agent automatically creates Windows answer files for supported Windows operating systems. You can use the same answer file for local boot and SAN boot. The Windows installation does not support multi-path SAN boot, but you can use a single path workflow to achieve SAN boot.

Table 8: Setup Windows PXE/vMedia Boot Task Inputs

Input	Description
Network Boot Manager drop-down list	Choose the network boot manager that you want to use. Choose one of the following: • PXE—PXE supports only TFTP protocol • iPXE-BIOS—iPXE-BIOS supports HTTP protocol by default • iPXE-UEFI—iPXE-UEFI supports TFTP protocol by default. However, you can modify the `ipxe-uefi.cfg` to support the HTTP protocol. See Setting Up UEFI as Network Boot Manager. The default option is **PXE**.
Target BMA field	The Bare Metal Agent accounts that have been added to Cisco UCS Director and are available for use.
OS Type drop-down list	The OS image that you want this PXE/vMedia boot request to install on the server. The drop-down list includes all OS images that have been created in Bare Metal Agent and are available for PXE installation.
Enable Hyper-V role for Windows Server 2016 check box	Check this check box if you want to enable Hyper-V role for Windows server 2016. This field is displayed when you choose the Windows 2016(x64) option in the **OS Type** drop-down list. **Note** If you want to enable Hyper-V on Windows 2012 and Windows 2012 R2, you should add the **`<selection name="Microsoft-Hyper-V" state="true" />`** in the answer files available in BMA (under <package> in <servicing> node). The answers files for Windows 2012 R2 and Windows 2012 are available in `/opt/cnsaroot/templates/Win2k12R2x64/autounatted.xml` and `/opt/cnsaroot/templates/Win2k12x64/autounattend.xml` location respectively.
Server MAC Address	The MAC address of the server that requires the PXE installation. This input is typically mapped to the MAC address output from the Create UCS Service Profile task.
OS Flavor Name field	The Windows OS edition name is required for successful PXE/vMedia boot of a Windows Server image. You must enter the exact character string used by Windows PE (WinPE). This string is case sensitive. For example, enter SERVERSTANDARD or SERVERENTERPRISE. For more information, see Determining the Windows OS Edition, on page 118. This value is used in the Windows answer file, which requires the correct name of the edition for the image installation process. The OS edition might be different for each type of Windows OS image.
Organization Name field	The name of the organization that is associated with the OS product key. This value is used by the Windows answer file. It could be a division within your company or the company name.
Product Key field	The product key (sometimes called the license key or software key) for the OS.

Input	Description
Host Name field	The hostname that you want to assign to the server after the PXE installation process is complete. Make sure the name complies with NetBIOS name restrictions.
Administrator Password field	The password that you want to assign to the administrative user on the server.
Confirm Password field	The password that you want to assign to the administrative user on the server.
IP Configuration Type drop-down list	Choose the configuration type. Choose one of the following: • Static • DHCP
Server Address field	The IP Address that you want to assign to the server. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Net Mask field	The subnet mask that you want to assign to the server after the PXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Gateway field	The default gateway IP address that you want to assign to the server after the PXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Name Server field	The DNS server that you want the server to use. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Timezone field	The time zone in which you want to configure the server.
Disk Partition Size (GB) field	The size, in GB, of the partition designated for the OS.

Input	Description
Additional Parameters field	Interface to add, edit, or delete single-line parameters that are used additionally for the PXE/vMedia boot request. You can add multiple parameters using this interface. To add a parameter, click (+). In the **Add Additional Parameter** box that appears, enter the parameter name and the value for the parameter. Use the **Edit** button to modify the parameter name or its value. Use the **Delete** button to delete a parameter. For example, you can use parameters to provide the minimum requirements for the Windows answer file. You can define parameters and their values to enhance the answer file to meet the requirements of your environment. These parameters are updated with the appropriate values in the Answer file template. The answer file templates used by Bare Metal Agent are available in the following locations: • Windows 2012 R2 x64—`/opt/cnsaroot/templates/Win2k12R2x64/autounattend.xml` • Windows 2012 x64—`/opt/cnsaroot/templates/Win2k12x64/autounattend.xml` • Windows 2008 R2 x64—`/opt/cnsaroot/templates/Win2k8R2x64/autounattend.xml` **Note** In the template files to retain dollar sign ($) and backslash (\), you must include a backslash (\) before the character.

Outputs from the Setup PXE/vMedia Boot Task and Setup Windows PXE/vMedia Boot Task

The following table describes the outputs from both the Setup PXE/vMedia Boot task and the Setup Windows PXE/vMedia Boot task.

Table 9: Setup PXE/vMedia Boot and Windows PXE/vMedia Boot Task Outputs

Input	Description	Type
OUTPUT_PXE_BOOT_ID	PXE Boot ID that was created for setup PXE boot request.	gen_text_input
OUTPUT_HOST_IP_ADDRESS	Host IP Address resolved by the Setup PXE task.	gen_text_input

Creating a PXE Boot Request in Cisco UCS Director

Before you begin

Create the OS image template that you want to use for the PXE boot in Bare Metal Agent.

Procedure

Step 1 Choose **Administration** > **Physical Accounts**.

Step 2 On the **Physical Accounts** page, click **Bare Metal Agents**.

Step 3 Click the row for the Bare Metal Agent account in which you want to set up the PXE boot request.

Step 4 From the **More Actions** drop-down list, click **View Details**.

Step 5 Click **PXE Boot Requests**.

Note You can also create a PXE Boot Request by choosing **Physical** > **Compute** and navigating to the pod, in the left pane, in which you want to set up the PXE boot request.

Step 6 Click **Add PXE Request**.

Step 7 On the **Add PXE Boot Request** screen, complete the following fields:

Name	Description
Network Boot Manager drop-down list	Choose the network boot manager that you want to use. Choose one of the following: • PXE—PXE supports only TFTP protocol • iPXE-BIOS—iPXE-BIOS supports HTTP protocol by default • iPXE-UEFI—iPXE-UEFI supports TFTP protocol by default. However, you can modify the `ipxe-uefi.cfg` to support the HTTP protocol. See Setting Up UEFI as Network Boot Manager. The default option is **PXE**.
Server MAC Address field	The MAC address of the server that requires the PXE or iPXE installation.
Host Name field	The hostname to be assigned to the server after the PXE or iPXE installation process is complete.
Root Password field	The password that you want to assign to the root user on the server. You need to re-enter this password in the next field to confirm it. **Note** Apply your organization's guidelines for maintaining the security of this password.

Name	Description
PXE Request for Windows check box	Check this check box if the PXE boot request is for a Windows OS. After you check this check box, a set of Windows-specific fields appears in this dialog box.
IP Configuration Type drop-down list	Choose the configuration type. Choose one of the following: • Static • DHCP
Server Address field	The IP Address that you want to assign to the server. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Net Mask field	The subnet mask that you want to assign to the server after the PXE or iPXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Gateway field	The default gateway IP address that you want to assign to the server after the PXE or iPXE installation process is complete. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
Server Name Server field	The DNS server that you want the server to use. This field is displayed only when you select the Static option in the **IP Configuration Type** drop-down list.
OS Type drop-down list	Choose the OS image that you want this PXE or iPXE boot request to install on the server. The drop-down list includes all OS image templates that have been created and are available for PXE or iPXE installation. This drop-down list displays in a different location in the dialog box, depending upon whether you check the **PXE Request for Windows** check box.
Management VLAN field	(Optional) The VLAN ID that you want to assign to the management interface on the server after the PXE or iPXE installation process is complete. This setting is used in ESX/ESXi deployments where VLAN tagging is implemented on the virtual switch. It sets the VLAN ID for tagging on the management vmkernel port.
OS Flavor Name field	(Required for a Windows OS only) The Windows OS edition name is required for successful PXE or iPXE boot of a Windows Server image. You must enter the exact character string used by Windows PE (WinPE). This string is case sensitive. For example, enter SERVERSTANDARD or SERVERENTERPRISE. For more information, see Determining the Windows OS Edition, on page 118. This value is used in the Windows answer file, which requires the correct name of the edition for the image installation process. The OS edition name might be different for each type of Windows OS image.
Organization Name field	(Required for a Windows OS only) The name of the organization that is associated with the OS product key. This value is used by the Windows answer file. It could be a division within your company or the company name.

Name	Description
Product Key field	(Required for a Windows OS only) The product key (sometimes called the license key or software key) for the OS.
Timezone drop-down list	Choose the time zone in which you want to configure the server.
Disk Partition Size (GB) field	(Required for a Windows OS only) The size, in GB, of the partition designated for the OS.
Additional Parameters interface	Interface to add, edit, or delete single-line parameters that are used additionally for the PXE or iPXE boot request. You can add multiple parameters using this interface. To add a parameter, click (+). In the **Add Additional Parameter** box that appears, enter the parameter name and the value for the parameter. Use the **Edit** button to modify the parameter name or its value. Use the **Delete** button to delete a parameter. For example, for a Windows OS, you can use parameters to provide the minimum requirements for the Windows answer file. You can define parameters and their values to enhance the answer file to meet the requirements of your environment. These parameters are updated with the appropriate values in the Answer file template. The answer file templates used by Bare Metal Agent are available in the following locations: • Windows 2012 R2 x64—`/opt/cnsaroot/templates/Win2k12R2x64/autounattend.xml` • Windows 2012 x64—`/opt/cnsaroot/templates/Win2k12x64/autounattend.xml` • Windows 2008 R2 x64—`/opt/cnsaroot/templates/Win2k8R2x64/autounattend.xml`
Server IP Address field	The static IP address that you want to assign to the server. This IP address is given to the server after the PXE or iPXE installation process is complete, and is the final IP address for the server. This IP address can be on a different network or subnet than the PXE network or Management network that you configured for Bare Metal Agent.
Network Mask field	The subnet mask that you want to assign to the server after the PXE or iPXE installation process is complete.
Gateway field	The default gateway IP address that you want to assign to the server after the PXE or iPXE installation process is complete.
Server Name Server field	The DNS server that you want the server to use. If no DNS server is required, leave this field blank.
Target BMA drop-down list	Choose the Bare Metal Agent that you want to use for this PXE or iPXE boot request. The Bare Metal Agent that you choose determines which OS images are available for the PXE or iPXE boot request.

Step 8 Click **Submit**.

Information about the new PXE Boot Request will appear as a new row in the **PXE Boot Request**, displaying the *ID* assigned to this request. The information includes the current *Status* of this request.

What to do next

After the PXE or iPXE boot request is in the Submitted state, you must set up the PXE or iPXE environment to create the Cisco UCS Director configuration files. You can activate a PXE or iPXE boot request that has a status of Submitted by selecting it and clicking **Setup PXE Environment**.

Viewing the PXE Request Configuration Files

Procedure

Step 1 Choose **Physical** > **Compute**.
Step 2 Choose **Administration** > **Physical Accounts**.
Step 3 On the **Physical Accounts** page, click **Bare Metal Agents**.
Step 4 Click the row for the Bare Metal Agent account in which you want to set up the PXE boot request.
Step 5 From the **More Actions** drop-down list, click **View Details**.
Step 6 Click **PXE Boot Requests**.

Note You can also create a PXE Boot Request by choosing **Physical > Compute** and navigating to the pod, in the left pane, in which you want to set up the PXE boot request.

Step 7 Click the row for the PXE boot request for which you want to view the configuration file details.
Step 8 From the **More Actions** drop-down list, click **View Configuration Files**.
Step 9 Choose the configuration file type from the **Select the file** drop-down list

The **View configuration files** window displays the configuration details of the selected file for a PXE request.

PXE Boot States

The following are the PXE boot states for PXE boot requests in Cisco UCS Director:

- Submitted—The PXE boot request has been submitted to Cisco UCS Director.
- Environment Setup—A Submitted PXE boot request has been transferred to Bare Metal Agent and that the environment required to perform a PXE boot is ready in Bare Metal Agent.

- In Progress—The bare metal server has communicated with Bare Metal Agent and the PXE configuration files and image files are being downloaded.
- Ready—The PXE boot process is complete. The server has booted with the newly installed operating system and Bare Metal Agent received a success notification from the server that it is ready.
- Failed—The PXE boot process started, but Bare Metal Agent did not receive a success notification from the server after the defined wait period expired.
- Archived—The PXE Request task included a rollback or delete.

Monitor PXE/vMedia Boot Setup Task

When included in an orchestration workflow, the Monitor PXE/vMedia Boot task monitors a particular PXE ID request until

- The PXE boot is ready.
- The maximum number of hours specified is reached before the PXE boot is ready.

Inputs for the Monitor PXE Boot Task

The following table describes the inputs for the Monitor PXE Boot Task:

Table 10: Monitor PXE Boot Task Inputs

Input	Description
PXE Boot Id	The ID of the PXE boot request that you want to monitor through the workflow.
Max Wait time (Hours)	The maximum length of time, in hours, that you want the task to wait for the PXE boot request to be ready.

Outputs from the Monitor PXE Boot Task

The Monitor PXE Boot task has no outputs.

Remove PXE/vMedia Boot Setup Task

When included in an orchestration workflow, the Remove PXE/vMedia Boot Setup task removes the directory and files that are created by the Setup PXE/vMedia Boot task for a particular PXE ID request.

Inputs for the Remove PXE Boot Setup Task

The following table describes the inputs for the Remove PXE Boot Setup Task.

Table 11: Remove PXE Boot Setup Task Inputs

Input	Description
PXE Boot Id	The ID of the PXE boot request for which you want to remove the setup directory and files.

Outputs from the Remove PXE Boot Setup Task

The Remove PXE Boot Setup task has no outputs.

Injecting Drivers When Installing RHEL 7 or CentOS 7 on UCS Modular Servers

When you install RHEL 7 or CentOS 7 on the UCS servers, manually inject drivers through the PXE.cfg file. The PXE.cfg file is available in the following location: `/opt/cnsaroot/templates/(RHEL 7/CentOS 7 OS Catalog name).`

The default PXE.cfg file contains the following line:

```
append initrd=images/(RHEL 7/CentOS 7 OS Catalog name)/isolinux/initrd.img ramdisk_size=9216
 noapic acpi=off ip=dhcp ks=$PXE_KS_URL
ksdevice= inst.repo=http://$PXE_NATIVE_WEBSERVER/(RHEL 7/CentOS 7 OS Catalog name)
net.ifnames=0 biosdevname=0
```

Note Here RHEL 7/CentOS 7 OS Catalog name is the name of the OS image provided in the ISO extractor script while creating the RHEL 7 or CentOS 7 OS image template in Bare Metal Agent.

To inject the drivers, update the location of the drivers in the PXE.cfg file by updating the line as shown below:

```
append initrd=images/(RHEL 7/CentOS 7 OS Catalog name)/isolinux/initrd.img ramdisk_size=9216
 noapic acpi=off ip=dhcp ks=$PXE_KS_URL
ksdevice= inst.repo=http://$PXE_NATIVE_WEBSERVER/(RHEL 7/CentOS 7 OS Catalog name)
inst.dd=http://$PXE_NATIVE_WEBSERVER/
(RHEL 7/CentOS 7 OS Catalog name )/(name of the driver disk) net.ifnames=0 biosdevname=0
```

The driver disk should be in the ISO image format and placed in the following location: `/opt/cnsa/images/(RHEL 7/CentOS 7 OS Catalog name)/`

Note

- Download the driver ISO image from the UCS Servers download page on the Cisco website.
- The parameter inst.dd helps load the driver images during PXE install.

Simultaneous Provisioning of Windows Server Operating Systems

You can use Bare Metal Agent to run parallel workflows and simultaneously deploy Windows server images on multiple bare metal servers.

Prerequisites for Simultaneous Deployment

To ensure that you can perform simultaneous deployment of Windows Server operating system images, you must perform the appropriate configuration required for the versions of the operating system that are described in the following topics, including:

- Adding the PowerShell packages to the `WinPE.wim` file
- Updating `startnet.cmd` with the IP addresses and other information required for your environment

Bare Metal Workflows

You do not need to make any changes to your existing bare metal provisioning workflows to support simultaneous deployment of Windows server operating systems.

A PXE boot task in a workflow can only provision one server with a Windows operating system. You cannot use a single PXE boot task to provision multiple servers, but you can execute PXE boot tasks simultaneously multiple times.

Maximum Number of Simultaneous Deployments

The maximum number of simultaneous deployments is dependent upon the bandwidth of your TFTP and PXE networks.

Minimum Supported Level of Bare Metal Agent

Simultaneous deployment of Windows server operating systems requires a minium of Bare Metal Agent, Release 5.4. It is not supported in earlier releases of Bare Metal Agent.

Files and Folders Used In Simultaneous Deployment

The following files and folders are used during simultaneous deployment of Windows operating systems:

PXElinux.cfg File

The `PXElinux.cfg` file contains the MAC addresses for each of the servers and points to the `WinPE.wim` file.

Samba Folder

The `/samba` folder contains a folder for each of the following items. Additional information about the script and folder is provided below.

- Windows images to be deployed on the bare metal servers

- `EnRoute.ps1` script
- `as-repository` folder

AS-Repository Folder

The `/samba/as-repository` folder contains a folder for each MAC address of the servers for which a Windows operating is to be deployed. The PXE boot task creates and stores a separate Windows answer file for each of these servers in the appropriate MAC address folder. This folder might not be created until after the first PXE boot workflow is run.

EnRoute.ps1 Script

The `EnRoute.ps1` script determines which Windows answer file in the `as-repository` folder belongs to the server that is being provisioned. If desired, you can customize this script. However, when you add the Bare Metal Agent to Cisco UCS Director, the script in the `as-repository` folder will revert to the default script without the customizations.

Windows Answer File

The Windows answer file contains settings and values that are used during the deployment of a Windows operating system. This answer file is typically named unattend.xml. During simultaneous deployment, a separate Windows answer file is created in each MAC address folder and then sent to the server to be used during the Windows operating system setup.

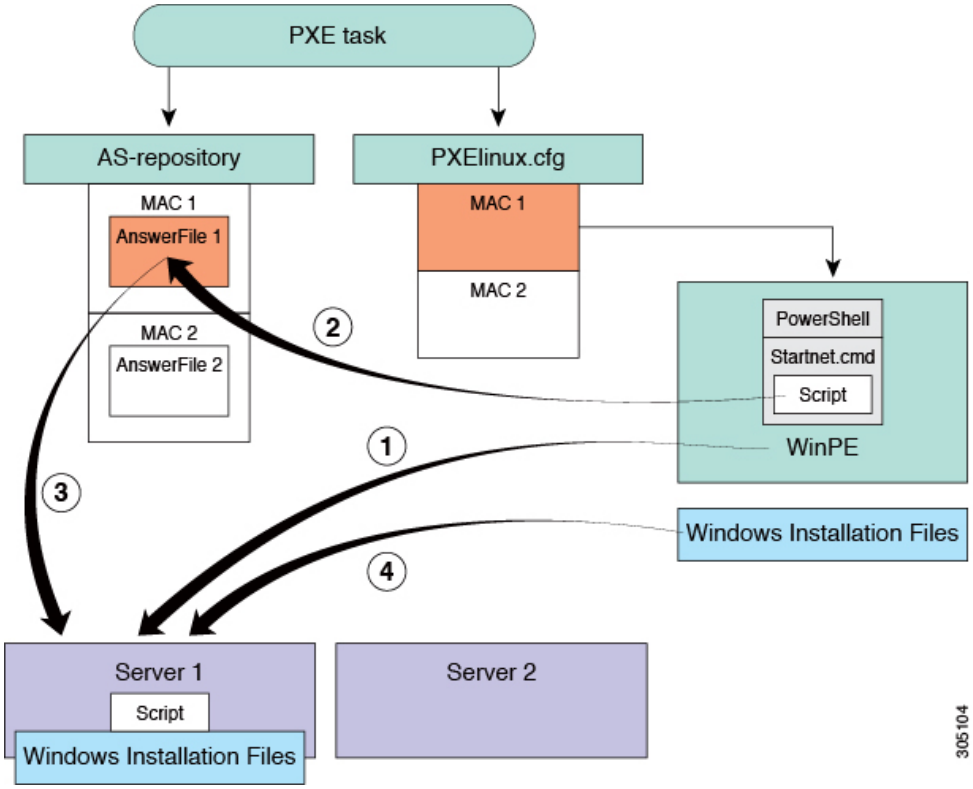
When the installation is successfully completed, the name of the answer file is changed to include "Completed."

For more information, see the Microsoft TechNet article on Understanding Answer Files.

Example: Simultaneous Deployment of Windows Server Operating Systems

This example describes what actions Bare Metal Agent performs when you execute two workflows at the same time, with each workflow designed to provision a bare metal server with a Windows operating system. The illustrations below describe how server 1 and server 2 are provisioned when the PXE tasks in the workflows are executed.

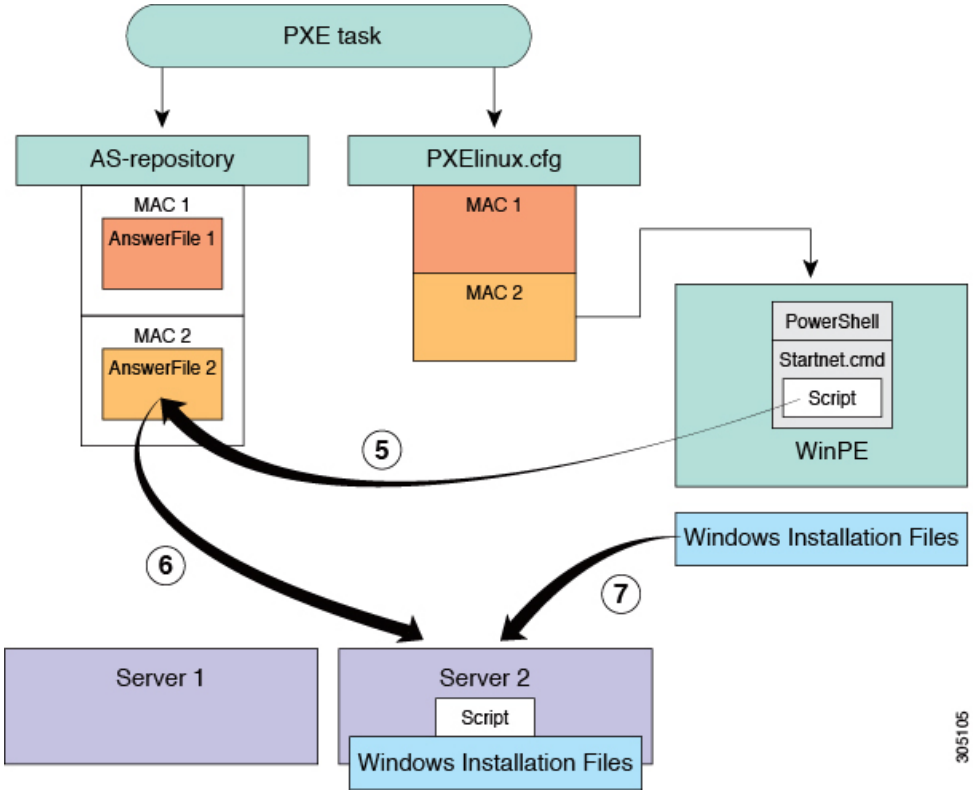
Figure 3: Server 1 Provisioning



When the PXE boot task is executed in the workflow that provisions Server 1, the steps shown in the above illustration occur:

Step	Action
1	Server 1 boots up. The `WinPE.wim` file, together with its PowerShell packages and `Startnet.cmd`, is copied to the server.
2	The `Startnet.cmd` calls the `EnRoute.ps1` script from the `/samba` folder on the Bare Metal Agent VM. A folder is created under `/samba/as-repository/` with MAC address of Server 1 as its name, for example, `/samba/as-repository/MAC 1`, and a Windows answer file is placed into that folder.
3	The `EnRoute.ps1` script compares the MAC address on Server 1 with the MAC address folders available in the `/samba/as-repository` folder and finds the Windows answer file for Server 1 in the `/samba/as-repository/MAC 1` folder.
4	Using the Windows answer file, the appropriate Windows operating system (shown as Windows installation files) is installed on Server 1. When the installation is successfully completed, the name of the answer file is changed to include "Completed."

Figure 4: Server 2 Provisioning



At the same time as Server 1 is being provisioned, when the PXE boot task is executed in the workflow that provisions Server 2, the steps shown in the above illustration occur:

Step	Action
5	Server 2 boots up. The `WinPE.wim` file, together with its PowerShell packages and `Startnet.cmd`, is copied to the server. The `Startnet.cmd` calls the `EnRoute.ps1` script from the `/samba` folder on the Bare Metal Agent VM. A folder is created under `/samba/as-repository/` with MAC address of Server 2 as its name, for example, `/samba/as-repository/MAC 2`, and a Windows answer file is placed into that folder.
6	The `EnRoute.ps1` script compares the MAC address on Server 2 with the MAC address folders available in the `/samba/as-repository` folder and finds the Windows answer file for Server 2 in the `/samba/as-repository/MAC 2` folder.
7	Using the Windows answer file, the appropriate Windows operating system (shown as Windows installation files) is installed on Server 2. When the installation is successfully completed, the name of the answer file is changed to include "Completed."

Prerequisites for Provisioning ESXi OS to Dell, HP, and UCSM Bare Metal Servers through vMedia

Before proceeding with the execution of workflow for provisioning ESXi OS for Dell, HP, and UCSM bare metal servers, the following prerequisites must be met:

Procedure

Modify the **boot.cfg** and **boot-uefi.cfg** configuration files. For more information, see Viewing and Editing the OS Configuration File Details.

a. In the **Content** field, enter 5 (seconds) for the **timeout** field.

b. If the **kernal** and **modules** have a forward slash (/), remove the forward slash (/) in the **prefix**.

c. If the **kernel** and **modules** do not have the forward slash (/), add the forward slash (/) in the **prefix**.

```
bootstate=0
title=Loading ESXi installer
timeout=5
prefix=/
kernel=b.b00
kernelopt=runweasel ks=cdrom:/KS.CFG loglevel=debug
modules=jumpstrt.gz --- useropts.gz --- features.gz --- k.b00 --- uc_intel.b00 --- uc_amd.b00 --
```

What to do next

Execute the required ESXi OS provisioning workflow tasks to provision the ESXi OS for the Dell, HP, and UCSM bare metal servers.

Prerequisites for Provisioning RHEL OS to Dell, HP, and UCSM Bare Metal Servers through vMedia

Before proceeding with the execution of workflow for provisioning RHEL OS for Dell and HP bare metal servers, the following prerequisites must be met:

Procedure

Step 1 Modify the **ks.cfg** and **ks-uefi.cfg** configuration files. For more information, see Viewing and Editing the OS Configuration File Details.

a. For Dell and HP bare metal servers, in the **Content** field, add the **cdrom** line and comment the **repo** and **url** lines as shown below.

```
authselect  --useshadow  --enablemd5
clearpart --all --initlabel
reboot
.........
text
cdrom
#repo --name="AppStream" --baseurl=http://$PXE_NATIVE_WEBSERVER/RHEL9.4/AppStream
.....
#url --url=http://$PXE_NATIVE_WEBSERVER/RHEL9.4
$PXE_DHCP_IP_TYPE network --bootproto=dhcp --device=link --activate --hostname=$PXE_NAME --onboot=on
$PXE_STATIC_IP_TYPE network --bootproto=static --device=link --activate --ip=$PXE_IP
--netmask=$PXE_NETMASK --gateway=$PXE_GATEWAY --hostname=$PXE_NAME
```

b. For UCSM bare metal servers, in the **Content** field, add the **cdrom** line and comment the **repo** and **url** lines as shown below.

```
authselect  --useshadow  --enablemd5
clearpart --all --initlabel
reboot
.........
text
cdrom
#repo --name="AppStream" --baseurl=http://$PXE_NATIVE_WEBSERVER/RHEL9.4/AppStream
.....
#url --url=http://$PXE_NATIVE_WEBSERVER/RHEL9.4
## Notifying back to Cisco UCS Director once the blade is up ##
wget http://$PXE_WEBSERVER_MGMT_VLAN_IP/$PXEID/notify.html
%end
```

Step 2 Log in to BMA CLI with bmaadmin credentials using an SSH or SFTP client.

Step 3 Execute the following command to create a temporary folder to copy the ISO file content.

```
sudo mkdir -p /opt/cnsaroot/web/RHEL/
```

Note Make a note of the path **opt/cnsaroot/web/RHEL/** as it is used as an input for a workflow.

Step 4 Execute the following command to copy the content from the provisioned ISO file (for example, rhel9v4) into the temporary folder.

```
sudo cp -r -u /opt/cnsaroot/images/{os catalog name}/. /opt/cnsaroot/web/RHEL/
```

Step 5 Execute the following command to provide the write permission on the ISO file.

```
sudo chown -R bmaadmin:bmaadmin /opt/cnsaroot/web/RHEL/
```

```
sudo chmod -R ug+w /opt/cnsaroot/web/RHEL/
```

Step 6 Open the **grub.cfg** file from the location **/opt/cnsaroot/web/RHEL/EFI/BOOT**.

Step 7 Perform the following changes to the **grub.cfg** file:

a. Enter 0 for the **set default** field.

b. Enter 5 (seconds) for the **set timeout** field.

c. Add **inst.ks=cdrom:/ks.cfg net.ifnames=0** to the menu items.

```
set default="0"

function load_video {
```

```
  insmod efi_gop
  insmod efi_uga
  insmod video_bochs
  insmod video_cirrus
  insmod all_video
}

load_video
set gfxpayload=keep
insmod gzio
insmod part_gpt
insmod ext2
set timeout=5
### END /etc/grub.d/00_header ###

search --no-floppy --set=root -l 'RHEL-9-4-0-BaseOS-x86_64'

### BEGIN /etc/grub.d/10_linux ###
menuentry 'Install Red Hat Enterprise Linux 9.4' --class fedora --class gnu-linux --class gnu
--class os {
       linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-9-4-0-BaseOS-x86_64
inst.ks=cdrom:/ks.cfg net.ifnames=0 quiet
       initrdefi /images/pxeboot/initrd.img
}
menuentry 'Test this media & install Red Hat Enterprise Linux 9.4' --class fedora --class gnu-linux
 --class gnu --class os {
      linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-9-4-0-BaseOS-x86_64 rd.live.check
 inst.ks=cdrom:/ks.cfg net.ifnames=0 quiet
       initrdefi /images/pxeboot/initrd.img
}
submenu 'Troubleshooting -->' {
        menuentry 'Install Red Hat Enterprise Linux 9.4 in text mode' --class fedora --class
gnu-linux --class gnu --class os {
                linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-9-4-0-BaseOS-x86_64
inst.text quiet
                initrdefi /images/pxeboot/initrd.img
        }
        menuentry 'Rescue a Red Hat Enterprise Linux system' --class fedora --class gnu-linux
--class gnu --class os {
                linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-9-4-0-BaseOS-x86_64
inst.rescue quiet
                initrdefi /images/pxeboot/initrd.img
        }
}
```

Note Make a note of the label **(RHEL-9-4-0-BaseOS-x86_64)** as it is used as an input for the workflow.

What to do next

Execute the required HP or Dell RHEL OS provisioning workflow tasks to provision the RHEL OS for the HP or Dell bare metal servers.

Prerequisites for Provisioning Windows OS to Dell Bare Metal Servers through vMedia

Before executing a workflow to provision Windows OS on a Dell bare metal server, ensure that the following prerequisites are met:

Procedure

Step 1 Log in to the BMA CLI using WinSCP with the bmaadmin credentials.

Step 2 Navigate to the appropriate directory.

- For Windows Server 2022:
  - Go to **/opt/cnsaroot/templates/Windows-StaticIP/Win2k22x64** if you assign a static IP.
  - Go to **/opt/cnsaroot/templates/Win2k22x64-DHCP** if you use DHCP.
- For Windows Server 2025:
  - Go to **/opt/cnsaroot/templates/Windows-StaticIP/Win2k25x64** if you assign a static IP.
  - Go to **/opt/cnsaroot/templates/Win2k25x64-DHCP** if you use DHCP.

Step 3 Remove the path variable.

- For Windows Server 2022:
  - If the Network-Boot-Manager is selected as iPXE-UEFI, remove the path variable **<Path>\\$PXE_TFTPSERVER\bits\Win2k22x64\sources\install.wim</Path>** inside the **InstallFrom** tag within the **OSImage** tag in the **autounattend-uefi.cfg** configuration file.
- For Windows Server 2025:
  - If the Network-Boot-Manager is selected as iPXE-UEFI, remove the path variable **<Path>\\$PXE_TFTPSERVER\bits\Win2k25x64\sources\install.wim</Path>** inside the **InstallFrom** tag within the **OSImage** tag in the **autounattend-uefi.cfg** configuration file.

What to do next

Execute the **IPMI WINDOWS Bare Metal Provisioning Using VMedia** workflow task after selecting the required Windows OS version from the **Windows Version** drop-down list to provision Windows OS on Dell bare metal servers.

Prerequisites for Provisioning Windows OS to HP Bare Metal Servers through vMedia

Before executing a workflow to provision Windows OS on an HP bare metal server, ensure that the following prerequisites are met:

Procedure

Step 1 Log in to the BMA CLI using WinSCP with the bmaadmin credentials.

Step 2 Navigate to the appropriate directory.

- For Windows Server 2022:
  - Go to **/opt/cnsaroot/templates/Windows-StaticIP/Win2k22x64** if you assign a static IP.
  - Go to **/opt/cnsaroot/templates/Win2k22x64-DHCP** if you use DHCP.
- For Windows Server 2025:
  - Go to **/opt/cnsaroot/templates/Windows-StaticIP/Win2k25x64** if you assign a static IP.
  - Go to **/opt/cnsaroot/templates/Win2k25x64-DHCP** if you use DHCP.

Step 3 Remove the path variable.

- For Windows Server 2022:
  - If the Network-Boot-Manager is selected as iPXE-UEFI, remove the path variable **<Path>\\$PXE_TFTPSERVER\bits\Win2k22x64\sources\install.wim</Path>** inside the **InstallFrom** tag within the **OSImage** tag in the **autounattend-uefi.cfg** configuration file.
- For Windows Server 2025:
  - If the Network-Boot-Manager is selected as iPXE-UEFI, remove the path variable **<Path>\\$PXE_TFTPSERVER\bits\Win2k25x64\sources\install.wim</Path>** inside the **InstallFrom** tag within the **OSImage** tag in the **autounattend-uefi.cfg** configuration file.

What to do next

Execute the **HpiLo WINDOWS Bare Metal Provisioning Using VMedia** workflow task after selecting the required Windows OS version from the **Windows Version** drop-down list to provision Windows OS on HP bare metal servers.

Prerequisites for Provisioning Windows OS to UCSM Bare Metal Servers through vMedia

Before executing a workflow to provision Windows OS on a UCSM bare metal server, ensure that the following prerequisites are met:

Procedure

Step 1 Log in to the BMA CLI using WinSCP with the bmaadmin credentials.

Step 2 Navigate to the appropriate directory.

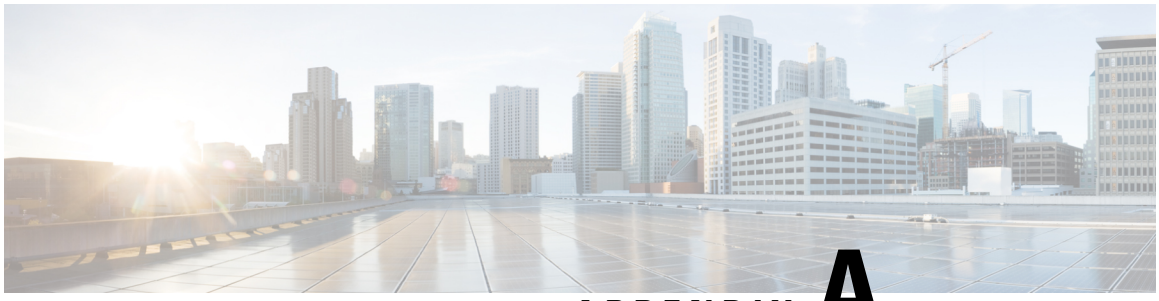
- For Windows Server 2022:
  - Go to **/opt/cnsaroot/templates/Windows-StaticIP/Win2k22x64** if you assign a static IP.
  - Go to **/opt/cnsaroot/templates/Win2k22x64-DHCP** if you use DHCP.
- For Windows Server 2025:
  - Go to **/opt/cnsaroot/templates/Windows-StaticIP/Win2k25x64** if you assign a static IP.
  - Go to **/opt/cnsaroot/templates/Win2k25x64-DHCP** if you use DHCP.

Step 3 Remove the path variable.

- For Windows Server 2022:
  - If the Network-Boot-Manager is selected as iPXE-UEFI, remove the path variable **<Path>\\$PXE_TFTPSERVER\bits\Win2k22x64\sources\install.wim</Path>** inside the **InstallFrom** tag within the **OSImage** tag in the **autounattend-uefi.cfg** configuration file.
- For Windows Server 2025:
  - If the Network-Boot-Manager is selected as iPXE-UEFI, remove the path variable **<Path>\\$PXE_TFTPSERVER\bits\Win2k25x64\sources\install.wim</Path>** inside the **InstallFrom** tag within the **OSImage** tag in the **autounattend-uefi.cfg** configuration file.

What to do next

Execute the **UCSM WINDOWS Bare Metal Provisioning Using VMedia** workflow task after selecting the required Windows OS version from the **Windows Version** drop-down list to provision Windows OS on UCSM bare metal servers.



APPENDIX A

Sample Operating System Configuration Template Files

This chapter contains the following sections:

- Encrypting the Root Password, on page 145
- Sample Configuration Template Files, on page 145

Encrypting the Root Password

Password encryption in the Kickstart configuration template file is supported. The root password is not encrypted if the OS template in the BMA does not support password encryption. Password encryption is supported only for ESXi, RHEL OS, and CentOS catalogs.

Sample Configuration Template Files

This section includes the sample configuration template files for different operating systems.



Important The sample configuration files included in this guide may not suite all the deployment scenarios. Review and modify the configurations based on your deployment environment.

Sample Linux Configuration Template Files

Sample Kickstart Configuration Template File for Linux Operating Systems

The following example shows the Kickstart configuration template file with password encryption (`ks.cfg`) that is required for Linux operating system images:

```
auth  --useshadow  --enablemd5
bootloader --append="rhgb quiet" --location=mbr --driveorder=sda
clearpart --all --initlabel

zerombr
ignoredisk --only-use=sda
```

Sample Operating System Configuration Template Files

```
text
firewall --disabled
firstboot --disable
keyboard us
lang en_US
logging --level=info
url --url=http://$PXE_NATIVE_WEBSERVER/IMAGECATALOGNAME
reboot
$PXE_DHCP_IP_TYPE network --bootproto=dhcp --device=eth0 --hostname=$PXE_NAME --onboot=on
$PXE_STATIC_IP_TYPE network --bootproto=static --device=eth0 --ip=$PXE_IP
--netmask=$PXE_NETMASK --gateway=$PXE_GATEWAY --vlanid=$PXE_MGMTVLAN --hostname=$PXE_NAME
--onboot=on
rootpw $ENCRYPTED $PXE_PASSWD
selinux --disabled
timezone --isUtc $PXE_TIMEZONE
install
part biosboot --fstype=biosboot --size=1 --ondisk=sda
part /  --fstype="ext3" --size=8000

%packages --nobase
wget
%end

%post

## Notifying back to Cisco UCS Director once the blade is up ##
wget http://$PXE_WEBSERVER/$PXEID/notify.html
%end

~
```

The following example shows the Kickstart configuration template file with password encryption (`ks-uefi.cfg`) that is required for Linux operating system images:

```
auth  --useshadow  --enablemd5
bootloader --append="rhgb quiet" --location=mbr --driveorder=sda
clearpart --all --initlabel

zerombr
ignoredisk --only-use=sda
text
firewall --disabled
firstboot --disable
keyboard us
lang en_US
logging --level=info
url --url=http://$PXE_NATIVE_WEBSERVER/IMAGECATALOGNAME
reboot
$PXE_DHCP_IP_TYPE network --bootproto=dhcp --device=eth0 --hostname=$PXE_NAME --onboot=on
$PXE_STATIC_IP_TYPE network --bootproto=static --device=eth0 --ip=$PXE_IP
--netmask=$PXE_NETMASK --gateway=$PXE_GATEWAY --vlanid=$PXE_MGMTVLAN --hostname=$PXE_NAME
--onboot=on
rootpw $ENCRYPTED $PXE_PASSWD
selinux --disabled
timezone --isUtc $PXE_TIMEZONE
install

part /boot/efi --fstype=efi --grow --maxsize=200 --size=50
part /boot --fstype=ext3 --size=500

part swap --fstype="swap" --size=1024
part pv.01 --size=10240
volgroup vg0 pv.01
logvol /home --vgname=vg0 --size=500 --name=home
```

```
logvol / --vgname=vg0 --grow --size=1 --name=root




%packages --nobase
wget
%end

%post

## Notifying back to Cisco UCS Director once the blade is up ##
wget http://$PXE_WEBSERVER/$PXEID/notify.html
%end
```

Sample PXE Configuration Template File for Linux Operating Systems

The following example shows the PXE configuration template file (`pxe.cfg`) that is required for Linux operating system images:

```
default linux

label linux
kernel vmlinuz

append initrd=initrd.img ramdisk_size=9216 noapic acpi=off ip=dhcp ks=$PXE_KS_URL

prompt 0
timeout 0
```

Sample iPXE Configuration Template File for Linux Operating Systems

The following example shows the iPXE configuration template file (`ipxe.cfg`) that is required for Linux operating system images:

```
default linux
label linux
kernel http://$PXE_NATIVE_WEBSERVER/$PXE_OS/isolinux/vmlinuz
append initrd=http://$PXE_NATIVE_WEBSERVER/$PXE_OS/isolinux/initrd.img ramdisk_size=9216
noapic acpi=off ip=dhcp ks=$PXE_KS_URL ksdevice=eth0
inst.repo=http://$PXE_NATIVE_WEBSERVER/$PXE_OS net.ifnames=0 biosdevname=0
prompt 0
timeout 0
```

Sample VMware vSphere ESXi Configuration Template Files

Sample Kickstart Configuration Template File for VMware vSphere ESXi Operating Systems

The following example shows the Kickstart configuration template file with password encryption (`ks.cfg`) that is required for VMware vSphere ESXi operating system images:

```
vmaccepteula
rootpw $ENCRYPTED $PXE_PASSWD
#for Local boot
install --firstdisk --overwritevmfs
#for SAN boot
```

```
#install --firstdisk=remote --overwritevmfs

$PXE_DHCP_IP_TYPE network --bootproto=dhcp --vlanid=$PXE_MGMTVLAN
$PXE_STATIC_IP_TYPE network --bootproto=static --ip=$PXE_IP --netmask=$PXE_NETMASK
--gateway=$PXE_GATEWAY --vlanid=$PXE_MGMTVLAN  --nameserver=$PXE_NS --hostname=$PXE_NAME


#we poweroff ourselves in the 'post' section, and ucs will later power us on after changing
 the service profile
#reboot

%pre --interpreter=busybox
hwclock -d %LIVE_VAR_DATE_1% -t %LIVE_VAR_TIME_UTC_1%
date -s %LIVE_VAR_DATE_TIME_UTC_1%
cd /tmp

%firstboot --interpreter=busybox
cd /tmp


esxcfg-vswitch -A 'VM Network' vSwitch0



################################
# enable & start remote ESXi Shell  (SSH)
################################
vim-cmd hostsvc/enable_ssh
vim-cmd hostsvc/start_ssh

################################
# enable & start ESXi Shell (TSM)
################################
vim-cmd hostsvc/enable_esx_shell
vim-cmd hostsvc/start_esx_shell

$PXE_DHCP_IP_TYPE esxcli system hostname set --host=$PXE_NAME




%post --interpreter=busybox --ignorefailure=true

cd /tmp
localcli network firewall set --default-action true
localcli network firewall set --enabled false

## Notifying back to Cisco UCS Director once the blade is up ##
wget http://$PXE_WEBSERVER_MGMT_VLAN_IP/$PXEID/notify.html -O /tmp/notify.html
localcli network firewall set --default-action false
localcli network firewall set --enabled true

# Let us poweroff/shutdown our selves.
Poweroff
```

Sample PXE Configuration Template File for VMware vSphere ESXi Operating Systems

The following example shows the PXE configuration template file (`pxe.cfg`) that is required for VMware vSphere ESXi operating system images.

Important You can customize the configuration based on your requirements.

```
default image_name/menu.c32
menu title PXE Boot Home
timeout 70

label image_name
menu label Install VMware image_name
kernel image_name/mboot.c32
append -c /web/ks-repository/$PXE_ID/boot.cfg  +++
IPAPPEND 1
```

Sample iPXE Configuration Template File for VMware vSphere ESXi Operating Systems

The following example shows the iPXE configuration template file (`ipxe.cfg`) that is required for VMware vSphere ESXi operating system images:

```
default 1
timeout 100
prompt 1
label 1
KERNEL ipxe.lkrn
Append dhcp && chain http://$PXE_NATIVE_WEBSERVER/$PXE_WINDOWS_OS_REPOSITORY_LINK/boot.ipxe
```

Sample iPXE UEFI Configuration Template File for Windows

The following example shows the iPXE UEFI configuration template file (`ipxe-uefi.cfg`) that is required for windows:

```
#!ipxe
kernel ../wimboot
initrd ../Boot/BCD BCD
initrd ../Boot/boot.sdi boot.sdi
initrd ../Boot/WinPE.wim WinPE.wim
boot
```

Sample Windows Answer File

The following is an example of a Windows answer file, named `AUTOUNATTEND.XML`, that can be used to set up a Windows Server 2008 R2 OS image for use with Cisco UCS Director Bare Metal Agent.

```
<unattend>
 <servicing>
  <package action="configure">
    <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="6.1.7600.16385"

    processorArchitecture="amd64" publicKeyToken="xxxf3856ad364xxx" language=""/>
    <selection name="IIS-WebServerRole" state="false"/>
    <selection name="IIS-WebServer" state="false"/>
    <selection name="Microsoft-Hyper-V" state="true"/>
    <selection name="Microsoft-Hyper-V-Management-Clients" state="true"/>
    <selection name="Microsoft-Hyper-V-Management-Clients" state="true"/>
```

Sample Operating System Configuration Template Files

```
    <selection name="MultipathIo" state="true"/>
    <selection name="TelnetClient" state="true"/>
   </package>
 </servicing>
<settings pass="windowsPE">
 <component name="Microsoft-Windows-Setup" processorArchitecture="amd64"
  publicKeyToken="xxxf3856ad364xxx" language="neutral" versionScope="nonSxS">
  <ComplianceCheck>
 <DisplayReport>OnError</DisplayReport>
 </ComplianceCheck>
<Display>
   <VerticalResolution>600</VerticalResolution>
   <RefreshRate>60</RefreshRate>
   <HorizontalResolution>800</HorizontalResolution>
   <ColorDepth>32</ColorDepth>
 </Display>
 <EnableFirewall>false</EnableFirewall>
<UserData>
 <ProductKey>
  <WillShowUI>Never</WillShowUI>
  <Key>XXXXX-XXXXX-KQT8W-PMXWJ-XXXXX</Key>
 </ProductKey>
 <AcceptEula>true</AcceptEula>
 <FullName>Cisco</FullName>
 <Organization>CiscoUCSD</Organization>
 </UserData>
<DiskConfiguration>
 <WillShowUI>OnError</WillShowUI>
<Disk wcm:action="add">
<CreatePartitions>
<CreatePartition wcm:action="add">
 <Order>1</Order>
 <Type>Primary</Type>
 <Size>40000</Size>
 </CreatePartition>
 </CreatePartitions>
 <DiskID>0</DiskID>
 <WillWipeDisk>true</WillWipeDisk>
<ModifyPartitions>
<ModifyPartition wcm:action="add">
 <Active>true</Active>
 <Extend>false</Extend>
 <Format>NTFS</Format>
 <Label>OS</Label>
 <Letter>C</Letter>
 <Order>1</Order>
 <PartitionID>1</PartitionID>
 </ModifyPartition>
 </ModifyPartitions>
 </Disk>
 </DiskConfiguration>
<ImageInstall>
<OSImage>
<InstallTo>
 <DiskID>0</DiskID>
 <PartitionID>1</PartitionID>
 </InstallTo>
 <WillShowUI>Never</WillShowUI>
<InstallFrom>
<MetaData wcm:action="add">
 <Key>/IMAGE/NAME</Key>
 <Value>Windows Server 2008 R2 SERVERDATACENTER</Value>
 </MetaData>
 <Path>\\000.00.90.31\bits\sources\install.wim</Path>
```

```
 </InstallFrom>
 </OSImage>
 </ImageInstall>
 </component>
<component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"

 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
<SetupUILanguage>
 <UILanguage>en-US</UILanguage>
 </SetupUILanguage>
 <UserLocale>en-US</UserLocale>
 <UILanguage>en-US</UILanguage>
 <SystemLocale>en-US</SystemLocale>
 </component>
 </settings>
<settings pass="specialize">
<component name="Microsoft-Windows-International-Core" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
 <SystemLocale>en-US</SystemLocale>
 <UILanguage>en-US</UILanguage>
 <UILanguageFallback>en-US</UILanguageFallback>
 <UserLocale>en-US</UserLocale>
 </component>
<component name="Microsoft-Windows-TerminalServices-LocalSessionManager"
 processorArchitecture="amd64" publicKeyToken="nnnf3856ad364nnn"
 language="neutral" versionScope="nonSxS">
 <fDenyTSConnections>false</fDenyTSConnections>
 </component>
<component name="Microsoft-Windows-Deployment" processorArchitecture="amd64"
 publicKeyToken="31bf3856ad364nnn" language="neutral" versionScope="nonSxS">
<RunSynchronous>
<RunSynchronousCommand wcm:action="add">
 <Description>Disable IPv6</Description>
 <Path>reg add HKLM\SYSTEM\CurrentControlSet\Services\tcpip6\Parameters /v DisabledComponents
 /t
  REG_DWORD /d 255 /f</Path>
 <Order>1</Order>
 </RunSynchronousCommand>
<RunSynchronousCommand wcm:action="add">
 <Description>Disable Shutdown Tracker</Description>
 <Path>reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Reliability" /v ShutdownReasonOn
 /t
  REG_DWORD /d 0 /f</Path>
 <Order>2</Order>
 </RunSynchronousCommand>
 </RunSynchronous>
 </component>
<component name="Networking-MPSSVC-Svc" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
 <DomainProfile_EnableFirewall>false</DomainProfile_EnableFirewall>
 <PrivateProfile_EnableFirewall>false</PrivateProfile_EnableFirewall>
 <PublicProfile_EnableFirewall>false</PublicProfile_EnableFirewall>
 </component>
<component name="Microsoft-Windows-ServerManager-SvrMgrNc" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
 <DoNotOpenServerManagerAtLogon>true</DoNotOpenServerManagerAtLogon>
 </component>
<component name="Microsoft-Windows-OutOfBoxExperience" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
 <DoNotOpenInitialConfigurationTasksAtLogon>true</DoNotOpenInitialConfigurationTasksAtLogon>

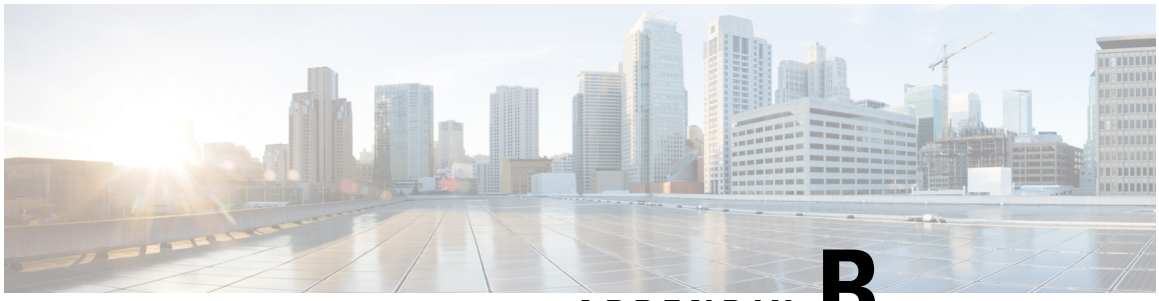
 </component>
<component name="Microsoft-Windows-powercpl" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
```

Sample Operating System Configuration Template Files

```
 <PreferredPlan>8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c</PreferredPlan>
 </component>
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
 <ComputerName>*</ComputerName>
 <ProductKey>XXXXX-XXXXX-KQT8W-PMXWJ-XXXXX</ProductKey>
 </component>
 </settings>
<settings pass="oobeSystem">
<component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
<Display>
 <ColorDepth>32</ColorDepth>
 <HorizontalResolution>800</HorizontalResolution>
 <VerticalResolution>600</VerticalResolution>
 <RefreshRate>60</RefreshRate>
 </Display>
<OOBE>
 <HideEULAPage>true</HideEULAPage>
 <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
 <NetworkLocation>Work</NetworkLocation>
 <ProtectYourPC>3</ProtectYourPC>
 </OOBE>
<VisualEffects>
 <FontSmoothing>ClearType</FontSmoothing>
 </VisualEffects>
<WindowsFeatures>
 <ShowInternetExplorer>true</ShowInternetExplorer>
 </WindowsFeatures>
 <TimeZone>Pacific Standard Time</TimeZone>
 <RegisteredOrganization/>
 <ShowWindowsLive>false</ShowWindowsLive>
<UserAccounts>
<AdministratorPassword>
 <Value>987654321abc???=</Value>
 <PlainText>false</PlainText>
 </AdministratorPassword>
 </UserAccounts>
<AutoLogon>
<Password>
 <Value>123456abc???</Value>
 <PlainText>false</PlainText>
 </Password>
 <Enabled>true</Enabled>
 <LogonCount>1</LogonCount>
 <Username>Administrator</Username>
 </AutoLogon>
<FirstLogonCommands>
<SynchronousCommand wcm:action="add">
 <CommandLine>cmd /c winrm quickconfig -quiet -transport:HTTP</CommandLine>
 <Description>Enable WinRS over HTTP to communicate with CPA</Description>
 <Order>1</Order>
 <RequiresUserInput>false</RequiresUserInput>
 </SynchronousCommand>
<SynchronousCommand wcm:action="add">
 <CommandLine>cmd /c winrm set winrm/config/client @{TrustedHosts="*"}</CommandLine>
 <Description>Adding trusted hosts value for winrm client</Description>
 <Order>2</Order>
 <RequiresUserInput>false</RequiresUserInput>
 </SynchronousCommand>
<SynchronousCommand wcm:action="add">
 <CommandLine>cmd /c net use R: \\000.00.90.31\bits /user:smbuser cisco123</CommandLine>
 <Description>Mapping the share to save the notification file</Description>
 <Order>3</Order>
```

```
 <RequiresUserInput>false</RequiresUserInput>
 </SynchronousCommand>
<SynchronousCommand wcm:action="add">
 <CommandLine>cmd /c ipconfig /all | findstr "Physical" >>
R:\notifications\completed.html</CommandLine>
 <Description>Writing the completed notification log with MAC address at
  Share mapped in previous step</Description>
 <Order>4</Order>
 <RequiresUserInput>false</RequiresUserInput>
 </SynchronousCommand>
<SynchronousCommand wcm:action="add">
 <CommandLine>cmd /c R:\notifications\completed.bat</CommandLine>
 <Description>executing powershell batch file like as wget</Description>
 <Order>5</Order>
 <RequiresUserInput>false</RequiresUserInput>
 </SynchronousCommand>
 </FirstLogonCommands>
 </component>
 </settings>
<settings pass="offlineServicing">
<component name="Microsoft-Windows-LUA-Settings" processorArchitecture="amd64"
 publicKeyToken="nnnf3856ad364nnn" language="neutral" versionScope="nonSxS">
 <EnableLUA>false</EnableLUA>
 </component>
 </settings>
 <cpi:offlineImage cpi:source="wim:D:/win2k8r2x64sp1/sources/install.wim#Windows
  Server 2008 R2 SERVERDATACENTER"/>
 </unattend>
```

Sample Operating System Configuration Template Files



APPENDIX B

Ports

This appendix contains the following sections:

- Cisco UCS Director TCP and UDP Port Usage, on page 155
- Port List, on page 157
- Multi-Node Port Requirements, on page 158

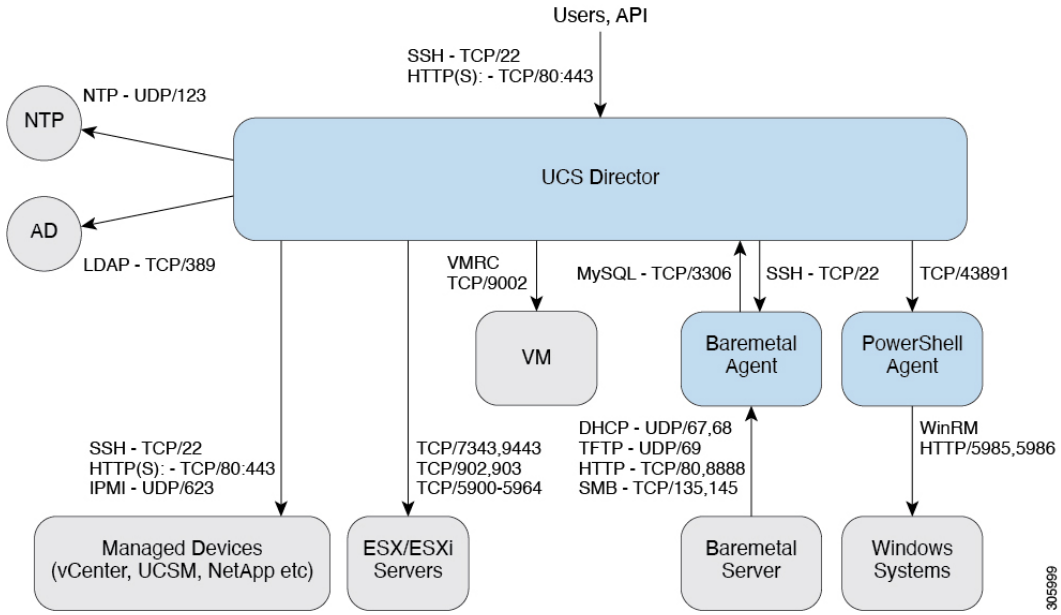
Cisco UCS Director TCP and UDP Port Usage

This section provides a list of the TCP and UDP ports that Cisco UCS Director uses for connections and communications with external applications or devices. The port usage depends upon whether you have deployed Cisco UCS Director on VMware vSphere or Microsoft Hyper-V.

Cisco UCS Director TCP and UDP Port Usage on VMware vSphere

The following figure shows the network ports used for communication between the Cisco UCS Director appliance and managed devices, ESX servers, Bare Metal Agent, PowerShell Agent, NTP, and Active Directory for an installation on VMware vSphere.

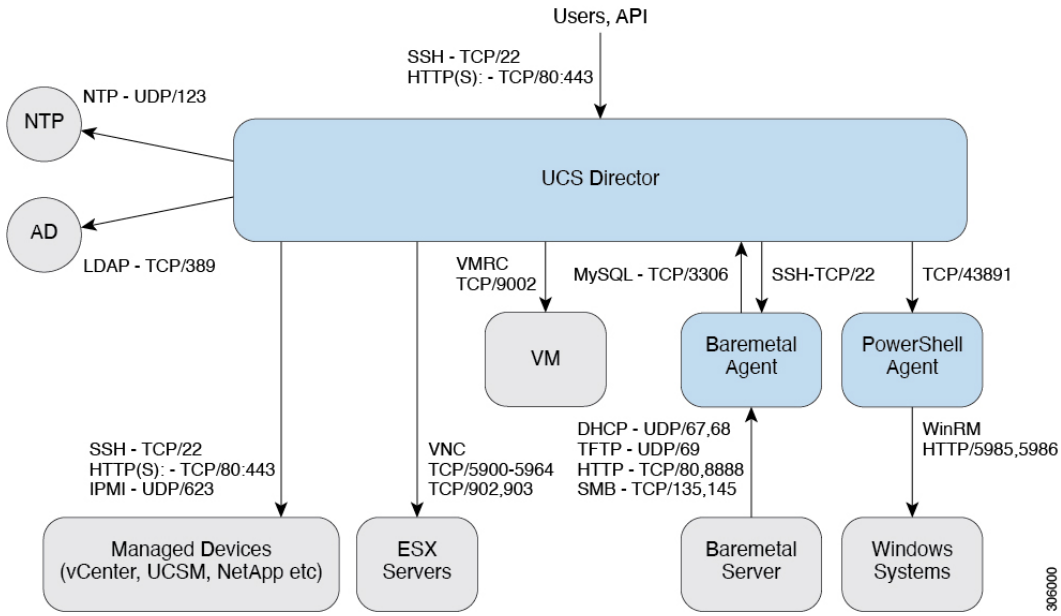
Figure 5: Cisco UCS Director TCP and UDP Port Usage



Cisco UCS Director TCP and UDP Port Usage on Microsoft Hyper-V

The following figure shows the network ports used for communication between the Cisco UCS Director appliance and managed devices, ESX servers, Bare Metal Agent, PowerShell Agent, NTP, and Active Directory for an installation on Microsoft Hyper-V.

Figure 6: Cisco UCS Director TCP and UDP Port Usage



Port List

Default Port	Protocol	Description
22	TCP	SSH
80	TCP/UDP	HTTP
8888	TCP	HTTP for Cisco UCS Director Bare Metal Agent
69	TFTP	TFTP for Cisco UCS Director Bare Metal Agent
443	UDP	HTTPS
27000/7279/8082 (Mgmt)	TCP	Citrix licensing
2598/1494/2112/2513	TCP	Virtual Desktop Agent for Desktops
67/68	UDP	DHCP
389/636 3268/3269	TCP/UDP TCP	Active Directory
53	TCP/UDP	DNS
123	TCP/UDP	NTP
3306	TCP/UDP	MariaDB
8787/5900-5964	TCP	Cisco UCS Director + VNC Connectivity
3389	TCP/UDP	Cisco UCS Director + RDP Connectivity
80/443/8080	TCP/UDP	Cisco UCS Director + NetApp Connectivity
80/443	UDP	Cisco UCS Director + Cisco UCS Manager Connectivity
80/443	UDP	Cisco UCS Director + vCenter Connectivity
3389	TCP/UDP	RDP
135/445	TCP	SMB/RPC
88	TCP/UDP	Kerberos
137	TCP/UDP	NetBIOS Name (nbname)
138	TCP/UDP	NetBIOS datagram (nbdatagram)
139	TCP	NetBIOS session (nbsession)
80/443	UDP	Desktop Delivery Controller <--> vCenter
8080 through ICA	TCP	Desktop Delivery Controller <--> Virtual Desktops

Default Port	Protocol	Description
1494/2598/2512/2513	TCP	Users (Citrix Recvr) <--> Virtual Desktops
389/636 (LDAP Ports)	TCP/UDP	Desktop Delivery Controller <--> Active Directory
389/636, 3268/3269, 53	TCP/UDP	Virtual Desktops <--> Active Directory + DNS
5985/5986	TCP	PowerShell Agent <-> Xendesktop through WinRM
43891	TCP/UDP	Cisco UCS Director <--> PowerShell Agent
80/8081	TCP	XenApp
902	TCP	VMwareESXi host management and VM customization and to execute VIX tasks
903	TCP	VMwareESXi host management and VM customization and to execute VIX tasks (for Vmware vCenter releases prior to 5.0)
9002	TCP	VMRC Connectivity

Multi-Node Port Requirements

The ports listed in Cisco UCS Director TCP and UDP Port Usage, on page 155 are applicable for both single and multi-node setups.

For a multi-node setup, the following port must be opened between the nodes:

- From the primary nodes to database nodes: port 3306