



Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for VMware

Cisco Video Surveillance, Release 7 OVA on Cisco UCS series servers

Americas Headquarters

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

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

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

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

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

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

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

Any Internet Protocol (IP) addresses 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.

Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for VMware
© 2012-2019 Cisco Systems, Inc. All rights reserved.



Preface iii

Revision History iii

Audience iv

Command Syntax Conventions v

CHAPTER 1

Deploying Cisco Video Surveillance Virtual Machines on the UCS Platforms 1-1

Contents 1-1

Introduction 1-2

Audience 1-2

Logical Topology 1-3

Summary Steps 1-3

Requirements 1-5

Platform Requirements 1-5

vSphere Client Requirements 1-6

Obtaining the Software Images 1-7

Installing and Configuring the Cisco VSM Virtual Machine 1-9

Installing the Cisco VSM Virtual Machine 1-9

Verify the VMFS Maximum Heap Size 1-14

Adding Hard Disks for Media Storage 1-15

Defining the VLAN for the VM 1-21

Configuring NTP Servers on the Blade 1-23

Powering On the Cisco VSM Virtual Machine 1-26

Change the Default VM Password and Network Settings 1-26

Release 7.5 and Later: CLI Method 1-27

Release 7.2 and Earlier: GUI Method 1-28

(Optional for Release 7.2 and Earlier) Use the Guest OS to Configure the Network Settings 1-29

Creating Video Repositories 1-33

Usage Notes 1-33

Understanding the Integration Script 1-34

Understanding Mount Points 1-34

Internal and External Storage Limitations 1-34

Obtaining the Storage Partition Script 1-34

32-bit Red Hat OS (Release 7.0 to Release 7.2) 1-34

64-bit Red Hat OS (Release 7.5 and Higher) 1-35

Understanding the Script Options	1-36
Release 7.5 and Later: Adding Storage Partitions	1-36
Run the Script With No Options	1-36
Run the Script with the Restore Option	1-40
Release 7.2 and Earlier: Adding Storage Partitions	1-41
External Storage Script: Release 7.2 and Earlier:	1-41
Internal Storage CLIs: Release 7.2 and Earlier	1-46
Completing the Initial Server Setup Using the Management Console	1-48
Usage Notes	1-48
Default Network Settings	1-48
Complete the Setup Wizard	1-50
Testing Network Connectivity	1-51
Adjusting Performance	1-51

CHAPTER 2

Recovering Cisco Video Surveillance VMs on the Cisco UCS Platforms 2-1

Assumptions	2-1
Summary Steps	2-2
Detailed Instructions: Recovering the VSM on the UCS	2-3



Preface

Last Updated: October 29, 2019

This document includes instructions to deploy a virtualized Cisco Video Surveillance Release 7.x server on a supported Cisco Unified Computing System platform. This document also includes instructions to recover a virtual machine image (.OVA), and configure high availability.

Revision History

Table 1 *Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms, Release 7 Revision History*

Release	Revision Date	Change Summary
	July 23, 2019	Removed the section on Configuring HA for Cisco VSM Operations Manager Release 7 VM Deployments
	June 8, 2018	Revised ESXi requirements and supported versions. See vSphere Client Requirements .
	February 14, 2018	Added support for ESXi 6.5 . See vSphere Client Requirements .
	November 21, 2017	Add additional VMware Hypervisor version support to vSphere Client Requirements , page 6 .
Release 7.8	October 2016	<ul style="list-style-type: none">• Minor updates
Release 7.7	October 2015	<ul style="list-style-type: none">• Updated supported VMware Hypervisor versions (see Requirements, page 5).• Added note regarding error message that may occur appear when using vSphere client 5.0.0 (see Installing and Configuring the Cisco VSM Virtual Machine, page 9).
	August 2015	<ul style="list-style-type: none">• In release 7.7 and higher, the <code>setup_media_storage.sh</code> script is also included in the OVA image, and can be run from <code>/usr/BWhttpd/bin</code>.• See Obtaining the Storage Partition Script, page 34 and Release 7.5 and Later: Adding Storage Partitions, page 36.
Release 7.6	October, 2014	<ul style="list-style-type: none">• Added instructions to configure the network settings using CLI commands in Release 7.5 and higher. See “Change the Default VM Password and Network Settings”.
Release 7.6	May, 2015	<ul style="list-style-type: none">• Clarified instructions to run the storage integration script. See “Release 7.5 and Later: Adding Storage Partitions”.

Table 1 *Cisco Video Surveillance Virtual Machine Deployment and Recovery Guide for UCS Platforms, Release 7 Revision History (continued)*

Release	Revision Date	Change Summary
Release 7.5	March, 2014	<ul style="list-style-type: none"> Added Release 7.2 and 7.5 OVA support. Revised the Deployment instructions for the following: <ul style="list-style-type: none"> Added “Verify the VMFS Maximum Heap Size” Added “Change the Default VM Password and Network Settings” Added CLI instructions to “Change the Default VM Password and Network Settings” Revised “Creating Video Repositories” for instructions to use a script. Updated the “Requirements” for Release 7.5 and additional 7.0-7.2 requirements. Updated “Adding Hard Disks for Media Storage” for Release 7.2 and earlier to add a paravirtual type SCSI controller to the virtual machine to control the video storage volumes. Revised “Completing the Initial Server Setup Using the Management Console” to include the initial network setup. Updated the “Internal and External Storage Limitations” Numerous minor changes and edits
Release 7.0.1	March, 2013	Added Release 7.0.1 support.
Release 7.0.1	May, 2013	<ul style="list-style-type: none"> Added support for the Cisco UCS E-Series platform, Added Recovery instructions (see the “Recovering Cisco Video Surveillance VMs on the Cisco UCS Platforms” section). Added VM HA instructions (Configuring HA for Cisco VSM Operations Manager Release 7 VM Deployment section). Updated the “Related Documentation” section.
Release 7.0.0	November, 2012	Initial draft.

Audience

This document is intended for use by Cisco System Engineers, Cisco Advanced Services Engineers, Physical Security Advanced Technology Provider (ATP) partners, and technical field staff that are developing and implementing Cisco Video Surveillance Manager 7 or later in a virtualized environment.

A successful implementation also requires additional knowledge in the following areas:

- VMware vSphere (version 5.0)
- Cisco UCS platform installation and management
- Cisco Video Surveillance Release 7 installation and configuration

Command Syntax Conventions

Table 2 describes the syntax used with the commands in this document.

Table 2 **Command Syntax Guide**

Convention	Description
boldface	Commands and keywords.
<i>italic</i>	Command input that is supplied by you.
[]	Keywords or arguments that appear within square brackets are optional.
{ x x x }	A choice of keywords (represented by x) appears in braces separated by vertical bars. You must select one.
^ or Ctrl	Represent the key labeled <i>Control</i> . For example, when you read ^D or <i>Ctrl-D</i> , you should hold down the Control key while you press the D key.
screen font	Examples of information displayed on the screen.
boldface screen font	Examples of information that you must enter.
< >	Nonprinting characters, such as passwords, appear in angled brackets.
[]	Default responses to system prompts appear in square brackets.





Deploying Cisco Video Surveillance Virtual Machines on the UCS Platforms

This guide describes how to deploy the Cisco Video Surveillance Manager (Cisco VSM) as a virtual machine (VM) on the Cisco Unified Computing System (UCS) platforms. Release 7 supports the Cisco UCS Express, and B-, C-, and E- Series platforms.

Refer to the following topics for more information.

Contents

- [Introduction, page 2](#)
 - [Audience, page 1-2](#)
 - [Logical Topology, page 1-3](#)
 - [Summary Steps, page 1-3](#)
 - [Requirements, page 1-5](#)
 - [Obtaining the Software Images, page 1-7](#)
- [Installing and Configuring the Cisco VSM Virtual Machine, page 9](#)
 - [Installing the Cisco VSM Virtual Machine, page 1-9](#)
 - [Adding Hard Disks for Media Storage, page 1-15](#)
 - [Defining the VLAN for the VM, page 1-21](#)
 - [Configuring NTP Servers on the Blade, page 1-23](#)
- [Powering On the Cisco VSM Virtual Machine, page 26](#)
- [Change the Default VM Password and Network Settings, page 1-26](#)
- [Creating Video Repositories, page 1-33](#)
 - [Usage Notes, page 1-33](#)
 - [Understanding Mount Points, page 1-34](#)
 - [Internal and External Storage Limitations, page 1-34](#)
 - [Obtaining the Storage Partition Script, page 1-34](#)
 - [Understanding the Script Options, page 1-36](#)
 - [Release 7.5 and Later: Adding Storage Partitions, page 1-36](#)

- Release 7.2 and Earlier: Adding Storage Partitions, page 1-41
- Completing the Initial Server Setup Using the Management Console, page 48
 - Default Network Settings, page 1-48
 - Complete the Setup Wizard, page 1-50
- Testing Network Connectivity, page 51
- Adjusting Performance, page 51

Introduction

Refer to the following topics before you begin.

- Audience, page 1-2
- Logical Topology, page 1-3
- Summary Steps, page 1-3
- Requirements, page 1-5



Note

This guide does not describe the configuration and operation of Cisco VSM, the Cisco UCS platforms, the UCS Manager, or other related products and features. For a full description of these products, see the [Related Documentation](#).

Audience

This guide is intended for use by Cisco System Engineers, Physical Security Advanced Technology Provider (ATP) partners, and technical field staff who develop and implement Cisco VSM and UCS Servers for data center and branch office solutions.

A successful implementation also requires additional knowledge in the following areas:

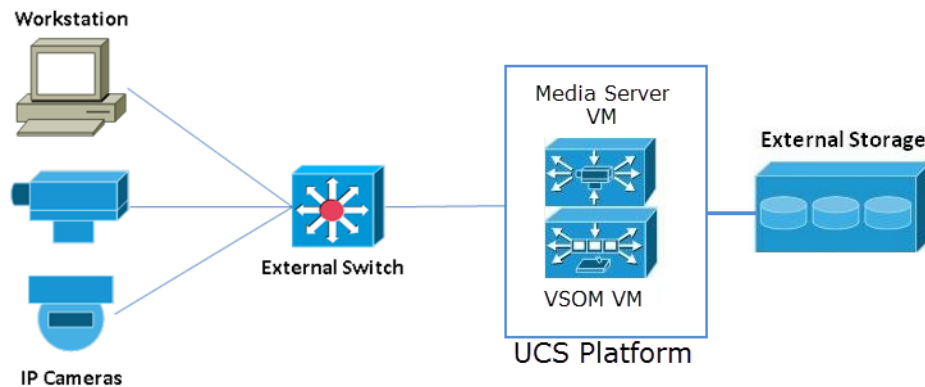
- VMware vSphere (version 5.x & 6.x)
- Cisco UCS platform installation and management
- Cisco Video Surveillance Manager installation and configuration

See the “[Related Documentation](#)” section on page A-1 for more information.

Logical Topology

Figure 1-1 illustrates the overall, logical topology of the networking and video surveillance components:

Figure 1-1 Logical Network Topology



- A UCS platform that runs the Cisco VSM virtual machine(s) that host the Media Server, the Operations Manager, or both.
- The Cisco VSM image (.ova file format) for the UCS platform.
- Various IP cameras, encoders and analog cameras.
- The operator workstations that run the Operations Manager client.
- An external network switch and external storage.

Summary Steps

To deploy Cisco VSM as a VM on the Cisco UCS platforms, do the following:

	Task	More Information	Task Complete? (✓)
Step 1	Install and configure the Cisco UCS platform.	Cisco Unified Computing and Servers: http://www.cisco.com/en/US/products/ps10265/index.html Cisco UCS Platform and VM Documentation (see “Related Documentation” section on page A-1).	<input type="checkbox"/>
Step 2	Install and configure video storage so it can be accessed by the VM.	Refer to the product documentation for your storage device.	<input type="checkbox"/>

	Task	More Information	Task Complete? (✓)
Step 3	Install and configure VMware.	<ul style="list-style-type: none"> Installing and Configuring VMware Tools: http://www.vmware.com/pdf/vmware-tools-installation-configuration.pdf VMware ESXi Configuration Guides: http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html Cisco UCS Platform and VM Documentation (see “Related Documentation” section on page A-1). 	<input type="checkbox"/>
Step 4	Download the OVF template files from the Cisco website. <ul style="list-style-type: none"> The template file format is .ova. For example: <code>Cisco_VSM-7.5-012_ucs-bc-1.2.ova</code> You can also download the OVF template file to a USB drive and attach the drive the computer. 	Obtaining the Software Images, page 1-7	<input type="checkbox"/>
Step 5	Deploy the Cisco Video Surveillance virtual machine template (.ova file). <ul style="list-style-type: none"> Be sure to Be sure to “Verify the VMFS Maximum Heap Size”. Complete the instructions to configure a virtual hard disk, vLAN and NTP server. 	Installing and Configuring the Cisco VSM Virtual Machine, page 1-9	<input type="checkbox"/>
Step 6	Power on the virtual machine.	Powering On the Cisco VSM Virtual Machine, page 1-26	<input type="checkbox"/>
Step 7	Change the default password for the localadmin user.	Change the Default VM Password and Network Settings, page 1-26	<input type="checkbox"/>
Step 8	Configure the storage partitions.	Creating Video Repositories, page 1-33	<input type="checkbox"/>
Step 9	Complete the initial server configuration and restart the server services, using the Cisco VSM Management Console.	Completing the Initial Server Setup Using the Management Console, page 1-48	<input type="checkbox"/>
Step 10	Verify network connectivity between the server, devices such as network cameras, and the Operations Manager.	Testing Network Connectivity, page 1-51	<input type="checkbox"/>

Requirements

The following table summarizes the platform and vSphere requirements for the examples and procedures described in this document.

- [Platform Requirements, page 1-5](#)
- [vSphere Client Requirements, page 1-6](#)

Platform Requirements

Table 1-1 *Platform Requirements*

Requirements	Complete? (✓)
<ul style="list-style-type: none"> • UCS B-Series Blades or UCS C-Series rack-mount server. • UCS Express—the ISR G2 must run IOS version 15.1(4)M or later. • E-Series—IOS version 15.2(4)M <p>Note See the data sheets for the latest guidelines: http://www.cisco.com/en/US/products/ps10818/products_data_sheets_list.html.</p>	<input type="checkbox"/>
UCS C-series: VMware ESX/ESXi are not supported for use with embedded MegaRAID controller. Refer to the Cisco UCS C-Series Rack Servers Install and Upgrade Guide for details.	<input type="checkbox"/>
UCS E-series supports multiple connectivity options: <ul style="list-style-type: none"> • GE0 is an internal interface that flows through the router PCIe. This option is recommended for VSM traffic if the connectivity is only through router's interface. • GE1 is an internal interface that flows through the MGF plane of the router. This option is preferred as it uses high speed switching fabric of the ISR and does not interfere with router PCIe. • GE2 & GE3 are external interfaces. This option can be used if Cisco VSM needs to operate independent of the router. Refer to the following link for configuration details: http://www.cisco.com/en/US/docs/unified_computing/ucs/e/1.0/guide/b_Getting_Started_Guide_chapter_01000.html	<input type="checkbox"/>
The platform must be configured with the required IP addresses for the management network.	<input type="checkbox"/>
External storage is installed as required by the Cisco UCS platform server.	<input type="checkbox"/>

vSphere Client Requirements

Table 1-2 vSphere Client Requirements

Subject	Requirement	Complete? (✓)
Hypervisor version	VMware Hypervisor version: ESXi 5.0, 5.1, 5.5.0, 6.0. On S3260: only ESXi 6.5 is supported On M4: only ESXi 6.0 and ESXi 6.5 are supported	<input type="checkbox"/>
UCSM version	Cisco Unified Computing System Manager (UCSM) version: 1.4 and later	<input type="checkbox"/>
VM (OVA) Requirements	<p>Cisco UCS B-Series and C-Series Servers</p> <ul style="list-style-type: none"> OVA image for 4-core servers For example: “Cisco Video Surveillance Manager 7.x OVA image for Cisco UCS B-series, C-series, and E-series (4-core) servers” (<code>Cisco_VSM-7.x_ucs-bc-<version>.ova</code>) 12 GB RAM (the 4-core OVA reserves 10.5 GB of RAM, and 1.5 GB of swap space is required) <p>Cisco UCS Express Servers</p> <ul style="list-style-type: none"> OVA image for 2-core servers. For example: “Cisco Video Surveillance Manager 7.x OVA image for Cisco UCS-Express (SRE 9xx) and E-series (2-core) servers” (<code>Cisco_VSM-7.x_ucs-express-<version>.ova</code>) 4 GB RAM (the 2-core OVA reserves 3 GB of RAM, and 1 GB of swap space is required) <p>Cisco UCS E-Series Servers</p> <ul style="list-style-type: none"> Supports the OVA image for both 2-core and 4-core servers: <code>Cisco_VSM-7.x_ucs-bc-<version>.ova</code> and <code>Cisco_VSM-7.x_ucs-express-<version>.ova</code> The OVA for 2-core servers requires 4 GB RAM The OVA for 4-core servers requires 12 BG RAM <p>Note See Obtaining the Software Images, page 1-7 for more information.</p>	<input type="checkbox"/>
Storage	<p>The total virtual disk space required to deploy OVA:</p> <p>Release 7.5 and later</p> <ul style="list-style-type: none"> OVA image for 4-core servers: requires 110GB (+ 512MB of swap space) OVA image for 2-core servers: requires 80GB (+ 512MB of swap space) <p>Release 7.2 and earlier</p> <ul style="list-style-type: none"> OVA image for 4-core servers: requires 106GB (+ 512MB of swap space) OVA image for 4-core servers: requires 76GB (+ 4GB of swap space) <p>Note The swap space is not included in the VM configuration, but is automatically taken from the datastore when the VM is deployed. Include this space when planning the total VM storage space requirements.</p>	<input type="checkbox"/>

Table 1-2 vSphere Client Requirements (continued)

Subject	Requirement	Complete? (✓)
VM support	<ul style="list-style-type: none"> UCS Express, C- and E- Series servers support a single Cisco VSM 7 virtual machine. Do not install additional VMs for other applications on the same server. Multiple VMs are supported on the UCS B- Series servers. 	<input type="checkbox"/>
VMFS Heap Size	See the “Verify the VMFS Maximum Heap Size” section on page 1-14.	<input type="checkbox"/>
Networking	<ul style="list-style-type: none"> 2 virtual network interface cards (vNICs) 2 virtual host bus adapters (vHBAs) 	<input type="checkbox"/>
Video partitions	<p>The maximum video partition storage sizes are:</p> <p>External FC SAN based Storage:</p> <ul style="list-style-type: none"> The maximum partition sizes are: <ul style="list-style-type: none"> 32-bit operating systems (such as Red Hat 5.8)—16 TB maximum size per partition 64-bit operating systems—100 TB maximum size per partition (the maximum size tested is 30TB with ten 4TB hard drives) There can be multiple media partitions, media1mediaN, based on the retention period for the video recordings of the cameras being hosted on the particular VM. <p>Internal RAID based Storage:</p> <ul style="list-style-type: none"> The maximum virtual disk size is 2TB. (http://blogs.vmware.com/vsphere/2011/07/new-vsphere-50-storage-features-part-1-vmfs-5.html) Multiple 2TB virtual disks can be added to the VM, based on the retention period for the video recordings of the cameras being hosted on the particular VM. <p>See the “Internal and External Storage Limitations” section on page 1-34</p>	<input type="checkbox"/>
RAID array	<p>Each VM should have exclusive access to its own RAID array (1VM:1RAID-Array).</p> <p>For UCS C-Series platforms, we recommend creating a single 12-drive RAID-6 RAID array, with a single virtual drive. VMware should be installed on this RAID volume, as well as using it for the data stores for the VSM virtual machine and video partitions.</p>	<input type="checkbox"/>

Obtaining the Software Images

To install the virtual machine, you must add the Cisco VSM Open Virtualization Format (OVF) template file to VMWare running on a Cisco USC platform. The template file format is .ova.

The .ova template files can be obtained from the [Video Surveillance Manager software download page](#).

Procedure

To download the .ova software images:

Step 1 Log in to the Cisco Video Surveillance Manager [software download page](#).

**Note**

To download the software, you must have a valid service contract associated to your Cisco.com profile. Contact your Cisco Account Team, Cisco Partner or Reseller for more information.

Step 2 Click **Video Surveillance Media Server Software**.

Step 3 Select the release number for your Cisco VSM deployment. For example: 7.5.0.

Step 4 Download the OVA image for your server platform.

Cisco UCS B-Series and C-Series Servers

- Download the OVA image for 4-core servers:

For example: Cisco Video Surveillance Manager 7.x OVA image for Cisco UCS B-series, C-series, and E-series (4-core) servers (**Cisco_VSM-7.x_ucs-bc-<version>.ova**)

Cisco UCS Express Servers

- Download the OVA image for 2-core servers.

For example: Cisco Video Surveillance Manager 7.x OVA image for Cisco UCS-Express (SRE 9xx) and E-series (2-core) servers (**Cisco_VSM-7.x_ucs-express-<version>.ova**)

Cisco UCS E-Series Servers

- Download the OVA image for either the 2-core and 4-core servers (the E-series server supports both)

Step 5 Follow the on-screen instructions to complete the download.

**Tip**

You can also access software downloads using the [Cisco Video Surveillance home page](#) or the Cisco software navigator for *IP Video Surveillance software*.

Installing and Configuring the Cisco VSM Virtual Machine

To install and configure the Cisco VSM virtual machine, complete the following procedures:

- [Installing the Cisco VSM Virtual Machine, page 1-9](#)
- [Verify the VMFS Maximum Heap Size, page 1-14](#)
- [Adding Hard Disks for Media Storage, page 1-15](#)
- [Defining the VLAN for the VM, page 1-21](#)
- [Configuring NTP Servers on the Blade, page 1-23](#)

After completing these tasks, continue to the following topics:

- [Powering On the Cisco VSM Virtual Machine, page 1-26](#)
- [Creating Video Repositories, page 1-33](#)
- [Completing the Initial Server Setup Using the Management Console, page 1-48](#)

Installing the Cisco VSM Virtual Machine

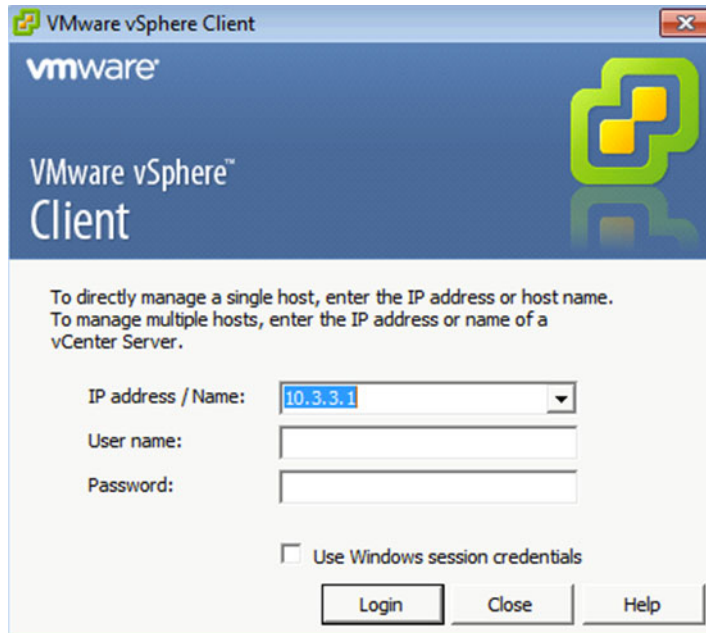
Installing the virtual machine entails adding the Cisco VSM Open Virtualization Format (OVF) template file (.ova format) to the VMware vSphere client, as described in the following procedure.

**Note**

UCS Express, C- and E- Series servers support a single Cisco VSM 7 virtual machine. Do not install VMs for other applications on the same server.

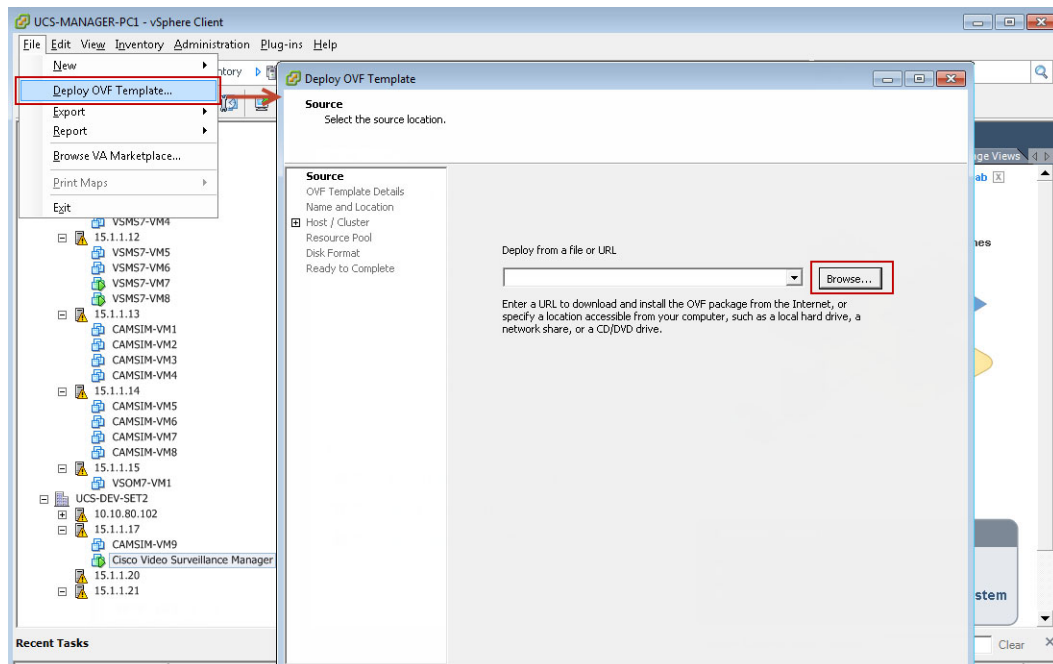
Procedure

- Step 1** Download the Cisco VSM Open Virtualization Format (OVF) template file from the Cisco web page to the computer where the vSphere client was previously installed.
- See the [“Obtaining the Software Images” section on page 1-7](#).
 - The template file format is .ova. For example: `Cisco_VSM-7.5-012_ucs-bc-1.2.ova`
 - You can also download the OVF template file to a USB drive and attach the drive the computer.
 - The OVF Template is approximately 2 GB in size. See the [“Requirements” section on page 1-5](#) for the amount of disk size required to deploy the VM (depending on the UCS platform). This requirement is for the VM only and does not include the video partition(s) disk space.
- Step 2** Launch the vSphere client.
- a. Select the **VMware vSphere Client** icon on the desktop or select **Start > VMware vSphere Client**.
 - b. Enter the vCenter Server’s IP address and credentials to access the vCenter server ([Figure 1-2](#)).

Figure 1-2 VMware vSphere Client Login Page

Step 3 Click **File > Deploy OVF Template** (Figure 1-3).

Step 4 Click **Browse** and select the .ova template file from a local disk, or enter the URL to download the file from the Internet.

Figure 1-3 Deploying the OVF Template from a File or URL

Step 5 Complete the remaining steps to deploy the template (Figure 1-4):



Note

(Cisco VSM 7.7 only) A warning message may appear using vSphere client 5.0.0,: "The OVA package is valid but consider the following warning..." You can safely ignore this warning and click on **Yes** to continue.

This warning occurs because the vSphere client 5.0.0 is an earlier version than what was used to build the OVF package (the OVF package contains some attributes that are not recognized by the importer). This does not impact the import process, which will continue and deploy the appliance properly.

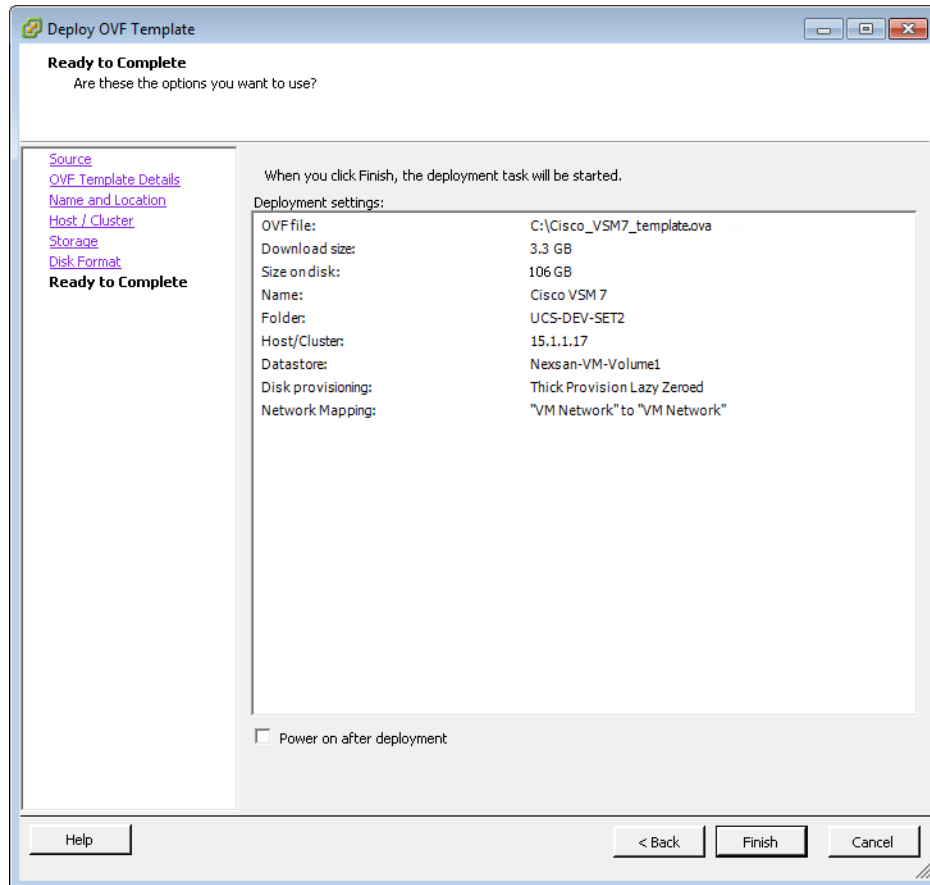
Setting	Description
OVF Template Details	Click Next to accept the default settings.
Name and Location	Enter the name and location for the VM. <ul style="list-style-type: none"> The name is displayed in the inventory tree (for example, "Cisco Video Surveillance Manager"). The location defines where the VM appears in the tree. Click Next to continue.
Host / Cluster	Select the specific host or cluster where you want to run the template.
Storage	Select where the VM files will be stored. It should be deployed a datastore on internal storage, not external storage. See the " Requirements " section on page 1-5 for the amount of disk size required to deploy the VM (depending on the UCS platform). This requirement is for the VM only and does not include the video partition(s) disk space.
Disk Format	Click Next to accept the default disk format (Thick Provisioned Lazy Zeroed).

Figure 1-4 Enter the OVF Template Properties

The screenshot shows the 'Deploy OVF Template' wizard window. The title bar reads 'Deploy OVF Template'. The main heading is 'Name and Location' with the instruction 'Specify a name and location for the deployed template'. On the left, a sidebar contains links: 'Source', 'OVF Template Details', 'Name and Location' (which is selected and highlighted with a blue box), 'Host / Cluster', 'Resource Pool', 'Disk Format', and 'Ready to Complete'. The main area has a 'Name:' text box containing 'VSM7' and a note: 'The name can contain up to 80 characters and it must be unique within the inventory folder.' Below this is the 'Inventory Location:' section, which shows a tree view with 'UCS-MANAGER-PC1' expanded, revealing 'UCS-DEV-SET1' and 'UCS-DEV-SET2'. At the bottom, there are three buttons: 'Help', '< Back', 'Next >', and 'Cancel'.

Step 6 Click **Finish** to accept the selected deployment settings (Figure 1-5).

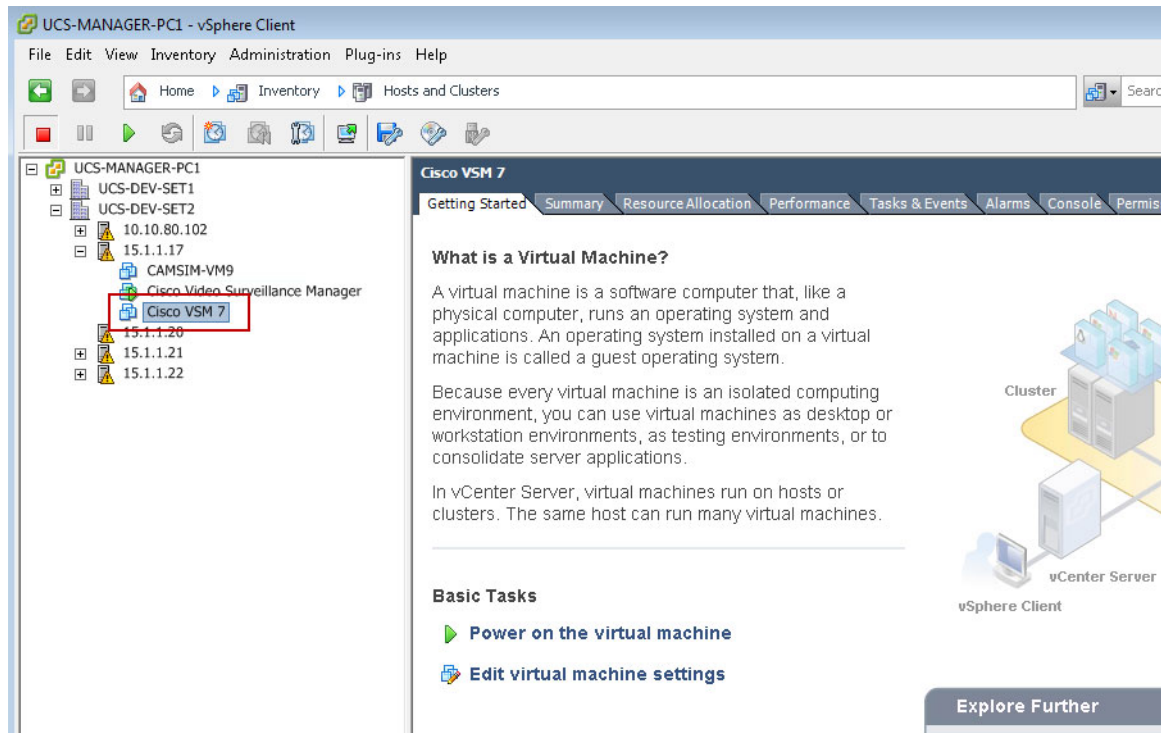
Figure 1-5 *Ready to Complete—Deployment Settings*



Step 7 Wait for the Cisco VSM template to deploy. Click **Close** when the success message appears.

Step 8 Verify that the VM displays under the host entry in the Inventory tree (Figure 1-6).

Figure 1-6 Cisco VSM VM in the vSphere Client



Tip

For more information about OVF Templates, see <http://www.vmware.com/technical-resources/interfaces/ovf.html>

Verify the VMFS Maximum Heap Size

Verify that the VMFS maximum heap size is set for the amount of storage accessed by the ESXi host.

See the following VMWare knowledge base articles for more information:

- [Setting virtual machine file system heap size values \(2048166\)](#)— to set the VMFS3.MaxHeapSizeMB
- [ESXi/ESX host reports VMFS heap warnings when hosting virtual machines that collectively use 4 TB or 20 TB of virtual disk storage \(1004424\)](#) — for the appropriate values for your VMWare version and the amount of VMFS storage the host will be accessing.

Adding Hard Disks for Media Storage

Before starting the VM, add virtual hard disks to the configuration to provide video storage space. Virtual hard disks allow you to use storage space on an available internal or external disk array.

We recommend using the Raw Device Mapping (RDM) option from a SAN storage device.

Before You Begin

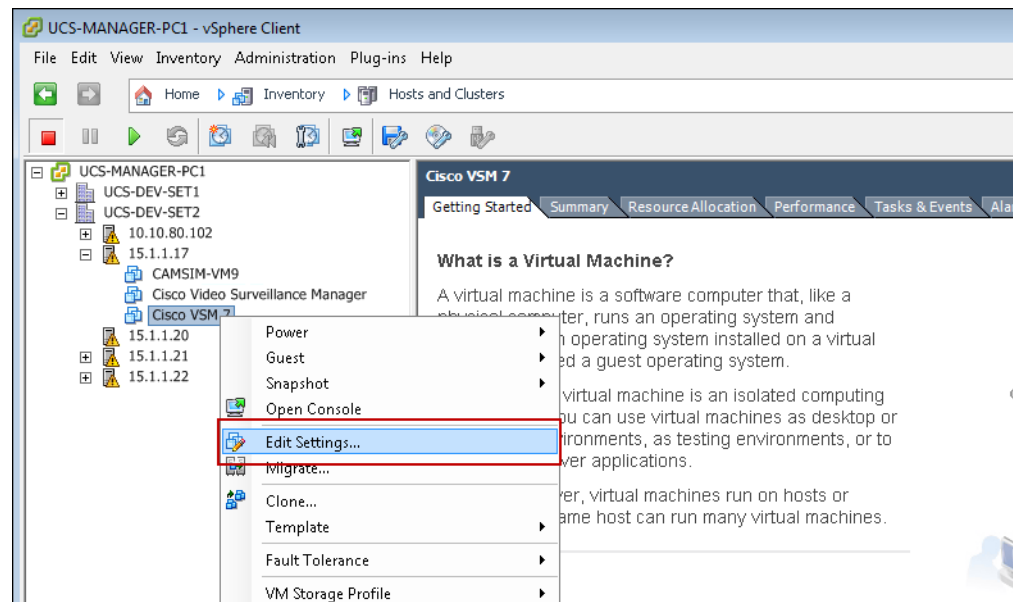
The physical storage media must be installed and accessible to the virtual machine.

Procedure

To add a virtual hard disk for use by the Cisco VSM VM, perform the following procedure.

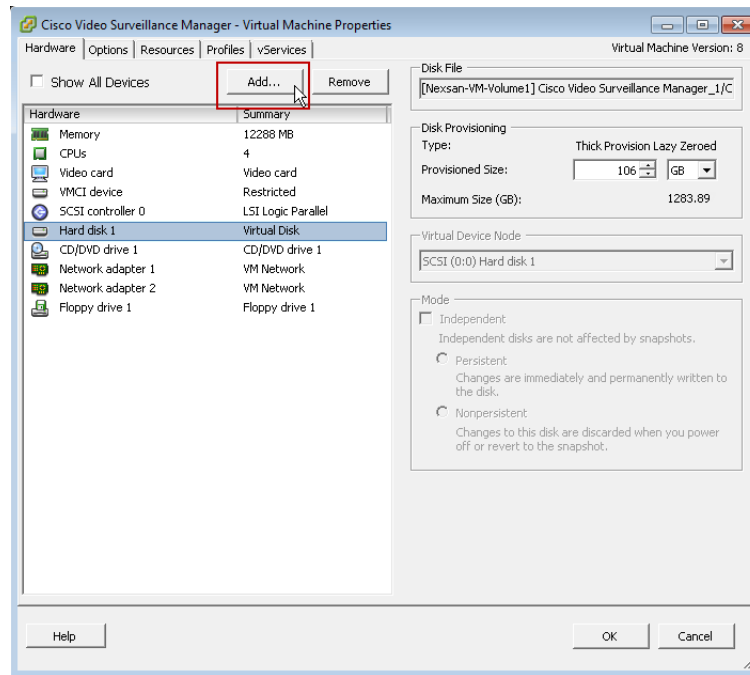
- Step 1** (Release 7.2 and earlier only) Add a Paravirtual type SCSI controller to the virtual machine to control the video storage volumes.
- This adds the SCSI controller before adding the hard disk if you are adding additional Media Servers to an existing deployment.
 - See the VMWare Knowledge Base article “[Adding a SCSI controller to the virtual machine \(1037094\)](#)” for instructions and more information.
 - This step is not required in Release 7.5 or later since the default VM controller is already a para-virtual SCSI interface.
- Step 2** In the inventory tree (left pane), right-click the VM name and select **Edit Settings** (Figure 1-7).

Figure 1-7 Editing the VM Settings



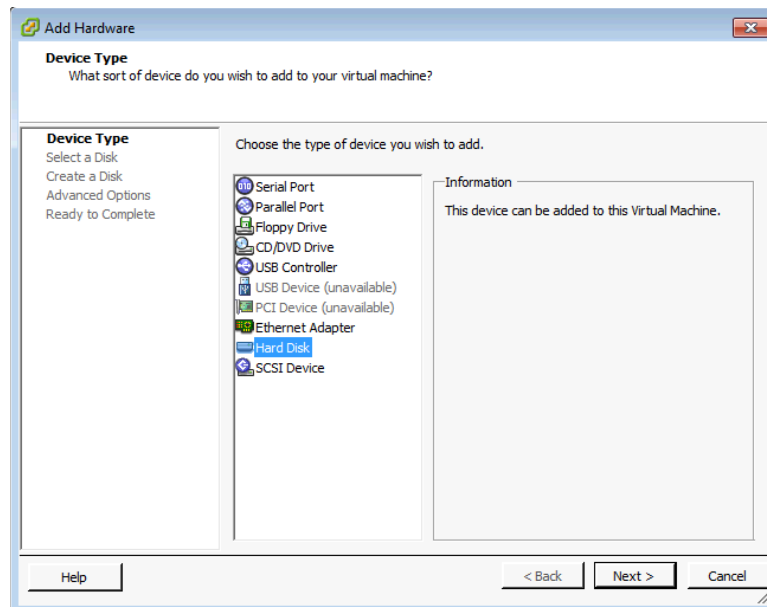
Step 3 Select **Hard disk** and click **Add** (Figure 1-8).

Figure 1-8 Adding a Hard Disk to the VM



Step 4 For device type, select **Hard Disk** and click **Next** (Figure 1-9).

Figure 1-9 Selecting the Hard Disk Device Type



Step 5 Select the type of disk to use (Figure 1-10).

Figure 1-10 Disk Options

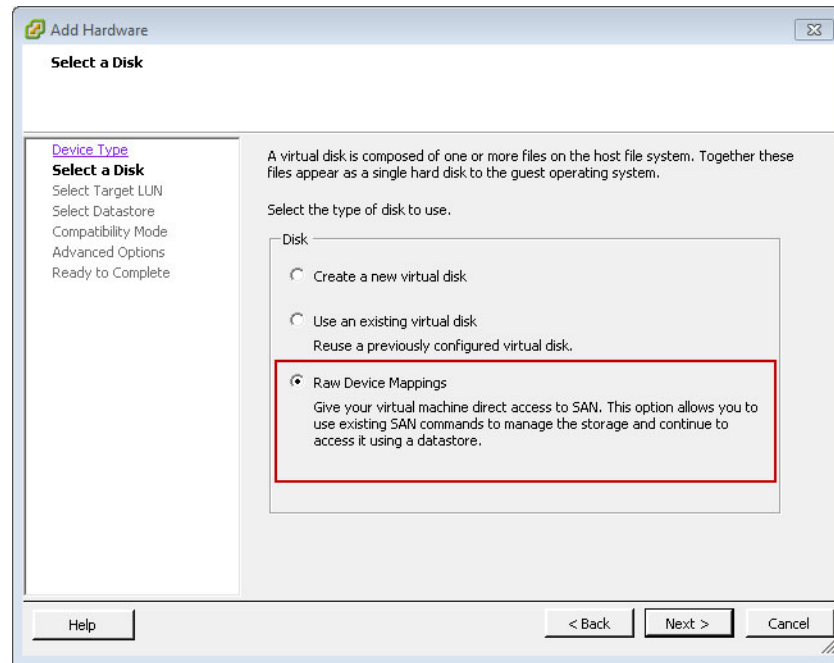


Table 1-3 Hard Disk Options

Disk Type	Description
Create a new virtual disk	We recommend using a virtual disk (VMDK) with the internal storage. You can add multiple disks of 2 TB or less (depending on the number of available hard disks and RAID configuration). If a larger disk size is required, use the external FC SAN storage (using the Raw Device Mapping option).
Use an existing virtual disk	This option is used only for VM recovery. See the “Recovering Cisco Video Surveillance VMs on the Cisco UCS Platforms” section on page 2-1 for more information.
Raw Device Mapping	Raw Device Mapping is used with external Fiber Channel-based SAN storage. <ul style="list-style-type: none"> Use this option if internal storage is not available or if disks greater than 2 TB are required. See the “Internal and External Storage Limitations” section on page 1-34 for more information. Internal storage cannot be configured as Raw Device Mappings.

**Tip**

For more information about Virtual Machine File Systems (VMFS) and RDMs, see http://pubs.vmware.com/vi301/san_cfg/wwhelp/wwhimpl/common/html/wwhelp.htm?context=san_cfg&file=esx_san_cfg_esx_and_san.4.13.html.

Step 6 Select the virtual disk options.

Raw Device Mapping (RDM) Options

The following table describes the recommended options for Raw Device Mapping (RDM) disks (used to create a disk from Fiber Channel-based SAN storage).

Table 1-4 *Raw Device Mapping (RDM) Option*

Screen	Description
Select Target LUN	Select the Logical Unit Number (LUN) that is configured on the SAN.
Select Datastore	Store with the virtual machine
Compatibility Mode	Physical
Advanced Options	Accept the defaults values

Virtual Disk Options

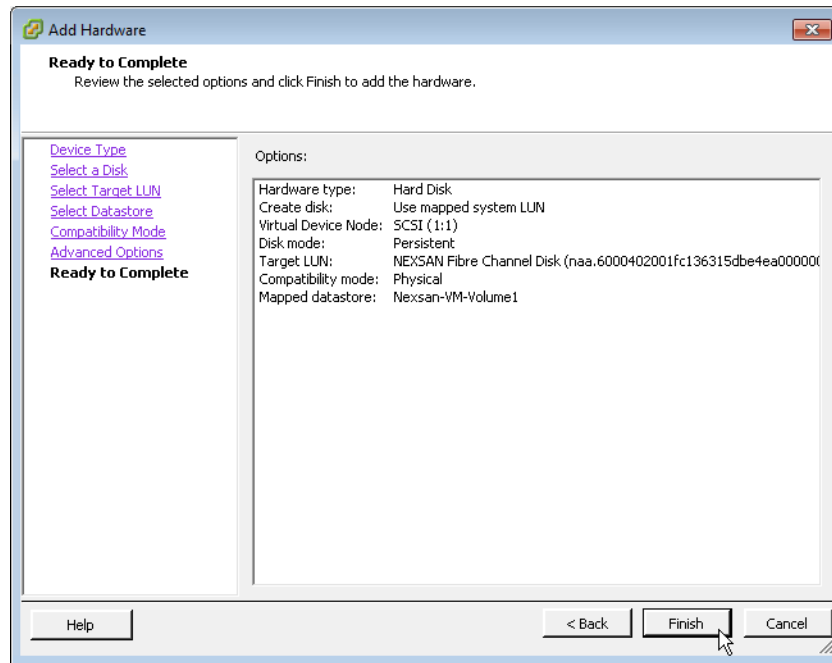
The following table describes the options for a virtual disk.

Table 1-5 *Virtual Disk Options*

Screen	Description
Create a Disk	<ul style="list-style-type: none"> • Disk size—The required media partition size. • Disk Provisioning—select Thick Provisioned Lazy Zeroed (recommended) • Location— <ul style="list-style-type: none"> – Store with the virtual machine: recommended for RDM disks (external SAN storage). – Specify a datastore or cluster: recommended for internal storage (you must also select the appropriate datastore that will accommodate the Disk Size).
Advanced Options	Accept the defaults options.

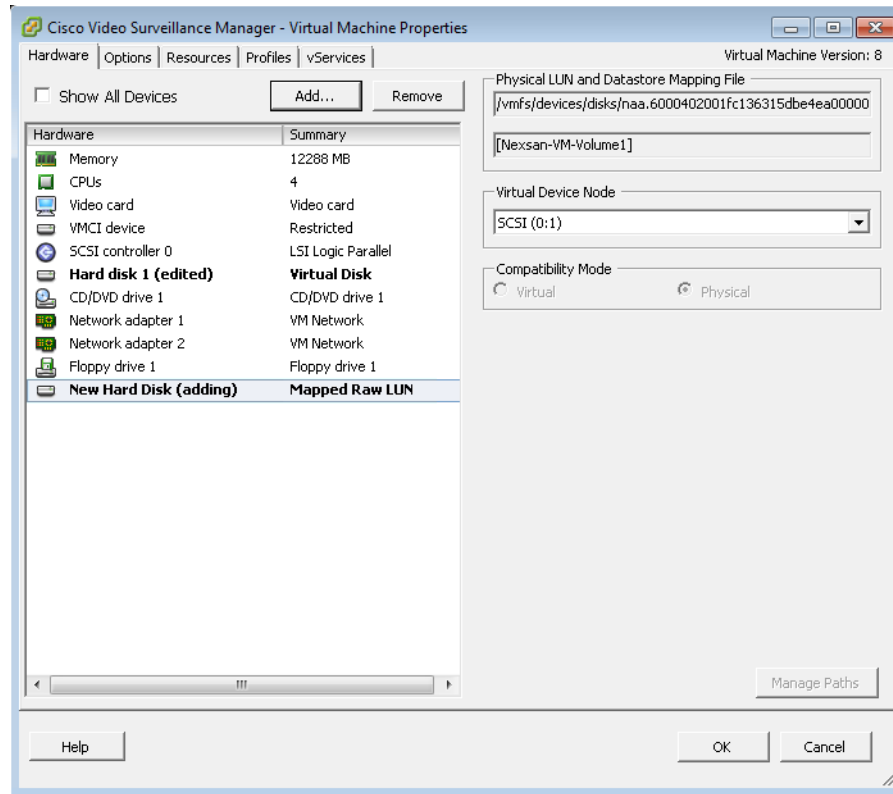
Step 7 Review hard disk summary and click **Finish** (Figure 1-11).

Figure 1-11 *New Hard Disk Summary*



- Step 8** Click **Finish** again to return to the Virtual Machine Properties screen and view the newly created hard disk.

Figure 1-12 Adding a New Hard Disk to the Cisco VSM VM



- Step 9** Click **OK**.

Defining the VLAN for the VM

Configure a vLAN if required by your network configuration.

By default, the virtual LAN (VLAN) ID (**ALL, 4095**) is set on all virtual interfaces.



Tip

- For more information about configuring network switches for VLAN tagging in VMware, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1266.
- For information about VLAN tagging, see http://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc_50%2FGUID-7225A28C-DAAB-4E90-AE8C-795A755FBE27.html.

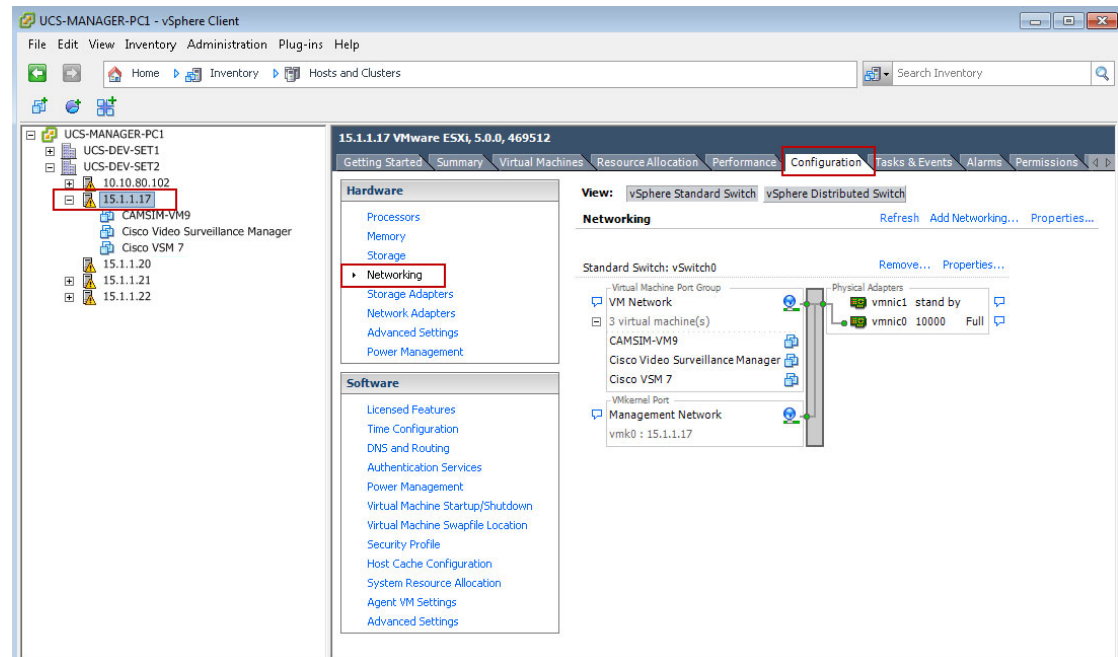
Procedure

Step 1

Open the VM networking properties (Figure 1-13):

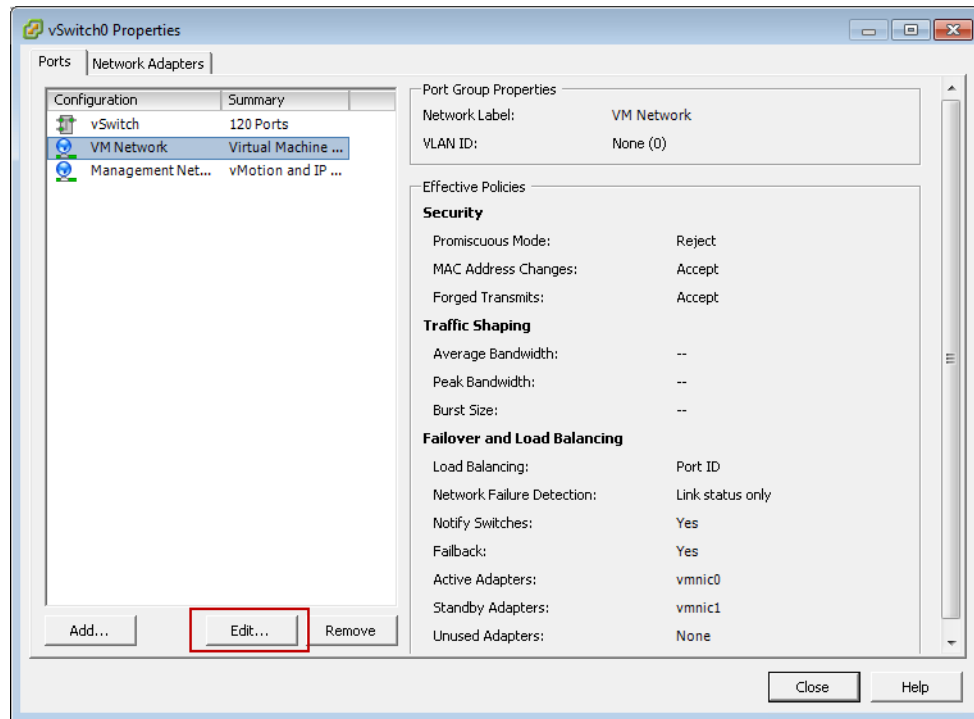
- In the left pane (Inventory tree), select the hypervisor name.
- Click the **Configuration** tab.
- Select **Networking** (in the Hardware section). The default Virtual Switch: **vSwitch 0** displays.
- Click the **Properties** link to configure the virtual switch's properties (Figure 1-14).

Figure 1-13 VM Switch Networking Properties—vSphere Client



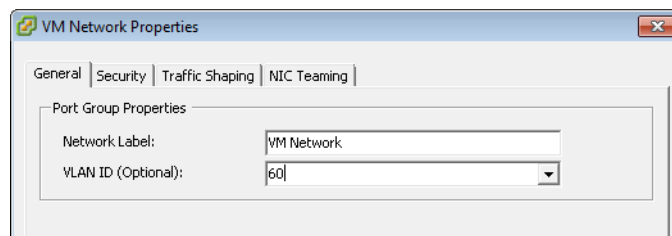
Step 2 Select **VM Network** and click **Edit** (Figure 1-14).

Figure 1-14 VM Switch Networking Properties—vSphere Client



The VM Network Properties screen displays (see Figure 1-15).

Figure 1-15 VM Network Properties—vSphere Client



Step 3 (Optional) Change the **VLAN ID** to the Cisco VSM VLAN ID (for example, **60**).

Step 4 Click **OK** to complete the network configuration.



Tip

For more information about VMWare vSphere documentation, see <http://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html>.

Configuring NTP Servers on the Blade

The server time synchronizes server operations, defines recording timestamps and backup schedules. We strongly recommend using the same network time protocol (NTP) server on all servers to ensure the time settings are accurate and identical. The clock should be set to use Coordinated Universal Time (UTC) and the appropriate time zone for the server.



Note

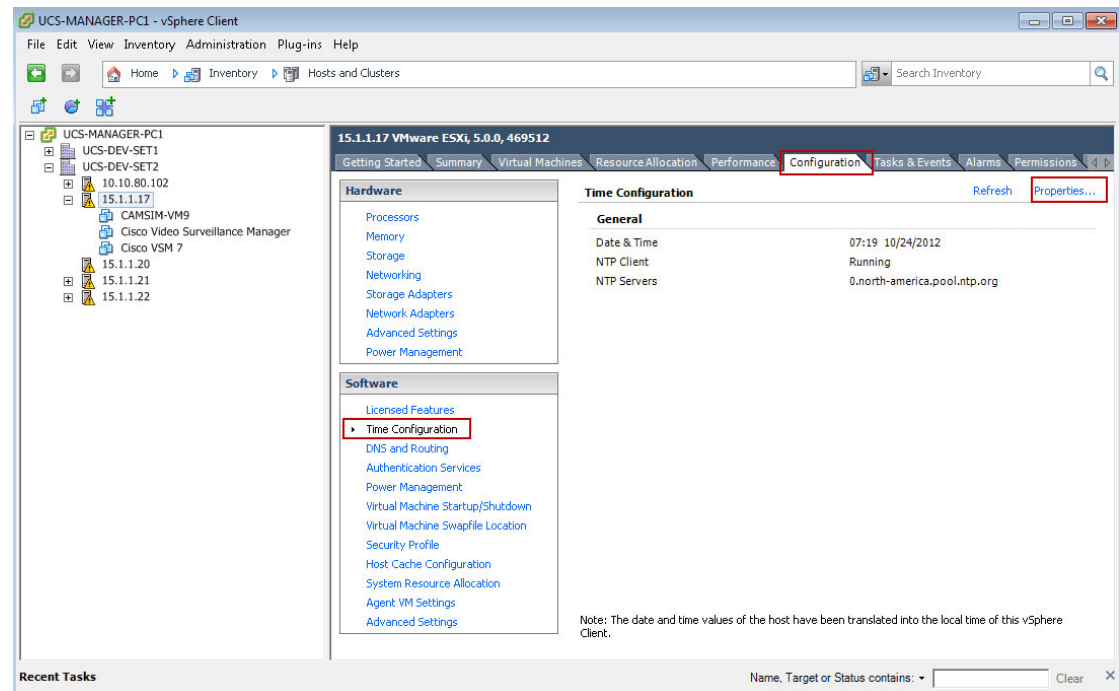
The NTP settings are also defined using the Cisco VSM Management Console. The first time you log on to the Cisco VSM server using a web-browser, you are prompted to complete the Initial Setup Wizard. An NTP server is required for all Media Server-only servers, and highly recommended for Operations Manager-only servers. See the [“Completing the Initial Server Setup Using the Management Console” section on page 1-48](#) for more information.

Procedure

Configure NTP on the VM as described in the following steps:

- Step 1** Open the Time Configuration setting.
- In the left pane (Inventory tree), select the hypervisor name (Figure 1-16).
 - Select the **Configuration** tab.
 - Select **Time Configuration** (in the Software area).
 - Click **Properties**.

Figure 1-16 Time Configuration Settings



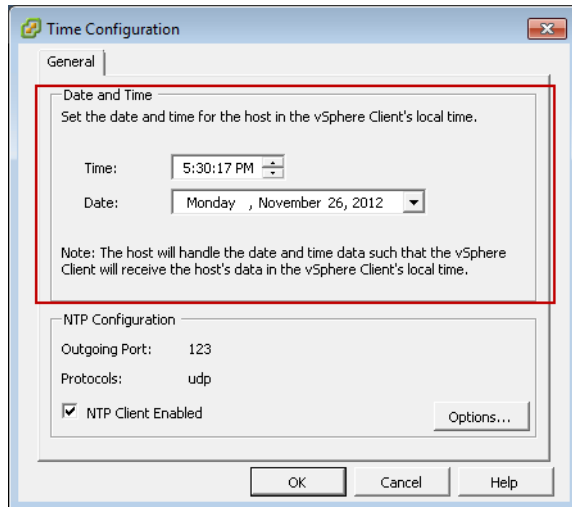
Step 2 Manually set the date and time (Figure 1-17).



Note

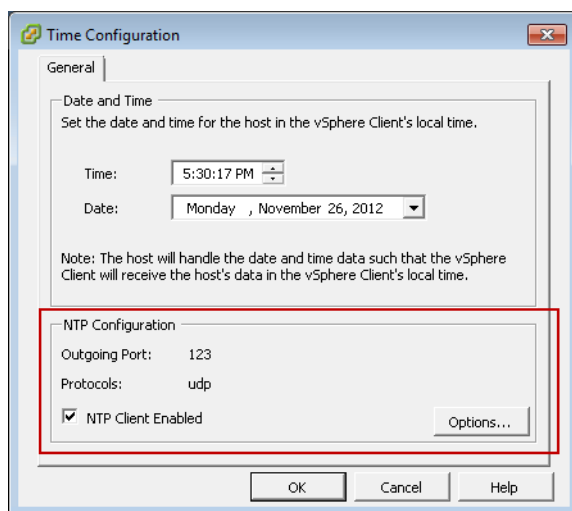
Manually set the date and time to ensure the VM time setting is correct immediately when the VM is started for the first time. This is necessary because the NTP synchronization may not occur immediately and possible system issues can occur if the VM time is significantly different from either the hardware platform, other Cisco VSM servers, or network cameras.

Figure 1-17 Manual Time and Date Configuration



Step 3 Check the **NTP Client Enabled** box and click **Options** (Figure 1-18).

Figure 1-18 NTP Configuration

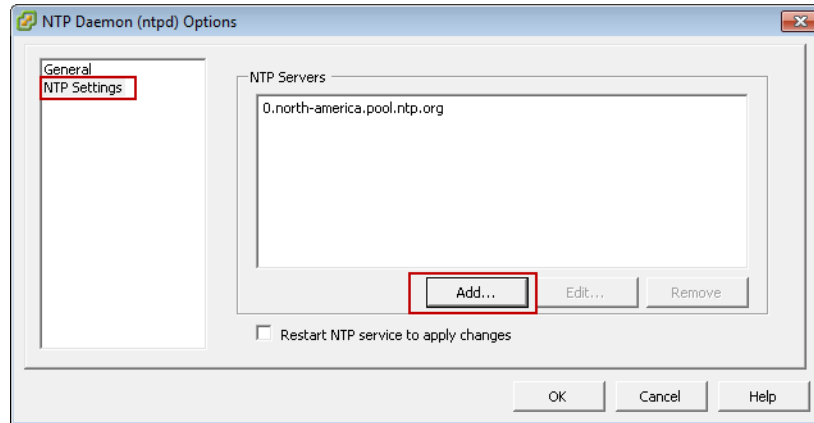


Step 4 Add the NTP server address (Figure 1-19).

- Select **NTP Settings**.
- Select **Restart NTP service to apply changes**.

- c. Click **Add**.
- d. Enter the NTP server IP address or hostname.

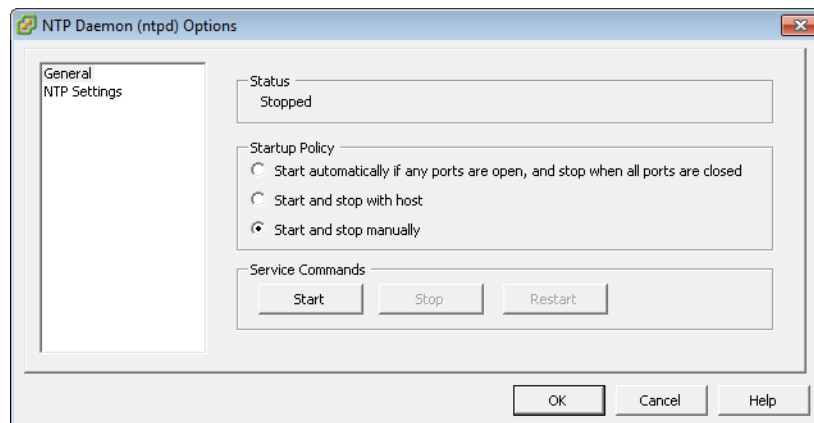
Figure 1-19 Adding the NTP Server Address



Step 5 Start the NTP server (Figure 1-20).

- a. Select **General**.
- b. Select a Startup Policy option.
- c. Click **Start**.

Figure 1-20 NTP Startup Policy Address



Step 6 Click **OK** to complete the NTP configuration.

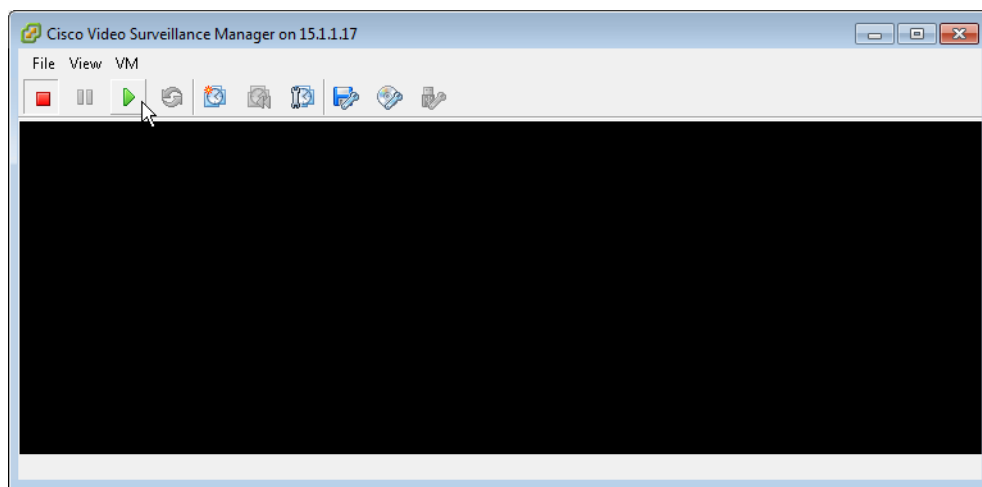
Powering On the Cisco VSM Virtual Machine

To power on the Cisco VSM virtual machine is similar to powering on a physical server. When powered on, the VM operating system boots, allowing you to access the VM and perform additional configuration of the Cisco VSM server.

Procedure

-
- Step 1** Right-click the Cisco VSM VM name, and select **Open Console** to launch the VM console.
- Step 2** Click the green arrow to power on the VM ([Figure 1-21](#)).

Figure 1-21 Power On the VM



- Step 3** Wait for the VM to boot.
- Step 4** Continue to [“Change the Default VM Password and Network Settings”](#).
-

Change the Default VM Password and Network Settings

The localadmin user is the account used by the Operations Manager to access the other Cisco VSM servers. The default password (**secur4u**) must be changed before accessing the Cisco VSM Management Console.

In addition, if the default static IP address (192.68.0.200) and DHCP IP address are not accessible to perform the initial VSM configuration, you can change the network settings using one of the following methods.

- [Release 7.5 and Later: CLI Method, page 1-27](#)—Use the Linux CLI to change the password and network settings.
- [Release 7.2 and Earlier: GUI Method, page 1-28](#)—Use the included GUI tools.

Release 7.5 and Later: CLI Method

Use the server CLI to change the localadmin user default password. You can also (optionally) configure the server network settings if the default static IP address (192.68.0.200) and DHCP IP address are not accessible to perform the initial VSM configuration.

Notes

- If multiple VMs are deployed on the same network using the default Eth0 IP address (192.68.0.200), the Eth0 address setting in the Cisco VSM Management Console will not be set (the field will be blank). This is because the operating system cannot configure the actual physical interface with duplicate IP addresses. To resolve this, enter a unique value for the Eth0 port on each deployed VM.
- You can modify the Eth0 IP address using the Cisco VSM Management Console, or the following CLI commands. See [Completing the Initial Server Setup Using the Management Console, page 1-48](#) for more information.
- The Red Hat GUI is not included in Release 7.5 and higher. Instead, use the CLI as described in the following procedure.

Procedure

- Step 1** (Required) Log into the server using a terminal application and change the default password for the localadmin user. For example:

```
login as: localadmin
Using keyboard-interactive authentication.
Password: secur4u

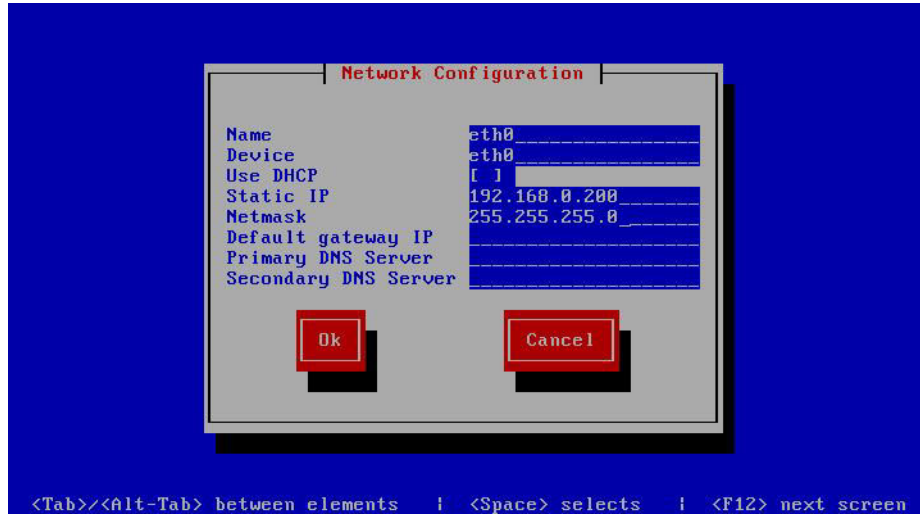
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user localadmin.
Changing password for localadmin.
(current) UNIX password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
localadmin@vsm-vm-server:~ #
```

- Step 2** (Optional) Configure the server network settings:

- a. Change to the root shell and launch the network configuration tool:

```
localadmin@vsm-vm-server:~ # sudo su -
root@vsm-vm-server ~# system-config-network
```

- b. Select **Device Configuration**.
- c. Select **eth0**.
- d. Update the Static IP, Netmask, Default Gateway IP, and Primary DNS Server ([Figure 1-22](#)).

Figure 1-22 Network Configuration Tool: Release 7.5 and Later

- e. Select **OK**.
- f. Select **Save** to save the settings.
- g. Select **Save & Quit**.
- h. At the CLI prompt, restart the network service to apply the new network configuration:


```
root@vsm-vm-server ~# service network restart
```

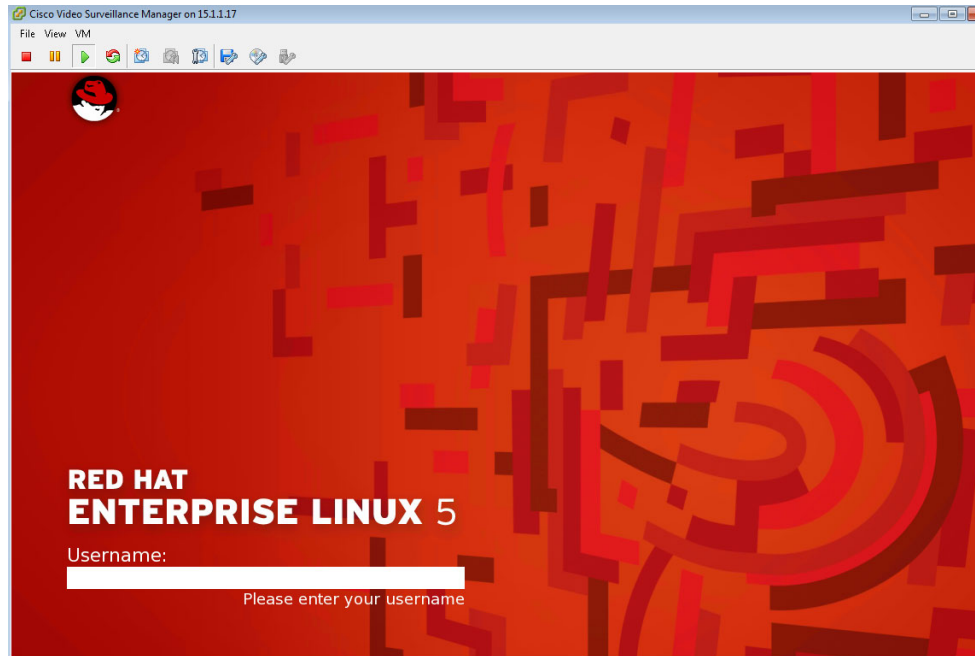
Step 3 (Required) Continue to the [“Creating Video Repositories”](#) section on page 1-33.

Release 7.2 and Earlier: GUI Method

In release 7.2 and earlier, use the included The Red Hat GUI tool .

Procedure

Step 1 (Required) Wait for the VM to boot and the Red Hat GUI interface to appear ([Figure 1-23](#)).

Figure 1-23 *Logging In to the VM Console: Release 7.2 and Earlier*

- Step 2** (Required) Enter the default VM username and password: **localadmin / secur4u**
- Step 3** (Required) Follow the on-screen prompts to enter and re-enter a new password (first login only).
- Step 4** (Optional) If you are unable to access the VM using the default static IP address or network-provided DHCP address, you can define the VM network settings using the guest OS GUI, as described in the following section:
- (Optional for Release 7.2 and Earlier) Use the Guest OS to Configure the Network Settings, page 1-29.
- Step 5** (Required) Continue to the “Creating Video Repositories” section on page 1-33.

(Optional for Release 7.2 and Earlier) Use the Guest OS to Configure the Network Settings

If you are unable to access the VM using the default static IP address or network-provided DHCP address, you can define the VM network settings using the guest OS GUI, as described in the following procedure.

Otherwise, continue to the “Complete the Setup Wizard” section on page 1-50.

After the network settings are changed, launch a web browser and connect to the Cisco VSM Management Console using the new IP address. You must complete the Initial Setup Wizard and restart the server using the browser-based Management Console, or the network settings will be revert back to the default settings (see Table 1-7 on page 1-49).

Procedure

- Step 1** Complete the following required procedure in the order shown:
- “Installing and Configuring the Cisco VSM Virtual Machine” section on page 1-9

- b. “Powering On the Cisco VSM Virtual Machine” section on page 1-26.
 - c. “Change the Default VM Password and Network Settings” section on page 1-26
 - d. “Creating Video Repositories” section on page 1-33
- Step 2** Power on the VM, if necessary (see the “Powering On the Cisco VSM Virtual Machine” section on page 1-26).
- Step 3** Right-click the desktop and select **Open Terminal**.
- Step 4** Enter the following commands to open the network configuration settings (Figure 1-24)
- ```
localadmin@localhost ~]$ xhost local:root
localadmin@localhost ~]$ sudo system-config-network
```
- Step 5** In the **Devices** tab, select the Eth0 port and click **Edit** (Figure 1-24).

**Figure 1-24 Network Configuration**



- Step 6** Change the network settings from the default 192.168.0.200 address to the desired network configuration (Figure 1-25).

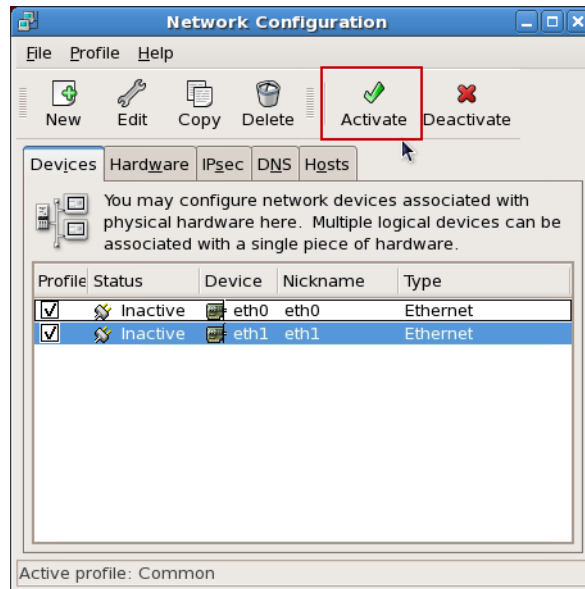
**Figure 1-25 Ethernet Device Configuration**

The screenshot shows the 'Ethernet Device' configuration window with the 'General' tab selected. The 'Nickname' field is set to 'eth0'. The 'Activate device when computer starts' checkbox is checked. The 'Automatically obtain IP address settings with:' dropdown is set to 'dhcp'. The 'DHCP Settings' section is collapsed. The 'Statically set IP addresses:' radio button is selected. The 'Manual IP Address Settings' section is expanded, showing the following values: Address: 192.168.3.16, Subnet mask: 255.255.255.0, and Default gateway address: 192.168.3.1. The 'Set MTU to:' and 'Set MRU to:' checkboxes are unchecked, with their respective values set to 0. The 'Cancel' and 'OK' buttons are at the bottom right.

- Step 7** Click **OK**.
- Step 8** (Optional) Revise the network configuration for the Eth1 port, if necessary, and click **OK**.
- Step 9** Select **File > Save** to save the configuration changes.

**Step 10** Click **Activate** to apply the updated configuration settings ([Figure 1-26](#)).

**Figure 1-26** *Activate the Network Configuration*



**Step 11** Follow the on-screen prompts to confirm the changes.

**Step 12** Do not restart the VM. Continue to [Complete the Setup Wizard, page 1-50](#).



**Note**

You must complete the Initial Setup Wizard and restart the server using the browser-based Management Console or the network settings will revert to the default values.



# Creating Video Repositories

Recorded video is stored in repositories on Cisco Media Servers. These repositories are separate partitions from the operating system (OS) partitions, and must be created using the integration scripts described in this section.

The integration script creates, formats, and mounts the partition, and then integrates it into Cisco VSM. If multiple external storage devices are connected, the script will create and integrate a separate partition for each device.

After the partitions are created, use the browser-based Operations Manager GUI interface to define which partition (repository) will be used for storing video, backups, and video clips.

Refer to the following topics for more information:

- [Usage Notes, page 1-33](#)
- [Understanding the Integration Script, page 1-34](#)
- [Understanding Mount Points, page 1-34](#)
- [Internal and External Storage Limitations, page 1-34](#)
- [Obtaining the Storage Partition Script, page 1-34](#)
  - [32-bit Red Hat OS \(Release 7.0 to Release 7.2\), page 1-34](#)
  - [64-bit Red Hat OS \(Release 7.5 and Higher\), page 1-35](#)
- [Understanding the Script Options, page 1-36](#)
- [Release 7.5 and Later: Adding Storage Partitions, page 1-36](#)
  - [Run the Script With No Options, page 1-36](#)
  - [Run the Script with the Restore Option, page 1-40](#)
- [Release 7.2 and Earlier: Adding Storage Partitions, page 1-41](#)
  - [External Storage Script: Release 7.2 and Earlier., page 1-41](#)
  - [Script Examples: Release 7.2 and Earlier, page 1-43](#)
  - [Internal Storage CLIs: Release 7.2 and Earlier, page 1-46](#)

## Usage Notes

- Each Cisco VSM server can have up to 32 video repositories for storing video, backups and video clips.
- Always create the video repositories before using the Cisco VSM Management Console described in the [“Completing the Initial Server Setup Using the Management Console”](#) section on [page 1-48](#).
- Each VM should have exclusive access to its own RAID array (1VM:1RAID-Array).
- After the VM configuration is complete, use the browser-based Operations Manager GUI interface to define which partition (repository) will be used for storing video, backups, and video clips. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

## Understanding the Integration Script

Each VM should have exclusive access to its own RAID array. For example, if you have a RAID-5 set of 10 drives with 3TB, then the entire ~25TB is provided as a single volume; the single volume appears to the Cisco VSM server as a single hard drive.

The integration scripts split the single storage volume into two partitions of equal size, formats the partitions, mounts them, and integrates them into Cisco VSM.

## Understanding Mount Points

Each repository (partition) has a mount point to specify the path through which the files are accessed. The common convention for naming repositories is /media#, with /media1 - /mediaN used for storage volumes.

## Internal and External Storage Limitations

### External FC SAN based Storage:

- The maximum partition sizes are:
  - 32-bit operating systems (such as Red Hat 5.8)—16 TB maximum size per partition
  - 64-bit operating systems—100 TB maximum size per partition (the maximum size tested is 50TB with ten 4TB hard drives)
- There can be multiple media partitions, media1 ....mediaN, based on the retention period for the video recordings of the cameras being hosted on the particular VM.

### Internal RAID based Storage:

- The maximum virtual disk size is 2TB.  
(<http://blogs.vmware.com/vsphere/2011/07/new-vsphere-50-storage-features-part-1-vmfs-5.html>)
- Multiple 2TB virtual disks can be added to the VM, based on the retention period for the video recordings of the cameras being hosted on the particular VM.

## Obtaining the Storage Partition Script

Download the appropriate script for the Cisco Video Surveillance release and OS you are deploying:

- [32-bit Red Hat OS \(Release 7.0 to Release 7.2\), page 1-34](#)
- [64-bit Red Hat OS \(Release 7.5 and Higher\), page 1-35](#)

### 32-bit Red Hat OS (Release 7.0 to Release 7.2)

For VM deployments running the 32-bit version of the Red Hat OS, download the `setup_external_storage.sh` script from [cisco.com](http://cisco.com).

#### Procedure

- 
- Step 1** Go to the [Cisco Product Support Page](#).

- Step 2** Click [Download Software](#).
  - Step 3** Click Video Surveillance Media Server Software.
  - Step 4** Select the 7.2 release page.
  - Step 5** Download the “**CPS-SS External storage configuration script for Video Surveillance Manager 7.2 and later**” (setup\_external\_storage-1.0.zip).
  - Step 6** Follow the onscreen instructions to complete the download.
  - Step 7** Complete the [Release 7.2 and Earlier: Adding Storage Partitions, page 1-41](#).
- 

## 64-bit Red Hat OS (Release 7.5 and Higher)

For VM deployments running the 64-bit version of the Red Hat OS, download the `setup_media_storage.sh` script from cisco.com.

**Tip**

In release 7.7 and higher, the `setup_media_storage.sh` script is also included in the OVA image, and can be run from `/usr/BWhttpd/bin`.

---

**Procedure**

- 
- Step 1** Go to the [Cisco Product Support Page](#).
  - Step 2** Click [Download Software](#).
  - Step 3** Click **Video Surveillance Media Server Software**.
  - Step 4** Select the **7.5.0** release page.
  - Step 5** Download the “**Video repository configuration script**” (setup\_media\_storage-1.0.zip).
  - Step 6** Follow the onscreen instructions to complete the download.
  - Step 7** Complete the [Release 7.5 and Later: Adding Storage Partitions, page 1-36](#).
-

## Understanding the Script Options

The storage script splits a single storage volume into two partitions of equal size, formats the partitions, mounts them, and integrates them into Cisco VSM.

The script offers the following options:

**Table 1-6** *Script Options*

| Script        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No parameters | Run the script with no parameters to discover any connected storage devices and create the new media partitions for use by Cisco VSM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Restore       | <p>Include the <b>restore</b> option (for example, <code>setup_media_storage.sh restore</code>) to retrieve and restore any media partitions that were previously configured on the disk so they can be used again. No new partitions are created using this restore option.</p> <p>Use this option only if the following previously occurred:</p> <ul style="list-style-type: none"> <li>• The script was previously run and the external storage partitions were successfully configured.</li> <li>• The Cisco VSM system software recovery procedure was executed (which removes the partitions from the Cisco VSM configuration).</li> </ul> <p>See the “<a href="#">Run the Script with the Restore Option</a>” section on page 1-40 for more information.</p> |
| Help          | Include the <b>help</b> option (for example, <code>setup_media_storage.sh -h</code> ) to view more information about the script options and version.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Release 7.5 and Later: Adding Storage Partitions

For Cisco VSM OVA's running Release 7.5 or later on Red Hat 6.4, run the `setup_media_storage.sh` script to add partitions from an internal or external storage system.



### Note

The script is supported with storage on the [Cisco Video Surveillance Storage System](#) in this release. See the [Cisco Video Surveillance Storage System Hardware Installation Guide](#) for more information.

## Run the Script With No Options



### Caution

The following steps erase the partition table on the specified volume, which deletes all data on the volume.

### Procedure

#### Step 1

Prepare for the external storage integration:

- a. If your platform uses external storage, install the external storage system as described in the [Cisco Video Surveillance Storage System Hardware Installation Guide](#).
- b. Add the storage to the Cisco VSM virtual machine as described in the “[Installing and Configuring the Cisco VSM Virtual Machine](#)” section on page 1-9.

- Step 2** (Release 7.5 and 7.6) Download the `setup_media_storage.sh` script to the server and make it executable.

**Tip**

In release 7.7 and higher, the `setup_media_storage.sh` script is also included in the OVA image, and can be run from `/usr/BWhttpd/bin`. Proceed to [Step 3](#).

- a. Download the script as described in the “[Obtaining the Storage Partition Script](#)” section on [page 1-34](#).
- b. Extract the `setup_media_storage.sh` script from the `setup_media_storage-1.0.zip`, and upload the script to the Cisco VSM server using a SFTP or SCP tool (as the user ‘localadmin’).
- c. Log in to the Cisco VSM server shell as the user ‘localadmin’ and move the script to `/usr/BWhttpd/bin/` with the following command:

```
[localadmin@vsm-server ~]$ sudo mv /var/lib/localadmin/setup_media_storage.sh
/usr/BWhttpd/bin/
```

- d. Make the `setup_media_storage.sh` script to be executable with the following command:

```
[localadmin@vsm-server ~]$ sudo chmod +x /usr/BWhttpd/bin/setup_media_storage.sh
```

- Step 3** (Optional) Display the Cisco VSM release details and the current filesystem disk space usage:

- a. Display the Cisco VSM build details to verify the release is supported:

```
[localadmin@vsm-server ~]$ sudo su -
[root@vsm-server ~]# cat /etc/Cisco-release
PRODUCT="VSM"
RELEASE="7.5.0"
OSVER=""
GOLD_DISK="VSM 7.5.0-cd15"
BUILDDATE="Fri March 14 10:37:12 PDT 2014"
```

- b. Display the filesystem disk space usage (in human readable format):

```
[root@vsm-server ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sdb1 7.9G 2.2G 5.4G 29% /
/dev/sdb7 50G 570M 47G 2% /mysql/data
/dev/sdb5 7.9G 2.8G 4.7G 38% /usr/BWhttpd
/dev/sdb3 32G 173M 30G 1% /var
/dev/sda1 146M 17M 122M 12% /boot
tmpfs 4.0G 4.0K 4.0G 1% /dev/shm
/dev/sdc1 5.4T 8.2M 5.4T 1% /media1
```

- Step 4** (Optional) Display the `help` output for command options and other information:

```
[root@vsm-server ~]# /usr/BWhttpd/bin/setup_media_storage help

setup_media_storage will configure storage volumes for use by VSM 7.x
It is currently optimized for RAID volumes.
Supported and recommended configuration for external storage arrays
 10 drive, RAID 5 arrays (9+1).
All other configurations are not supported and would cause
performance impacts.

usage:
 setup_media_storage [restore|help|]
 where
 restore will assume all partitioning and respective
 xfs formatting has been done. It will create
 the mount points, fstab entries and respective
 configuration
```

without argument it will look for existing partition  
and prompt the user if and only if partitioning info  
exists.

version: 1.0      date: 03/14/2014

**Step 5** Run the script from the directory where the script is located.

The script discovers any connected storage devices and creates new media partitions for use by Cisco VSM.

In the following example, the script is run without options, which creates new partitions.

```
[localadmin@vsm-server ~]$ sudo su -
[root@vsm-server ~]# /usr/BWhttpd/bin/setup_media_storage
setup_media_storage will configure storage volumes for use by VSM 7.5
It is optimizes alignment for the RAID array configuration.
Please ensure you have the RAID array drive count and RAID level per
storage volume before continuing.

Supported and recommended configuration for external storage arrays
10 drive, RAID 5 arrays (9+1).

Recommended configurations for VM with internal storage arrays
UCS E Series 2 drive, RAID 1 arrays (1+1).
UCS E Series 1 drive, RAID 0
UCS C-220 4 drive, RAID 5 arrays (3+1).
UCS C-240 12 drive, RAID 5 arrays (11+1).
UCS C-240 12 drive, RAID 6 arrays (10+2).

press return key to continue

DEV: VENDOR: MODEL: MOUNTED: SIZE:
/dev/sda VMware Virtual disk yes 0.11TiB
/dev/sdb VMware Virtual disk yes 0.68TiB
/dev/sdc VMware Virtual disk yes 0.05TiB
/dev/sdd NEXSAN NXS-B01-000 no 0.91TiB
/dev/sde NEXSAN NXS-B01-000 yes 20.7TiB

Storage devices available to configure for media storage:

/dev/sdd

Please confirm the storage volumes to configure
Enter "all" or individual device names separated by spaces:
all

Devices to configure: /dev/sdd

WARNING: /dev/sdd
WARNING: It appears the storage volume requested has existing partitioning
information and may possibly contain video data.
Continuing will erase all data on the volume.
Are you sure you want to proceed? [yes/no] yes

WARNING: Misidentifying RAID parameters could cause significant performance
degradation.

Please enter the number of hard drives in the RAID array of:
/dev/sdd.
[10]
```

```

Please enter the RAID level of the RAID array behind /dev/sdd [0 1 5 or 6].
[5]

DEVICE(S) = /dev/sdd
ARRAY_DRIVE COUNT = 10
RAID LEVEL = 5
DATA_DRIVE COUNT = 9

Are you sure? [y/n] y
mkfs.xfs: Specified data stripe width 2304 is not the same as the volume stripe width
2048
mounted /dev/sdd1 (UUID=7e1fbf48-66e2-44d0-b2fc-a45929aa8af0) on /media5
[root@vsm-server ~]#

```



**Note** After running the script, the newly created /media partitions are available for recording in Cisco VSM, without needing to reboot the server.

**Step 6** Enter the command **df -h** to display the available media repositories (/media1, /media2 and/or /media3) created by the script.

**Step 7** Verify that the filesystem disk space usage and external storage partitions are correct.

- a. Display the filesystem disk space usage (the **-h** option displays the results in human readable format):

```

[root@vsm-server ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda2 7.9G 1.6G 6.0G 21% /
tmpfs 5.4G 124K 5.4G 1% /dev/shm
/dev/sda8 53G 700M 50G 2% /mysql/data
/dev/sda6 7.9G 3.2G 4.3G 43% /usr/BWhttpd
/dev/sda4 32G 400M 30G 2% /var
/dev/sdc1 50G 37M 50G 1% /media2
/dev/sdb1 700G 40G 661G 6% /media1
/dev/sde1 21T 37M 21T 1% /media4
/dev/sdd1 931G 37M 931G 1% /media5

```

- b. Verify the results by listing the contents of each partition.

Use the **-al** option to list all results in long format.:

```

[root@vsm-server ~]# ls /media5
file_1 file_dir

```

**Step 8** Continue to [“Completing the Initial Server Setup Using the Management Console” section on page 1-48.](#)



**Note** After the server configuration is complete, use the browser-based Operations Manager GUI interface to define which partition (repository) will be used for storing video, backups, and video clips. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

## Run the Script with the Restore Option

The **restore** option retrieves and restores any media partitions that were previously configured on the disk so they can be used again.

This option is used after the Cisco VSM system software is recovered, since the recovery process deletes any Cisco VSM storage partitions from the Cisco VSM configuration.



**Tip**

See the [“Understanding the Script Options”](#) section on page 1-36 for more information.

### Procedure

**Step 1** Restore the Cisco VSM system software.

See the [Cisco Video Surveillance Manager Recovery Guide \(UCS Platform\)](#) for more information.

**Step 2** Complete the [“Release 7.5 and Later: Adding Storage Partitions”](#) section on page 1-36, except use the **restore** option to the integration script.

For example:

```
[localadmin@vsm-server ~]$ sudo su -
[root@vsm-server ~]# /usr/BWhttpd/bin/setup_media_storage restore
setup_media_storage will configure storage volumes for use by VSM 7.5
It is optimizes alignment for the RAID array configuration.
Please ensure you have the RAID array drive count and RAID level per
storage volume before continuing.
```

```
Supported and recommended configuration for external storage arrays
10 drive, RAID 5 arrays (9+1).
```

```
Recommended configurations for VM with internal storage arrays
UCS E Series 2 drive, RAID 1 arrays (1+1).
UCS E Series 1 drive, RAID 0
UCS C-220 4 drive, RAID 5 arrays (3+1).
UCS C-240 12 drive, RAID 5 arrays (11+1).
UCS C-240 12 drive, RAID 6 arrays (10+2).
```

```
press return key to continue
```

| DEV:     | VENDOR: | MODEL:       | MOUNTED: | SIZE:   |
|----------|---------|--------------|----------|---------|
| /dev/sda | VMware  | Virtual disk | yes      | 0.11TiB |
| /dev/sdb | VMware  | Virtual disk | yes      | 0.68TiB |
| /dev/sdc | VMware  | Virtual disk | yes      | 0.05TiB |
| /dev/sdd | NEXSAN  | NXS-B01-000  | no       | 0.91TiB |
| /dev/sde | NEXSAN  | NXS-B01-000  | yes      | 20.7TiB |

```
Storage devices available to configure for media storage:
```

```
/dev/sdd
```

```
Please confirm the storage volumes to configure
```

```
Enter "all" or individual device names separated by spaces:
all
```

```
Devices to configure: /dev/sdd
```

```
Found /media5 on /dev/sdd1
mounted /dev/sdd1 (UUID=7e1fbf48-66e2-44d0-b2fc-a45929aa8af0) on /media5
```



**Step 3** Verify that the filesystem disk space usage and external storage partitions are correct.

- a. Display the filesystem disk space usage (the **-h** option displays the results in human readable format):

```
[root@vsm-server ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda2 7.9G 1.6G 6.0G 21% /
tmpfs 5.4G 124K 5.4G 1% /dev/shm
/dev/sda8 53G 700M 50G 2% /mysql/data
/dev/sda6 7.9G 3.2G 4.3G 43% /usr/BWhttpd
/dev/sda4 32G 400M 30G 2% /var
/dev/sdc1 50G 37M 50G 1% /media2
/dev/sdb1 700G 40G 661G 6% /media1
/dev/sde1 21T 37M 21T 1% /media4
/dev/sdd1 931G 37M 931G 1% /media5
```

- b. Verify the results by listing the contents of each partition.

Use the **-al** option to list all results in long format.:

```
[root@vsm-server ~]# ls /media5
file_1 file_dir
```

**Step 4** Continue to [“Completing the Initial Server Setup Using the Management Console” section on page 1-48](#).



**Note**

After the server configuration is complete, use the browser-based Operations Manager GUI interface to define which partition (repository) will be used for storing video, backups, and video clips. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

## Release 7.2 and Earlier: Adding Storage Partitions

For Cisco VSM OVAs running Release 7.2 or earlier on Red Hat 5.8, use the following methods to add storage partitions from either an external or internal storage source.

- [External Storage Script: Release 7.2 and Earlier](#), page 1-41
  - [Script Examples: Release 7.2 and Earlier](#), page 1-43
- [Internal Storage CLIs: Release 7.2 and Earlier](#), page 1-46

### External Storage Script: Release 7.2 and Earlier:

For Cisco VSM OVAs running Release 7.2 or earlier on Red Hat 5.8, use the **setup\_external\_storage.sh** script to add partitions from external storage. The script discovers any connected storage devices and creates new media partitions for use by Cisco VSM.



**Note**

Only storage on the [Cisco Video Surveillance Storage System](#) is supported in this release. See the [Cisco Video Surveillance Storage System Hardware Installation Guide](#) for more information.

**Caution**

The following steps erase the partition table on the specified volume, which deletes all data on the volume.

**Procedure**

- 
- Step 1** Install the external storage system as described in the [Cisco Video Surveillance Storage System Hardware Installation Guide](#).
- Step 2** Add the storage to the Cisco VSM virtual machine as described in the “[Installing and Configuring the Cisco VSM Virtual Machine](#)” section on page 1-9.
- Step 3** Obtain the correct script for your OS and Cisco VSM release as described in the “[Obtaining the Storage Partition Script](#)” section on page 1-34.
- Step 4** Run the script from the directory where the script is located (see the [Script Examples: Release 7.2 and Earlier](#), page 1-43).
- Step 5** Follow the onscreen prompts to complete the script.
- Step 6** Enter the command `df -h` to display the available media repositories (/media1, /media2 and/or /media3) created by the script.

**Tip**

Refer to the following [Script Examples: Release 7.2 and Earlier](#) for more information.

- Step 7** Continue to “[Completing the Initial Server Setup Using the Management Console](#)” section on page 1-48.

**Note**

After the server configuration is complete, use the browser-based Operations Manager GUI interface to define which partition (repository) will be used for storing video, backups, and video clips. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

---

## Script Examples: Release 7.2 and Earlier

The following examples show how to use the `setup_external_storage` script to add storage partitions to a Cisco VSM server from a supported (and connected) external storage system.

- [Example to Run a Script for a Single External Storage System, page 1-43](#)
- [Example to Run the Script for Multiple External Storage Systems, page 1-44](#)

### Example to Run a Script for a Single External Storage System

The following example creates a single media repository (/media1) from a single external storage system.

```
[localadmin@localhost ~]$ sudo su -
[root@localhost ~]# cd
[root@localhost ~]# cd bin
[root@localhost bin]# ./setup_external_storage
user friendly !!!

get_external_storage_devices
/sys/block/sda/ :
/sys/block/sdb/ :
using the next MEDIA_PART_NUMBER = 0
WARNING: /dev/sdb has partitioning and or data
WARNING: It appears the external storage has existing partitioning and
possibly video data. Continuing will erase any data on external
partitions.
Are you sure you want to proceed? [yes/no]
yes

===== Creating Partition Tables =====
DEVICE /dev/sdb

create_partition_table /dev/sdb
parted /dev/sdb mklabel gpt
Warning: The existing disk label on /dev/sdb will be destroyed and all data on this disk
will be lost. Do you want to continue?
Yes/No? Yes

Information: You may need to update /etc/fstab.

===== Creating Partitions =====
create_partitions_on_device /dev/sdb
stripe size = 18432
START_S=34 SIZE_S=10
number of partitions: 1
stripe size = 18432
START_S=36864 SIZE_S=7501327MB
parted /dev/sdb mkpart primary xfs 36864s 100%
Information: You may need to update /etc/fstab.

===== Formatting Partitions and =====
===== Creating fstab entries, mount pts =====

format_partitions_on_device /dev/sdb
format partition: /dev/sdb1
mkfs.xfs: Specified data stripe width 2304 is not the same as the volume stripe width 1024
update_fstab_device_mount_log UUID=e5869ccd-073b-4956-aa57-882220ea0ad3 /media1
update_device_name /dev/sdb 1 /media1
parted /dev/sdb name 1 /media1
Configuring VSMS
cisco 0:off 1:off 2:on 3:on 4:on 5:on 6:off
cisco_kernelTweaks 0:off 1:off 2:on 3:on 4:on 5:on 6:off
```

```
[root@localhost bin]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda2 7.9G 1.6G 6.0G 21% /
tmpfs 5.4G 4.0K 5.4G 1% /dev/shm
/dev/sda8 53G 624M 50G 2% /mysql/data
/dev/sda6 7.9G 2.9G 4.6G 39% /usr/BWhttpd
/dev/sda4 32G 269M 30G 1% /var
/dev/sdb1 6.9T 37M 6.9T 1% /media1
```

### Example to Run the Script for Multiple External Storage Systems

The following example creates a multiple media repositories (/media1, /media2, and /media3) from multiple external storage systems.

```
[root@localhost bin]# ./setup_external_storage
user friendly !!!

get_external_storage_devices
/sys/block/sda/ :
/sys/block/sdb/ :
/sys/block/sdc/ :
/sys/block/sdd/ :
using the next MEDIA_PART_NUMBER = 0
WARNING: /dev/sdb has partitioning and or data
WARNING: /dev/sdc has partitioning and or data
WARNING: /dev/sdd has partitioning and or data
WARNING: It appears the external storage has existing partitioning and
possibly video data. Continuing will erase any data on external
partitions.

Are you sure you want to proceed? [yes/no]
yes

===== Creating Partition Tables =====
DEVICE /dev/sdb

create_partition_table /dev/sdb
parted /dev/sdb mklabel gpt
Warning: The existing disk label on /dev/sdb will be destroyed and all data on this disk
will be lost. Do you want to continue?
Yes/No? Yes
Information: You may need to update /etc/fstab.

DEVICE /dev/sdc

create_partition_table /dev/sdc
parted /dev/sdc mklabel gpt
Warning: The existing disk label on /dev/sdc will be destroyed and all data on this disk
will be lost. Do you want to continue?
Yes/No? Yes

Information: You may need to update /etc/fstab.

DEVICE /dev/sdd

create_partition_table /dev/sdd
parted /dev/sdd mklabel gpt
Warning: The existing disk label on /dev/sdd will be destroyed and all data on this disk
will be lost. Do you want to continue?
Yes/No? Yes

Information: You may need to update /etc/fstab.
```

```

===== Creating Partitions =====
create_partitions_on_device /dev/sdb
stripe size = 18432
START_S=34 SIZE_S=10
number of partitions: 1
stripe size = 18432
START_S=36864 SIZE_S=26004731MB
parted /dev/sdb mkpart primary xfs 36864s 100%
Information: You may need to update /etc/fstab.

create_partitions_on_device /dev/sdc
stripe size = 18432
START_S=34 SIZE_S=10
number of partitions: 1
stripe size = 18432
START_S=36864 SIZE_S=1024001MB
parted /dev/sdc mkpart primary xfs 36864s 100%
Information: You may need to update /etc/fstab.

create_partitions_on_device /dev/sdd
stripe size = 18432
START_S=34 SIZE_S=10
number of partitions: 1
stripe size = 18432
START_S=36864 SIZE_S=1024001MB
parted /dev/sdd mkpart primary xfs 36864s 100%
Information: You may need to update /etc/fstab.

===== Formating Partitions and =====
===== Creating fstab entries, mount pts =====

format_partitions_on_device /dev/sdb
format partition: /dev/sdb1

format_partitions_on_device /dev/sdc
format partition: /dev/sdc1

format_partitions_on_device /dev/sdd
format partition: /dev/sdd1
update_fstab_device_mount_log UUID=dffda463-3be1-490a-98ca-603731031c37 /media1
update_device_name /dev/sdb 1 /media1
parted /dev/sdb name 1 /media1
update_fstab_device_mount_log UUID=c963bdb4-6ef3-4055-9d6e-cc3337fe8893 /media2
update_device_name /dev/sdc 1 /media2
parted /dev/sdc name 1 /media2
update_fstab_device_mount_log UUID=35adf103-81bc-462b-8b94-8f047b250089 /media3
update_device_name /dev/sdd 1 /media3
parted /dev/sdd name 1 /media3
Configuring VSMS
cisco 0:off 1:off 2:on 3:on 4:on 5:on 6:off
cisco_kernelTweaks 0:off 1:off 2:on 3:on 4:on 5:on 6:off

[root@localhost bin]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/sda2 7.9G 1.6G 6.0G 21% /
tmpfs 5.4G 4.0K 5.4G 1% /dev/shm
/dev/sda8 53G 624M 50G 2% /mysql/data
/dev/sda6 7.9G 2.9G 4.6G 39% /usr/BWhttpd
/dev/sda4 32G 269M 30G 1% /var
/dev/sdb1 24T 37M 24T 1% /media1
/dev/sdc1 954G 37M 954G 1% /media2
/dev/sdd1 954G 37M 954G 1% /media3
[root@localhost bin]#

```

## Internal Storage CLIs: Release 7.2 and Earlier

For Cisco VSM OVAs running Release 7.2 or earlier on Red Hat 5.8, complete the following steps to add a media partition from an internal storage system.

- Log into the server and enter the CLI commands as described.
- The following steps erase the partition table on the specified volume, which deletes all data on the volume.
- Partition and mount an `sd#` device for each hard-disk added to the VM.

### Procedure

- 
- Step 1** Install the external storage system as described in the [Cisco Video Surveillance Storage System Hardware Installation Guide](#).
- Step 2** Add the storage to the Cisco VSM virtual machine as described in the “[Installing and Configuring the Cisco VSM Virtual Machine](#)” section on page 1-9.
- Step 3** Log in to the Media Server as the “localadmin” user and follow these steps to
- Create a GPT partition on a volume.
 

```
localadmin@linux:~> sudo su -
linux:~ # parted /dev/sdb
linux:~ # parted> mklabel gpt
linux:~ # parted> mkpart primary xfs 100%
```
  - Verify the partition creation, partition number and size:
 

```
linux:~ # parted> print
```
  - Quit the Parted partition editor:
 

```
linux:~ # parted> quit
```
  - Create the Linux file system on the partition:
 

```
linux:~ # mkfs.xfs -f -L media# /dev/sdb1
```

**-L** specifies a label for the partition filesystem.

**-f** overwrites the existing filesystem on the LUN being configured, if necessary, and creates a new label and filesystem.

*media#* is the media partition you choose (e.g. /media1, /media2, etc.).

*sdb#* is the partition number output in previous steps (e.g. /dev/sdb1).
  - Create a partition directory:
 

```
linux:~ # mkdir /media#
```
  - Add a fstab entry:
 

```
linux:~ # vi /etc/fstab
LABEL=media# /media# xfs rw,nodiratime,noatime 0 0
```
- Step 4** Repeat [Step 3](#) to partition and mount an `sd#` device for each hard-disk added to the VM.
- Step 5** Verify the mounts:
- ```
linux:~ # mount -a
```

- Step 6** Reboot the Cisco VSM virtual machine by logging out and selecting the **Reboot** option at the bottom of the screen.
- Step 7** Continue to [“Completing the Initial Server Setup Using the Management Console” section on page 1-48](#).

**Note**

After the server configuration is complete, use the browser-based Operations Manager GUI interface to define which partition (repository) will be used for storing video, backups, and video clips. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

Completing the Initial Server Setup Using the Management Console

After the Cisco VSM virtual machine is installed and configured, you must complete the Cisco Video Surveillance server configuration using the browser-based Cisco VSM Management Console. The first time you log on to the Management Console, an Initial Setup Wizard guides you through the basic configuration that includes the following settings.

Refer to the following topics for more information:

- [Usage Notes, page 1-48](#)
- [Default Network Settings, page 1-48](#)
- [Complete the Setup Wizard, page 1-50](#)

Usage Notes

- Complete the [“Creating Video Repositories” section on page 1-33](#) before completing the initial server setup wizard, or errors with the network settings can occur on co-located servers (servers that host both the Operations Manager and Media Server services).
- (Release 7.2 and earlier) You can also use the Guest OS to configure the network settings if you are unable to access the VM using the default static IP address or network-provided DHCP address. See the [“\(Optional for Release 7.2 and Earlier\) Use the Guest OS to Configure the Network Settings” section on page 1-29](#).
- Click **Help** in the Management Console for more information, or see the [Cisco Video Surveillance Management Console Administration Guide](#).

Default Network Settings

The Cisco VSM server includes two network ports with the following default configuration:

- Eth0 port—static IP address 192.168.0.200
- Eth1 port—DHCP

Release 7.5 and Later

You can also change the default network settings using CLI commands, if the default static IP address (192.68.0.200) and DHCP IP address are not accessible to perform the initial VSM configuration.

See [Release 7.5 and Later: CLI Method, page 1-27](#).

Release 7.2 and Earlier

If you cannot access either of these addresses with a web browser, you can also change the network settings using the guest OS console, and then use the Cisco VSM Management Console to complete the configuration and restart the server. See the [“\(Optional for Release 7.2 and Earlier\) Use the Guest OS to Configure the Network Settings” section on page 1-29](#).

Table 1-7 summarizes the network access and configuration options.

Table 1-7 Network Configuration Options

Method	Description
Default static address 192.168.0.200	<p>Enter the default 192.168.0.200 address in a web browser to connect to the server and complete the Initial Setup Wizard (which includes the server network configuration).</p> <ul style="list-style-type: none"> If multiple VMs are deployed on the same network using the default Eth0 IP address (192.68.0.200), the Eth0 address setting in the Management Console will not be set (the field will be blank). This is because the operating system cannot configure the actual physical interface with duplicate IP addresses. To resolve this, enter a unique value for the Eth0 port on each deployed VM. You can modify the Eth0 IP address using the Cisco VSM Management Console, or the following CLI commands. See the following for more information: <ul style="list-style-type: none"> Change the Default VM Password and Network Settings, page 1-26 Cisco Video Surveillance Management Console Administration Guide
DHCP-provided address	<p>Enter the DHCP-provided IP address in a web browser to connect to the server and complete the Initial Setup Wizard (which includes the server network configuration).</p> <p>Usage Notes:</p> <ul style="list-style-type: none"> Change the default hostname for each server from “localhost” to a unique value, such as “vsom01”, “mediaserver02”, etc. If multiple servers have the same hostname, server connection errors will occur since the DNS server will be unable to properly resolve the hostname for each server. The network must include a DHCP server configured to provide an IP address. See your network administrator for information regarding the IP addresses assigned to the server. When deploying multiple Cisco VSM virtual machines at a time, we recommended using a DHCP server to assign IP addresses for initial access to the Management Console. You will not be able to access multiple servers configured with the same default static IP address.
Manually configure the network settings using the VM guest OS	<p>(Release 7.2 and earlier)</p> <p>Log in to the VM console and change the network settings using the guest OS (RedHat Linux).</p> <ul style="list-style-type: none"> Use this method if you cannot access the VM using the default IP address or DHCP-provided address. After configuring the new IP address in the guest OS, you must immediately use the browser-based Management Console to complete the Initial Setup Wizard and restart the server. <p>See the “(Optional for Release 7.2 and Earlier) Use the Guest OS to Configure the Network Settings” section on page 1-29.</p>



Note

You may also need to configure one or more vLANs for the virtual machine to be able to access the default IP address, a DHCP address, or any other address that may be assigned to the virtual machine. See the “[Defining the VLAN for the VM](#)” section on page 1-21 for more information.

Complete the Setup Wizard

Use the browser-based Cisco VSM Management Console to complete the initial server setup.

Procedure

-
- Step 1** Complete the Virtual Machine installation in the following order:
- [Installing and Configuring the Cisco VSM Virtual Machine, page 1-9](#)
 - [Powering On the Cisco VSM Virtual Machine, page 1-26](#)
 - [Creating Video Repositories, page 1-33](#)
- Step 2** Launch a web browser and enter an IP address described in [Table 1-7](#) to access the Cisco VSM Management Console.
- Step 3** Enter the VM password you entered in [Change the Default VM Password and Network Settings, page 1-26](#).



Note The username “localadmin” is read-only and cannot be changed.

- Step 4** Click **Log In**.
- Step 5** Enter a new password when prompted.
- Step 6** Complete the Initial Setup Wizard to enable the server services, change the network settings, configure NTP servers, and other settings.



Tip See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information about the services and settings supported in your Cisco VSM release.

- Step 7** Click **Restart Services** to save the changes and restart the server.
- Step 8** Re-login to the Cisco VSM Management Console.
- Step 9** Configure additional server settings, if necessary.
- Click the **Help** menu in the Management Console for more information.
 - See the [Cisco Video Surveillance Management Console Administration Guide](#) for more information.
- Step 10** Use the Cisco VSM Operations Manager to perform additional configuration and administrative tasks.
- For example, go to the Media Server configuration page and define which partition (repository) will be used for storing video, backups, and video clips. See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
 - See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.
-

Testing Network Connectivity

To verify that network connectivity is working properly between endpoints, including IP cameras and Operations Manager workstations, perform the following steps:

Procedure

-
- Step 1** From a terminal window on the Cisco VSM VM, ping the gateway, cameras, and Operations Manager client PCs to ensure proper connectivity.
 - Step 2** Log on to the Cisco VSM Management Console and ensure that all Cisco services are running and operational (go to **Monitor > System Summary** and scroll down to the **Service Status** section).
 - Step 3** Log on to the browser-based Cisco VSM Operations Manager to verify that you can access the GUI. Click **Cameras** to add cameras and verify connectivity. Click **System Settings > Media Servers** to add the servers, verify connectivity, and make additional configuration changes, if necessary.
-

Adjusting Performance

These performance tips are highly dependent on your specific virtualized environment. For example, if you have more VMs running on the same host as Cisco VSM, then VSM may not have enough CPU cycles. The alert “Load Average Critical” may appear on those VSM servers. If this occurs, you may be able to resolve the issue by setting a CPU reservation on ESXi.

On a CPU, the reservation is a guarantee for clock cycles and you define the reservation in MHz. If you define CPU reservation on a virtual machine, the vmkernel CPU scheduler will give it a minimum of the defined resources. If a virtual machine is not using its resources, the CPU cycles are not wasted on the physical host. Other machines can use it. CPU reservation make sure that a VM will always get access to physical CPU in a committed environment.

Procedure

-
- Step 1** In the vSphere Client inventory, right-click the virtual machine and select **Edit Settings**.
 - Step 2** Click the **Resources** tab and select **CPU**.
 - Step 3** Under **Reservation**, define an acceptable value to guarantee CPU allocation for this virtual machine.
 - Step 4** Click **OK** to save your changes.
-



Recovering Cisco Video Surveillance VMs on the Cisco UCS Platforms

Recovery is used to replace an existing VM with a OVA deployment of the same release. This entails shutting down the existing VM, deploying the new VM, and transferring the storage and other properties to the new VM.

Refer to the following topics for more information.

- [Assumptions, page 2-1](#)
- [Summary Steps, page 2-2](#)
- [Detailed Instructions: Recovering the VSM on the UCS, page 2-3](#)

Assumptions

The following instructions assume that the system configuration and data was previously backed up and is available for restoring on the new image.

For backup instructions, see the [Cisco Video Surveillance Management Console Administration Guide](#).

Summary Steps

Review the following summary steps before you begin. Use the [“Detailed Instructions: Recovering the VSM on the UCS” section on page 2-3](#) to complete the recovery process.

Table 2-1 Summary Steps

	Task	Description
Step 1	Backup the server configuration using the Cisco VSM Management Console	The configuration data from the existing VM will be restored to the new VM. The data will be lost if not backed up and restored. See the Cisco Video Surveillance Management Console Administration Guide .
Step 2	Download the replacement OVA image from the Cisco website. Note The new VM should be the same version as the old VM being replaced.	Download the OVA image that will replace the existing VM. See the “Obtaining the Software Images” section on page 1-7
Step 3	Power off the existing Cisco VSM virtual machine (VM).	The existing VM must be powered off before it is replaced. All video processing and user access to the virtual machine will be lost during the recovery process.
Step 4	Deploy the new (replacement) VM.	Add the new replacement VM to the vSphere Client configuration.
Step 5	Connect the new (replacement) VM to the existing media virtual disk (used by the old VM).	Associates the storage from the old VM to the new replacement VM.
Step 6	Complete the configuration on the new VM. The configuration should be the same as the old VM. <ul style="list-style-type: none"> • Define a vLAN (if required). • Define the NTP settings. • Power On the VM and change the default password. • Configure the network settings. 	You must manually apply the same configurations from the old VM to the new VM.
Step 7	Restore the video repositories.	Restores the existing video repositories to the new VM, which retains the existing video archives.
Step 8	Complete the Initial Setup using the Cisco VSM Management Console.	Use the browser-based Management Console to preform the initial server setup. See the “Completing the Initial Server Setup Using the Management Console” section on page 1-48
Step 9	Restore the VSOM and Media Server configurations.	Restores the configuration data that was backed up from the old VM. See the Cisco Video Surveillance Management Console Administration Guide .

Table 2-1 Summary Steps (continued)

	Task	Description
Step 10	Verify that the data is restored by logging on to the VSOM and viewing live video from cameras and playing back archives.	See the Cisco Video Surveillance Operations Manager User Guide to check cameras, video streams and recordings to verify that the replacement VM is working properly.
Step 11	Delete the old VM from the vSphere Inventory tree.	Permanently deletes the old VM from the vSphere Client software.

Detailed Instructions: Recovering the VSM on the UCS

Procedure

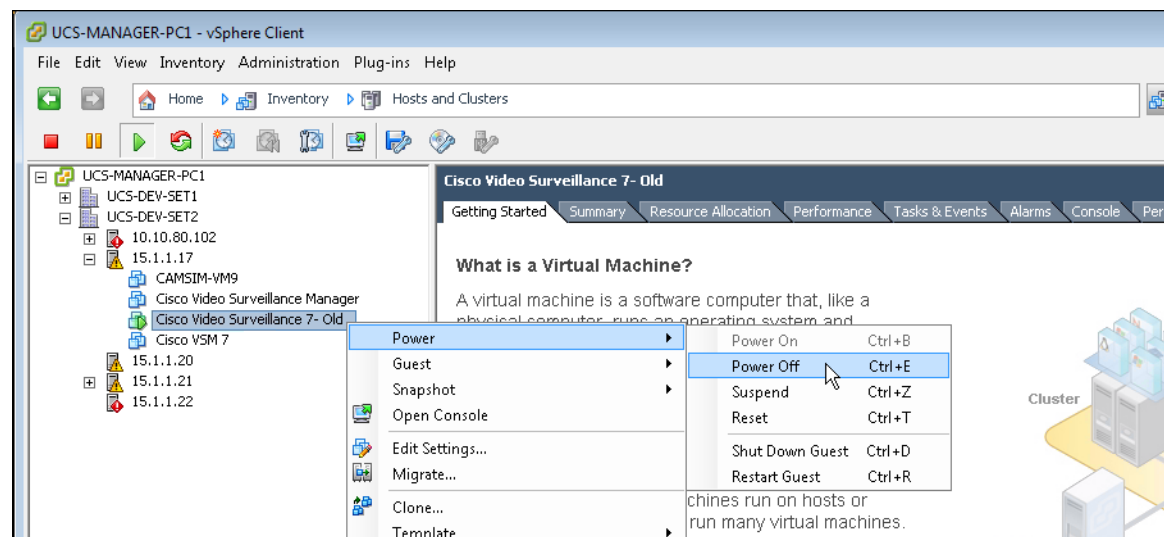
- Step 1** Before you begin, backup the server configuration using the Cisco VSM Management Console (see the [Cisco Video Surveillance Management Console Administration Guide](#)). If the server hosts both the Operations Manager and Media Server, back up both configurations.
- Step 2** Download the replacement OVA image from the Cisco website.
See the [“Obtaining the Software Images”](#) section on page 1-7.



Note Template files are typically large in size. We recommend downloading and copying it to universal serial bus (USB) flash to avoid download delays.

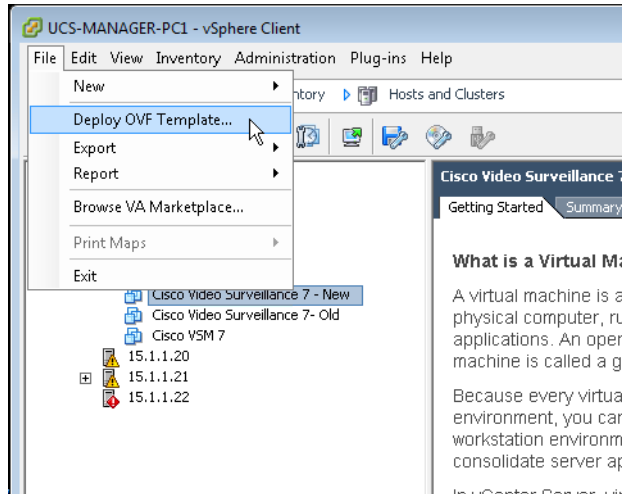
- Step 3** Power off the existing Cisco VSM virtual machine (VM):
- Launch the vSphere Client software ([Figure 2-1](#)).
 - Right-click the VM in the left pane (Inventory tree).
 - Select **Power > Power Off**.
 - Click **Yes** to confirm the action.

Figure 2-1 vSphere Client Software—Powering Off the VSM VM



- Step 4** Deploy the new (replacement) VM (Figure 2-2).
- Select **File > Deploy from OVF Template**.

Figure 2-2 Deploying the OVF Template



- Click **Browse** and select the .ova template file from a local disk, or enter the URL to download the file from the Internet.
- Enter the remaining settings to deploy the template (Table 2-2):

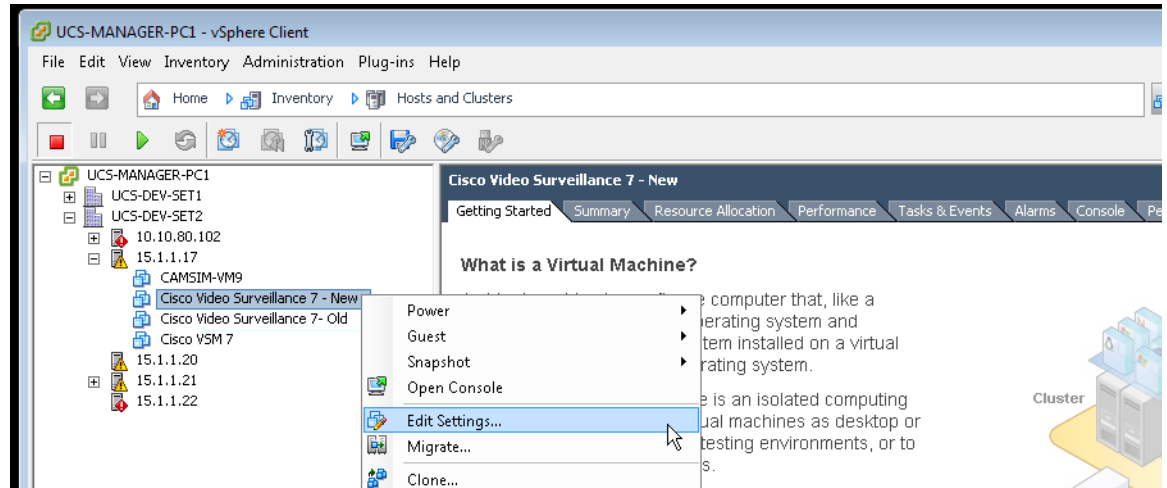
Table 2-2 OVA Deployment Settings

Setting	Description
OVF Template Details	Click Next to accept the default settings.
Name and Location	<p>Enter the name and location for the VM.</p> <ul style="list-style-type: none"> The name is displayed in the inventory tree (for example, “Cisco Video Surveillance Manager”). The location defines where the VM appears in the tree. <p>Click Next to continue.</p>
Host / Cluster	Select the specific host or cluster where you want to run the template.
Storage	<p>Select where the VM files will be stored. It should be deployed a datastore on internal storage, not external storage.</p> <p>See the “Requirements” section on page 1-5 for the amount of disk size required to deploy the VM (depending on the UCS platform). This requirement is for the VM only and does not include the video partition(s) disk space.</p>
Disk Format	Click Next to accept the default disk format (Thick Provisioned Lazy Zeroed).

- Click **Finish** to accept the selected deployment settings.
- Wait for the Cisco VSM template to deploy. Click **Close** when the success message appears.
- Verify that the VM displays under the host entry in the Inventory tree (Figure 2-3).

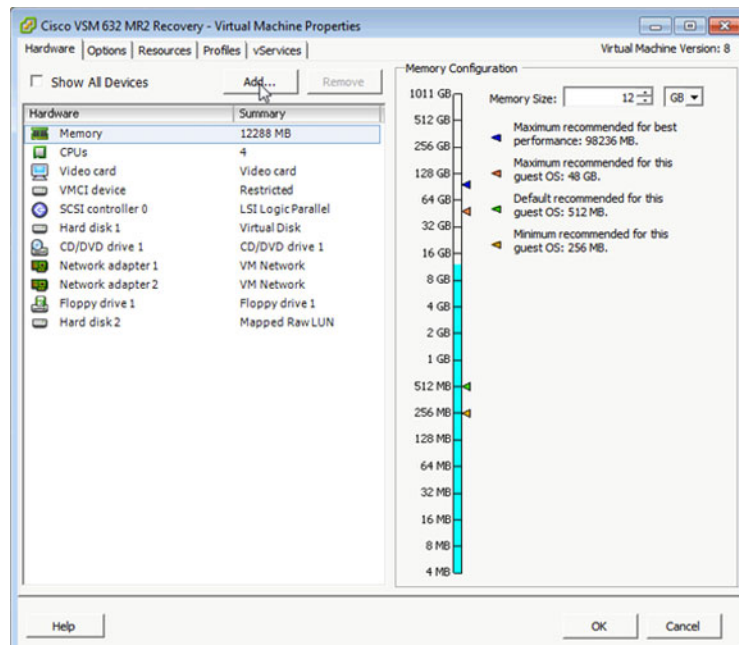
- Step 5** Connect the new (replacement) VM to the existing media virtual disk (used by the old VM).
- Right-click the new VM and select **Edit Settings** (see [Figure 2-3](#)).

Figure 2-3 *Edit Settings*



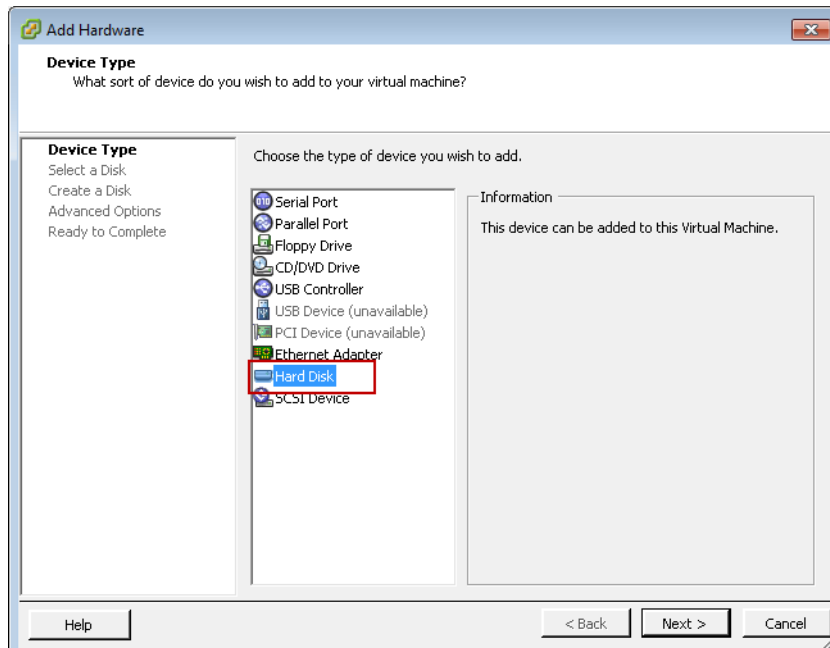
- Click **Add** (Properties screen in [Figure 2-4](#)).

Figure 2-4 *Adding a Hard Disk*



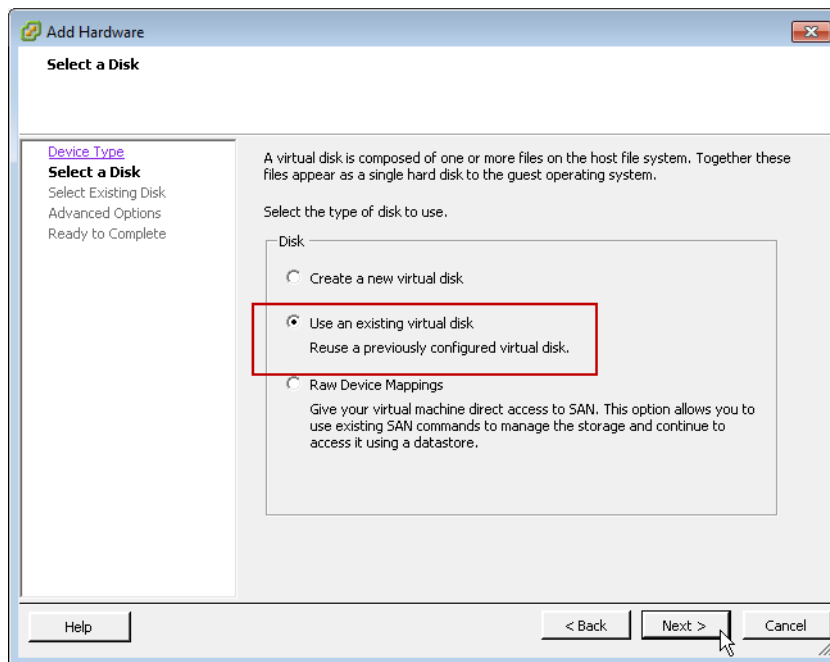
- c. Select **Hard Disk** and click **Next** (Figure 2-5).

Figure 2-5 *Selecting Device Type (Hard Disk)*



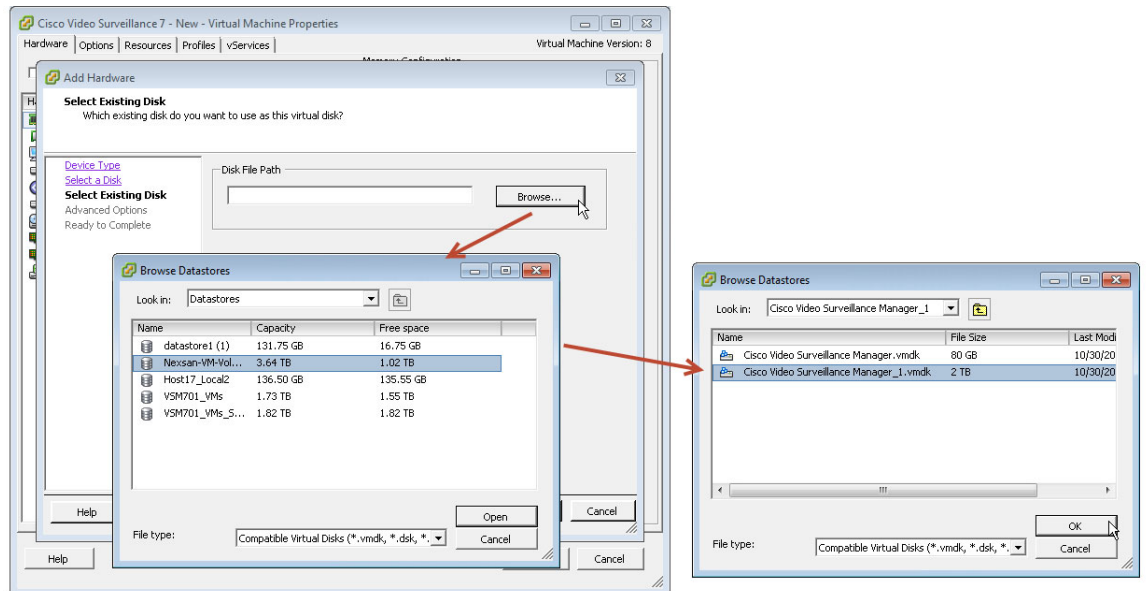
- d. Select **Use an existing virtual disk** and click **Next** (Figure 2-6).

Figure 2-6 *Selecting the Disk Type to Use*



- e. Click **Browse** to navigate to the datastore in the old VM directory (see [Figure 2-7](#)).

Figure 2-7 *Browsing and Selecting a Datastore*



- f. Select the appropriate media disk from the existing VM and click **OK**.

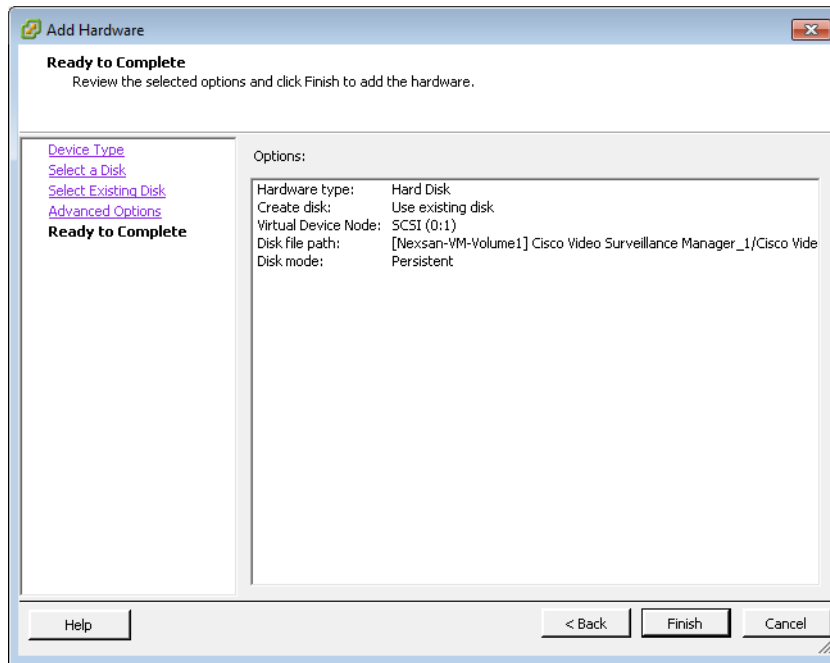


Tip

See the [“Adding Hard Disks for Media Storage”](#) section on page 1-15 for more information about the hard disk configuration for the old VM.

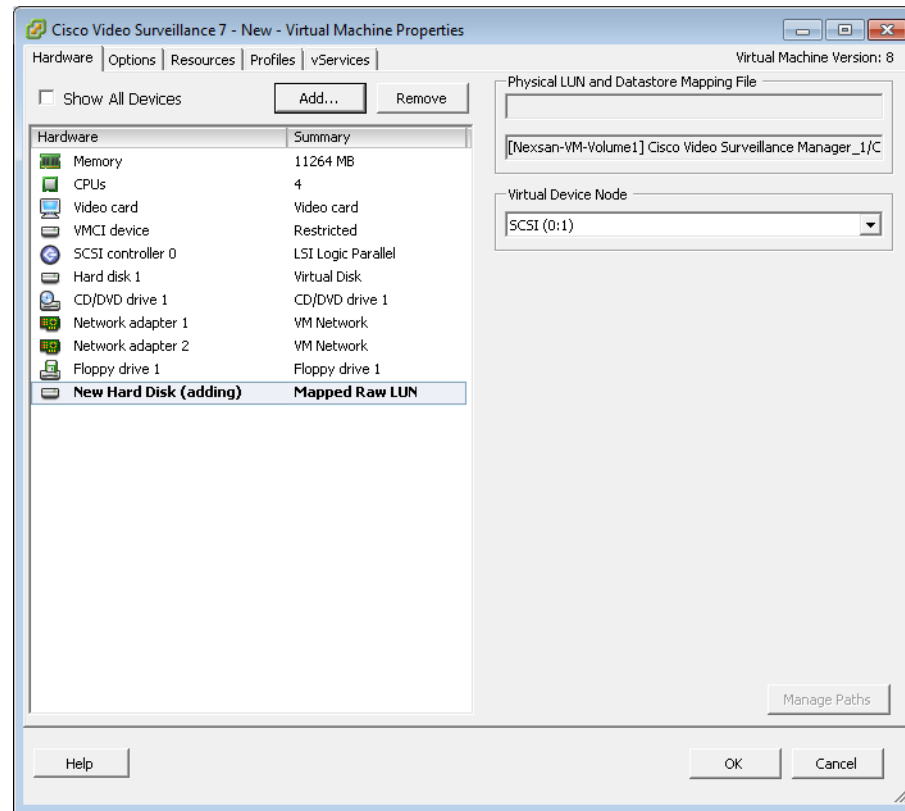
- g. Complete the remaining steps by selecting the default values and then click **Finish** (see Figure 2-8).

Figure 2-8 **Ready to Complete**



- h. Click OK to exit the VM Properties page (Figure 2-9).

Figure 2-9 Adding a Hard Disk



- Step 6** Complete the following steps to complete the configuration on the new VM.
The configuration should be the same as the old VM.

	Task	Instructions
a.	Define a vLAN (if required by your network configuration).	Defining the VLAN for the VM, page 1-21
b.	Define the NTP settings.	Configuring NTP Servers on the Blade, page 1-23
c.	Power on the VM.	Powering On the Cisco VSM Virtual Machine, page 1-26.
d.	Change the VM password.	Change the Default VM Password and Network Settings, page 1-26.
e.	Add the video repositories.	Creating Video Repositories, page 1-33.
f.	Complete the initial server setup and configure the network settings.	Completing the Initial Server Setup Using the Management Console, page 1-48

Step 7 Restore the video repositories.

Complete one of the following procedures for the OVA version you are restoring.

OVA Release 7.5 or Later

Note The video repositories include the video files from the original (old) VM. You must restore these repositories to the new VM or the video files will be lost.

- a. Switch to the root user permissions

```
localadmin@linux:~> sudo su -
```

- b. Run the storage integration script with the recovery option `setup_media_storage.sh -r` as described in the [“Release 7.5 and Later: CLI Method”](#) section on page 1-27

For example:

```
[localadmin@vsm-server ~]$ sudo su -
[root@vsm-server ~]# /usr/BWhttpd/bin/setup_media_storage restore
```

- c. Continue to [Step 8](#).

OVA Release 7.2 and Earlier

Note The video repositories include the video files from the original (old) VM. You must restore these repositories to the new VM or the video files will be lost.

- a. Switch to the root user permissions

```
localadmin@linux:~> sudo su -
```

- b. Find the available media partitions:

- Find the available media partitions listed by labels ([Figure 2-10](#)).

```
linux:~# ls -al /dev/disk/by-label
```

Figure 2-10 Example Output for the Listed Media# Repositories

```
[root@localhost /]# ls -al /dev/disk/by-label/
total 0
drwxr-xr-x 2 root root 160 Apr 29 13:14 .
drwxr-xr-x 6 root root 120 Apr 29 13:14 ..
lrwxrwxrwx 1 root root 10 Apr 29 13:14 media1 -> ../../sdb1
lrwxrwxrwx 1 root root 10 Apr 29 13:14 media2 -> ../../sdc1
lrwxrwxrwx 1 root root 10 Apr 29 13:14 mysqldata -> ../../sda6
lrwxrwxrwx 1 root root 10 Apr 29 13:14 SWAP-sda5 -> ../../sda5
lrwxrwxrwx 1 root root 10 Apr 29 13:14 usrBWhttpd -> ../../sda3
lrwxrwxrwx 1 root root 10 Apr 29 13:14 var -> ../../sda2
[root@localhost /]#
```

- c. Note down all the `media#` listed in the output.

[Figure 2-10](#) shows example output.

- d. Create a partition directory:

```
linux:~ # mkdir /media#
```

- e. Add an fstab entry:

```
linux:~ # vi /etc/fstab
```

For example:

```
[root@localhost ~]# vi /etc/fstab
LABEL=media# /media# xfs rw,nodiratime,noatime
0 0
```

- f. Verify the mounts:

```
linux:~ # mount -a
```

- g. After successfully creating the partition, change ownership of the partition to the nobody account and group using the following command:

```
linux:~ # chown nobody:nobody /media1
```

- h. Repeat these steps to mount an `sd#` device with a `media#` label for each hard-disk added to the VM.
- i. Reboot the Cisco VSM virtual machine (log out and select the **Reboot** option at the bottom of the screen).
- j. Continue to [Step 8](#).

Step 8 Complete the Initial Setup using the Cisco VSM Management Console.

See the [“Completing the Initial Server Setup Using the Management Console”](#) section on page 1-48.

Step 9 Restore the VSOM and Media Server configurations.

See the [Cisco Video Surveillance Management Console Administration Guide](#).

Step 10 Verify that the data is restored:

- a. Log on to the browser-based Operations Manager.
- b. Configure the Media Server options for the `/media1` and `/media0` partitions.
- c. View live video from cameras and playing back archives.

See the [Cisco Video Surveillance Operations Manager User Guide](#) for more information.

Step 11 Delete the old VM from the left pane (Inventory tree):

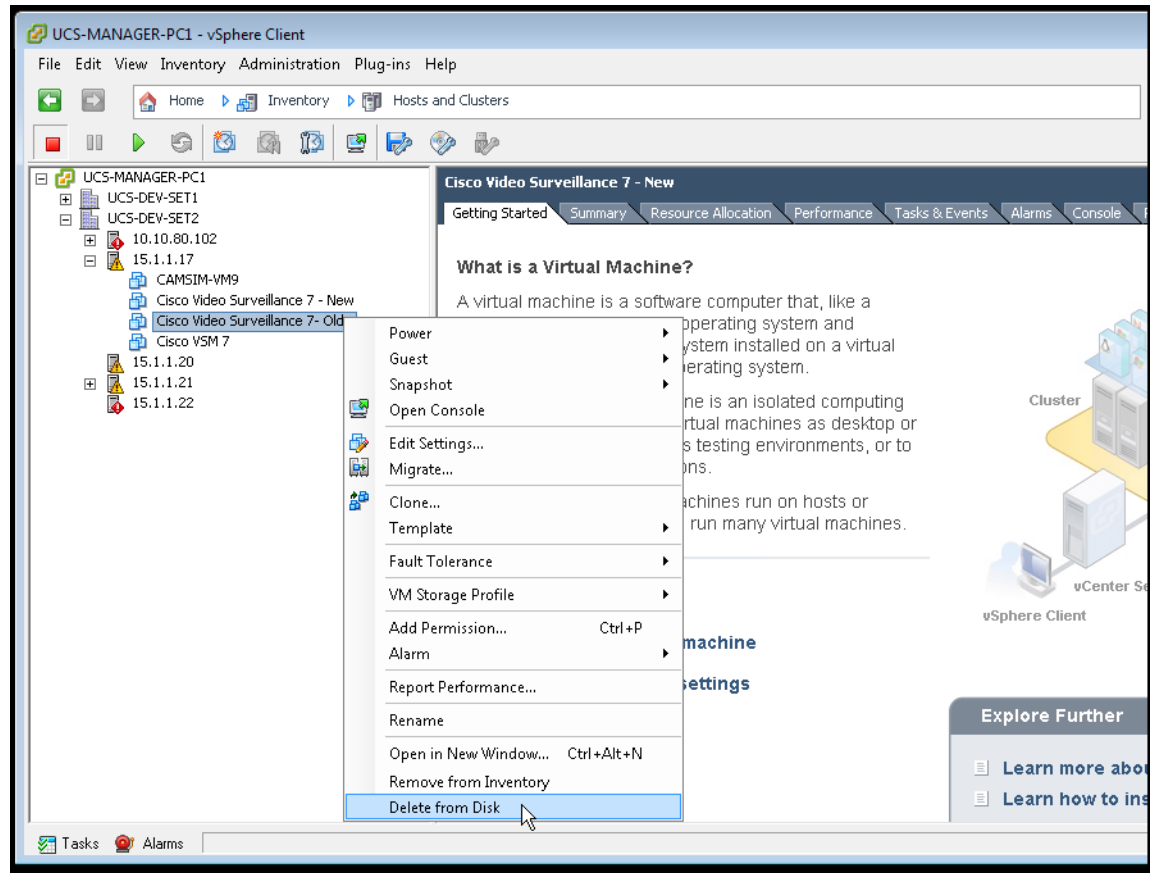
- a. Right-click the old (non-functional) VSM VM.
- b. Select **Delete from Disk** (see [Figure 2-11](#)).



Caution

Do not delete the original machine until all the previous steps in the recovery procedure have been completed.

Figure 2-11 Deleting the VSM VM from the Disk





Related Documentation

Use one of the following methods to access the Cisco Video Surveillance (Cisco VSM) documentation:

- Go to the [Cisco Video Surveillance documentation web site](#).
- See the [Cisco Video Surveillance 7 Documentation Roadmap](#) for descriptions and links to Cisco Video Surveillance documentation, server and storage platform documentation, and other related documentation.

