Cisco Expressway Install and Upgrade Guide (X15.4)

First Published: 2026-01-22

Last Modified: 2026-04-03

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)

© 2026 Cisco Systems, Inc. All rights reserved.

CONTENTS

PART I **Introduction** 7

CHAPTER 1 **About the Documentation** 1

About Cisco Expressway Deployment on a Hypervisor 1

Change History 1

New and Changed Information 1

Getting License Keys 2

Related Documents 2

PART II **Introduction to Supported Virtualization Environments** 5

CHAPTER 2 **Hypervisors Used** 7

VMware vSphere ESXi 7

Nutanix AHV 7

Cisco NFVIS-for-UC (Network Function Virtualization Infrastructure Software) 8

CHAPTER 3 **Requirements and Limitations** 9

Virtualization Requirements 9

ESXi Requirements 11

PART III **System Management** 13

CHAPTER 4 **System Requirements** 15

Supported Platforms 15

Virtual Machine Requirements 16

How to Modify Expressway VM Capacity 17

Co-residency Support 17

PART IV Deploying Expressway Virtual Machine on the Different Hypervisors 19

CHAPTER 5 VMware vSphere ESXi 21

Installing the Expressway VM using vCenter or vSphere Client 21

Installation Process 21

Configuring the VM Host 21

Deploying OVA to Host Managed by vCenter 22

Configuring the VM Guest to Standalone ESXi Host 23

Deploying OVA to Standalone ESXi Host 25

Automating the Deployment Process 28

CHAPTER 6 Nutanix AHV 31

VM Deployment using OVA 31

VM Lifecycle Management 32

Performance Monitoring 32

CHAPTER 7 Cisco NFVIS-for-UC 33

Deploying Virtual Machines 33

Managing Virtual Machines 36

Monitoring Virtual Machines 36

PART V Configuring the Deployed Virtual Machines 39

CHAPTER 8 Configure Expressway after Deployment 41

Configuring the Hypervisors 41

Set the Root and Admin Password Using the Install Wizard 41

Set the Root and Admin Password Using SSH 42

PART VI Post Installation Tasks 45

CHAPTER 9 Expressway Service Selection, Licenses, and Basic Configuration 47

Next Steps: Service Selection, Licenses, and Basic Configuration 47

CHAPTER 10 ESXi specific - Creating a Backup of Your System and Deleting Existing Snapshots 49
Creating Backups 49
Deleting Existing Snapshots 50

CHAPTER 11 Hardware References 51
Serial Interface 51
Ethernet Interfaces (NICs) 51
ESXi specific - Allocating a Virtual NIC to a Physical NIC Interface 51

PART VII Additional Hypervisor Information - ESXi specific 55

CHAPTER 12 Additional Information 57
Upgrading or Downgrading an Expressway VM 57
Clustering for Resilience and Capacity 58
Migrating from a Physical Appliance to a VM 58
Migrating the VM between ESXi Hosts (use VMware VMotion) 58
Unsupported ESXi Features 58
Licensing 59
Security Hardening 59

CHAPTER 13 Troubleshooting 61
Checking VMware Compatibility 61
VMware Checklist 61
Isolating a Possible Root Cause 62
Possible Issues 63
Analyzing the Cause of VMware Issues 64
Restoring the Default Configuration (Factory Reset) 64
Before You Begin 64
Prerequisites 65
Process to Reset to the Default Configuration 65
Resetting Your Administrator Password or Root Password 66

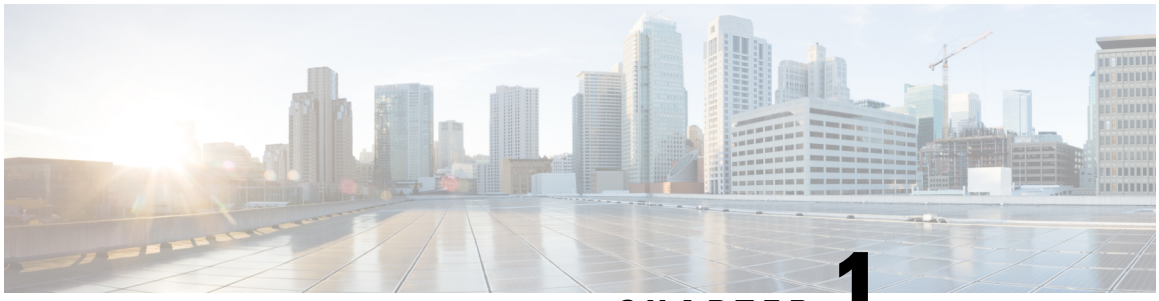
CHAPTER 14 Deploying Multiple Datastores 67

Deploying Multiple Datastores 67

PART I

Introduction

- About the Documentation, on page 1



CHAPTER 1

About the Documentation

- About Cisco Expressway Deployment on a Hypervisor, on page 1
- Change History, on page 1
- New and Changed Information, on page 1
- Getting License Keys, on page 2
- Related Documents, on page 2

About Cisco Expressway Deployment on a Hypervisor

Cisco Expressway (Expressway) software supports flexible deployment options and is available as a virtualized application for various Hypervisors. This lets enterprises run Expressway on a choice of Virtual Machine (VM) hardware platforms for ease of management and deployment in an existing data center. With a suitably specified VM platform, Expressway running on a Hypervisor performs identically to Expressway running on its appliance hardware.

Change History

Table 1: Change History

Date	Change	Reason
March 2026	Republished the guide Updated the tables in the "Virtualization Requirements" section in the "Requirements and Limitations" chapter.	X15.4 release
February 2026	First published for Cisco Expressway X15.4 release.	X15.4 release

New and Changed Information

New Hypervisor Support for On-premises Calling Solutions

Cisco Expressway X15.4 release introduces support for additional virtualization options. In addition to VMware vSphere ESXi, X15.4 supports Cisco NFVIS-for-UC and Cisco Compute Hyperconverged with Nutanix (CCHN) for on-premises calling deployments. These additions allow on-premises customers to choose between traditional VMware support, a Cisco-native virtualization layer for appliances, or a robust hyperconverged infrastructure (HCI) solution.

Getting License Keys

If you use PAK-based licensing, option keys for licenses can be obtained after the Expressway VM is installed, using the Expressway VM serial number (available from the Option key page and in the footer of the Expressway web interface).

Related Documents

The following documents may help with setting up your environment:

Table 2: Links to Virtualization Docs for 15 SU4 (VMware vSphere ESXi, Cisco NFVIS-for-UC, Nutanix AHV in CCHN)

Reference	Link
Cisco Virtualization Guide for Cisco On-premises Calling Applications	Solution Guide - Virtualization Guide for On-prem Calling
Virtualization Requirements by Application	Resource
UCM+IMP+SME 15 SU4	Guide
CER 15 SU4	
CUC 15 SU4	*COMING SOON*
Expressway X15.4	Cisco Expressway Installation Guide
DI ESN 15 SU4	Article on help.webex.com

Table 3: Related Reference Documents for Expressway

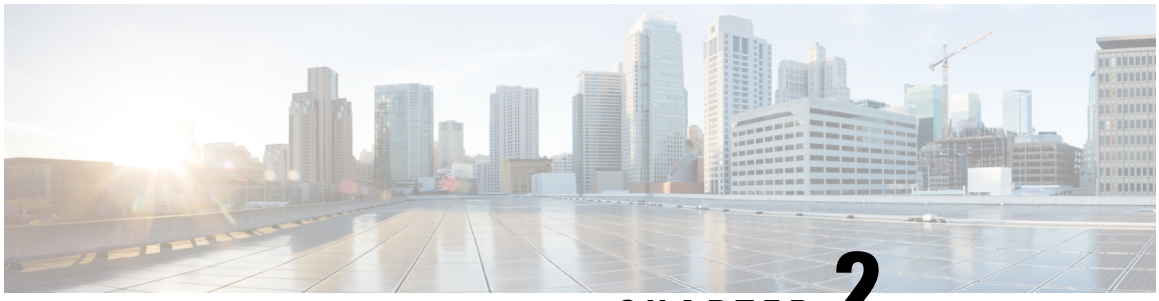
Reference	Links
Expressway Basic Configuration (Expressway-C with Expressway-E) Deployment Guide	*Expressway Basic Configuration (Expressway-C with Expressway-E) Deployment Guide*
Expressway Cluster Creation and Maintenance Deployment Guide	*Expressway Cluster Creation and Maintenance Deployment Guide*
Certificate Creation and Use With Expressway Deployment Guide	*Certificate Creation and Use With Expressway Deployment Guide*
Cisco Expressway Configuration Guides	Link
Cisco Expressway IP Port Usage Configuration Guide	Link

Reference	Links
Cisco Expressway Administrator Guide	Maintain and Operate Guides
Configuration and Administration of IM and Presence Service on Cisco Unified Communications Manager	Configuration Guides
Cisco Collaboration System 10.x Solution Reference Network Designs (SRND)	"Directory Integration and Identity Management" chapter in the Guide
SAML SSO Deployment Guide for Cisco Unified Communications Applications	Cisco Unified Communications Manager Maintain and Operate Guides
Jabber Client Configuration details:	• *Cisco Jabber for Windows* • *Cisco Jabber for iPad* • *Cisco Jabber for Android* • *Cisco Jabber for Mac*

PART II

Introduction to Supported Virtualization Environments

- Hypervisors Used, on page 7
- Requirements and Limitations, on page 9



CHAPTER 2

Hypervisors Used

- VMware vSphere ESXi, on page 7
- Nutanix AHV, on page 7
- Cisco NFVIS-for-UC (Network Function Virtualization Infrastructure Software), on page 8

VMware vSphere ESXi

VMware ESXi (formerly named ESXi, now renamed back to ESX in version 9.0) is an enterprise-class, type-1 hypervisor developed by VMware and Broadcom. As a Type 1 hypervisor, ESXi runs directly on bare-metal hardware without requiring a host operating system, providing direct access to hardware resources for enhanced performance and efficiency.

Cisco on-premises applications are supported on VMware vSphere ESXi running on a broad spectrum of Cisco Calling Appliances, Cisco General-purpose Compute/Storage, and third-party General-purpose Compute/Storage.

Note

- For more information, see "Chapter 4: System Requirements".
- For more information on Cisco on-premises calling applications support on ESXi 8.0, see the section “Virtualization Requirements for VMware vSphere ESXi”. in Cisco Virtualization Guide for Cisco On-premises Calling Applications.
- For more information on Cisco on-premises calling applications' support of vSphere ESXi 7.0 and older, see Cisco Collaboration Virtualization.
- For more information on vSphere ESXi, see Broadcom.com.

Nutanix AHV

Nutanix is a hyperconverged infrastructure (HCI) platform that integrates compute, storage, and networking into a single, software-defined system, providing a robust foundation for hybrid cloud deployments.

Acropolis Hypervisor (AHV) is a hypervisor from Nutanix that runs alongside Acropolis OS (AOS) hyperconvergence software and Prism Central (PC), a web-based, centralized management software. These products are all part of Nutanix Cloud Infrastructure (NCI) or Nutanix Cloud Platform (NCP) portfolios.

Cisco Compute Hyperconverged with Nutanix (CCHN) is a joint solution that runs Nutanix software on Cisco hardware, with joint support from both companies.

Cisco on-premises applications are supported on Nutanix AHV, AOS, and PC with CCHN hardware.

Note

- For more information, see "Chapter 4: System Requirements".
- For more information on Cisco on-premises calling applications support on ESXi 8.0, see the section “Virtualization Requirements for VMware vSphere ESXi”. in Cisco Virtualization Guide for Cisco On-premises Calling Applications.
- For more information on Nutanix software, see the Nutanix Home page.
- For more information on CCHN hardware, see Cisco Compute Hyperconverged with Nutanix.
- For more information on Cisco On-premises calling applications support on Cisco Compute Hyperconverged with Nutanix, see the section “Virtualization Requirements for Nutanix AHV” in Cisco Collaboration Virtualization.

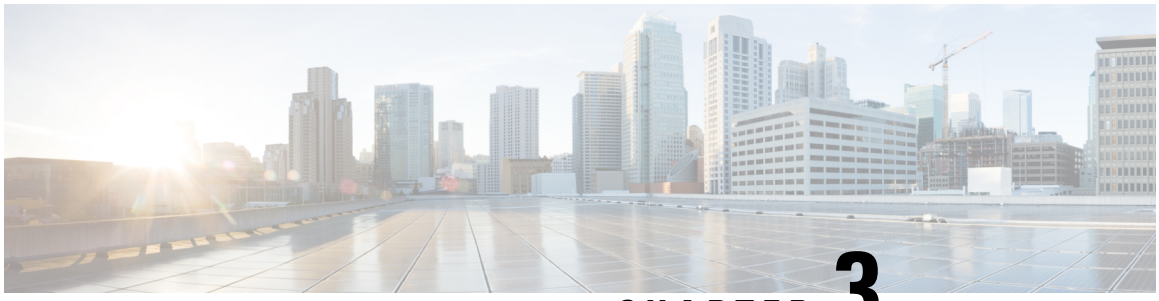
Cisco NFVIS-for-UC (Network Function Virtualization Infrastructure Software)

Cisco NFVIS (Network Function Virtualization Infrastructure Software) is a hypervisor product from Cisco's Enterprise Network Function Virtualization (Enterprise NFV) portfolio. It is a special-purpose Linux/KVM-based virtualization layer for deploying select application workloads on select Cisco hardware.

Cisco NFVIS-for-UC is a special edition of NFVIS. Selecting Cisco On-premises Calling Applications are supported on Cisco NFVIS-for-UC (not the base Cisco NFVIS product) on select Cisco Calling Appliances only.

Note

- For more information, see "Chapter 4: System Requirements".
- For more information on Cisco on-premises calling applications support on ESXi 8.0, see the section “Virtualization Requirements for VMware vSphere ESXi”. in Cisco Virtualization Guide for Cisco On-premises Calling Applications.
- For more information on the base Cisco NFVIS from Cisco Enterprise NFV, see the following:
  - Optimize the virtualization layer
  - Cisco Enterprise NFV Infrastructure Software
- For more information on Cisco on-premises calling applications support on Cisco NFVIS-for-UC, see the section “Virtualization Requirements for Cisco NFVIS-for-UC” in Cisco Collaboration Virtualization.



CHAPTER 3

Requirements and Limitations

- Virtualization Requirements, on page 9
- ESXi Requirements, on page 11

Virtualization Requirements

Application/Hypervisor Compatibility

See the following table for compatibility of Unified Communications Manager and the IM and Presence Service with hypervisor releases.

- Only the listed major/minor releases are supported, with a minimum required maintenance or patch release.
- Unlisted major/minor release trains are not supported.
- For support of subsequent maintenance or patch releases, see the Cisco Virtualization Guide for Cisco On-premises Calling Applications.

	Compatible Hypervisor Major/Minor Releases with Minimum Maintenance		
	VMware vSphere ESXi	**Cisco NFVIS-for-UC**	**Nutanix AHV**
Cisco Expressway Series			
Release X15.4	8.0 U1 7.0 U3	4.18.2a	AHV 10.0 + AOS /PC 7.0
Release X15.0 through X15.4 and later releases	8.0 U1 7.0 U3	Not supported	Not supported

Virtual Machine Configurations and CPU Minimum Base Frequencies

This section details the minimum specifications required for virtual machine configurations.

Applications are supported only with specific virtual machine (VM) configurations.

You must deploy these VMs using the latest Cisco-provided OVA file (VMware or Nutanix) or NFVIS TAR.GZ file (see the Readme file for important notes.)

- For Expressway, the files are available here: Cisco Software Central - Software Downloads.
- One base OVA is used for both VMware vSphere ESXi and Cisco NFVIS for UC, while a set of base OVAs is used for Nutanix AHV.

See the following table for the required and supported virtual machine configurations.

- Each VM represents a particular application capacity point and has a minimum required CPU base frequency.
- For more information on how these are used, see the Cisco Virtualization Guide for Cisco On-premises Calling Applications. The guide is available at the following locations:
  - Cisco Collaboration Systems Release 15
  - Cisco Unified Communications Manager (CallManager)-Install and Upgrade Guides

Table 4: Required/Supported Virtual Machine Configurations

Component and Capacity Point	vCPU	Physical CPU Required Minimum Base Frequency	vRAM	vDisk			vNIC
				ESXi	NFVIS-for-UC	Nutanix AHV	
Small	2	3600 MHz (2 x 1.8 GHz)	4 GB	132 GB	140 GB	140 GB	1 GB
Medium	2	4800 MHz (2 x 2.4 GHz)	6 GB	132 GB	140 GB	140 GB	1 GB
Large (extra performance and scalability capabilities)	8	25600 MHz (8 x 3.2 GHz)	8 GB	132 GB	140 GB	140 GB	1 GB

For more information on how these are used, see the Cisco Virtualization Guide for Cisco On-premises Calling Applications. The guide is available at the following locations:

Two Large Expressway VMs can co-reside on a UCS server with two eightcore 3.2 GHz processors all dedicated to Expressway, when hyperthreading is enabled. To allow for hypervisor overhead, the CPU reservation is set to 16000 MHz, but the full allocation of 8x 3.2 GHz CPU cores must be made available to each Large Expressway VM. The reservation does not limit maximum Expressway CPU speed, as the Expressway can use the headroom provided by the higher specification host.

For all deployment sizes, you need the following:

- Hypervisor host operational and running a supported version of the Hypervisor (see ESXi Requirements).

From X15.0.2, **Expressway no longer supports ESXi 6.7 or earlier versions.**

- Reserved RAM, CPU, and NIC as per table above.
- Subject to bandwidth constraints, Large VMs can run with 1 Gbps NIC.

ESXi Requirements

Note The minimum versions specified here are subject to VMware support. The versions are correct when this documentation is published, but if VMware subsequently withdraws support for any stated version, you may need to use newer ESXi versions.

The minimum VMware ESXi version required to host a new virtual Expressway X15.0.2 deployment is VMware ESXi 7.0. Cisco does not support new Expressway VMs hosted on ESXi 6.7 or earlier (VMware no longer supports these versions).

New deployments of X15 are compatible only with VMware ESXi versions 7.0 U1 and 8.0 U1 and later. Expressway is supported on any subsequent ESXi minor release version.

The VMware Virtual Machine Hardware Version embedded in the OVA may change on a per-release basis. If it is updated, it can impact which versions of ESXi it can be deployed on. Current compatibility and historical reference information is available at: Virtualization for Cisco Expressway Series.

For upgrade instructions, see your VMware documentation.

Note If you migrate an existing VM to a different host, you must shut down the VM before you move it.

More information

- Instructions about installing new Cisco Expressway VMs are in the Cisco Expressway on Virtual Machine Installation Guide on the Expressway Install and Upgrade Guides page.
- Instructions about how to upgrade a single (non-clustered) Expressway VM are also in the Cisco Expressway on Virtual Machine Installation Guide.
- Instructions about upgrading a clustered Expressway VM system are in the Cisco Expressway Cluster Creation and Maintenance Deployment Guide on the Cisco Expressway Series Configuration Guides page.
- For information about VMware supported versions, see Product Lifecycle Matrix.

If using the vSphere client, configure the network properties through the console.

Limitation

- This issue applies to Expressways running as virtualized systems with certain ESXi versions using VMware vCenter 7.0.x *(Prior to X15.0.2 for which this is not a valid configuration)*. It was found during testing using VMware vCenter 7.0.1 with ESXi 6.7.0 to deploy an Expressway OVA. The *Ready to complete* final page of the *Deploy OVF Template* wizard displays template values instead of the actual

values entered on the earlier wizard pages. The issue is cosmetic, and when you click “FINISH” the OVA will deploy as expected using the entered values. Bug ID CSCvw64883 refers.

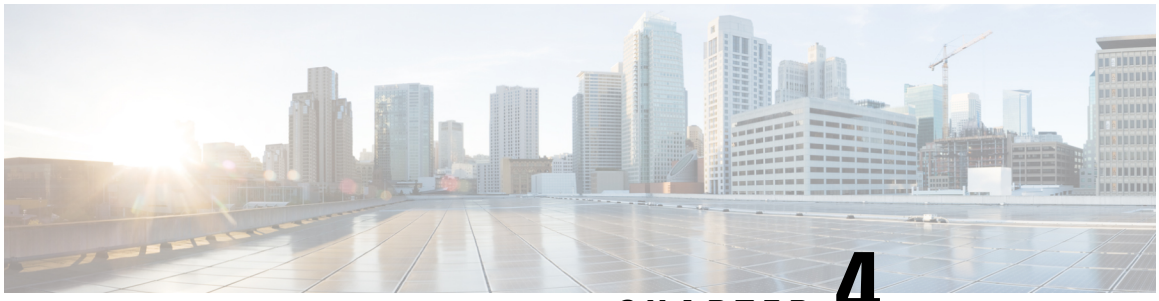
- Video calling capacity may be restricted if the ESXi Side-Channel-Aware Scheduler is enabled, and CPU load exceeds 70%.
- With physical appliances, the **Advanced Networking** feature allows the speed and duplex mode to be set for each configured Ethernet port. You cannot set port speeds for virtual machine-based systems.

  Also, virtual machine-based systems always show the connection speed between Expressway and Ethernet networks as 10000 Mb/s, regardless of the actual physical NIC speed. This is due to a limitation in virtual machines, which cannot retrieve the actual speed from the physical NIC(s).

PART III

System Management

- System Requirements, on page 15



CHAPTER 4

System Requirements

- Supported Platforms, on page 15
- Virtual Machine Requirements, on page 16
- How to Modify Expressway VM Capacity, on page 17
- Co-residency Support, on page 17

Supported Platforms

The following is a list of software X15.4.0 supported platforms:

- VMware vSphere ESXi on Cisco or 3rd party Hardware.
- Cisco NFVIS-for-UC hypervisor on BE6K, BE7K, CE1400V appliances only
- Nutanix AHV/AOS on Cisco Compute Hyperconverged with Nutanix hardware only (no appliances, no 3rdparty).
  - AHV version 10.0 with AOS version 7.0.
  - PrismCentral version 2024.3

Note

- For more information, see "Chapter 2: Hypervisors Used"
- For more information, see "Cisco Virtualization Guide for Cisco On-premises Calling Applications".

Supported Hardware

Cisco Expressway validates virtual CPU and memory reservations at boot time. If the documented reservations are not configured in the hypervisor, Expressway will display a hardware compliance warning even if the underlying host CPU exceeds the required performance. This behavior is expected.

Warning Your current hardware does not meet supported VM configuration requirements.

Cisco HCI Infrastructure, which supports Nutanix.

Note CE1400V is not supported as a hypervisor with Nutanix.

See Virtualization for Cisco Expressway for the current list of supported UCS Tested Reference Configurations and specs-based supported platforms.

Virtual Machine Requirements

Note We strongly recommend you not to use any power management features.

Important Make sure that the following requirements are in place:

- VT is enabled in the BIOS before you install the hypervisor.
- *This is specific to ESXi only.* The VM host "**Virtual Machine Startup/Shutdown**" setting is configured to "**Allow Virtual machines to start and stop automatically with the system**", and the VM Expressway has been moved to the Automatic startup section.

Do not change the MAC address of the VM

The serial number of a virtual Expressway is based on the virtual machine's MAC address. The serial number is used to validate Expressway licenses and to identify Expressways that are registered to the Cisco Webex cloud. Do not change the MAC address of the Expressway virtual machine when using VMware tools or similar.

Use the VM .ova/tar.gz file for initial VM installation only

The VM Expressway is licensed using information that is generated at the time of virtual machine deployment. If the .ova or NFVIS tar.gz is used to install additional instances they would be unique, new licensing information would be created, and to use the new VM, new release and license keys would need to be purchased. To upgrade a VM Expressway, follow the procedure under Upgrading or Downgrading an Expressway VM, on page 57, using the `VM.ova` or `tar.gz` version of the Expressway software.

Take a backup after completion

After the VM installation is complete, we recommend that you take a backup of the configuration.

Caution Do not take VMware snapshots of Cisco Expressway systems. The process interferes with database timing and negatively impacts performance.

How to Modify Expressway VM Capacity

Increasing the capacity of a VM-based Expressway from a smaller deployment size to a larger deployment (Small -> Medium -> Large) or decreasing the capacity from a larger deployment to a smaller one (Large -> Medium -> Small) **cannot be done by simply increasing or decreasing the underlying vCPUs and memory hardware resources of the VM**. The correct method to upgrade or downgrade is to deploy a new VM of the required deployment size and then restore the existing configuration (smaller VM for upgrade and larger VM for downgrade) onto the new one.

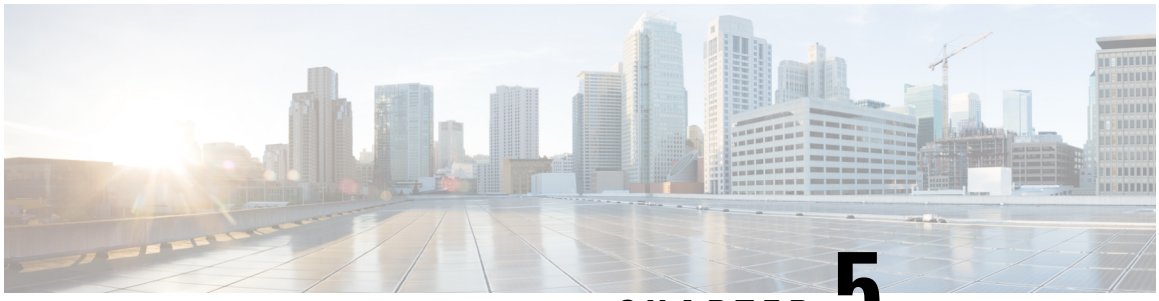
Co-residency Support

For more information, see Cisco Virtualization Guide for Cisco On-premises Calling Applications.

PART IV

Deploying Expressway Virtual Machine on the Different Hypervisors

- VMware vSphere ESXi , on page 21
- Nutanix AHV, on page 31
- Cisco NFVIS-for-UC, on page 33



CHAPTER 5

VMware vSphere ESXi

- Installing the Expressway VM using vCenter or vSphere Client, on page 21
- Deploying OVA to Host Managed by vCenter, on page 22
- Configuring the VM Guest to Standalone ESXi Host, on page 23
- Deploying OVA to Standalone ESXi Host, on page 25
- Automating the Deployment Process, on page 28

Installing the Expressway VM using vCenter or vSphere Client

Installation Process

This process guides you through installing Expressway VM using vCenter or vSphere client. Before you start the installation, make sure all the system requirements are in place, as detailed in the chapter, System Requirements.

Configuring the VM Host

Before you begin

Ensure that the VM host is configured with a valid NTP server – the same NTP server that will be specified in Expressway.

Procedure

Step 1 Select the host.

Step 2 Go to the **Configuration** tab.

Step 3 Select **Time configuration**.

Step 4 Select **Properties**.

If the date and time were red on the previous page, set the date and time manually to the current time.

Step 5 Click **Options**.

Step 6 Select **NTP Settings**.

Step 7 Click **Add**.

Step 8 Enter the IP address of the NTP server.

Step 9 Click **OK**.

Step 10 Select the **Restart NTP service to apply changes** check box.

Step 11 Click **OK**.

Step 12 Click **OK**.

What to do next

The following section describes how to deploy the ova to host using vCenter. If you are using vSphere, skip this section and go to Deploying OVA to Standalone ESXi Host.

Deploying OVA to Host Managed by vCenter

These instructions represent a typical installation. The Deploy OVF Template wizard dynamically changes to reflect host configuration.

Procedure

Step 1 If the .ova file is already preloaded onto the ESXi Host datastore (for example, in Cisco Business Edition 6000 deployments):

a) Using a web browser, go to `https:///folder` supplying any required credentials (typically the same username and password as used to log into vCenter).

b) Navigate through the index of datacenters to find the .ova file you want to deploy from the datastore.

c) Right click on the .ova file and select **Copy Link Location**.

(If the .ova file is not preloaded onto the datastore, you can select and upload it in the following steps.)

Step 2 Log in to vCenter to access the ESXi Host.

Step 3 Select **File** > **Deploy OVF Template.**

Step 4 On the **Source** page, identify where the .ova file is located, and then click **Next**.

- If the .ova file is already preloaded onto the ESXi Host datastore, paste the URL you copied from step 1 above. You may have to re-enter username and password credentials so that vCenter can access the web server.
- If the .ova file is not preloaded on the datastore, **Browse** to the location of the .ova file.

Step 5 On the **OVF Template Details** page, check that the Publisher certificate is valid and click **Next**.

Step 6 On the **End User License Agreement** page:

a) Read the EULA.

b) If you accept the EULA, click **Accept**. Click **Next**.

Step 7 On the **Name and Location** page enter a **Name** for this Expressway VM guest, for example "**`Virtual_Expressway`**" and click **Next**.

Important

When deploying a VM to ESXi version 6.0 or later, you must not use a backslash or forward slash in the VM name as the characters are unsupported and it can cause errors during the deployment. You must remove the slash from the default name of Cisco Expressway/VCS Base.

Step 8 On the **Deployment Configuration** page, select the appropriately sized deployment:

a) Select **`Small`**, **`Medium`** or **`Large`** depending on the capabilities of the VMware host.

The default is Medium. See System Requirements, on page 15 for details about resource requirements. If the VMware host has insufficient resources, the virtual Expressway will fail to power on / boot.

b) Click **Next**.

Step 9 On the **Host / Cluster** page, select where you want to run the virtual Expressway and click **Next**.

Step 10 On the **Resource Pool** page, select where you want to run the virtual Expressway and click **Next**.

Step 11 On the **Storage** page, select the location onto which the virtual Expressway will be deployed and click **Next**.

Step 12 On the **Disk Format** page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.

Step 13 On the **Network Mapping** page, select the network mapping that applies to your infrastructure (the default is **VM Network**) and then click **Next**.

Important
In Expressway versions 12.5.3 and earlier, the network name must contain only ASCII characters. From 12.5.4 release, network name can also contain non-ASCII characters.

Step 14 On the **Properties** page, configure the network properties of the virtual Expressway and click **Next**.

The properties you can set include Expressway's IPv4 and IPv6 settings, the timezone, hostname and domain, up to five NTP servers, and up to five DNS servers. For automated deployments you can also enter an RSA SSH public key to securely set the root and admin passwords via SSH. If you do not enter a public key, you must set the passwords during the Install Wizard process.

Important
The hostname and domain name must contain only ASCII characters.

Step 15 On the **Ready to Complete** page:

a) Confirm the deployment settings.
b) Select the **Power on after deployment** check box.
c) Click **Finish**.

The installation process will begin, and a progress bar will be displayed.

The Expressway OVA is now deployed as a Guest on the VM Host.

Configuring the VM Guest to Standalone ESXi Host

These instructions describe how to configure the VM Guest as a standalone host using the Install Wizard.

Note

- If you encounter issues or enter incorrect information during the wizard you can press Ctrl+D to restart.
- The pre-X8.9 default passwords of the admin and root accounts are well known. You must use strong passwords for these accounts. If your new system is on X8.9 or later, you must supply non-default passwords.
- The pre-X8.9 default passwords of the admin and root accounts are well known. You must use strong passwords for these accounts. If your new system is on X8.9 or later, you must supply non-default passwords.
- The default timezone is UTC but you can search for your desired timezone. You can also change it later in the web interface by going to **System** > **Time**.
- The default values support tab completion.

Procedure

Step 1 Select the VM guest and then select the **Console** tab.

The VM guest will take some time to boot, create its second hard disk partition and then reboot to the Install Wizard.

Step 2 Follow the prompts given by the Install Wizard to specify the following:

- Whether you want to use IPv4, IPv6 or Both.
- The LAN 1 IPv4 subnet mask of the Expressway (if you have selected IPv4).
- The IP address of the default gateway of the Expressway.
- The root password. Should be unique, do not use the same password as for admin account.
- The admin password. Should be unique, do not use the same password as for root account.
- Whether you want to enable the web UI.
- Whether you want to use SSH to administer the Expressway.
- The timezone.

Step 3 After the wizard is finished the following message will appear:

```
Installation wizard complete

Press Enter to continue the boot and apply the configuration.
```

Press **Enter**.

Step 4 After it has applied the configuration and rebooted, the Expressway is ready to use. You should now be able to access the Expressway using a web browser.

What to do next

You can now manage the Expressway licensing and basic configuration; see Expressway Service Selection, Licenses, and Basic Configuration.

Deploying OVA to Standalone ESXi Host

These instructions represent a typical installation. The Deploy OVF Template wizard dynamically changes to reflect host configuration.

Note The desktop vSphere Client is not available from vSphere 6.5 and later.

Before you begin

Important When deploying an OVF template in vSphere, the IPv4 address fields are mandatory and must be populated even if the "Enable IPv4" option is not enabled.

Procedure

Step 1 If the .ova file is already preloaded onto the ESXi Host datastore (for example, in Cisco Business Edition 6000 deployments):

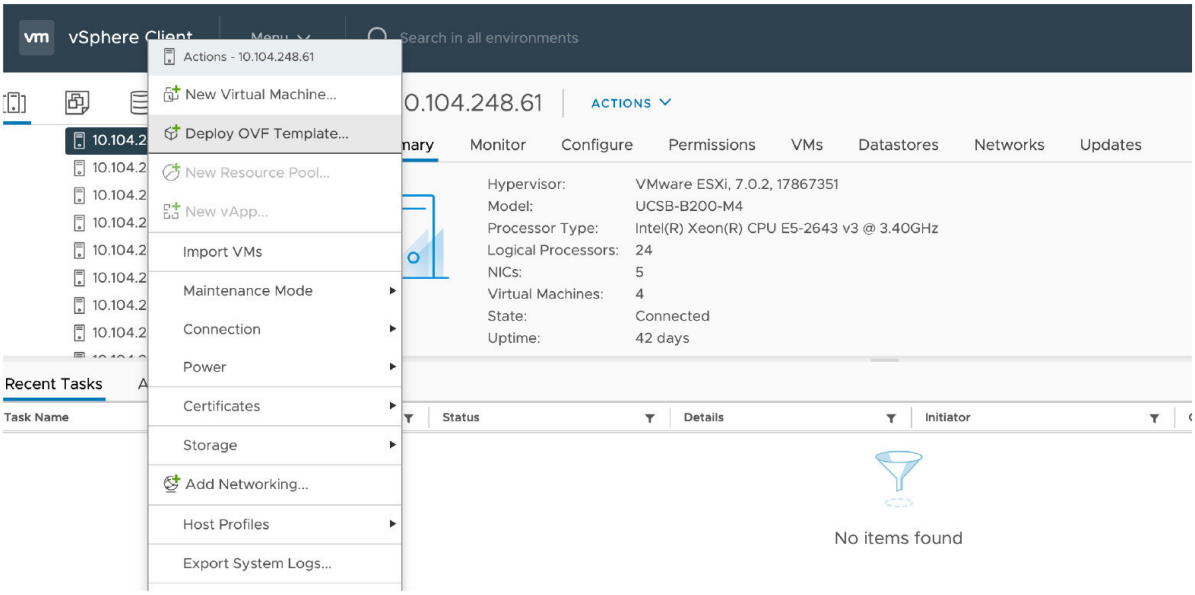
a) Using a web browser, go to `https://<VMwareHost>/folder` supplying any required credentials (typically the same username and password as used to log into the vSphere client).
b) Navigate through the index of datacenters to find the .ova file you want to deploy from the datastore.
c) Right click on the `.ova` file and select **Copy Link Location**.

(If the `.ova` file is not preloaded onto the datastore, you can select and upload it in the following steps.)

Step 2 Log in to the vSphere client to access the ESXi Host.

Step 3 Select **File** > **Deploy OVF Template**.

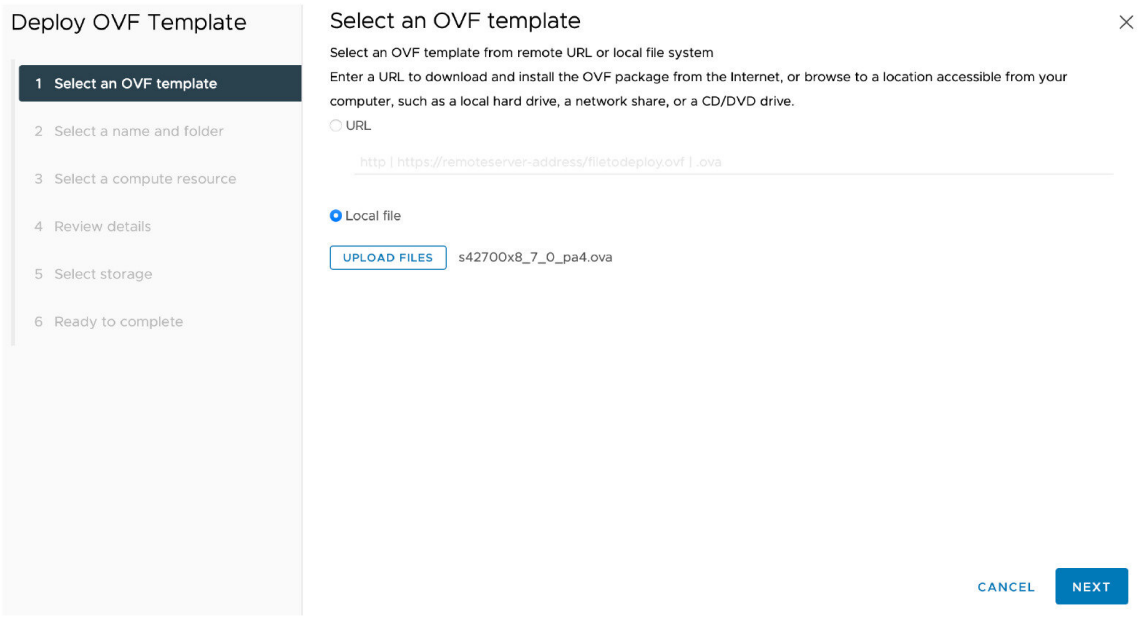
Figure 1: Deploy OVF Template



Step 4 On the **Source** page, identify where the .ova file is located, and then click **Next**.

- If the .ova file is already preloaded onto the ESXi Host datastore, paste the URL you copied from step 1 above. You may have to re-enter username and password credentials so that the vSphere client can access the web server.
- If the `.ova` file is not preloaded on the datastore, **Browse** to the location of the .ova file.

Figure 2: Browse .ova File



Step 5 On the **OVF Template Details** page, check that the Publisher certificate is valid and click **Next**.

Step 6 On the **End User License Agreement** page:

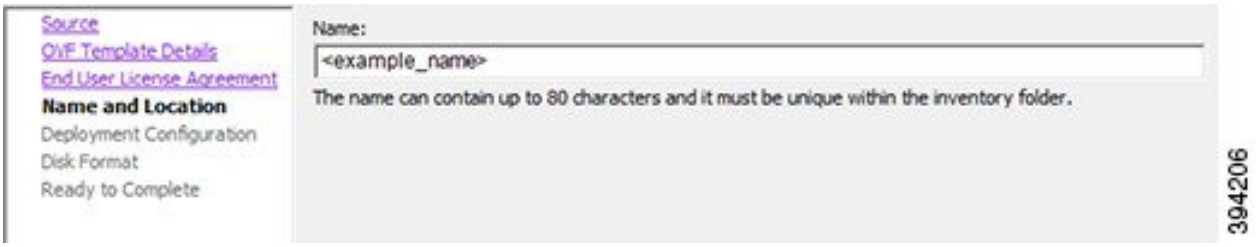
a. Read the EULA

b. If you accept the EULA, click **Accept**. Click **Next**.

Step 7 On the **Name and Location** page enter a **Name** for this Expressway VM guest, for example "Virtual_Expressway" and click **Next**.

Important
When deploying a VM to ESXi version 6.0 or later, you must not use a backslash or forward slash in the VM name as the characters are unsupported and it can cause errors during the deployment. You must remove the slash from the default name of Cisco Expressway/VCS Base

Figure 3: Name and Location



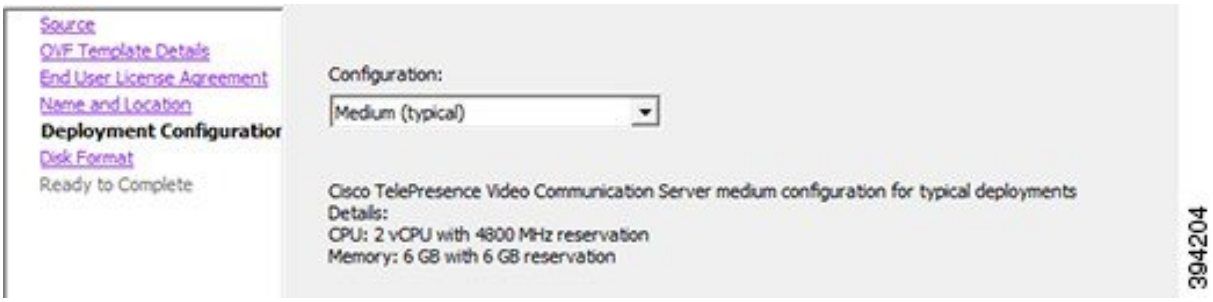
Step 8 On the **Deployment Configuration** page, select the appropriately sized deployment:

a) Select **`Small`**, **`Medium`** or **`Large`** depending on the capabilities of the VMware host.

The default is **`Medium`**. See System Requirements, on page 15 for details about resource requirements. If the VMware host has insufficient resources, the virtual Expressway will fail to power on / boot.

b) Click **Next**.

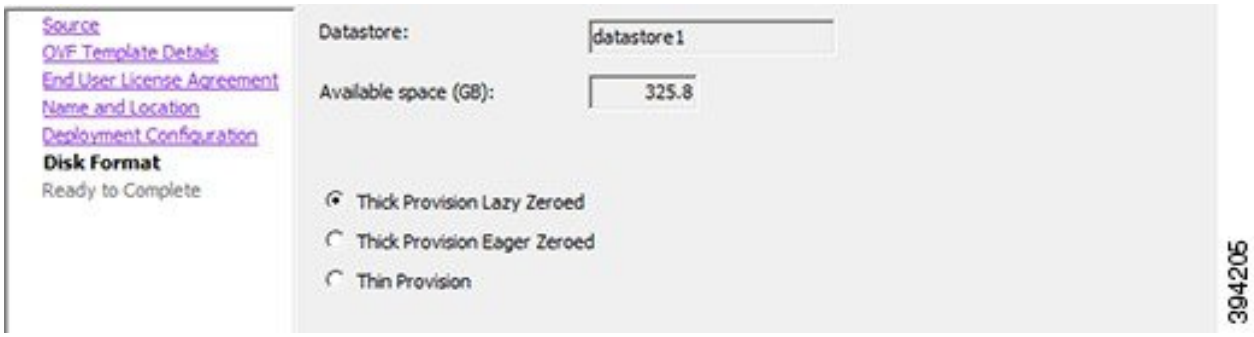
Figure 4: Deployment Configuration



Step 9 On the **Disk Format** page, ensure that the default disk format of **Thick Provision Lazy Zeroed** is selected and then click **Next**.

Thin Provision is not supported as VM performance may degrade during resizing of a partition.

Figure 5: Disk Format



Step 10 On the **Ready to Complete** page:

a) Confirm the deployment settings.
b) Select the **Power on after deployment** check box.
c) Click **Finish**.

The installation process will begin, and a progress bar will be displayed.

The Expressway ova is now deployed as a guest on the VM Host.

Automating the Deployment Process

We recommend deploying an Expressway VMware OVA in an automated manner. To do this:

Procedure

Step 1 Deploy the VM using VMware's OVFTool:

```
Ovftool -acceptAllEulas -ds=<vsphere datastore> --powerOn -noSSLVerify
--name=<name of VM> --prop:ip4.address=<ip address> --prop:ip4.gateway=<gateway>
--prop:ip4.netmask=<subnet mask> --prop.dmi.enable=<enable>
--prop.dmi.ip4.address=<dmi ipv4 address> --prop.dmi.ip4.netmask=<dmi ipv4 netmask>
--prop.dmi.ip6.address=<dmi ipv6 address> --prop:default.dns=1.1.1.1 -nw=<vsphere network>
--X:waitForIp --prop:ssh.public.key='<public ssh key>' <OVA file>
```

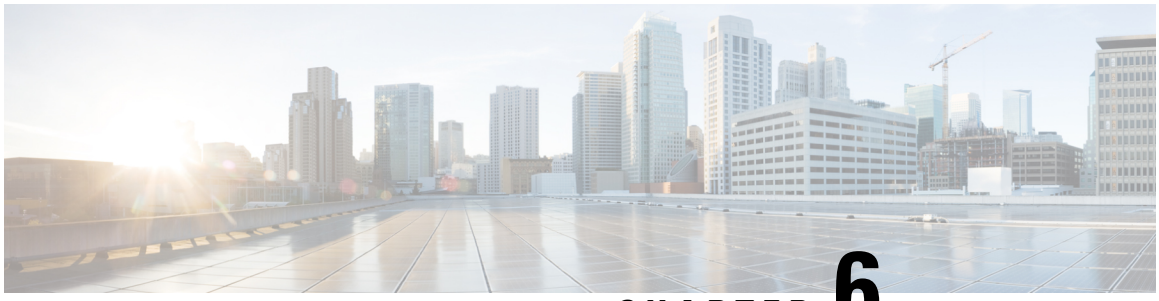
For more details of the command syntax, including examples, see the OVFTool User's Guide.

Step 2 Configure the *root* and *admin* passwords using ssh on port 5022 or port 22. See the section Set the Root and Admin Password Using SSH.

Note
This property `--prop:ssh.use.standard.port=True` can be used to install wizard to listen on port 22. Otherwise, the install wizard listens on port 5022.

Step 3 There are multiple ways to automate the deployment, for example, you can use Python Paramiko SSH library command:

```
{{command = '{"admin.password": "x", "root.password": "x"}\n'}}
```



CHAPTER 6

Nutanix AHV

- VM Deployment using OVA, on page 31
- VM Lifecycle Management, on page 32
- Performance Monitoring, on page 32

VM Deployment using OVA

This section outlines procedures for deploying, managing, and monitoring Virtual Machines (VMs) in the Nutanix environment using Open Virtualization Format (OVF) files.

Procedure

Step 1 Log in to the **Nutanix Prism Central or management** portal to access the **Infrastructure** dashboard.

Step 2 Navigate to **Compute** > **OVAs** under the **Infrastructure** menu. Select the option to upload your OVA file, either by browsing local storage or providing a remote URL.

Step 3 Ensure you select the specific Nutanix-compatible image, typically identified by the **XXXX_nutanix.ova**.

Step 4 For local uploads, you can track progress in real time or delegate the process to a background task. URL-based uploads will trigger a "`Successfully created OVA upload task`" notification.

Step 5 Monitor the ingestion process status at any time by navigating to **Activity** > **Tasks**. Once complete, the image will appear as **Active** in the **OVA**s section.

Step 6 Select the uploaded OVA and navigate to **Actions** > **Deploy as VM**.

While the OVA includes preconfigured parameters, you must manually define the CPU allocation.

Note
Nutanix implementations currently support only **Medium** and **Large** deployment profiles.

Step 7 Under the **Network**s section, click **Edit** to map the virtual interfaces to the appropriate subnets. You must assign a network to all three interfaces to satisfy deployment prerequisites.

Note
Ensure the boot mode is set to **Legacy BIOS**.

In **Management** settings, set the system time zone to match your local time zone.

Review the configuration summary and select **Create VM**. You can track the provisioning status via the quick-view drawer in the top-right corner.

What to do next

For Managing Virtual Machine, see Virtual Machine Lifecycle Management.

VM Lifecycle Management

Procedure

Step 1 Navigate to **Compute** > **VMs** to locate and verify the newly provisioned instance.

Step 2 Access the **VM details** page.

Note
The remote console is unavailable until the instance is initialized.

Step 3 To start the machine, navigate to **More** > **Power On**.

Step 4 Once the VM is in a "**Running**" state, click the **Console** button to launch the **interactive remote management interface**.

Step 5 Use the **More** menu to execute specific power state changes:

- **Guest Reboot:** Initiates a graceful restart signal to the Guest OS.
- **Reset:** Performs a hard reset of the virtual hardware, then immediately powers on.
- **Power-Cycle:** Executes an immediate cold boot of the VM.
- **Guest Shutdown:** Sends an ACPI signal to gracefully terminate the OS.

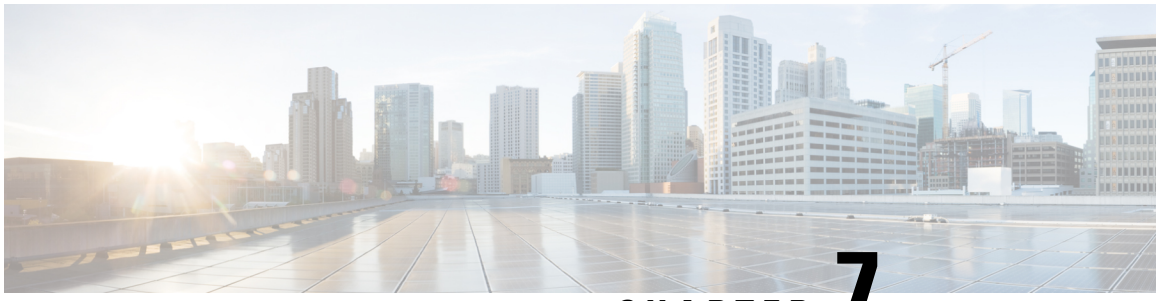
What to do next

For information on "Monitoring the Performance", see Performance Monitoring.

Performance Monitoring

Select the **Metrics** tab within the **VM** view to access real-time performance data.

The system tracks 23 distinct telemetry points, providing deep visibility into CPU utilization, memory residency, IOPS, and I/O read/write latency.



CHAPTER 7

Cisco NFVIS-for-UC

- Deploying Virtual Machines, on page 33
- Managing Virtual Machines, on page 36
- Monitoring Virtual Machines, on page 36

Deploying Virtual Machines

Upload ISO Image to Datastore: This section provides instructions for deploying, managing, and monitoring Virtual Machines (VMs) within the NFVIS management portal.

NFVIS supports two registration methods:

- **Local Registration:** Upload the **XXXX_NFVIS.tar.gz** file directly from your workstation.
- **Remote Registration:** Import the file from a network location via HTTP, FTP, or SCP.

Before you begin

Verify that the correct Product ID (PID), such as BE6k or BE7k, is displayed on the dashboard.

Note NFVIS requires the `.tar.gz` distribution package; standard Expressway `.ova` files are not supported.

Procedure

Step 1 To upload an image using the **local registration** method, perform the following:

a) Navigate to **Configuration** > **Virtual Machine** > **Images** > **Image Repository**.

b) **Select File**

Click the **Select File** field and choose a file with a supported format (.iso, .ova, .tgz, .tar, .gz, .img, .vmdk, .qcow2, .raw, .docker). For example, s42700x15_4_0_NFVIS.tar.gz is selected.

c) **Upload the File** *(if not already uploaded)*

Click **+ Upload File** to upload the selected file or **Delete File** to remove an existing one.

```
An "Image upload started" notification will appear.
```

d) **Select Destination**

From the **Select Destination** dropdown, choose the target datastore. For example, `datastore1(internal)`

e) **Image Name**

The **Image Name** automatically populates in the field. This is the default selection. For example, `s42700x15_4_0_NFVIS.tar.gz`

f) **Select VM Workload Type**

In the **VM Workload Type** dropdown field, `Calling` should appear by default.

Note
Make sure you select the **VM Workload Type** as `Calling` if it does not.

g) **Select VM Type**

From the **VM Type** dropdown, choose the VM type: `EXPRESSWAY`.

h) **Enable Dedicated Cores**

Select the **Dedicated Cores** check box. For production environments, this is necessary to meet documented performance expectations.

i) To submit the registration, click the **Upload File** button.
j) Monitor the progress via the *blue* status indicator. Once complete, a *green* checkmark will appear.
k) The system will automatically detect the image type as Expressway and identify the version. The initial state will show as "`Create`" and transition to "`Active`" once the image is ready.

Step 2 To upload an image using the **remote registration** method, perform the following:

a) Navigate to **Configuration** > **Virtual Machine** > **Images** > **Image Repository**.
b) To select the Remote Registration, click **Register Image** and select **Remote Image Registration** option.
c) To configure the Image Details, enter a descriptive name in the **Image Name** field. For example, `exwy-15.4`.
d) To configure the Remote Server Connection Protocol, enter the following details:

- **Protocol**: Select from the drop-down list (HTTP/HTTPS/FTP/SCP).
- **IP Address:** Enter the server hostname or IP address.
- **Image File Path:** Enter the directory path to the ISO file with the image name.

e) Enter the Configure Authentication details for FTP/SCP (only).

- **Username:** Enter the username for the remote server.
- **Password:** Enter the password.

f) **Select VM Type**

From the **VM Type** dropdown, choose the VM type: `EXPRESSWAY`.

g) **Enable Dedicated Cores**

Select the **Dedicated Cores** check box. For production environments, this is necessary to meet documented performance expectations.

h) To submit the registration, click the **Submit** button.

NFVIS performs the following:

- Download the ISO image from the remote server
- Upload and parse the OVA file
- Register the image
- Automatically create profiles/flavors from OVA metadata

i) To verify registration, wait for the process to complete. The image should appear in the Image Repository with the status **Active**. Verify that flavors are populated from the OVA file.

Note
Downloading large files may take several minutes.

Step 3 **Deploy VM via NFVIS Portal**

a) Navigate to **Configuration** > **Deploy** to deploy a new virtual machine. The interface will display a canvas showing existing VM connections.
b) Select an option from the VM. Select the **Calling** menu to view available applications and choose **Expressway**.

Note
If your application type is not listed, select OTHER. If necessary, you can change the name of the VM Type created.

c) Choose the required image from the drop-down list. Images are populated based on the VM type selected.
d) Select the uploaded `.tar.gz` file and choose the appropriate deployment profile.
e) To configure Network Connections, perform the following in the Network Design section:

- Locate the VM icon on the canvas.
- Drag a line from the VM to the desired network.
- Connect to the appropriate network(s) for your deployment. Enter the directory path to the ISO file.
- Add additional networks as required.

Note
Network Mapping: Use the interactive canvas to drag and connect the VM to your desired network segments.

f) Click **Deploy** to initiate the process. You can monitor the progress on the canvas or via the **Notifications** tab.

```
A confirmation message will appear upon successful deployment.
```

What to do next

To know more about managing virtual machines, see Managing Virtual Machines.

Managing Virtual Machines

Administrative tasks and power operations are handled through the management interface.

Procedure

Accessing VM Details:

- Navigate to **Configuration** > **Virtual Machine** > **Manage**. Click on a specific VM name to view interface configurations and software image details.
- **Network Configuration:** Click the **Edit** button next to the `VM name` to modify network assignments based on your environmental requirements.
- **Console Access:** Click the **Cursor** icon to launch the CLI console in a new browser tab.
- **Power Operations:**
  - **Reload:** Located under **Action Items**, this performs an immediate Power-On or hard reset.
  - **Switch Power:** Use this to gracefully shut down or power on the VM.
- **Event Logging:** Review the **Logs** section under **Action Items** to verify VM events, such as shutdown, reboot, or power-off sequences.

What to do next

To learn more about monitoring virtual machines, see Monitoring Virtual Machines..

Monitoring Virtual Machines

NFVIS provides real-time performance metrics and resource allocation data to ensure system health.

Performance Metrics

Navigate to **Monitoring** > **Virtual Machine** and select a VM from the canvas to view the following telemetry:

- **CPU Utilization:** Tracks performance for all vCPUs.
- **Memory Utilization:** Monitors overall RAM consumption.
- **vNIC & Network Stats:** Displays throughput (Rx/Tx) and packet drop rates.
- **Disk Utilization:** Monitors data for virtual disks A and B.
- **Historical Data:** All metrics can be filtered by duration: 5 minutes, 1 hour, 6 hours, 1 day, or 5 days.

Host Resource Allocation

To view the physical resource distribution, navigate to **Monitoring** > **Host** > **Resource Allocation**.

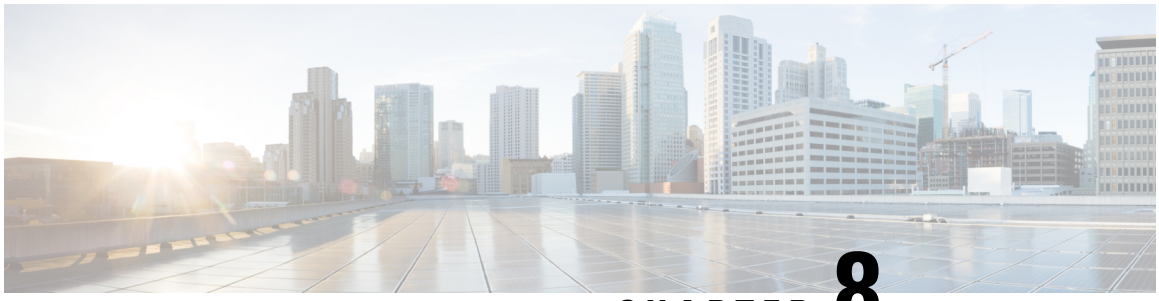
This page provides a high-level overview of:

- **CPU Allocation:** Available vs. allocated CPU sockets.
- **Memory & Disk:** Total virtual memory and physical hard disk availability.

PART V

Configuring the Deployed Virtual Machines

- Configure Expressway after Deployment, on page 41



CHAPTER 8

Configure Expressway after Deployment

The chapter implies to all three hypervisors.

1. VMware vSphere ESXi
2. Nutanix AHV
3. Cisco NFVIS-for-UC

This chapter explains the method to configure Expressway after deployment.

• Configuring the Hypervisors, on page 41

Configuring the Hypervisors

These instructions describe how to set the root and admin password over SSH if you entered an RSA SSH public key in the **VM Properties** page – used primarily for automated deployments - or using the Install Wizard.

Note You can ignore any floppy read errors that appear, as they are not relevant to this deployment mode.

Set the Root and Admin Password Using the Install Wizard

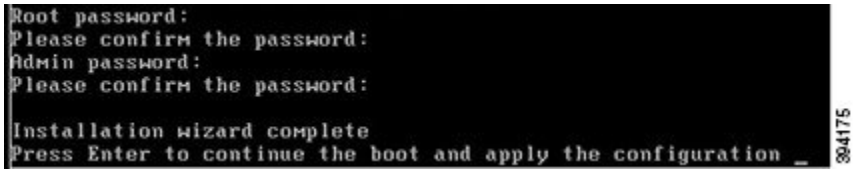
Procedure

Step 1 Select the VM guest and then select the **Console** tab.
You are taken to Install Wizard.

Step 2 Enter and confirm your root and admin passwords. You will also be prompted to set any property you did not set in VMware.

Note
These passwords should be unique; do not use the same password for admin and root accounts.

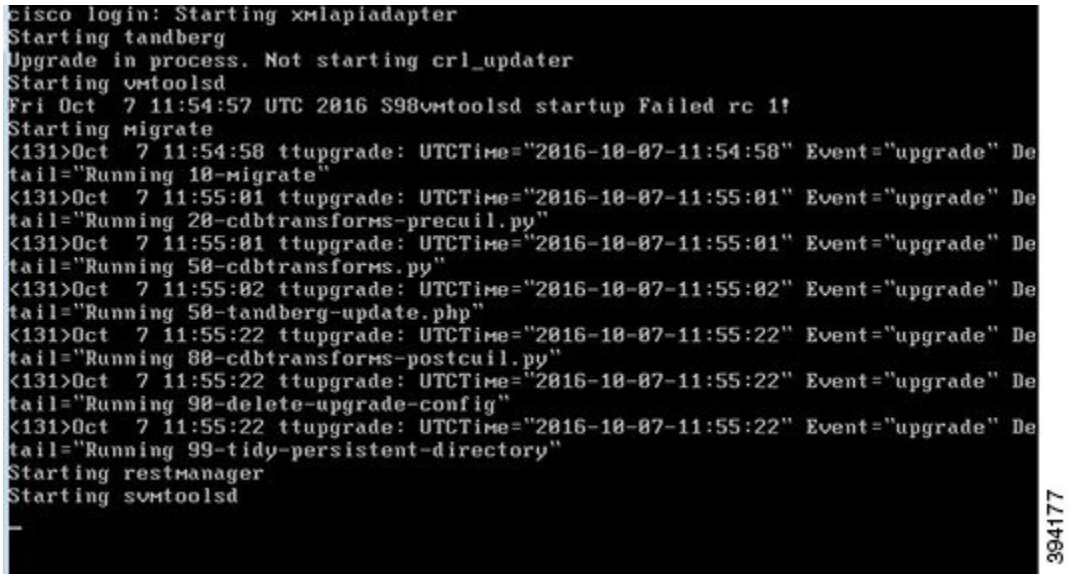
Figure 6: Enter Root and Admin Password



Step 3 Press Enter to apply the configuration.

Step 4 The Expressway will apply the configuration and reboot.

Figure 7: Configuration Applied



You should now be able to access the Expressway using a web browser.

You can now order your option keys; see Expressway Service Selection, Licenses, and Basic Configuration.

Set the Root and Admin Password Using SSH

The vSphere client or OVF Tool (for install Expressway) provides an interface to set the *root* and *admin* password.

You can set the *root* and *admin* password using Secure Shell Protocol (SSH) on any one of the following ports.

- Port 5022
- Port 22

Port 5022

1. The Install Wizard starts an SSH daemon, listening on port 5022, to set the *root* and *admin* password.

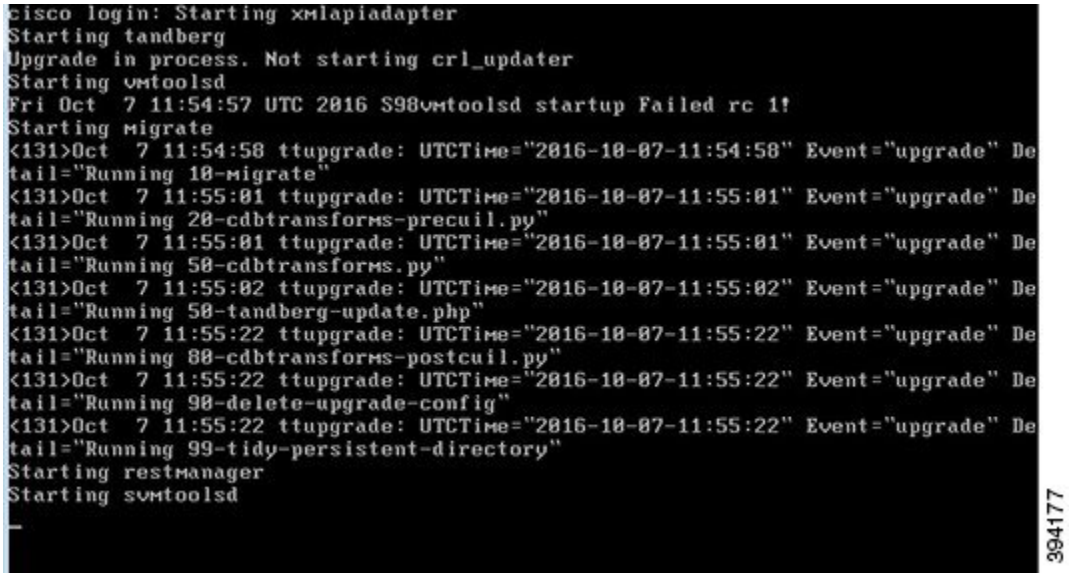
2. Connect as user “wizard” using an SSH client on port 5022 (for example, `ssh wizard@192.168.0.100 -p 5022`).
3. Follow the prompt to set `admin.password` and `root.password`.

Figure 8: Set Admin and Root Password

4. The Expressway will apply the configuration and reboot.

Result:

Figure 9: Configuration Applied



You should now be able to access the Expressway using a web browser.

You can now order your option keys; see Expressway Service Selection, Licenses, and Basic Configuration.

Port 22

1. The Install Wizard starts an SSH daemon, listening on port 22 (Standard SSH port), to set the *root* and *admin* password.
2. Connect as user “wizard” using an SSH client on port 22 (for example, `ssh wizard@192.168.0.100`).

3. Follow the prompt to set `admin.password` and `root.password`.
4. The Expressway will apply the configuration and reboot.

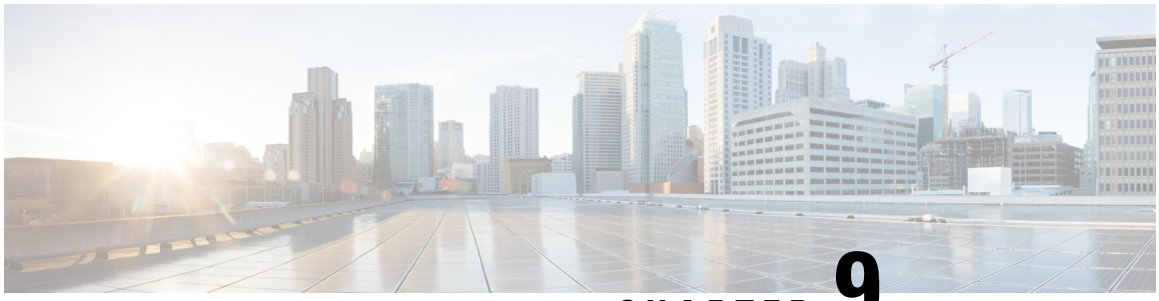
You should now be able to access the Expressway using a web browser.

You can now order your option keys; see Expressway Service Selection, Licenses, and Basic Configuration.

PART VI

Post Installation Tasks

- Expressway Service Selection, Licenses, and Basic Configuration, on page 47
- ESXi specific - Creating a Backup of Your System and Deleting Existing Snapshots, on page 49
- Hardware References, on page 51



CHAPTER 9

Expressway Service Selection, Licenses, and Basic Configuration

• Next Steps: Service Selection, Licenses, and Basic Configuration, on page 47

Next Steps: Service Selection, Licenses, and Basic Configuration

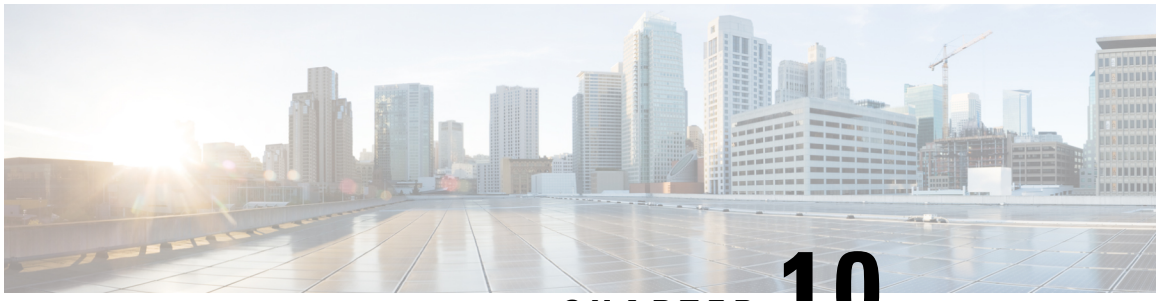
When you have the option keys:

Procedure

Step 1 Log in to the Expressway via a web browser as admin.

Step 2 Please refer to the *Basic Configuration Deployment Guide* on the Cisco Expressway Series configuration guides page to guide you through how to select services, apply licenses, and configure this VM Expressway ready for operation (including DNS, NTP, zones, and search rules).

Step 3 After the Expressway has been configured it is good practice to backup the Expressway configuration using the Expressway backup facility (see next section).



CHAPTER 10

ESXi specific - Creating a Backup of Your System and Deleting Existing Snapshots

This chapter is applicable ONLY for ESXi.

- Creating Backups, on page 49
- Deleting Existing Snapshots, on page 50

Creating Backups

We recommend that you regularly create backups of your configuration, as follows.

Caution Do not take VMware snapshots of Cisco Expressway systems. The process interferes with database timing and negatively impacts performance.

Procedure

Step 1 Go to **Maintenance** > **Maintenance Mode** and switch **Maintenance Mode** On.

Step 2 Go to **Maintenance** > **Backup and Restore**.

Step 3 You can optionally add a password for your backup file.

Step 4 Click **Create system backup file**.

Step 5 Save the backup file.

Note
When you restore your system from a backup, it does not include Active Directory credentials. You will need to add them in order to access the Active Directory domain.

Deleting Existing Snapshots

Procedure

Step 1 Make a backup of your configuration.

Step 2 Shutdown the Expressway:

a) Go to **Maintenance** > **Restart Options** and click **Shutdown**.

b) Click **OK** to shut down the system.

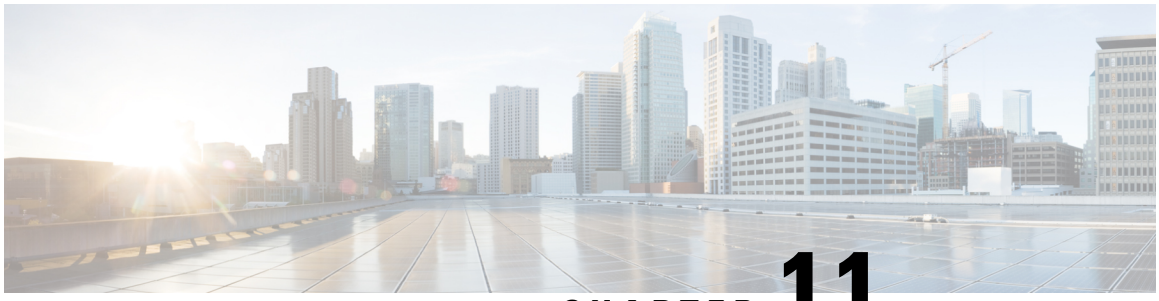
Step 3 Power off the VM.

Step 4 Right-click on the VM and select **Manage Snapshots**.

Step 5 In the **Snapshot Manager**, select **Delete All Snapshots**.

Step 6 Click **Yes** in the confirmation dialog box.

Step 7 Click **Close** to exit the Snapshot Manager.



CHAPTER 11

Hardware References

- Serial Interface, on page 51
- Ethernet Interfaces (NICs), on page 51
- ESXi specific - Allocating a Virtual NIC to a Physical NIC Interface, on page 51

Serial Interface

A VM Expressway has no physical serial interface; the serial interface is accessible through the console tab of the VM guest.

You can use CTRL+ALT to exit from the Console window (this is identified in the bottom right corner of the vSphereClient window).

Ethernet Interfaces (NICs)

In VM Expressway the LAN interfaces are Virtual NICs. Appropriate drivers are set up as VM Expressway is installed; configuration of IP addresses is carried out through the standard Expressway interface.

VM Expressway allocates 3 virtual NICs:

- The first is used for the standard LAN 1 interface.
- The second is used if Dual Network interfaces are enabled (LAN 2).
- The third is reserved for future use.

ESXi specific - Allocating a Virtual NIC to a Physical NIC Interface

Virtual NICs can be assigned to physical interfaces as follows:

Procedure

Step 1 Ensure that the physical NIC on the VM host is connected and operational.

Step 2 Set up or check that there are Virtual Switches (vNetwork Distributed Switches) for each physical NIC. (Select the host on which the VM Expressway will run, select the **Configuration** tab and select **Networking**.)

Step 3 Ensure that there is at least one Virtual Machine Port Group (with associated VLAN IDs) set up for each physical NIC.

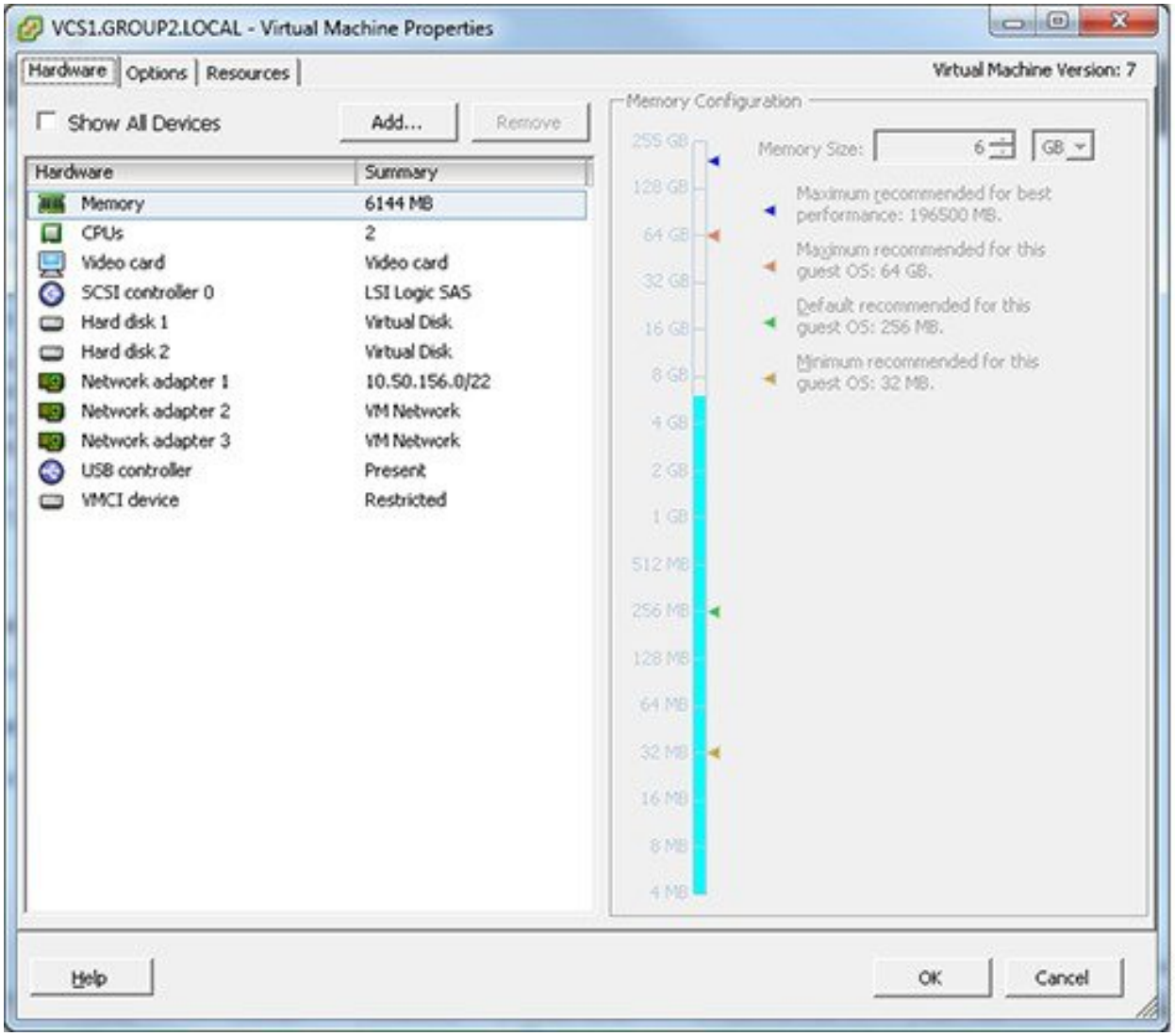
a) To add a new Virtual Machine Port Group, click **Properties** on the appropriate Virtual Switch or vNetwork Distributed Switch.

b) Follow the network wizard.

Step 4 Note the name of a Virtual Machine Port Group connecting to the required NIC.

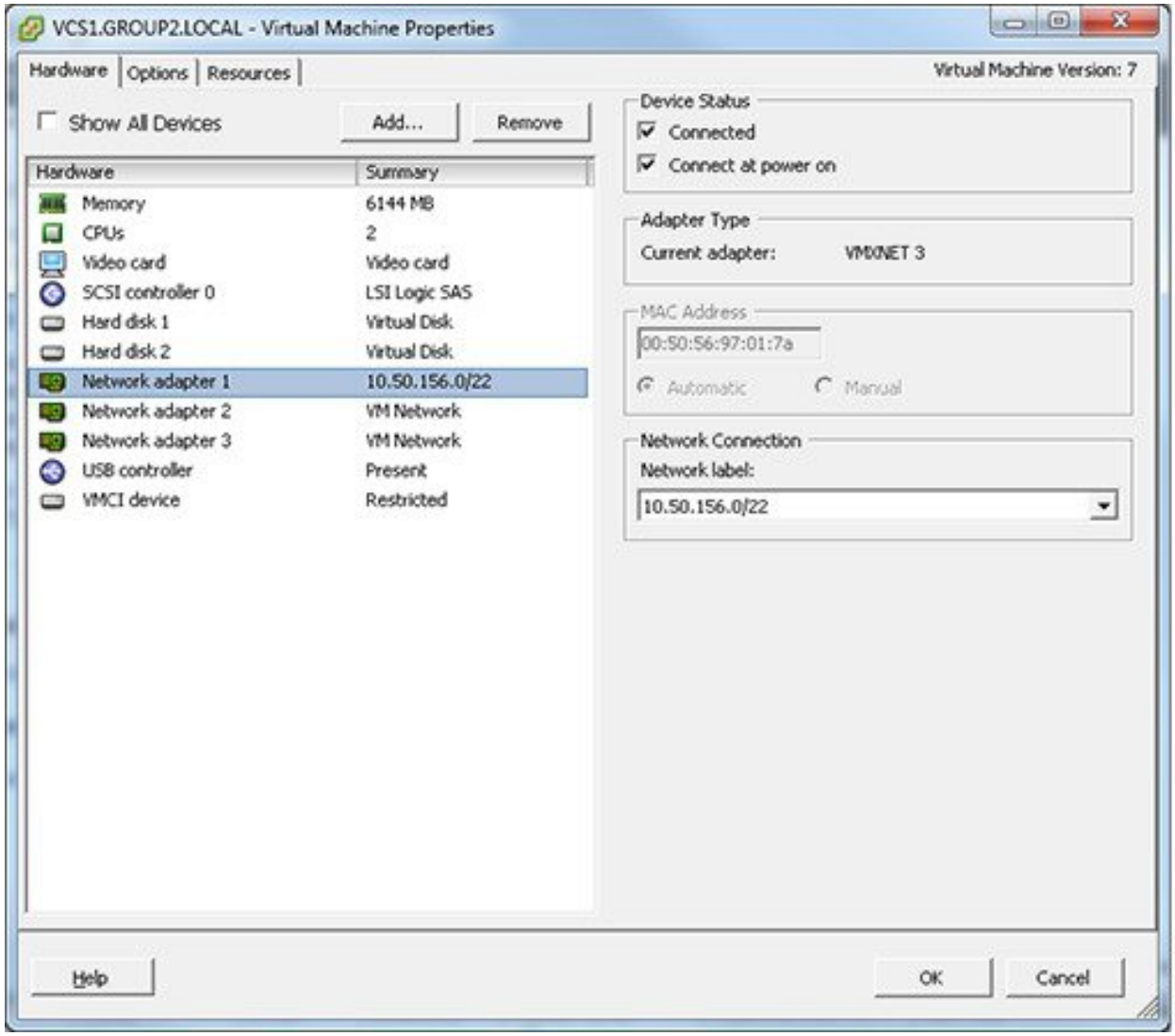
Step 5 Select the VM guest; right click it and select **Edit settings…**

Figure 10: Edit Settings



Step 6 Select the required network adaptor (Network adaptor 1 = LAN 1, Network adaptor 2 = LAN 2).

Figure 11: Select Network Adaptor



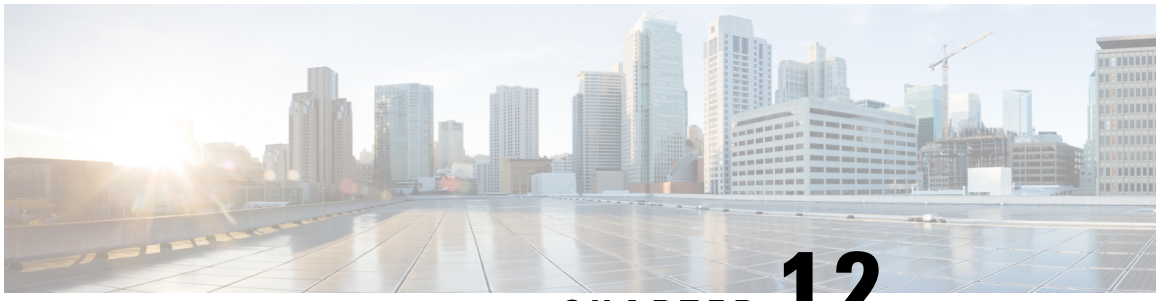
Step 7 Select the appropriate Network label (Virtual Machine Port Group) to associate the Expressway LAN interface with the required physical NIC.

Step 8 After a few seconds the Expressway will be able to communicate over the physical interface.

PART VII

Additional Hypervisor Information - ESXi specific

- Additional Information, on page 57
- Troubleshooting, on page 61
- Deploying Multiple Datastores, on page 67



CHAPTER 12

Additional Information

- Upgrading or Downgrading an Expressway VM, on page 57
- Clustering for Resilience and Capacity, on page 58
- Migrating from a Physical Appliance to a VM, on page 58
- Migrating the VM between ESXi Hosts (use VMware VMotion), on page 58
- Unsupported ESXi Features, on page 58
- Licensing, on page 59
- Security Hardening, on page 59

Upgrading or Downgrading an Expressway VM

Before you begin

Profile Information is Removed from Backups

From X12.6, Expressway backup files do not include system profile information (ProfileID value). This is to prevent a known issue with unexpected changes to sizing if a backup is restored across a different sized deployment. Therefore, device profiles are unaffected by backup and restore operations. Refer to Bug ID CSCvs59766.

Procedure

Step 1 Take a backup of the smaller (or the larger for downgrade) VM configuration. Use the Expressway's backup function, not the hypervisor backup or VMware snapshot function.

Step 2 Install and deploy the new, larger (or smaller for downgrade) VM as described in this guide.

Step 3 Restore the configuration of the (old) smaller (or the larger for downgrade) VM onto the newly deployed VM. Note that profile information will not be included in the backup/restore.

Clustering for Resilience and Capacity

If you cluster Expressway VMs, we strongly advise you to use at least two physical hardware hosts. Hardware resilience requires Expressway peers to run on at least two different hardware platforms.

For the current maximum supported round trip delay (RTT) and hop distances between peers, see the *Cisco Expressway Cluster Creation and Maintenance Deployment Guide* for your version, on the Cisco Expressway Series configuration guides page.

Migrating from a Physical Appliance to a VM

If you are migrating from a physical appliance to a VM, the backup/restore process (**Maintenance** > **Backup and restore**) can be used to transfer configuration between the two installations. You will receive a warning message, but you will be allowed to continue.

Migrating the VM between ESXi Hosts (use VMware VMotion)

If you need to move Expressway to a new host, you must use VMware VMotion to perform the host migration.

Before you start, there may be glitches (packet loss/jitter) in media for calls that are interworked by Expressway as the VM is moved. We recommend that a VMotion move is carried out when there is minimal activity on the VM Expressway. To ensure this, before you carry out the move put the Expressway VM into maintenance mode (**Maintenance** > **Maintenance mode**) and wait for active calls to clear.

Unsupported ESXi Features

VMware Fault Tolerant Mode

VMware fault tolerant mode is not supported (because the Expressway uses multiple cores).

VMware HA

We do not support VMware High Availability. We recommend clustering for resilience. If you need to move virtual Expressway, you can use VMotion.

VMware Snapshots

We do not support VMware snapshots. We recommend you take regular backups of the Expressway instead.

Shutdown VCS/Expressway VMs Before Upgrading ESXi Host

We recommend shutting down VCS/Expressway virtual machines (VMs) before upgrading ESXi host. Not shutting down the VMs can damage or cause database (DB) instability to the VCS/Expressway servers.

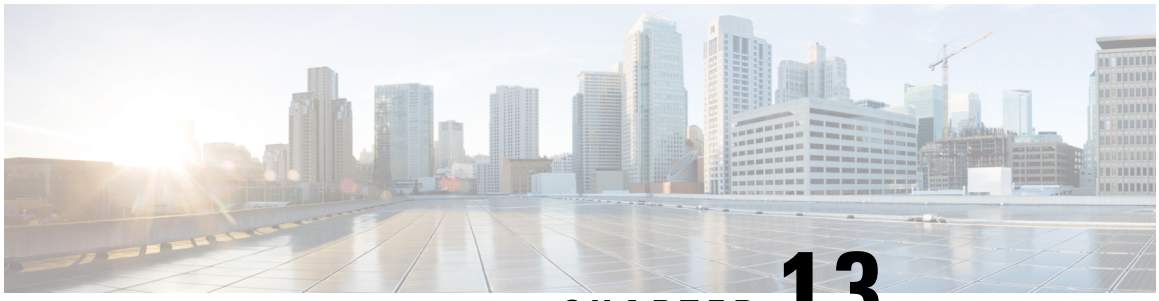
Licensing

A virtual Expressway requires licensing in the same way that an Expressway appliance requires licensing.

Do not copy the VM, as the Expressway serial number will change and the existing license keys and option keys will be invalidated. If you need to move Expressway to a new host, use VMware VMotion to perform the host migration.

Security Hardening

Information on how to deploy and operate VMware products in a secure manner is available from the VMware Security Hardening Guides.



CHAPTER 13

Troubleshooting

- Checking VMware Compatibility, on page 61
- VMware Checklist, on page 61
- Isolating a Possible Root Cause, on page 62
- Possible Issues, on page 63
- Analyzing the Cause of VMware Issues, on page 64
- Restoring the Default Configuration (Factory Reset), on page 64
- Resetting Your Administrator Password or Root Password, on page 66

Checking VMware Compatibility

If you use third-party hardware to host the VM Expressway application, check the hardware compatibility. You can do this with the VMware compatibility guide tool from http://www.vmware.com/resources/compatibility/search.php.

VMware Checklist

Procedure

Step 1 Check accessibility to the VM host server (by ping, physical console access, SSH remote access, KVM-over-IP console, and so on).

Step 2 Check network connectivity of the VMkernel (by executing the **vmkping** command using Tech Support Mode to verify network connectivity from the VMkernel NIC level).

Step 3 If you have problems connecting to the vSphere Client management console, execute the **command/sbin/services.sh** from an SSH session to restart the ESXi management agent.

Step 4 Check the VM host server utilization. CPU utilization, memory utilization, disk access speed, storage access speed, network access status, power utilization, and so on.

If any specific application causes high utilization, stop or restart this application to isolate the overall VM host performance level. Or execute the command **esxtop** from Tech Support Mode to list all system processes running on the ESXi host application.

Step 5 Check the ESXi server file log (`hostd.logs`) under the folder `/var/log/vmware`. This log contains common error logs such as iSCI naming error, authentication error, and host convertibility error.

Step 6 Verify that adequate disk space is available on the physical volume that stores the database files. Free up disk space if necessary.

Step 7 Validate authentication to the vCenter Server database. The vCenter Server service may not be able to authenticate with the database if:

a) There are permission issues with the database when importing from one instance to another.

b) The password on the account you are using to authenticate to the database has changed but the password in the registry has not.

c) The vCenter Server database user is not granted correct permissions.

Isolating a Possible Root Cause

Potential issue area	What to look for
Storage	Look for the VM store application image stored either on the local drive, SAN, or NFS. VMs often freeze or hang up if the application fails to access the storage. *ESXi:* Possible error messages are: • vCenter Server does not start. • vCenter Server is slow to respond. • vCenter Server fails after an indefinite amount of time.
Network	Any network failure or locking causes a connection failure between the VM and the virtual network. Also, if using NFS or iSCSI, storage may cause application failures because the application cannot access the file system.
DNS	*ESXi:* DNS server failures or communication failures between DNS and the VM server may cause the VMware application or the VM Expressway application to fail.
vCenter Server	If vCenter is not operating properly, although the VM Expressway application is still up and running, you may lose connection to the VM Expressway application from the network.
Host application	*ESXi:* Check for any critical alarms in the VM application for events at the host or application level (check the event information in vSphere Client). *NFVIS-for-UC:* Check for relevant entries in the 'notification' tab. *Nutanix:* Review recent tasks under **Activity/Tasks** in Prism Central.

Possible Issues

VM image fails to boot

If the VM image fails to boot, check the VT (Virtualization Technology) setting in BIOS. This needs to be enabled for hosting VMs. If it is not set, set it and reinstall ESXi then load the .ova file.

Expressway application fails to start

Look at the `/tmp/hwfail` file – its content indicates any violations in the installation.

For example, Expressway reserves 3 virtual NICs – these are required in the Expressway, do not try deleting one or more of them otherwise hwfail is created and the VM Expressway will not run.

Configured NTP does not work

For NTP to work on Expressway, the same NTP must also be configured on the VM host.

Guest console in vSphere 5 fails to run on some Microsoft platforms

When attempting to open a console screen from vSphere for the VM:

- Error message: "`The VMRC console has disconnected...attempting to reconnect.`"
- Screen remains black.

The following operating systems are at risk:

- Windows 7 64 bit – reported on VMware forum (http://communities.vmware.com/thread/333026)
- Windows Server 2008 R2 (64-bit) – found by use.

Web page/IP address unreachable after OVA deployment

This issue can be caused by a cache issue in the gateway switch.

To resolve, access vCenter, go to the console and ping the gateway: ping <`gateway_ip_address`>.

Clustering status incorrect after recreating a VM within a cluster

When recreating a VM within a cluster, the cluster must be broken and recreated for it to function correctly.

To resolve, take the following steps:

1. Back up the existing configuration from the original node you want to recreate.
2. Upgrade all nodes to X12.5.4.
3. Shut down guest on the original node.
4. Start up a new VM using the X12.5.4 .ova file and give it the same IP address as the original node.
5. Restore the backup configuration from the original node onto the new VM.
6. Rebuild the cluster and add the cluster configuration on the other nodes.

7. After approximately 10 minutes, clustering status on the **Status** > **Clustering** page should accurately indicate a normal status for the cluster.

Raid controller synchronization

If the VMware system is synchronizing its RAID disks, disk performance is seriously degraded. We strongly recommend that Expressway is not installed or run on VM platforms where RAID disks are in a degraded or synchronizing state.

Analyzing the Cause of VMware Issues

If issues exist with VMware on the Expressway host, we recommend that you collect logs from the host for analysis, using the following procedure:

Procedure

Step 1 Using the vSphere client (or the vCenter Server managing this ESXi host) connect to the ESXi host on which the Expressway is running.

Step 2 Go to **File** > **Export** > **Export System logs**, choose the appropriate ESXi host and go with the default settings.

What to do next

After you have downloaded the logs, analyze them or have them analyzed to determine the issue.

More information on exporting logs can be found at: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=653.

Restoring the Default Configuration (Factory Reset)

Rarely, it may be necessary to run the “factory-reset” script on your system. This reinstalls the software image and resets the configuration to the default, functional minimum.

Before You Begin

If you've upgraded since the system was first set up, be aware that the reset reinstalls your latest software version.

The system uses the default configuration values that currently apply in the software version installed by the reset. These may differ from your previously configured values, especially if the system has been upgraded from an older version. In particular this may affect port settings, such as multiplexed media ports. After restoring the default configuration you may want to reset those port settings to match the expected behavior of your firewall. (As described below, optionally it's possible to retain a few configuration values like option keys, SSH keys, and FIPS140 mode, but we recommend that you reset all these values.)

Prerequisites

- As the virtual machine console is required to complete this process, **you need appropriate VMware access inorder to open the VM console.**
- The factory reset procedure described below rebuilds the system based on the most recent successfully installed software image. A file containing the software image in tar.gz format, named `tandberg-image.tar.gz`, stored in the `/mnt/harddisk/factory-reset/` system folder is used for the reinstallation. In some cases this file is not present on the system (most commonly with a fresh VM installation that has not been upgraded). If so, you must first put this file in place using SCP as root.

Process to Reset to the Default Configuration

You must do this procedure from the console. Because the network settings are rewritten, all calls and any SSH session used to initiate the reset will be dropped and you won't be able to see the procedure output.

The process takes approximately 20 minutes.

Procedure

Step 1 Log in to the system as **root**.

Step 2 Type **`factory-reset`**

Step 3 Answer the questions as required. The recommended responses will reset the system completely to a factory default state:

Table 5:

Prompt	Recommended response
Keep option keys [YES/NO]?	NO
Keep FIPS140 configuration [YES/NO]?	NO
Keep IP configuration [YES/NO]?	NO
Keep ssh keys [YES/NO]?	NO
Keep server certificate, associated key and CA trust store [YES/NO]? This option does not preserve SNI / domain certificates, which are always deleted regardless of what you respond. Only the server certificate and associated key and CA trust store are saved (if you respond YES).	NO
Keep root and admin passwords [YES/NO]?	NO
Save log files [YES/NO]?	NO

Step 4 Confirm that you want to proceed.

Step 5 After the VM boots, you are taken to the Install Wizard. You must complete the wizard through the VM console. Some of the questions in the wizard may be skipped depending on your responses in step 3, but even if you preserved the IP configuration and password, you still need to complete the Install Wizard through the VM console.

Note
If you were using FIPS140 and you want to enable it again, see the relevant section in the Expressway Administrator Guide.

Resetting Your Administrator Password or Root Password

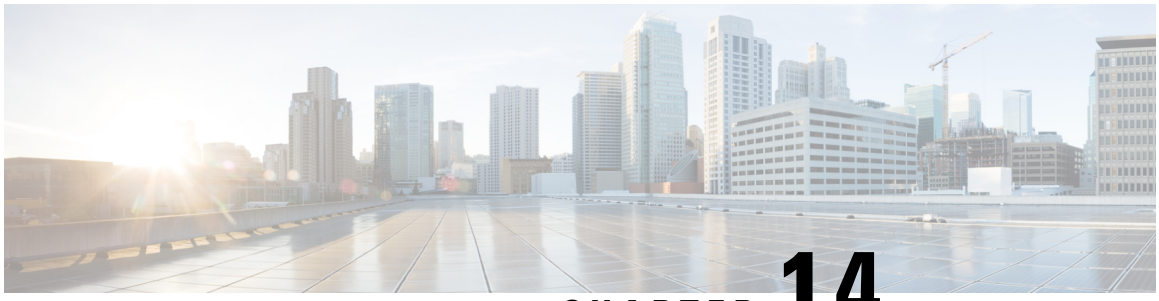
If you have forgotten the password for either an administrator account or the **root** account and you are using a VM (Virtual Machine) Expressway, you can reset it using the following procedure:

Procedure

Step 1 Open the vSphere client.
Step 2 Click on the link **Launch Console**.
Step 3 Reboot the Expressway.
Step 4 In the vSphere console log in with the username **`pwrec`**. No password is required.
Step 5 When prompted, select the account (root or the username of the administrator account) whose password you want to change.
Step 6 You will be prompted for a new password.

What to do next

The **pwrec** account is only active for one minute following a reboot. After that time you will have to reboot the system again to reset the password.



CHAPTER 14

Deploying Multiple Datastores

• Deploying Multiple Datastores, on page 67

Deploying Multiple Datastores

This process should be carried out during the initial build of the VM host, if the VM host has two or more RAID arrays of disk storage. This configuration enables vSphere / vCenter to know about all the datastores.

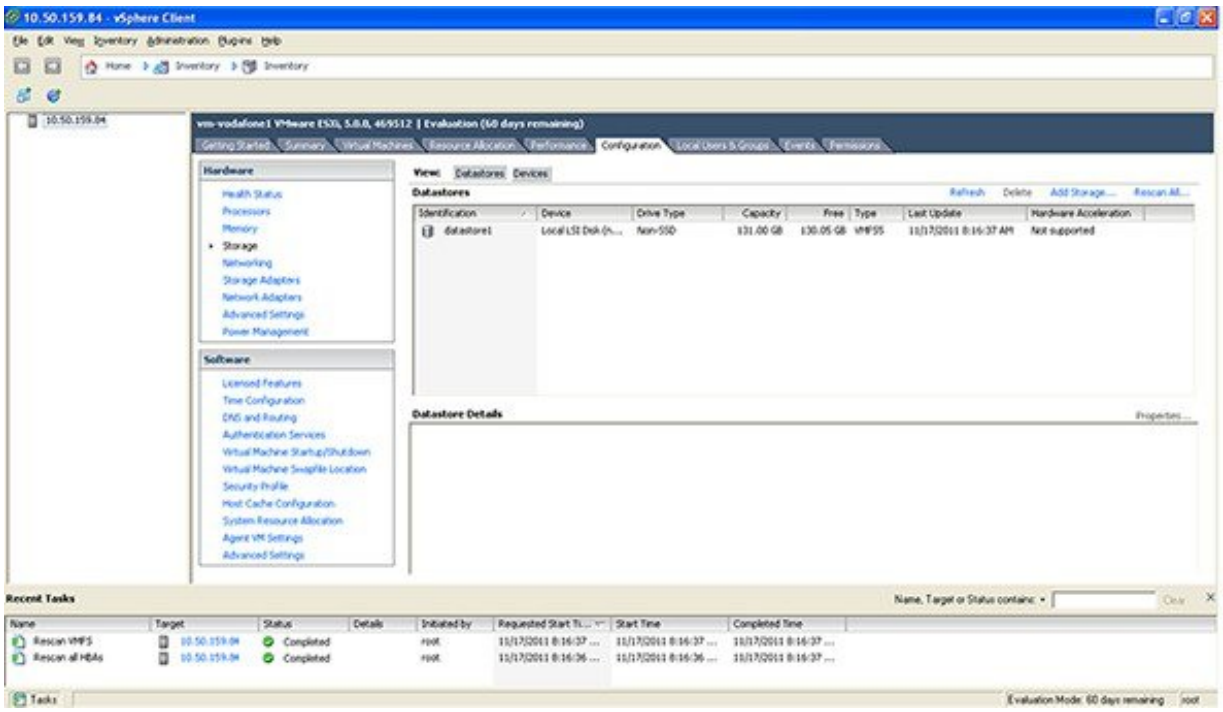
Procedure

Step 1 From vSphere or vCenter Inventory list select the relevant Host.

Step 2 Select the **Configuration** tab.

Step 3 Select **Storage**.

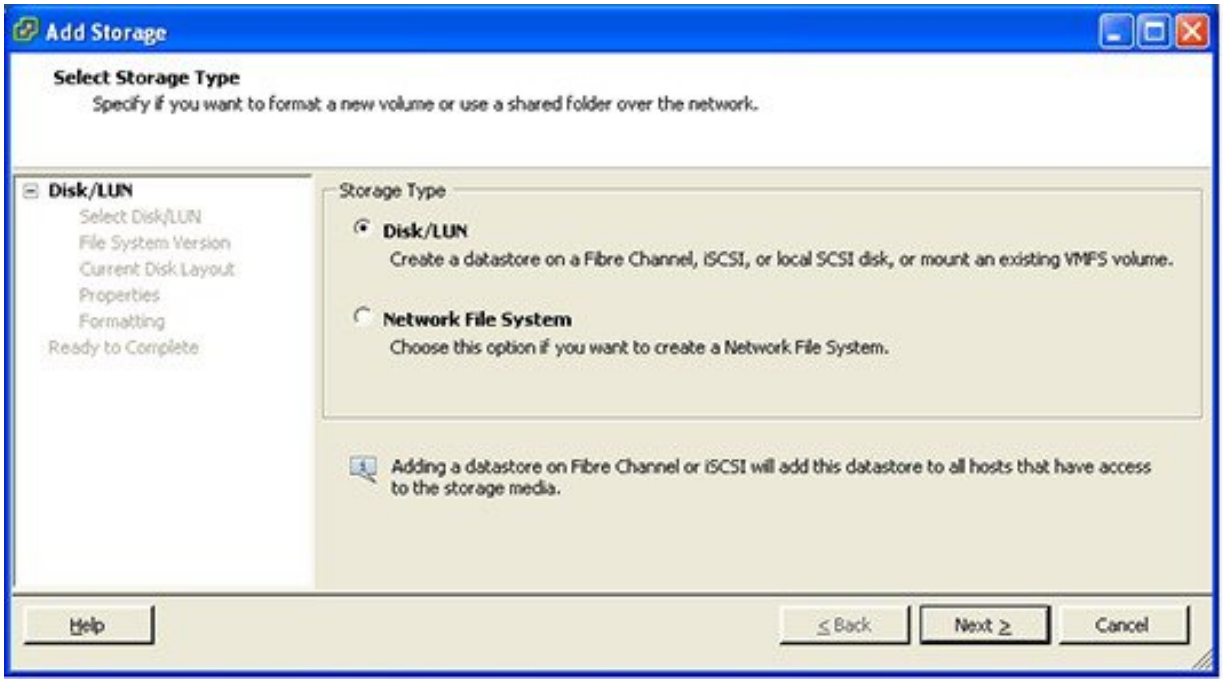
Figure 12: Select Storage



Step 4 Select **Add Storage …** (on the right hand side window).

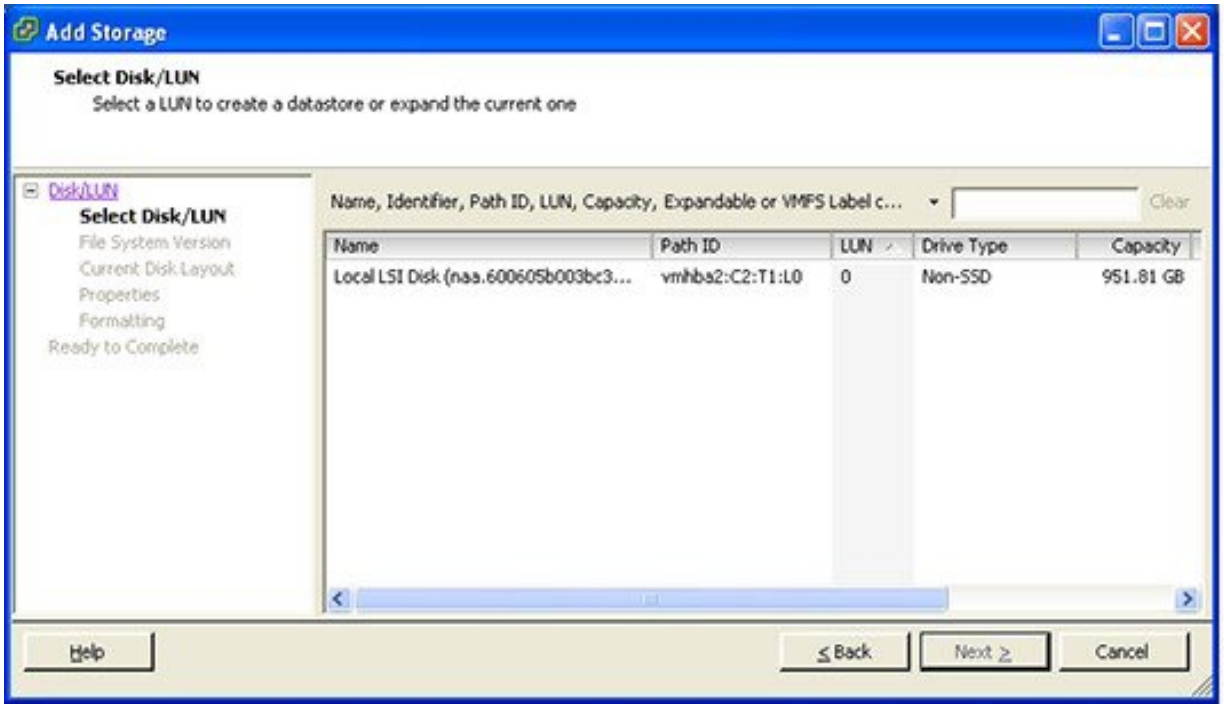
Step 5 Select **Disk/LUN** and click **Next**.

Figure 13: Select Disk/LUN



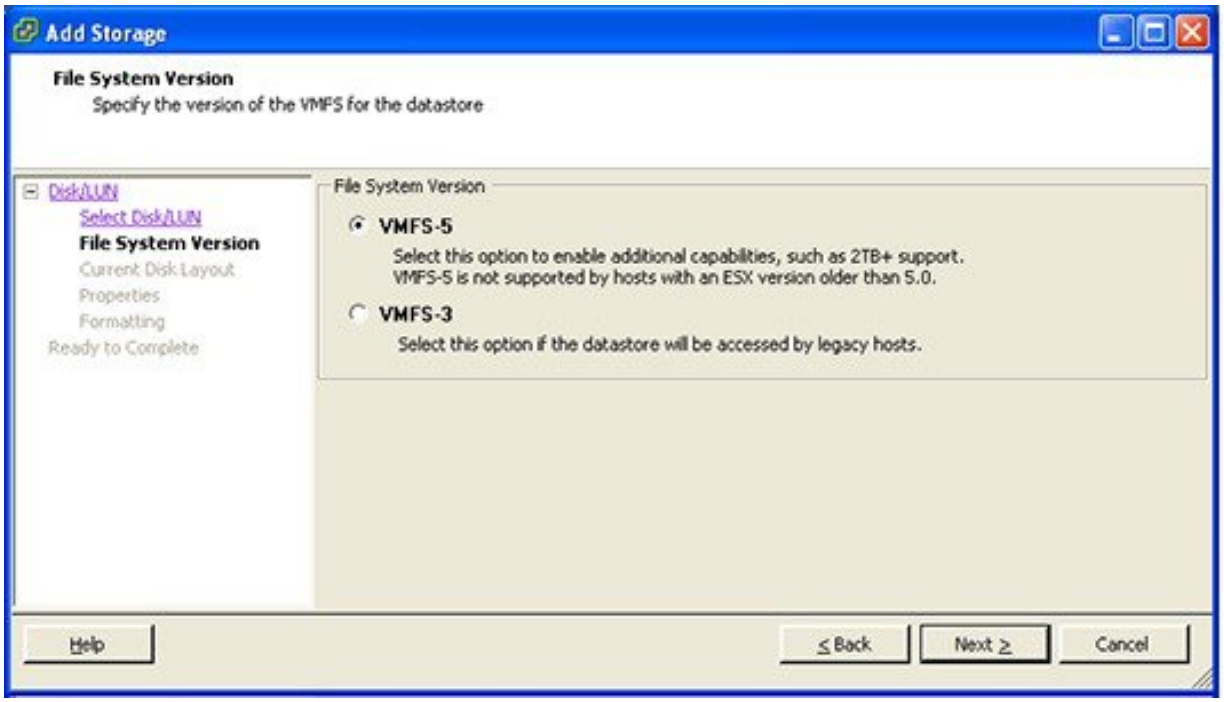
Step 6 Under **Disk/LUN** select the required Disc/LUN from the list presented and click **Next**.

Figure 14: Required Disc/LUN



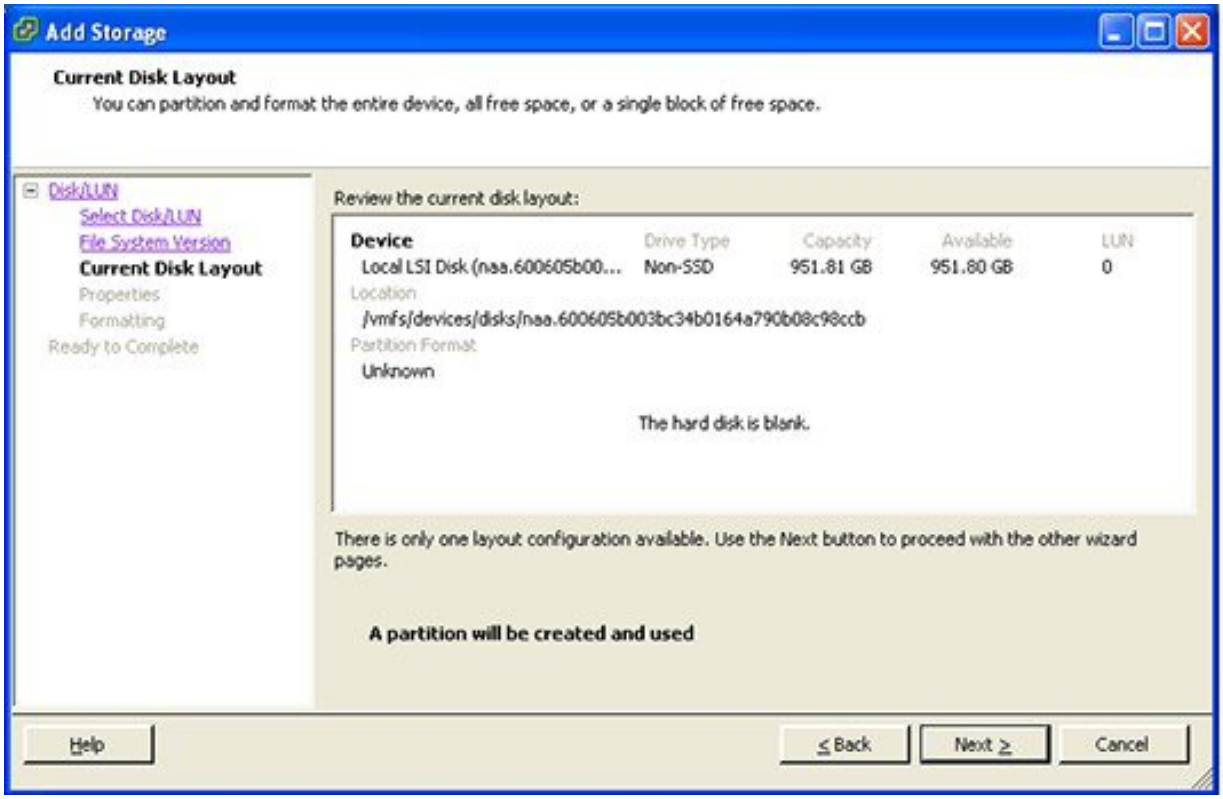
Step 7 On the **File System Version** page select **VMFS-5** and then click **Next**.

Figure 15: Select VMFS-5



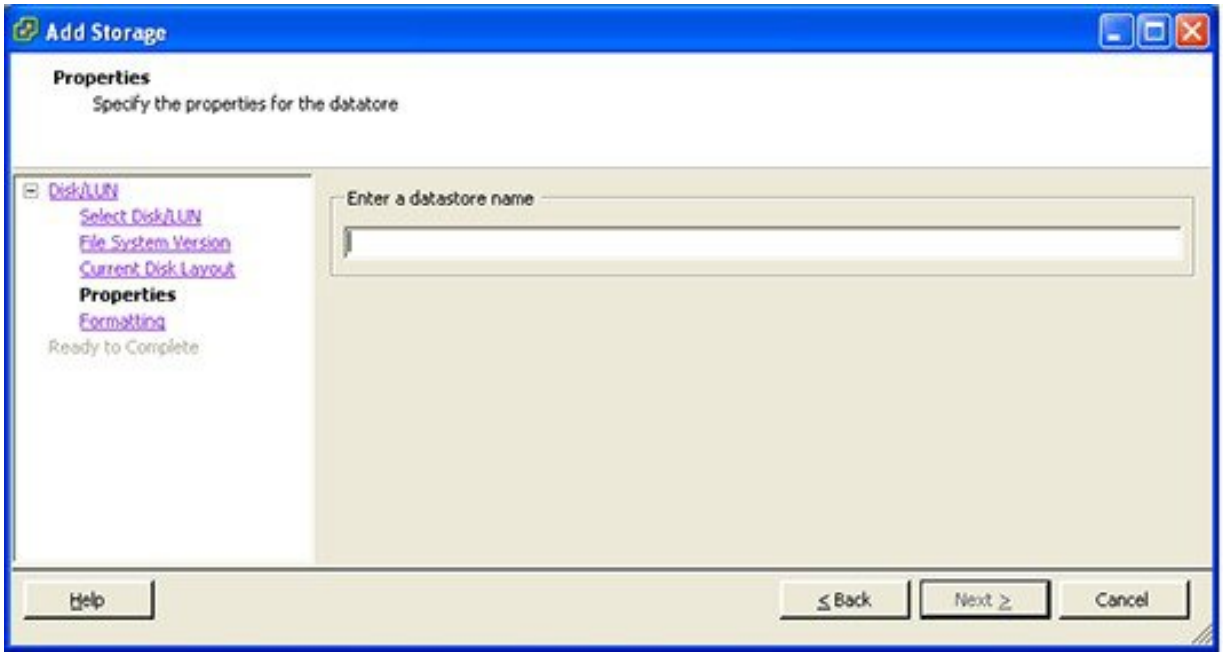
Step 8 On the **Current Disk Layout** page verify the details and then click **Next**.

Figure 16: Verify Details



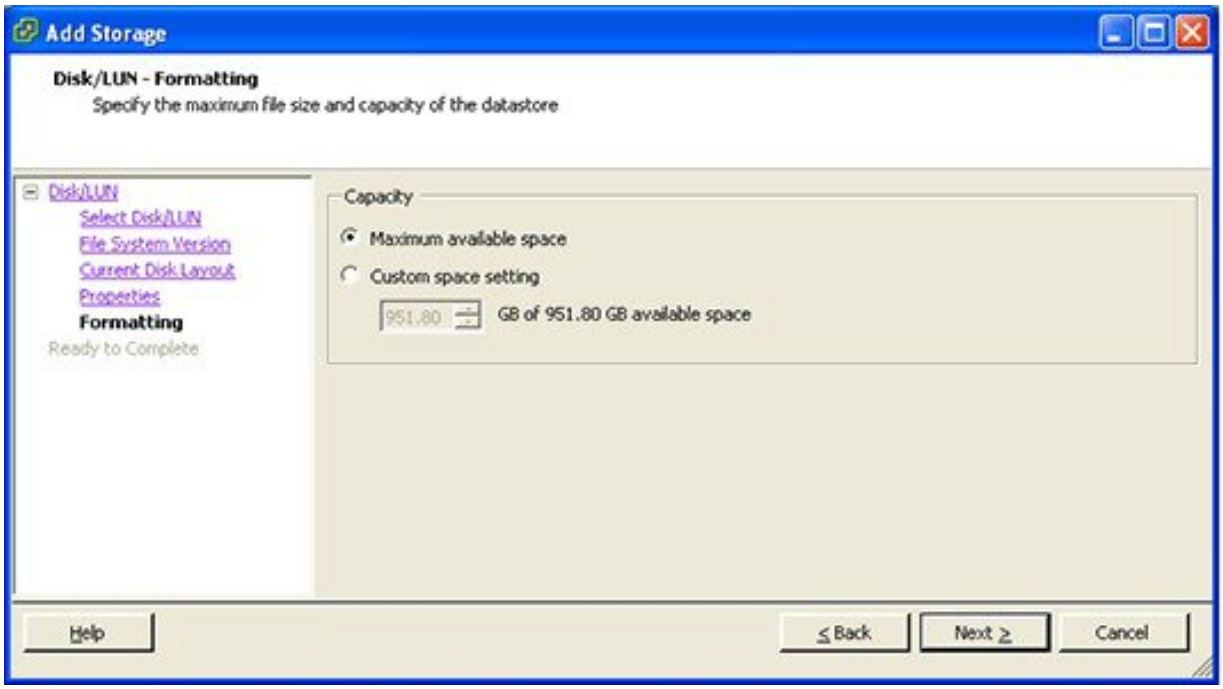
Step 9 On the **Properties** page enter a name for the new datastore and then click **Next**.

Figure 17: Name for New Datastore



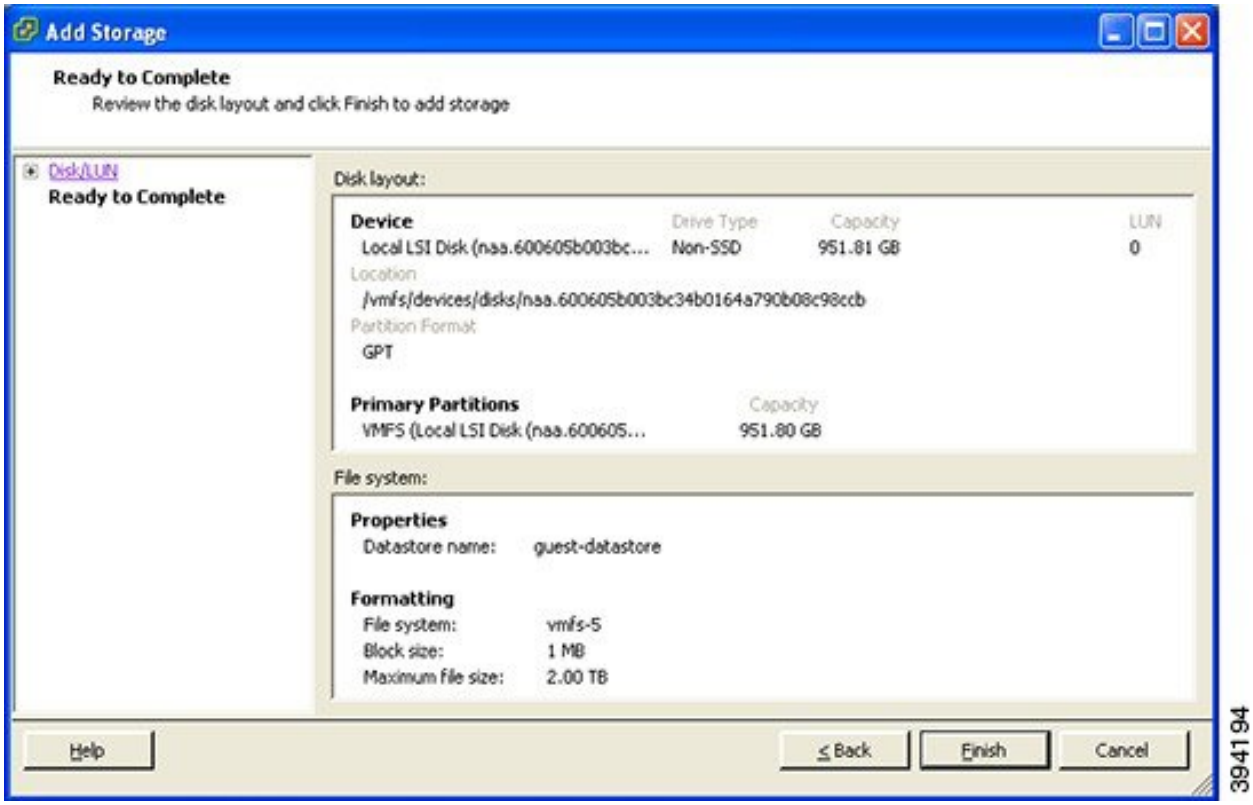
Step 10 On the **Formatting** page select **Maximum available space** and then click **Next**.

Figure 18: Select Maximum Available Space



Step 11 On the **Ready to Complete** page verify the details and then click **Finish**.

Figure 19: Verify the Details



Step 12 Wait for the Create VMFS Datastore task to complete.

Step 13 On completion, the new datastore will be listed under the **Storage** section.

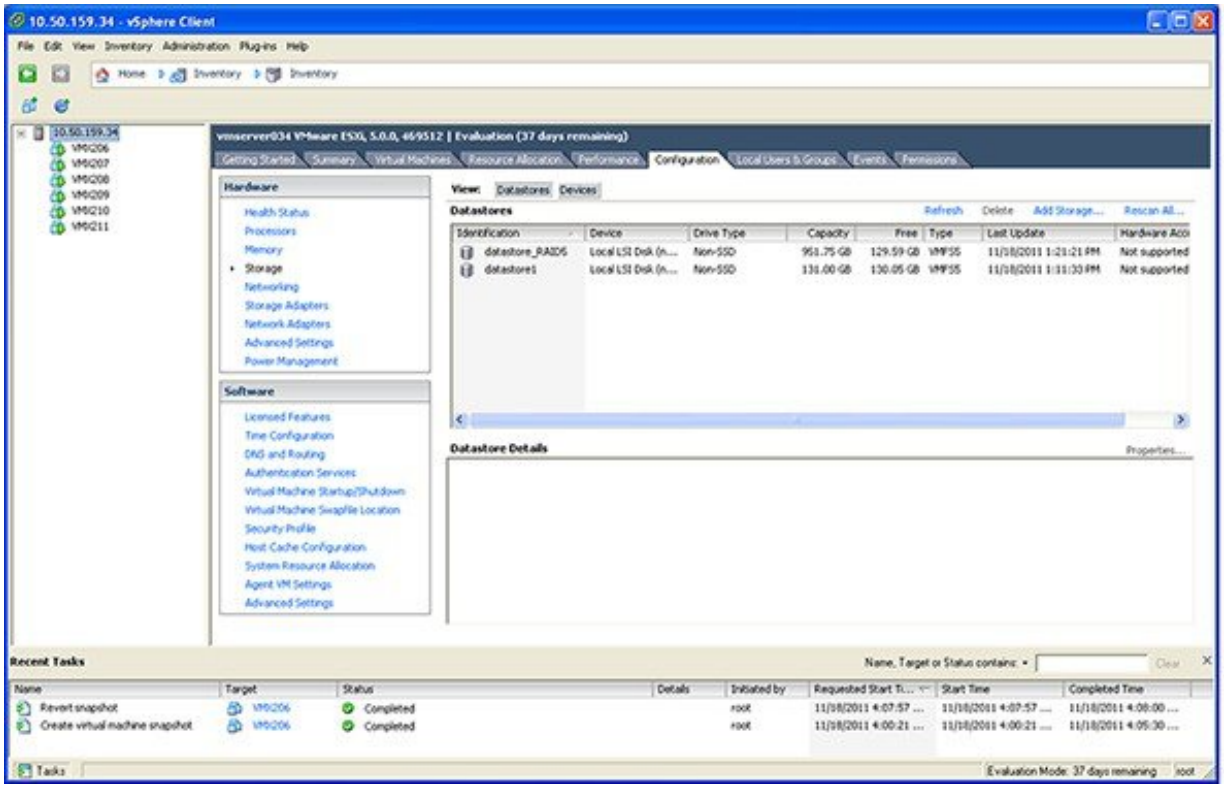



Figure 20: New Datastore