

VMware® PRESS

# Official Cert Guide

Learn, prepare, and practice for exam success

# VCP-DCV

Rough Cuts



JOHN A. DAVIS  
STEVE BACA  
OWEN THOMAS

# **VCP-DCV Official Cert Guide**

**Steve Baca, Owen Thomas, John A. Davis**

**VMWare Press**

# **Contents**

**Chapter 1 vSphere Overview, Components, and Requirements**

**Chapter 2 Storage Infrastructure**

**Chapter 3 Network Infrastructure**

**Chapter 4 Clusters and High Availability**

**Chapter 5 vCenter Server Features and Virtual Machines**

**Chapter 6 VMWare Product Integration**

**Chapter 7 vSphere Security**

**Chapter 8 vSphere Installation**

**Chapter 9 Configure and Manage Virtual Networks**

**Chapter 10 Monitoring and Managing Clusters and Resources**

**Chapter 11 Manage Storage**

**Chapter 12 Manage vSphere Security**

**Chapter 13 Manage vSphere and vCenter Server**

**Chapter 14 Virtual Machine Management/Provision, Migrate, Replication**

## **Chapter 15 Final Preparation**

# Table of Contents

## **Chapter 1. vSphere Overview, Components and Requirements**

“Do I Know This Already?” Quiz

Foundation Topics

vSphere Components and Editions

vCenter Server Topology

Infrastructure Requirements

Other Requirements

VMware Cloud vs. VMware Virtualization

Summary

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Definitions of Key Terms

Answer Review Questions

## **Chapter 2. Storage Infrastructure**

“Do I Know This Already?” Quiz

Foundation Topics

Storage Models and Datastore Types

vSAN Concepts

vSphere Storage Integration

Storage Multipathing and Failover

Storage Policies

Storage DRS (SDRS)

Exam Preparation Tasks

Definitions of Key Terms

Complete the Tables and Lists from Memory

Review Questions

## **Chapter 3. Network Infrastructure**

## **Chapter 4. Clusters and High Availability**

“Do I Know This Already?” Quiz

Foundation Topics

Cluster Concepts and Overview

Distributed Resource Scheduler (DRS)

vSphere High Availability (HA)

Other Resource Management and Availability Features

## Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

## **Chapter 5. vCenter Server Features and Virtual Machines**

“Do I Know This Already?” Quiz

### Foundation Topics

vCenter Server and vSphere

Virtual Machine File Structure

Virtual Machine Snapshots

Virtual Machine Settings

Virtual Machine Migration

Virtual Machine Cloning

## Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

## **Chapter 6. VMWare Product Integration**

## **Chapter 7. vSphere Security**

“Do I Know This Already?” Quiz

Foundation Topics

vSphere Certificates

vSphere Permissions

ESXi and vCenter Server Security

vSphere Network Security

Virtual Machine Security

Available Add-on Security

Summary

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Definitions of Key Terms

Answer Review Questions

## **Chapter 8. vSphere Installation**

“Do I Know This Already?” Quiz

Foundation Topics

Install ESXi hosts

Deploy vCenter Server Components

Configure Single Sign-On (SSO)

Initial vSphere Configuration

Summary

Exam Preparation Tasks

Review All the Key Topics

Complete the Tables and Lists from Memory

Definitions of Key Terms

Answer Review Questions

## **Chapter 9. Configure and Manage Virtual Networks**

## **Chapter 10. Managing and Monitoring Clusters and Resources**

“Do I Know This Already?” Quiz

Foundation Topics

Create and Configure a vSphere Cluster

Create and Configure a vSphere DRS Cluster

Create and Configure a vSphere HA Cluster

Monitor and Manage vSphere Resources

Events, Alarms, and Automated Actions

Logging in vSphere

Exam Preparation Tasks

Review All Key Topics

Complete the Tables and Lists from Memory

Define Key Terms

Review Questions

## **Chapter 11. Manage Storage**

## **Chapter 12. Manage vSphere Security**

“Do I Know This Already?” Quiz

Foundation Topics

Configure and Manage Authentication and Authorization

Configure and Manage vSphere Certificates

General ESXi Security Recommendations

Configure and Manage ESXi Security

Other Security Management

Summary

Exam Preparation

Review All the Key Topics

Complete the Tables and Lists from Memory

Answer Review Questions

## **Chapter 13. Manage vSphere and vCenter Server**

“Do I Know This Already?” Quiz

Foundation Topics

vCenter Server Backup

Upgrade to vSphere 7.0

Using vSphere Lifecycle Manager

Manage ESXi Hosts

Monitor and Manage vCenter Server

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

## **Chapter 14. Manage Virtual Machines**

“Do I Know This Already?” Quiz

Foundation Topics

Create and Configure Virtual Machines

Manage Virtual Machines

Advanced Virtual Machine Management

Content Library

Exam Preparation Tasks

Review All Key Topics

Define Key Terms

Review Questions

### **Chapter 15. Final Preparation**

# **Chapter 1. vSphere Overview, Components and Requirements**

**This chapter covers the following topics:**

- vSphere Components and Editions
- vCenter Server Topology
- Infrastructure Requirements
- Other Requirements
- VMware Cloud vs. VMware Virtualization

This chapter contains information related to VMware 2V0-21.20 exam objectives 1.1, 1.2, 2.1, 4.1, 4.1.1, 4.1.2, and 4.4.

## “Do I Know This Already?” Quiz

### vSphere Components and Editions

#### vSphere Components

#### Editions and Licenses

### vCenter Server Topology

#### Single Sign-on (SSO) Domain

#### Enhanced Linked Mode

### vCenter HA

### Infrastructure Requirements

#### Compute and System Requirements

#### vCenter Server

#### ESXi

## Storage Requirements

vCenter Server Appliance

ESXi

## Network Requirements

Networking Concepts

vCenter Server Network Requirements

ESXi Network Requirements

## Infrastructure Services

AD

DNS

NTP

## Other Requirements

Additional Requirements

User Interfaces

vCenter Server File-Based Backup and  
Restore

GUI Installer

Distributed Power Management (DPM)

vSphere Replication Requirements

vCenter High Availability Requirements

SDDC Requirements

VSAN

NSX

vRealize Suite

## VMware Cloud vs VMware Virtualization

Server Virtualization

VMware SDDC

vCloud Suite and Private Clouds

VCF and Hybrid Clouds

VMC on AWS

VMware vCloud Director

Cloud Automation

Summary

Review All the Key Topics

Complete the Tables and Lists from Memory

Definitions of Key Terms

Answer Review Questions

This chapter introduces vSphere 7.0, describes its major components, and identifies its requirements.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section.

Regardless, the authors recommend that you read the entire chapter at least once. **Table 1-1** outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 1-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions Covered in This Section
vSphere Components, and Editions	1,2
vCenter Server Topology	3,4
Infrastructure Requirements	5,6
Other Requirements	7,8
VMware Cloud vs VMware Virtualization	9,10

1. You plan to deploy vSphere 7.0 for three ESXi hosts and want to deploy the minimum vCenter

Server edition that supports vMotion. Which Center Server edition do you choose?

- a.** Essentials
- b.** Essentials Plus

- c.** Foundation
- d.** Standard

**2.** You plan to deploy vSphere 7.0 and want to minimize virtual machine downtime by proactively detecting hardware failures and placing the host in quarantined or maintenance mode. Which feature do you need?

- a.** vSphere High Availability
- b.** Proactive HA
- c.** Predictive DRS
- d.** vCenter HA

**3.** You are preparing to deploy and manage a vSphere environment. Which vCenter Server component provides Security Assertion Markup Language (SAML) tokens?

- a.** vCenter Lookup Service
- b.** VMware Directory Service
- c.** tcServer
- d.** STS

**4.** You plan to deploy another vCenter Server in your vSphere 7.0 environment and want it to use an existing vSphere Single Sign-on Domain. What should you do?

- a.** During the vCenter Server deployment, join an existing SSO domain.

- b.** Prior to the vCenter Server deployment, deploy an external PSC
    - c.** During the vCenter Server deployment, connect to an external PSC.
  - d.** Configure vCenter HA
- 5.** You plan to deploy a vCenter Server 7.0 appliance to support 350 ESXi hosts and 4500 virtual machines. What is the minimum memory you should plan for the vCenter Server appliance?
  - a.** 37 GB
  - b.** 56 GB
  - c.** 28 GB
  - d.** 19 GB
- 6.** You are interested in booting your ESXi hosts using UEFI. Which of the following is a key consideration?
  - a.** After installing ESXi 7.0 you can change the boot type between BIOS and UEFI using the Direct Console User Interface.
  - b.** ESXi boot from UEFI is deprecated in ESXi 7.0
  - c.** After installing ESXi 7.0 you can change the boot type between BIOS and UEFI using the vSphere Client.
  - d.** After you install ESXi 7.0, changing the boot type between BIOS and UEFI is not supported.
- 7.** You are planning the backup and recover for a new vCenter Server appliance using the file based backup feature in the vCenter Server

Appliance Management Interface. Which protocol is not supported?

**a.** NFS

**b.** FTP

**c.** HTTPS

**d.** SCP

**8.** You are planning the procedures to manage a new vSphere 7.0 environment, which of the following is not a supported browser for the vSphere Client?

**a.** Microsoft Internet Explorer 11.0.96 for Windows users

**b.** Microsoft Edge 38 for Windows users

**c.** Safari 5.0 for Mac users

**d.** Firefox 45 for Mac users

**9.** You need to include on-premise cloud automation software to improve up the delivery of IT services and applications in your vSphere based SDDC. Which of the following should you choose?

**a.** VMware Cloud Assembly

**b.** VMware Service Broker

**c.** vCloud Director

**d.** vRealize Automation

**10.** You want a simple path to the hybrid cloud by leveraging a common infrastructure and consistent operational model for on-premise and off-premise data centers. What should you use?

**a.** vRealize Suite

**b.** VCF

- c.** vCloud Director
- d.** Cloud Automation

## VSPHERE COMPONENTS AND EDITIONS

VMware vSphere is a suite of products that you can use to virtualize enterprise datacenters and build private clouds.

### vSphere Components

**Table 1-2** describes the installable VMware products are the core components in a vSphere environment.

**Table 1-2** Installable Core vSphere Components

Component	Description
vCenter Server	The major management component in the vSphere environment. Its services include vCenter Server, vSphere Web Client, vSphere Auto Deploy, vSphere ESXi Dump Collector, and the components that were associated with the Platform Services Controller in prior versions: vCenter Single Sign-On, License Service, Lookup Service, and VMware Certificate Authority.
ESXi Server	The physical host (including the hypervisor) on which virtual machines run.

Some optional, vSphere features require the deployment of additional components and specific vSphere licensing. **Table 1-3** describes two of these optional components, which require deploying additional virtual appliances.

**Table 1-3** Optional vSphere Components

Optional Component	Description
vSphere Replication	An extension to VMware vCenter Server that provides hypervisor-based virtual machine replication and recovery.
vCenter High Availability	Provides protection for the vCenter Server Appliance (VCSA) against host, hardware, and application failures. Provides automated active / passive failover with minimal downtime. It can also be used to significantly reduce downtime when you patch VCSA.

Many vSphere features, such as those described in [Table 1-4](#), require specific vSphere licensing and configuration, but do not require the installation or deployment of additional software or virtual appliances.

**Table 1-4** Available vSphere Features

---

Available vSphere Features	Description
vCenter Appliance File-Based Backup and Restore	A feature introduced in vSphere 7.0 that enables you to backup and restore the vCenter Server appliances
vMotion	Provides live virtual machine migrations with negligible disruption from a source ESXi host to a target ESXi host.
vSphere HA	Automated failover protection for VMs against host, hardware, network, and guest OS issues. In case of host system failure, cold migrates and restarts failed VMs on surviving hosts.
Distributed Resource Scheduler (DRS)	Places VMs at power on appropriate ESXi hosts and migrates VMs when there is contention utilizing live (vMotion) migrations of VMs when necessary.
Storage vMotion	Live migrations with negligible disruption of VMs from a source datastore to a target datastore.
Fault Tolerance (FT)	Automated, live failover protection for VMs against host, hardware, network, and guest OS issues.
Distributed Power Management (DPM)	Optimizes power consumption in an ESXi cluster.
Proactive HA	Minimizes VM downtime by proactively detecting hardware failures and placing the host Quarantined Mode or Maintenance Mode.
Content Library	Centralized repository used manage and distribute templates, ISO files, scripts, vApps, and other files associated with VMs.
Host Profiles	Provides a means to apply a standard configuration to a set of ESXi hosts.

The add-on products in [Table 1-5](#) are commonly used in a vSphere environment and are discussed in this guide. These products can be sold separately from vSphere.

**Table 1-5** Add-on Products

---

Product	Description
VSAN	A product that provides a SAN experience to your vSphere environment leveraging local storage in the ESXi hosts. It tightly integrates with vSphere and is the leading Hyper-Converged Infrastructure (HCI) solution to provide a flash-optimized, secure, and simple to use SAN.
NSX	A product that adds software based virtualized networking and security to a vSphere environment.
vRealize Suite	A suite of products that add operations (vRealize Operations Manager), automation (vRealize Automation), and orchestration (vRealize Orchestrator) to a vSphere environment.

**Note**

Although it is an add-on product, VSAN is covered in the VCP-DCV exam and in this guide.

The vSphere Host client is a web-based interface provided by each ESXi host. It is available immediately following the installation of a host. Its primary purpose is to provide a GUI for configuration, management, and troubleshooting purposes when vCenter Server is not available. For example, during the implementation of a new vSphere environment, you could use the vSphere Host Client to create virtual machines for running DNS, Active Directory, and vCenter Server database prior to deploying vCenter Server. For another example, you could use the vSphere Host Client to power-down, troubleshoot, reconfigure, and restart the vCenter Server virtual machine.

The HTML 5-based vSphere Client is the preferred web-based GUI for managing vSphere. It is provided by services running in the vCenter Server. The Flash-based vSphere Web Client used in previous vSphere versions has been deprecated and is no longer available.

## Editions and Licenses

VMware vSphere comes in many editions, where each edition is intended to address specific use cases by providing specific features. When planning for a vSphere environment, you should prepare to procure at least three line items, a vCenter Server license, a vSphere license, and support for the environment. The vCenter Server license line item should identify the desired edition and quantity (number of vCenter Server instances).

**Table 1-6** provides a summary of the features that are provided with each edition of vCenter Server 7.

**Table 1-6** vCenter Server Editions

Feature	Essentials	Essentials Plus	Foundation	Standard
Number of ESXi hosts	3 (2 CPU Max)	3 (2 CPU Max)	4	2000
vCenter License	Packaged with vSphere license in Essentials	Packaged with vSphere license in Essentials Plus	Sold separately from vSphere license	Sold separately from vSphere license
Basic level vCenter features, like single pane of glass management, Lifecycle manager, and VMware Converter	Supported	Supported	Supported	Supported
Common vCenter features like vMotion and vSphere HA, vSphere Replication	Not supported	Supported	Supported	Supported
Advanced Features like vCenter Server High Availability (VCHA), vCenter Server Backup and Restore	Not supported	Not supported	Not supported	Supported

You need to obtain vSphere license to apply to license physical CPUs on your ESXi hosts. Starting with vSphere

7.0, one vSphere CPU license covers up to 32 cores. If a CPU has more than 32 cores, you need additional CPU licenses. The number of vSphere CPU licenses consumed by an ESXi host is determined by the number of physical CPUs on the host and the number of cores in each physical CPU.

For example, you can assign a vSphere license for ten 32-core CPUs to any of the following combinations of hosts:

- Five hosts with 2 CPUs and 32 cores per CPU
- Five hosts with 1 CPU with 64 cores per CPU
- Two hosts with 2 CPUs and 48 cores per CPU and two hosts with 1 CPU and 20 cores per CPU

The major editions of vSphere 7.0 are Standard and Enterprise Plus. Other editions may be licensed in different manners than the major editions. For example, the vSphere Desktop edition (for VDI environments) and VMware vSphere Remote Office Branch Office (for IT remote sites) are licensed on per virtual machine.

Table 1-7 provides *some* of the features that are provided with the major editions of vSphere 7.0.

**Table 1-7** vSphere Editions

Feature	Standard	Enterprise Plus
vSphere HA, vSphere Replication, Storage vMotion, Quick Boot, vCenter Backup and Restore, VVOLs	Supported	Supported
Distributed Switch, Proactive HA, NIOC, SIOC, Storage DRS, DRS, DPM, VM Encryption, Cross-vCenter vMotion, Long Distance vMotion, vTrust Authority, SR-IOV, vSphere Persistent Memory	Not supported	Supported
Fault Tolerance	Supported up to 2 vCPUs	Supported up to 8 vCPUs

## VCENTER SERVER TOPOLOGY

This section describes the architecture for the vCenter Server.

In vSphere 6.x, multiple vCenter Server topologies and configuration are supported, involving components and technologies such as vCenter Server Appliance, vCenter Server for Windows, embedded database (Postgres), external (SQL Server or Oracle) database, external Platform Services Controller (PSC), embedded PSC, Enhanced Linked Mode, and Embedded Linked Mode. In vSphere 7.0, The vCenter Server configuration and topology is much simpler.

Beginning in vSphere 7.0, the vCenter Server appliance is required. Windows based vCenter Servers are not supported. External PSCs are not supported. Embedded PSCs are not used in vCenter Server 7.0. Instead, the services are directly integrated into the vCenter Server appliance and are no longer described as a part of PSC. For example, in vSphere 7.0, the *Platform Services Controller Administration* publication is replaced with the *vSphere Authentication* publication. Table 1-8 describes the main services in the vCenter Server Appliance and related services in the ESXi host.

**Table 1-8** Services in the vCenter Server Appliance

---

<b>Service</b>	<b>Description</b>
vCenter Single Sign-On	An authentication service which utilizes a secure token exchange mechanism rather than requiring components to authenticate users per component.
Security Token Service (STS)	This component is part of vCenter Single Sign-On and provides Security Assertion Markup Language (SAML) tokens which are used to authenticate users to other vCenter components instead of requiring users to authenticate to each component. Once a user authenticates to vCenter Single Sign-On, they are granted SAML tokens which are then used for authentication.
Administration server	Provides vCenter Single Sign-On administration and configuration from the vSphere Client.
vCenter Lookup Service	This service contains the topology of the vSphere infrastructure allowing secure communication between vSphere components.
VMware Directory Service	The directory service for the vCenter Single Sign-On (SSO) domain (vsphere.local).
vCenter Server Plug-ins	Applications that add functionality to vCenter. These usually consist of server and client components.
vCenter Server Database	This database contains the status of all virtual machines, ESXi hosts, and users. It is deployed via the vCenter Server deployment wizard.
tcServer	Co-installed with vCenter, this service is used by web services such as ICIM/Hardware status, Performance charts, WebAccess, Storage Policy-Based Services, and vCenter Service status.
License Service	Used to stores the available licenses and manages the license assignments for the entire vSphere environment
vCenter Server Agent	This is installed on an ESXi host when that host is added to vCenter's inventory. This service collects, communicates, and runs actions initiated from the vSphere Client.
Host Agent	Administrative agent installed with the ESXi installation. Responsible for collecting, communicating, and running actions initiated from the Host Client.

If you upgrade or migrate a vCenter Server deployment that uses an external PSC, you must converge the PSC into a vCenter Server appliance that you specify. In domains with multiple vCenter Server instances, you must identify the SSO replication partner for each subsequent vCenter Server. If you upgrade or migrate using the GUI-based installer, the wizard prompts you to specify the replication topology. If you upgrade or migrate using the CLI-based installer, you specify the replication topology using the JSON templates. During the upgrade or migration process, the new vCenter Server 7.0 appliance incorporates the former PSC services, enabling you to decommission the original external PSC.

## Single Sign-on (SSO) Domain

Each vCenter Server is associated with a vCenter Single Sign-On (SSO) domain, whose default name is `vsphere.local`. You can change the SSO domain name during deployment. The SSO domain is considered the local domain for authentication to vCenter Server and other VMware products, such as vRealize Operations.

During the vCenter Server appliance deployment, you must create an SSO domain or join an existing SSO domain. The domain name is used by the VMware Directory Service (`vmdir`) for all Lightweight Directory Access Protocol (LDAP) internal structuring. You should give your domain a unique name that is not used by OpenLDAP, Microsoft Active Directory, and other directory services.

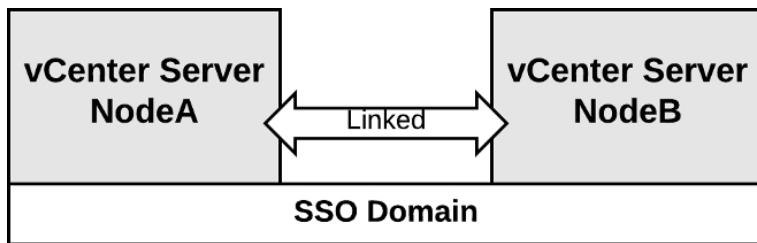
You can add users and groups to the SSO domain. You can add an Active Directory or LDAP identity source and allow the users and groups in that identity source to authenticate

## Enhanced Linked Mode



You can use Enhanced Linked Mode to link multiple vCenter Server systems. With Enhanced Linked Mode, you can log in to all linked vCenter Server systems simultaneously and manage the inventories of the linked systems. This mode replicates roles, permissions, licenses, and other key data across the linked systems. To join vCenter Server systems in Enhanced Linked Mode, connect them to the same vCenter Single Sign-On (SSO) domain, as illustrated in [Figure 1-1](#). Enhanced Linked Mode requires the vCenter Server Standard licensing level, and is not supported with vCenter Server Foundation or vCenter Server Essentials. Up to 15

vCenter Server appliance instances can be linked together by utilizing Enhanced Linked Mode



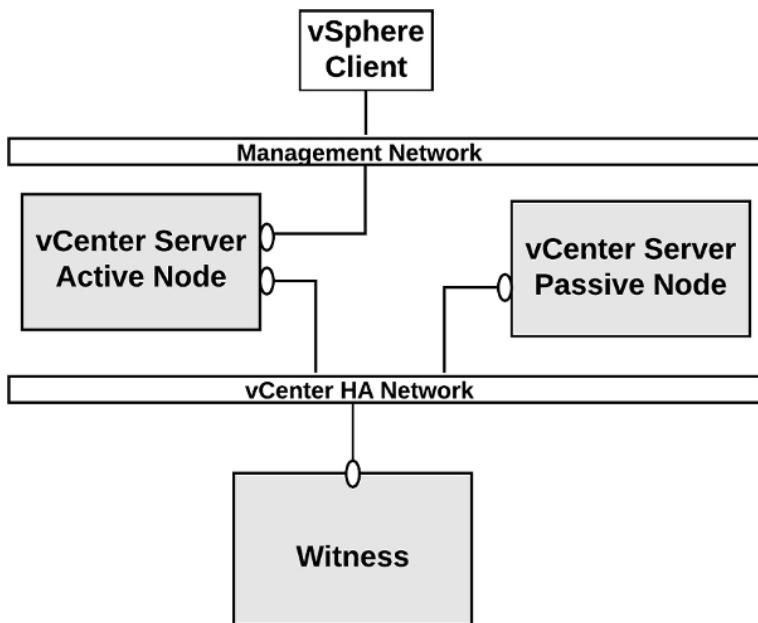
**Figure 1-1** Enhanced Linked Mode with Two vCenter Server 7.0 Appliances

## vCenter HA

A vCenter HA cluster consists of three vCenter Server instances. The first instance, initially used as the Active node, is cloned twice to a Passive node and to a Witness node. Together, the three nodes provide an active-passive failover solution.

Deploying each of the nodes on a different ESXi instance protects against hardware failure. Adding the three ESXi hosts to a DRS cluster can further protect your environment.

When vCenter HA configuration is complete, only the Active node has an active management interface (public IP), as illustrated in [Figure 1-2](#). The three nodes communicate over a private network called vCenter HA network that is set up as part of configuration. The Active node is continuously replicating data to the Passive node.



**Figure 1-2** Enhanced Linked Mode with Two vCenter Server 7.0 Appliances

All three nodes are necessary for the functioning of this feature. Table 1-9 provides details for each the node.

**Table 1-9** vCenter HA Node Details

Node Type	Description
Active	Is active vCenter Server instance. Uses a public IP address for the management interface. Replicates data to the Passive node using the vCenter HA network. Communicate with the Witness node using the vCenter HA network.
Passive	Is cloned from the Active node. Uses the vCenter HA network to constantly receive updates from the Active node. Automatically takes over the role of the Active node if a failure occurs.
Witness	Is a lightweight clone of the Active node Provides a quorum to protect against a split-brain situations

## INFRASTRUCTURE REQUIREMENTS

This section describes some of the main infrastructure requirements that you should address prior to implementing vSphere.

## Compute and System Requirements

When preparing to implement a vSphere environment you should prepare a sufficient amount of supported compute (CPU and memory) resources as described in this section.

### vCenter Server

The VCSA 7.0 appliance can be deployed on ESXi hosts 7.0 or later, which can be managed by vCenter Server 7.0 or later.

To prepare for deployment of vCenter Server, you should plan to address the compute specifications in [Table 1-10](#)

**Table 1-10** Compute Specifications for the vCenter Server Appliance

Component	Number of CPUs	Memory
Tiny Environment Up 10 hosts or 100 virtual machines	2	12 GB
Small Environment Up 100 hosts or 1000 virtual machines	4	19 GB
Medium Environment Up 400 hosts or 4000 virtual machines	8	28 GB
Large Environment Up 1000 hosts or 10,000 virtual machines	16	37 GB
X-Large Environment Up 2000 hosts or 35,000 virtual machines	24	56 GB

**Note**

If you want an ESXi host with more than 512 LUNs and 2048 paths then you should deploy a vCenter Server Appliance for a large or x-large environment.

### ESXi

To install ESXi 7.0, ensure the hardware system meets the following requirements

## Key Topic

- A supported system platform as provided in the *VMware Compatibility Guide*.
- Two or more CPU cores.
- A supported 64-bit x86 processors as provided in the *VMware Compatibility Guide*.
- The CPU's NX/XD bit must be enabled in the BIOS.
- 4 GB or more of physical RAM. (VMware recommends 8GB or more for production environments)
- To support 64-bit virtual machines, hardware virtualization (Intel VT-x or AMD RVI) must be enabled on the CPUs
- One or more supported Ethernet controllers, Gigabit or faster as provided in the *VMware Compatibility Guide*.
- A SCSI disk or a local, non-network, RAID LUN with unpartitioned space for the virtual machines.
- For Serial ATA (SATA), a disk connected through supported SAS controllers or supported on-board SATA controllers.
- A boot disk of at least 8 GB for USB or SD devices, and 32 GB for other HDD, SSD, NVMe, and other device types. The boot device must not be shared between ESXi hosts

### Note

SATA disks are considered remote, not local. These disks are not used as a scratch partition by default because they are considered remote. You cannot connect a SATA CD-ROM device to a virtual machine on an ESXi 7.0 host. To use the SATA CD-ROM device, you must use IDE emulation mode

For vSphere 7.0 you should ensure you meet the ESXi booting considerations.

- You can boot using the Unified Extensible Firmware Interface (UEFI), which enables boot from hard drives, CD-ROM drives, or USB media.
- VMware Auto Deploy supports network booting and provisioning of ESXi hosts with UEFI.
- Boot systems from disks larger than 2 TB if the system firmware add-in card firmware supports it per vendor documentation.

**Note**

Changing the host boot type between legacy BIOS and UEFI is not supported after you install ESXi 7.0

## Storage Requirements

When preparing to implement a vSphere environment you should prepare a sufficient amount of supported storage resources as described in this section.

### vCenter Server Appliance

To prepare for the deployment of vCenter Server Appliance, you should plan to address their storage requirements. [Table 1-11](#) contains the storage requirements for a VCSA. It allows for Lifecycle Manager which runs as a service in VCSA.

**Table 1-11** Storage Sizes for the vCenter Server Appliance

Deployment Size	Default Storage Size	Large Storage Size	X-Large Storage Size
Tiny	415 GB	1490 GB	3245 GB
Small	480 GB	1535 GB	3295 GB
Medium	700 GB	1700 GB	3460 GB
Large	1065 GB	1765 GB	3525 GB
X-Large	1805 GB	1905 GB	3665 GB

## **ESXi**

Installing ESXi 7.0 requires a boot device that is a minimum of 8 GB. Upgrading to 7.0 requires a 4 GB minimum boot device. When booting from a local disk, SAN or iSCSI LUN, a 32-GB disk is required to allow for the creation of the boot partition, boot banks, and a VMFS\_L ESX=OSData volume. The ESX-OSData volume replaces the legacy /scratch partition, VM-tools, and core dump location. If no local disk is found, ESXi 7.0 functions in degraded mode and it places the /scratch partition on the ESXi host's ramdisk and links it to /tmp/scratch. You can reconfigure /scratch to use a separate disk or LUN. For best performance and memory optimization, do not run the ESXi host in degraded mode. Likewise, when installing ESXi 7.0 on USB and SD devices, the installer attempts to allocate a scratch region on a local disk, otherwise it places /scratch on the ramdisk.

**Note**

You cannot roll back to an earlier version of ESXi after upgrading. A backup would have to be made prior of the boot device to then restore from after the upgrade.

The following are recommended for ESXi 7.0 installations:

- 8 GB USB or SD with 32 GB local disk. Boot partitions reside on USB or SD and ESXi-OSData resides on local disk.
- Local disk with 32 GB minimum. This contains boot and ESX-OSData.
- Local disk with 142 GB or more. This contains boot, ESX-OSData, and a VMFS datastore.

## **Network Requirements**

### **Networking Concepts**

In order to prepare for network virtualization in vSphere, you should understand some the following concepts.

- **Physical Network:** A network of physical machines that are connected so that they can send data to and receive data from each other.
- **Virtual Network:** A network of virtual machines running on a physical machine that are connected logically to each other so that they can send data to and receive data from each other.
- **Opaque Network:** An opaque network is a network created and managed by a separate entity outside of vSphere. For example, logical networks that are created and managed by VMware NSX appear in vCenter Server as opaque networks of the type `nsx.LogicalSwitch`. You can choose an opaque network as the backing for a VM network adapter. To manage an opaque network, use the management tools associated with the opaque network, such as VMware NSX Manager or the VMware NSX API management tools
- **vSphere Standard Switch:** Works much like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. A vSphere standard switch can be connected to physical switches by using physical Ethernet adapters, also referred to as uplink adapters.
- **VMkernel TCP/IP Networking Layer:** Provides connectivity to hosts and handles the standard infrastructure traffic of vSphere vMotion, IP storage, Fault Tolerance, and vSAN.

VMware recommends using network segmentation in vSphere environments for separating each type of VMkernel traffic and virtual machine traffic. You can

implement network segments using unique VLANs and IP subnets. Here is a set of commonly used network segments in vSphere.

- Management
- vMotion
- vSphere Replication
- vSphere High Availability heartbeat
- Fault Tolerance
- IP Storage
- Virtual Machine (typically segregated further by application or by other factors, such as test and production)

### vCenter Server Network Requirements

Table 1-12 provides details for *some* of the required network connectivity involving vCenter Server. For each applicable connection, you should ensure that your network and firewall allow the described connectivity.

**Table 1-12** Required Ports for vCenter Sever

---

<b>Protocol / Port</b>	<b>Description</b>	<b>Required for</b>
TCP 22	System port for SSHD.	vCenter Server. Must be open for upgrade of the appliance.
TCP 80	vCenter Server requires port 80 for direct HTTP connections. Port 80 redirects requests to HTTPS port 443.	vCenter Server
TCP 88	This port must be open to join Active Directory.	vCenter Server
TCP / UDP 389	This is the LDAP port number for the Directory Services for the vCenter Server group.	vCenter Server to vCenter Server
TCP 443	The default port used by vCenter Server to listen for connections from the vSphere Web Client and SDK clients	vCenter Server to vCenter Server
TCP / UDP 514	vSphere Syslog Collector port for vCenter Server and vSphere Syslog Service port for vCenter Server Appliance	vCenter Server
TCP / UDP 902	The default port that the vCenter Server system uses to send data to managed hosts.	vCenter Server
TCP 1514	vSphere Syslog Collector TLS port for vCenter Server	vCenter Server
TCP 2012	Control interface RPC for Single Sign-On	vCenter Server
TCP 2014	RPC port for VMware Certificate Authority (VMCA) APIs	VMCA
TCP / UDP 2020	Authentication framework management	vCenter Server

TCP 5480	Appliance Management Interface (VAMI)	vCenter Server
TCP / UDP 6500	ESXi Dump Collector port.	vCenter Server
TCP 7080, 12721	Secure Token Service (internal ports)	vCenter Server
TCP 7081	vSphere Client (internal ports)	vCenter Server
TCP 7475, 7476	VMware vSphere Authentication Proxy	vCenter Server
TCP 8084	vSphere Lifecycle Manager SOAP port used by vSphere Lifecycle Manager client plug-in.	vSphere Lifecycle Manager
TCP 9084	vSphere Lifecycle Manager Web Server Port used by ESXi hosts to access host patch files from vSphere Lifecycle Manager server.	vSphere Lifecycle Manager
TCP 9087	vSphere Lifecycle Manager Web SSL port used by vSphere Lifecycle Manager client plugin for uploading host upgrade files to vSphere Lifecycle Manager server.	vSphere Lifecycle Manager
TCP 9443	vSphere Web Client HTTPS	vCenter Server

## ESXi Network Requirements

Table 1-13 provides details for *some* of the required network connectivity involving ESXi. For each applicable connection, you should ensure that your network and firewall allow the described connectivity.

**Table 1-13** Required Ports for ESXi

---

Protocol / Port	Service	Direction	Description
TCP 5988	CIM Server	Inbound	Server for Common Information Model (CIM)
TCP 5989	CIM Secure Server	Inbound	Secure Server for CIM
UDP 8301, 8302	DVSSync	Inbound, Outbound	Used for synchronizing states of distributed virtual ports between hosts that have VMware FT record/replay enabled
TCP 902	NFC	Inbound, Outbound	ESXi uses Network File Copy (NFC) for operations such as copying and moving data between datastores.
UDP 12345, 23451	vSAN Clustering Service	Inbound, Outbound	Used by vSAN nodes for multicast to establish cluster members and distribute vSAN metadata..
UDP 68	DHCP	Inbound, Outbound	DHCP client for IPv4.
UDP 53	DNS	Inbound	DNS Client
TCP / UDP 53	DNS	Outbound	DNS Client
TCP / UDP 8200, 8100, 8300	Fault Tolerance	Inbound	Traffic between hosts for vSphere Fault Tolerance (FT).
TCP / UDP 80, 8200, 8100, 8300	Fault Tolerance	Outbound	Supports vSphere Fault Tolerance (FT).
TCP 2233	VSAN Transport	Inbound	vSAN reliable datagram transport for vSAN storage IO.
TCP 22	SSH	Inbound	SSH Server
TCP 902, 443	vSphere Web Client	Inbound	Allows user connections from vSphere Web client
TCP / UDP 547	DHCPv6	Outbound	DHCP client for IPv6.
UDP 9	WOL	Outbound	Wake on LAN
TCP 3260	iSCSI	Outbound	Supports software iSCSI
TCP 8000	vMotion	Outbound	Supports vMotion
UDP 902	vCenter Agent	Outbound	Used by the vCenter Agent

## Infrastructure Services

In addition to providing the required compute, storage, and network infrastructure, you should provide supporting infrastructure services, such as Active Directory (AD), Domain Name Services (DNS), and Network Time Protocol (NTP).

### AD

In many vSphere environments, vCenter Single Sign-On (SSO) is integrated with directory services, such as Microsoft Active Directory (AD). SSO can authenticate users from its own internal users and groups, and it can connect to trusted external directory services such as AD. If you plan to leverage AD for an SSO identity source, you should ensure the proper network connectivity,

service account credentials, and AD services are available and ready for use.

If you plan to install vCenter Server for Windows and use AD identity sources, you should ensure the Windows server is a member of the AD domain but is not a domain controller.

**Note**

If the system that you use for your vCenter Server installation belongs to a workgroup rather than a domain, then vCenter Server is not able to discover all domains and systems available on the network when using some features.

## DNS

You may wish to assign static IP addresses and resolvable fully qualified domain names (FQDNs) to your vSphere components, such as vCenter Server and ESXi hosts. Before installing these components, you should ensure that the proper IP addresses and FQDNs entries are registered in your Domain Name System (DNS). You should configure forward and reverse DNS records.

For example, prior to deploying the vCenter Server appliance, you should assign a static IP address and host name in DNS. The IP address must have a valid (internal) domain name system (DNS) registration. During the vCenter Server installation, you must provide the FQDN or the static IP. VMware recommends using the FQDN. You should ensure that DNS reverse lookup returns the appropriate FQDN when queried with the IP address of the vCenter appliance. Otherwise, the installation of the Web Server component that supports the vSphere Web client fails.

When you deploy the vCenter Server Appliance, the installation of the Web server component that supports the vSphere Web Client fails if the installer cannot look up the fully qualified domain name (FQDN) for the appliance from its IP address. Reverse lookup is

implemented using PTR records. If you plan to use an FQDN for the appliance system name, you must verify that the FQDN is resolvable by a DNS server.

Starting with vSphere 6.5, vCenter Server supports mixed IPv4 and IPv6 environment. If you want to set up the vCenter Server Appliance to use an IPv6 address version, use the fully qualified domain name (FQDN) or host name of the appliance.

Ensure that each vSphere Web Client instance and each ESXi host instance can successfully resolve the vCenter Server FQDN.

Ensure that the ESXi host management interface has a valid DNS resolution from the vCenter Server and all vSphere Web Client instances. Ensure that the vCenter Server has a valid DNS resolution from all ESXi hosts and all vSphere Web Clients.

## NTP

Ensure that you provide time synchronization between the nodes. All vCenter Server instances must be time synchronized. ESXi hosts must be time synchronized to support features such as vSphere HA. In most environments, you should plan to use NTP sever for time synchronization. Prior to implementing vSphere, verify that the NTP servers are running and available.

Be prepared to provide the names or IP addresses for the NTP servers when installing vSphere components, like vCenter Server and, ESXi. For example, during Stage 2 of the deployment of a vCenter Server Appliance, you can choose to **synchronize time with NTP servers** and provide a list of NTP server name or IP addresses separated by commas. Alternatively, you choose to allow the appliance to **synchronize time with the ESXi host**.

**Note**

If a vCenter Server Appliance is set for NTP time synchronization, it ignores its `time_tools-sync` Boolean parameter. Otherwise, if the parameter is TRUE, VMware Tools synchronizes the time in the appliance's guest OS with the ESXi host.

## OTHER REQUIREMENTS

This section describes a few additional requirements for a few of the optional components (see [Table 1-3](#)), available vSphere features ([Table 1-4](#)), and add-on products (see [Table 1-5](#)).

### Additional Requirements

Here are a few requirements for some specific, commonly used vSphere features.

#### User Interfaces

The VMware Host Client and vSphere Client utilize HTML5. The Flash-based vSphere Web Client is not supported in vSphere 7. For Windows users, VMware supports Microsoft Edge 38 and later, Microsoft Internet Explorer 11.0.96 and later, Mozilla Firefox 45 and later, Google Chrome 50 and later, and Safari 5.1 and later. For Mac users, VMware supports Safari 5.1 and later, Mozilla Firefox 45 and later, and Google Chrome 50 and later.

#### vCenter Server File-Based Backup and Restore

If you plan to schedule file-based backups using the VAMI, you must prepare a FTP, FTPS, HTTP, HTTPS, or SCP server with sufficient disk space to store the backups.

#### GUI Installer

You can use the GUI installer to interactively install a vCenter Server Appliance. To do so, you must run the GUI deployment from a Windows, Linux, or Mac

machine that is in the network on which you want to deploy the appliance.

### **Distributed Power Management (DPM)**

DPM requires the ability to wake a host from standby mode, which means it needs the ability to send a network command to the host to power on. For this feature, DPM requires iLO, IPMI, or a Wake On LAN network adapter to be present in each participating host in the cluster. DPM must be supplied with the proper credentials to access the interface and power on the host.

## **vSphere Replication Requirements**

In order to use vSphere Replication 8.3, you must deploy a vSphere Replication Management Service (VRMS) appliance. Optionally, you can add nine additional vSphere Replication Service (VRS) appliances. You should plan for the compute, storage, and network needs of these appliances.

The VRMS appliance requires 2 vCPUs and 8 GB memory. Optionally, you can configure it for 4 vCPUs. Each VRS appliance requires 2 vCPUs and 716 MB memory. The amount of CPU and memory resources consumed by the vSphere Replication Agent on each host is negligible.

Each VRMS and VRS appliance contains two virtual disks whose sizes are 13 BG and 9 GB. To thick provision these virtual disks, you must provide 22 GB storage. If you do not reserve the memory, you should provide storage for the VRMS (8 GB) and VRS (716 MB each) swap files.

Each appliance has at least one network interface and requires at least one IP address. Optionally, you can use separate network connections to allow each appliance to separate management and replication traffic.

The main storage requirement for vSphere Replication is to support the target datastore to where the VMs will be replicated. At a minimum in the replication target datastore, you should provide enough storage to replicate each virtual disk, to support each replicated VM's swap file, and to store each VM's multiple point in time captures (snapshots).

## vCenter High Availability Requirements



The minimum software version for the nodes in a vCenter HA cluster is vCenter Server 6.5. The minimum software versions for the environment (such as a management cluster) where the vCenter HA nodes live is ESXi 6.0 and vCenter Server 6.0. Although not required, VMware recommends that you use a minimum of three ESXi hosts with DRS rules to separate the nodes onto separate hosts. You must use a vCenter Server appliance Small or larger deployment size (not Tiny) and a vCenter Server Standard (not Foundation) license. A single vCenter Server license is adequate for a single vCenter HA cluster. vCenter HA works with VMFS, NFS, and vSAN datastores.

You must configure the appropriate virtual switch port groups prior to configuring vCenter HA. The vCenter HA network connects the Active, Passive, and Witness nodes, replicates the server state, and monitors heartbeats. The vCenter HA network must be on a different subnet than the management network, must provide less than 10 ms latency between nodes, and must not use a default gateway. The vCenter HA and management network IP addresses must be static.

You can use the Set Up vCenter HA wizard in the vSphere Client to configure vCenter HA. You will have

the option to perform an automatic configuration or a manual configuration. The automatic configuration requires a self-managed vCenter Server rather than a vCenter Server that resides in a management cluster that is managed by another vCenter Server. The automatic configuration automatically clones the initial (Active node) vCenter Server to create the Witness and Passive nodes. The manual configuration requires you to clone the Active node yourself but gives you more control.

After configuration is complete, the vCenter HA cluster has two networks, the management network on the first virtual NIC and the vCenter HA network on the second virtual NIC.

## SDDC Requirements

To build a Software Defined Data Center (SDDC), you may plan to implement additional VMware products, such as VSAN, NSX, and vRealize Suite. Here are some of the requirements you should address.

### VSAN

When preparing to implement VSAN, verify that the ESXi hosts meet the vSAN hardware requirements. All capacity devices, drivers, and firmware versions in your vSAN configuration must be certified and listed in the vSAN section of the *VMware Compatibility Guide*.

Table 1-14 provides the storage device requirements for VSAN hosts.

---

**Table 1-14** Storage Device Requirements for VSAN Hosts

<b>Component</b>	<b>Requirements</b>
Cache	One SAS or SATA solid-state disk (SSD) or PCIe flash device.
Virtual Machine Data Storage	For hybrid group configuration, ensure that at least one SAS or NL-SAS magnetic disk is available.  For all-flash group configuration, ensure that at least one SAS, or SATA solid-state disk (SSD), or PCIe flash device is available.
Storage Controllers	One SAS or SATA host bus adapter (HBA), or a RAID controller that is in passthrough mode or RAID 0 mode.

Prepare a network for VSAN traffic. This is the network in which you will connect a VMkernel network adapter for each ESXi host. For non-stretched VSAN clusters the network should provide a maximum Round Trip Time (RTT) of 1 ms.

## NSX

When preparing to implement NSX, ensure that you address the hardware and network latency requirements.

A typical NSX Data Center for vSphere (NSX-V) implementation involves deploying an NSX Manager, three NSX Controllers, and one or more NSX Edges.

[Table 1-15](#) provides the hardware requirements for these NSX-V version 6.4 devices.

**Table 1-15** Hardware Requirements for NSX Appliances

<b>Appliance</b>	<b>Memory</b>	<b>vCPUs</b>	<b>Disk Space</b>
NSX Manager	16 GB	4 or 8	60 GB
NSX Controller	4 GB	4	28 GB
NSX Edge	Compact: 512 MB Large: 1 GB Quad Large: 2 GB X-Large: 8 GB	Compact: 1 Large: 2 Quad Large: 4 X-Large: 6	X-Large: 2.75 GB Other: 1 GB

You should ensure that the network latency is no higher than 150 ms RTT for NSX Manager connections with NSX Controllers, vCenter Server, and ESXi hosts.

## vRealize Suite

vRealize Operations (vROps) is a tool that provides monitoring and analytics of a vSphere environment. This includes smart alerts as well as identifying under or oversized virtual machines. Many businesses use vROps to improve operations of their vSphere and SDDC. They use it for many other purposes, such as capacity planning, proactively remediate issues, reclaim wasted resources, and compliance.

vRealize Automation is cloud automation software that speeds up the delivery of infrastructure and application resources on-premises and in the public cloud. It provides self-service and policy-based automation. Many businesses use vRealize Automation to automate processes and improve up the delivery of IT services and applications.

vRealize Network Insight (vRNI) is a tool that can collect details and flows from your physical and virtual network infrastructure. You can use it as a tool to help you plan and monitor your software defined network. Many businesses use vRNI for micro-segmentation planning and network troubleshooting in an SDDC.

vRealize Log Insight (vRLI) is a tool that can collect and analyze logs from your vSphere components, virtual machines, physical machines, and entire infrastructure. Many businesses use vRLI to centrally collect and analyze logs from the entire SDDC.

## **VMWARE CLOUD VS. VMWARE VIRTUALIZATION**

This section provides brief explanations for virtualization and cloud technologies.

### **Server Virtualization**

VMware vSphere 7.0 is the industry leading virtualization and cloud platform. It provides virtualization (abstraction, pooling, and automation) of x86-64 based server hardware and related infrastructure, such as network switches. It provides live workload migrations, high availability, and efficient management at scale in a secured infrastructure.

## VMware SDDC



A software defined data center (SDDC) is a data center that leverages logical infrastructure services that are abstracted from the underlying physical infrastructure. It allows any application to run on a logical platform that is backed by any x86-64, any storage, and any network infrastructure. Pioneered by VMware, the SDDC is the ideal architecture for private, public, and hybrid clouds. It extends virtualization concepts to all data center resources and services.

The SDDC includes compute virtualization (vSphere), network virtualization (NSX), and software defined storage (VSAN and VVOLs) to deliver abstraction, pooling and automation of the compute, network, and storage infrastructure services. It includes vRealize Automation and vRealize Operations to deliver policy based, automated management of the data center, services, and applications.

## vCloud Suite and Private Clouds

VMware vCloud Suite is an enterprise-ready private cloud software suite that includes vSphere for data center virtualization and VMware vRealize Suite for cloud management platform.

## **VCF and Hybrid Clouds**

Hybrid clouds are clouds that are a combination of private clouds, public clouds, and on-premises infrastructure. It is the result of combining any cloud solution with in-house IT infrastructure.

VMware Cloud Foundation (VCF) is the industry's most advanced hybrid cloud platform. It provides a complete set of software-defined services for compute, storage, networking, security, and cloud management to run enterprise apps in private or public environments. It delivers a simple path to the hybrid cloud by leveraging a common infrastructure and consistent operational model for on-premise and off-premise data centers.

## **VMC on AWS**

VMware Cloud (VMC) on AWS is an integrated cloud offering jointly developed by AWS and VMware that provides a highly scalable, secure service that allows organizations to seamlessly migrate and extend their on-premises vSphere-based environments to the AWS Cloud. You can use it to deliver a seamless hybrid cloud by extending your on-premises vSphere environment to the AWS Cloud

## **VMware vCloud Director**

VMware vCloud Director is a cloud service-delivery platform used by some cloud providers to operate and manage cloud-based services. Service providers can use vCloud Director to deliver secure, efficient, and elastic cloud resources to thousands of customers.

## **Cloud Automation**

VMware Cloud Assembly and VMware Service Broker are software as a service (SaaS) offerings that address similar

use cases as VMware vRealize Automation addresses on-premise.

## SUMMARY

You completed reading the this chapter vSphere overview, components, and requirements. You can use the remain sections in the chapter to prepare for associated exam questions.

## REVIEW ALL THE KEY TOPICS

Table 1-16 provides a detailed discussion of the most important CMOS/BIOS settings. Use this table as a quick reference to the settings you need to make or verify in any system. Examples of these and other settings are provided in the following sections.



**Table 1-16** Key Topics

Key Topic Element	Description	Pages
Table 1-7	vSphere Editions	
Paragraph	Enhanced Linked Mode	
List	ESXi system hardware requirements	
Paragraph	vCenter HA Requirements	
Paragraph	VMware SDDC	

## COMPLETE THE TABLES AND LISTS FROM MEMORY

Print a copy of Appendix B, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

## DEFINITIONS OF KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary.

### Glossary

**vCenter Single Sign-on (SSO):** vCenter Single Sign-On is an authentication broker and security token exchange infrastructure.

**VMC:** VMware Cloud (VMC) on AWS is an integrated cloud offering jointly developed by AWS and VMware that provides a highly scalable, secure service that allows organizations to seamlessly migrate and extend their on-premises vSphere-based environments to the AWS Cloud

**Hybrid Clouds:** Hybrid clouds are clouds that are a combination of private clouds, public clouds, and on-premises infrastructure

**vCenter HA:** vCenter HA is a native high availability solution for VCSA.

**vSphere HA:** vSphere HA provides automated failover protection for VMs against host, hardware, network, and guest OS issues. In case of host system failure, cold migrates and restarts failed VMs on surviving hosts.

**DRS:** Distributed Resource Scheduler (DRS) balances VM workload in a cluster based on compute usage. Includes live (vMotion) migrations of VMs when necessary.

Proactive HA: Proactive HA minimizes VM downtime by proactively detecting hardware failures and placing the host Quarantined Mode or Maintenance Mode.

## ANSWER REVIEW QUESTIONS

- 1.** You plan to implement vSphere 7.0 and use vSphere Fault Tolerance to protect virtual machines with two vCPUs. Which is the minimum vSphere Edition that you need?
  - a.** vSphere Essentials Plus
  - b.** vSphere Foundations
  - c.** vSphere Standard
  - d.** vSphere Enterprise Plus
  
- 2.** You are planning the deployment of vSphere 7.0. Where should you place the VMware Directory Service?
  - a.** In the embedded PSC (not an external PSC)
  - b.** In an external PSC (not an embedded PSC)
  - c.** Either in the external PSC or embedded PSC
  - d.** In the vCenter Server
  
- 3.** You are planning the deployment of ESXi in a vSphere 7.0 environment and want to minimize memory per ESXi host. What is the minimum host memory that VMware recommends for a production environment?
  - a.** 4 GB
  - b.** 8 GB
  - c.** 16 GB
  - d.** 24 GB

**4.** You are planning to install vCenter Server 7.0 and want to use the GUI Installer. Which of the following is a supported location from which to **run** the installer? (Choose 2)

- a.** The Host Client on an ESXi Host
- b.** The Appliance Management Interface
- c.** Windows
- d.** Mac

**5.** Which of the following is the industry's most advanced hybrid cloud platform?

- a.** VMware Cloud Assembly
- b.** VCF
- c.** VMC on AWS
- d.** vRealize Automation

# Chapter 2. Storage Infrastructure

This chapter covers the following topics:

- Storage Models and Datastore Types
- VSAN Concepts
- vSphere Storage Integration
- Storage Multipathing and Failover
- Storage Policies
- Storage DRS (SDRS)

This chapter contains information related to VMware 2V0-21.20 exam objectives 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5, 1.4, 1.6.5, 1.9, 1.9.1, 5.5, 7.4, 7.4.1, 7.4.2, 7.4.3

## “Do I Know This Already?” Quiz

### Storage Models and Datastore Types

#### How Virtual Machines Access Storage

#### Storage Virtualization – Traditional Model

##### Storage Device or LUN

##### Virtual Disk

##### Local Storage

##### Fibre Channel

##### iSCSI

##### FCoE

##### NAS / NFS

##### VMFS

Raw Device Mappings (RDMs)

Software Defined Storage Models

VSAN

vVOLs

Storage Policy Based Management

I/O Filters

Datastore Types

VMFS

NFS

vVOLs Datastore

vSAN Datastore

Storage in vSphere with Kubernetes

VMware NVMe

Requirements for NVMe over PCIe

Requirements for NVMe over RDMA  
(RoCE v2)

Requirements for NVMe over Fibre  
Channel

VMware High Performance Plug-in  
(HPP)

vSAN Concepts

vSAN Characteristics

vSAN Terminology

What is New in VSAN 7.0

VSAN Deployment Options

Standard Cluster

2 Host vSAN Cluster

Stretched Cluster

VSAN Limitations

vSAN Space Efficiency

SCSI Unmap

Deduplication and Compression

RAID 5 and RAID 6 Erasure Coding

vSAN Encryption

vSAN File Service

VSAN Requirements

VSAN Planning and Sizing

Fault Domains Planning

Hardware Requirements

Cluster Requirements

Software Requirements

Network Requirements

License Requirements

Other vSAN Considerations

VSAN Network Best Practices

Boot Devices and VSAN

Persistent Logging in a VSAN Cluster

VSAN Policies

vSphere Storage Integration

VASA

VAAI

VAAI Block Primitives

VAAI NAS Primitives

VAAI Thin Provisioning Primitives

Virtual Volumes (VVols)

Storage Multipathing and Failover

Pluggable Storage Architecture (PSA)

VMware Native Multipathing Plugin

Storage Array Type Plug-ins (SATPs)

Path Selection Plug-ins

PSA Summary

## Storage Policies

Storage Policy Based Management

Virtual Disk Types

vSAN Specific Storage Policies

## Storage DRS (SDRS)

Initial Placement and Ongoing Balancing

Space Utilization Load Balancing

I/O Latency Load Balancing

SDRS Automation Level

SDRS Thresholds and Behavior

SDRS Recommendations

Anti-affinity Rules

Datastore Cluster Requirements

NIOC, SIOC, and SDRS

Review All Key Topics

## Definitions of Key Terms

## Complete the Tables and Lists from Memory

## Review Questions

This chapter provides details for the storage infrastructure, both physical and virtual, involved in a vSphere 7.0 environment.

# **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section. Regardless, the authors recommend that you read the

entire chapter at least once. Table 2-1 outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 2-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
Storage Models and Datastore Types	1, 2
VSAN Concepts	3, 4
vSphere Storage Integration	5, 6
Storage Multipathing and Failover	7
Storage Policies	8, 9
Storage DRS (SDRS)	10

- 1.** You need to configure a virtual machine to utilize N-Port ID Virtualization (NPIV). Which of the following are required? (Choose two.)
  - a.** iSCSI
  - b.** vVOLs
  - c.** RDM
  - d.** FCoE
  - e.** vSAN
  - f.** VMFS
- 2.** You are preparing to implement vSphere with Kubernetes. Which type of virtual disk must you provide for storing logs, emptyDir and ConfigMaps?
  - a.** Ephemeral
  - b.** Container image
  - c.** Persistent volume
  - d.** Non-persistent volume.

- 3.** You are planning to implement a vSphere stretched cluster. Which of the following statements is true?
- a.** You should not enable DRS in automatic mode.
  - b.** You should disable HA datastore heartbeats.
  - c.** If you set PFFT to 0, then you may be able to use SMP-FT
  - d.** If one of the fault domains is inaccessible, then you cannot provision virtual machines.
- 4.** You are planning to implement RAID6 erasure coding for a virtual disk stored in a vSAN datastore. What percentage of the required capacity will be usable?
- a.** 50%
  - b.** 67%
  - c.** 75%
  - d.** 100%
- 5.** You are preparing want to leverage VAAI in your vSphere environment. Which of the following primitives will not be available for your virtual machines stored in NFS datastores?
- a.** Atomic Test and Set
  - b.** Full File Clone
  - c.** Extended Statistics
  - d.** Reserve Space
- 6.** You are planning to implement vVOLs. Which of the following are logical I/O proxies?
- a.** Data-vVol instances
  - b.** Storage Providers

- c.** Storage Containers
  - d.** Protocol Endpoints
- 7. You are explaining how vSphere interacts with storage systems. Which of the following steps may occur when VMware NMP receives an I/O request?
  - a.** The PSP issues the I/O request on the appropriate physical path.
  - b.** The SATP issues the I/O request on the appropriate physical path.
  - c.** The PSP activates the inactive path
  - d.** The PSP calls the appropriate SATP
- 8. In your vSphere environment where VASA is not implemented, you are planning to leverage storage policies associated with devices in your storage array. Which type of storage policies should you create?
  - a.** VM Storage Policy for Host-Based Data Services
  - b.** VM Storage Policy for vVols
  - c.** VM Storage Policy for Tag-Based Placement
  - d.** vSAN Storage Policy
- 9. You are configuring storage policies for use with your vSAN cluster. Which of the following is not an available option?
  - a.** Number of replicas per object
  - b.** Number of disk stripes per object
  - c.** Primary level of failures to tolerate
  - d.** Secondary level of failures to tolerate

**10.** You are testing Storage DRS involving a datastore where the utilized space on one datastore is 82% and 79% on another datastore. You observe that SDRS does not make a migration recommendation. What may be the reason?

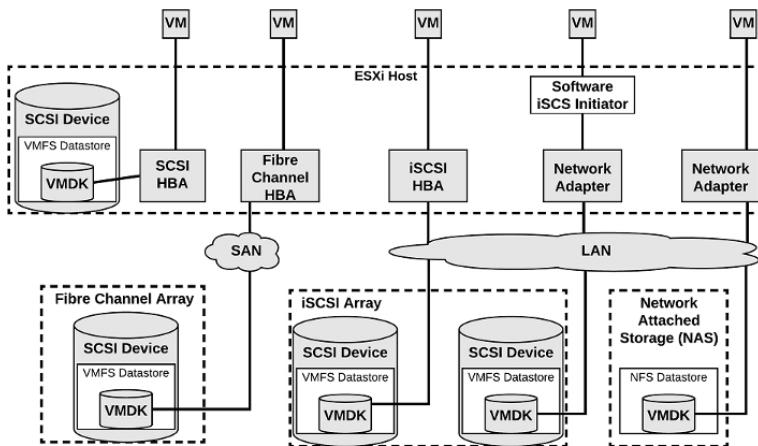
- a.** The Space Utilization Difference threshold is set too low.
- b.** The Space Utilization Difference threshold is set too high.
- c.** The Space Utilization Difference threshold is set to 78%
- d.** The Space Utilization Difference threshold is set to 80%

## **STORAGE MODELS AND DATASTORE TYPES**

This section describes the storage models and datastore types available in vSphere and how virtual machines access storage.

### **How Virtual Machines Access Storage**

A virtual machine communicates with its virtual disk stored on a datastore by issuing SCSI commands. The SCSI commands are encapsulated into other forms, depending on the protocol that the ESXi host uses to connect to a storage device on which the datastore resides, as illustrated in [Figure 2-1](#).



**Figure 2-1** Virtual Machine Storage

## Storage Virtualization – Traditional Model

Storage virtualization refers to a logical abstraction of physical storage resources and capacities from virtual machines. ESXi provides host-level storage virtualization. In vSphere environments, a traditional model is built around the following storage technologies and ESXi virtualization features.

### Storage Device or LUN

In common ESXi vocabulary, the terms *device* and *LUN* are used interchangeably. The terms represent storage volumes that are presented to the host from a block storage system and is available to ESXi for formatting.

### Virtual Disk

Virtual disks are sets of files that reside on a datastore that is deployed on physical storage. From the standpoint of the virtual machine, each virtual disk appears as if it were a SCSI drive connected to a SCSI controller. The physical storage is transparent to the virtual machine guest operating system and applications.

### Local Storage

Local storage can be internal hard disks located inside your ESXi host and external storage systems connected to the host directly through protocols such as SAS or SATA. Local storage does not require a storage network to communicate with your host.

## **Fibre Channel**

Fibre Channel (FC) is a storage protocol that a storage area network (SAN) uses to transfer data traffic from ESXi host servers to shared storage. It packages SCSI commands into FC frames. The ESXi host uses Fibre Channel host bus adapters (HBAs) to connect to the FC SAN, as illustrated in [Figure 2-1](#). Unless you use direct-connected Fibre Channel storage, you need Fibre Channel switches to route storage traffic. If your host contains FCoE (Fibre Channel over Ethernet) adapters, you can connect to your shared Fibre Channel devices by using an Ethernet network.

## **iSCSI**

Internet SCSI (iSCSI) is a SAN transport that can use Ethernet connections between ESXi hosts and storage systems. To connect to the storage systems, your hosts use hardware iSCSI adapters or software iSCSI initiators with standard network adapters.

With hardware iSCSI HBAs, the host connects to the storage through a hardware adapter that offloads the iSCSI and network processing. Hardware iSCSI adapters can be dependent and independent. With software iSCSI adapters, the host uses a software-based iSCSI initiator in the VMkernel and a standard network adapter to connect to storage. Both the iSCSI HBA and the Software iSCSi Initiator are illustrated in [Figure 2-1](#).

## **FCoE**

If an ESXi host contains FCoE (Fibre Channel over Ethernet) adapters, it can connect to shared Fibre

Channel devices by using an Ethernet network.

## NAS / NFS

Using NFS, vSphere stores your virtual machines files on remote file servers accessed over a standard TCP/IP network. ESXi 7.0 uses Network File System (NFS) protocol version 3 and 4.1 to communicate with the NAS/NFS servers, as illustrated in [Figure 2-1](#). You can use NFS datastores to store and manage virtual machines in the same way that you use the VMFS datastores.

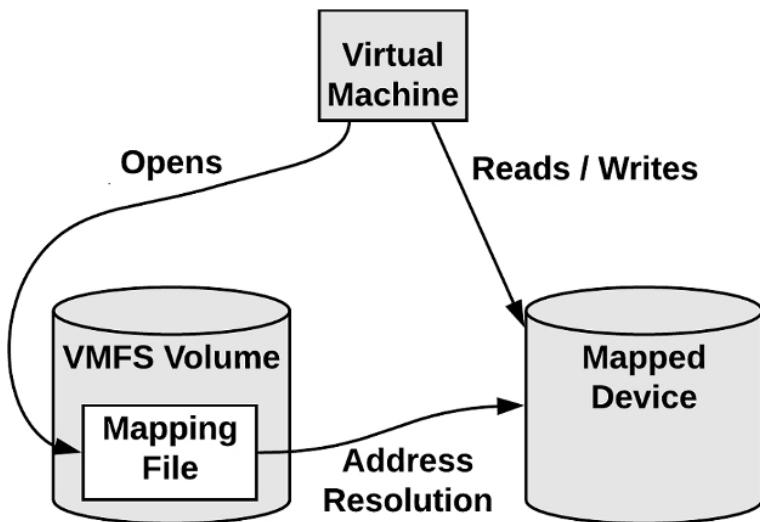
## VMFS

The datastores that you deploy on block storage devices use the native vSphere Virtual Machine File System (VMFS) format. It is a special high-performance file system format that is optimized for storing virtual machines.

## Raw Device Mappings (RDMs)



An RDM is a mapping file containing metadata that resides in a VMFS datastore and acts as a proxy for a physical storage device (LUN), allowing a virtual machine to access the storage device directly. It gives you some of the advantages of direct access to a physical device and keeps some of the management advantages of VMFS based virtual disks. The components involved with an RDM are illustrated in [Figure 2-2](#).



**Figure 2-2** RDM Diagram

You can envision an RDM as a symbolic link from a VMFS volume to the storage device. The mapping makes the storage device appear as a file in a VMFS volume. The virtual machine configuration references the RDM, not the storage device. RDMs support two compatibility modes.

- Virtual compatibility mode: The RDM acts much like a virtual disk file, enabling extra virtual disk features, such as the use of virtual machine snapshot and the use of disk modes (dependent, independent – persistent, independent – nonpersistent).
- Physical compatibility mode, The RDM offers direct access to the SCSI device supporting applications that require lower-level control.

Virtual disk files are preferred over RDMs for manageability. You should only use RDMs when necessary. Use Cases for RDMs include the following.

- You plan to install software in the virtual machine that requires features inherent to the SAN, such as SAN management, storage base snapshots, or storage-based replication. The RDM enables the

virtual machine to have the required access to the storage device.

- You plan to configure MSCS clustering in a manner that spans physical hosts, such as virtual-to-virtual clusters and physical-to-virtual clusters. You should configure the data and quorum disks as RDMs rather than virtual disk files.

Benefits of RDMs include the following.

- User-Friendly Persistent Names: Much like naming a VMFS datastore, you can provide a friendly name to a mapped device, rather than using its device name.
- Dynamic Name Resolution: If physical changes (such as adapter hardware changes, path changes, or device relocation) occur, the RDM is updated automatically. The virtual machines do not need to be updated, because they reference the RDM,
- Distributed File Locking: VMFS distributed locking is used to make it safe for two virtual machines on different servers to access the same LUN.
- File Permissions: Permissions are set on the mapping file to effectively apply permissions to the mapped file, much like they are applied to virtual disks.
- File System Operations: Most file system operations that are valid for an ordinary file can be applied to the mapping file and redirected to the mapped device.
- Snapshots: Virtual machine snapshots can be applied to the mapped volume, but not when the RDM is used in physical compatibility mode.
- vMotion: You can migrate the virtual machine with vMotion, as vCenter Server uses the RDM as a

proxy, which enables the use of the same migration mechanism used for virtual disk files.

- SAN Management Agents: Enables the use of SAN management agents (SCSI target-based software) inside a virtual machine, which require hardware-specific SCSI commands. This requires physical compatibility mode for the RDM.
- N-Port ID Virtualization (NPIV): You can use NPIV technology that allows a single Fibre Channel HBA port to register with the fabric using multiple worldwide port names (WWPNs). This ability makes the HBA port appear as multiple virtual ports, each having its own ID and virtual port name. Virtual machines can then claim each of these virtual ports and use them for all RDM traffic. NPIV requires the use of virtual machines with RDMs.

**Note**

To support vMotion involving RDMs, be sure to maintain consistent LUN IDs for RDMs across all participating ESXi hosts.

**Note**

To support vMotion for NPIV enabled virtual machines, place the RDM files, virtual machine configuration file, and other virtual machines in the same datastore. You cannot perform Storage vMotion when NPIV is enabled.

## Software Defined Storage Models

In addition to abstracting underlying storage capacities from VMs, as traditional storage models do, software-defined storage abstracts storage capabilities. With the software-defined storage model, a virtual machine becomes a unit of storage provisioning and can be managed through a flexible policy-based mechanism. The model involves the following vSphere technologies

### VSAN

vSAN is a layer of distributed software that runs natively on each hypervisor in the cluster. It aggregates local or direct-attached capacity creates a single storage pool shared across all hosts in the vSAN cluster.

## **vVOLs**

Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives that are stored natively inside a storage system. You do not provision Virtual volumes directly. Instead, they are automatically created when you create, clone, or snapshot a virtual machine. Each virtual machine can be associated to one or more virtual volumes.

The Virtual Volumes (vVols) functionality changes the storage management paradigm from managing space inside datastores to managing abstract storage objects handled by storage arrays. With Virtual Volumes, each virtual machine (rather than a datastore) is a unit of storage management. You can apply storage policies per virtual machine, rather than per LUN or datastore.

## **Storage Policy Based Management**

Storage Policy Based Management (SPBM) is a framework that provides a single control panel across various data services and storage solutions, including vSAN and Virtual Volumes. Using storage policies, the framework aligns application demands of your virtual machines with capabilities provided by storage entities.

## **I/O Filters**

I/O filters are software components that can be installed on ESXi hosts and can offer additional data services to virtual machines. Depending on implementation, the services might include replication, encryption, caching, and so on.

## **Datastore Types**

In vSphere 7.0, you can use the following datastore types.

## VMFS

You can create VMFS datastores on fiber channel, iSCSI, FCoE, and local storage devices. ESXi 7.0 supports VMFS versions 5 and 6 for read and write. ESXi 7.0 does not support VMFS version 3. **Table 2-2** compares the features and functionalities of VMFS versions 5 and 6.

**Table 2-2** Comparing VMFS Versions 5 and 6

Features and Functionalities	VMFS5	VMFS6
Access for ESXi hosts version 6.5 and later	Yes	Yes
Access for ESXi hosts version 6.0 and earlier	Yes	No
Datastores per host	512	512
512n storage devices	Yes	Yes (default)
512e storage devices	Yes. Not supported on local 512e devices.	Yes (default)
4Kn storage devices	No	Yes
Automatic space reclamation	No	Yes
Manual space reclamation through the esxcli command.	Yes	Yes
Space reclamation from guest OS	Limited	Yes
GPT storage device partitioning	Yes	Yes
MBR storage device partitioning	Yes  For a VMFS5 datastore that has been previously upgraded from VMFS3.	No
Storage devices greater than 2 TB for each VMFS extent	Yes	Yes
Support for virtual machines with large capacity virtual disks, or disks greater than 2 TB	Yes	Yes
Support of small files of 1 KB	Yes	Yes
Default use of ATS-only locking mechanisms on storage devices that support ATS.	Yes	Yes
Block size	Standard 1 MB	Standard 1 MB
Default snapshots	VMFSsparse for virtual disks smaller than 2 TB. SEsparse for virtual disks larger than 2 TB.	SEsparse
Virtual disk emulation type	512n	512n
vMotion	Yes	Yes
Storage vMotion across different datastore types	Yes	Yes
High Availability and Fault Tolerance	Yes	Yes
DRS and Storage DRS	Yes	Yes
RDM	Yes	Yes

When working with VMFS datastores in vSphere 7.0, consider the following.

- **Datastore Extents.** A spanned VMFS datastore must use only homogeneous storage devices, either

**512n**, **512e**, or **4Kn**. The spanned datastore cannot extend over devices of different formats.

- **Block Size.** The block size on a VMFS datastore defines the maximum file size and the amount of space a file occupies. VMFS5 and VMFS6 datastores support the block size of 1 MB.
- **Storage vMotion.** Storage vMotion supports migration across VMFS, vSAN, and Virtual Volumes datastores. vCenter Server performs compatibility checks to validate Storage vMotion across different types of datastores.
- **Storage DRS.** VMFS5 and VMFS6 can coexist in the same datastore cluster. However, all datastores in the cluster must use homogeneous storage devices. Do not mix devices of different formats within the same datastore cluster.
- **Device Partition Formats.** Any new VMFS5 or VMFS6 datastore uses GUID partition table (GPT) to format the storage device. The GPT format enables you to create datastores larger than 2 TB. If your VMFS5 datastore has been previously upgraded from VMFS3, it continues to use the master boot record (MBR) partition format, which is characteristic for VMFS3. Conversion to GPT happens only after you expand the datastore to a size larger than 2 TB

## NFS

You can create NFS datastores on NAS storage. ESXi 7.0 supports NFS protocols version 3 and 4.1. To support both versions, ESXi 7.0 uses two different NFS clients.

Table 2-3 compares the capabilities of NFS versions 3 and 4.1.

**Table 2-3** NFS Versions 3 and 4.1 Characteristics

---

Characteristics	NFS 3	NFS 4.1
Security mechanisms	AUTH_SYS	AUTH_SYS and Kerberos (krb5 and krb5i)
Encryption algorithms with Kerberos	N/A	AES256-CTS-HMAC-SHA1-96 and AES128-CTS-HMAC-SHA1-96
Multipathing	Not supported	Supported through the session trunking
Locking mechanisms	Proprietary client-side locking	Server-side locking
Hardware acceleration	Supported	Supported
Thick virtual disks	Supported	Supported
IPv6	Supported	Supported for AUTH_SYS and Kerberos
ISO images presented as CD-ROMs to virtual machines	Supported	Supported
Virtual machine snapshots	Supported	Supported
Virtual machines with virtual disks greater than 2 TB	Supported	Supported

**Table 2-4** compares vSphere 7.0 features and related solutions supported by NFS versions 3 and 4.1.

**Table 2-4** NFS Versions 3 and 4.1 Support for vSphere Features and Solutions

Features and Functionalities	NFS 3	NFS 4.1
vMotion and Storage vMotion	Yes	Yes
High Availability (HA)	Yes	Yes
Fault Tolerance (FT)	Yes	Yes Supports the new FT mechanism introduced in vSphere 6.0 that supports up to four vCPUs, not the legacy FT mechanism.
Distributed Resource Scheduler (DRS)	Yes	Yes
Host Profiles	Yes	Yes
Storage DRS	Yes	No
Storage I/O Control	Yes	No
Site Recovery Manager	Yes	No
Virtual Volumes	Yes	Yes
vSphere Replication	Yes	Yes
vRealize Operations Manager	Yes	Yes

When you upgrade ESXi from a version earlier than 6.5, existing NFS 4.1 datastores automatically begin supporting functionalities that were not available in the previous ESXi release, such as Virtual Volumes and hardware acceleration. ESXi does not support automatic datastore conversions from NFS version 3 to NFS 4.1. You can use Storage vMotion to migrate virtual machines from NFS3 datastores to NFS4.1 datastores. In some

cases, a storage vendor may provide a conversion method from NFS 3 to NFS 4.1. In some cases, you may be able to unmount the NFS 3 datastore from all hosts and remount it as NFS 4.1. The datastore can never be mounted by using both protocols at the same time.

### **vVOLs Datastore**

You can create a vVols datastore in an environment with a compliant storage system. A virtual volume, which is created and manipulated out of band by a vSphere APIs for Storage Awareness (VASA) provider, represents a storage container in vSphere. The VASA provider maps virtual disk objects and their derivatives, such as clones, snapshots, and replicas, directly to the virtual volumes on the storage system. ESXi hosts access virtual volumes through an intermediate point in the data path, called the protocol endpoint. The protocol endpoints serve as a gateway for I/O between ESXi hosts and the storage system, using Fibre Channel, FCoE, iSCSI, or NFS.

### **vSAN Datastore**

You can create a vSAN datastore in a vSAN cluster. vSAN is a hyperconverged storage solution, which combines storage, compute, and virtualization into a single physical server or cluster. The following section describes the concepts, benefits, and terminology associated with vSAN.

## **Storage in vSphere with Kubernetes**

To support the different types of storage objects in Kubernetes, vSphere with Kubernetes provides three types of virtual disks, which are ephemeral, container image, and persistent volume.

A vSphere Pod requires ephemeral storage to store Kubernetes objects, such as logs, emptyDir volumes, and ConfigMaps.. The ephemeral, or transient, storage exists if the vSphere Pod exists.

The vSphere Pod mounts images used by its containers as image virtual disks, enabling the container to use the software contained in the images. When the vSphere Pod life cycle completes, the image virtual disks are detached from the vSphere Pod. You can specify a datastore to use as the container image cache, such that subsequent pods can pull it from the cache rather than the external container registry.

Some Kubernetes workloads require persistent storage to store the data independent of the pod. Persistent volume objects in vSphere with Kubernetes are backed by the First Class Disks on a datastore. A First Class Disk (FCD), which is also called a an Improved Virtual Disk, is a named virtual disk that is not associated with a VM. To provide the persistent storage, you can use the Workload Management feature in the vSphere Client to associate one or more storage policies with the appropriate namespace.

## **VMware NVMe**

NVMe storage is a low latency, low CPU usage, and high performance alternative to SCSI storage. It is designed for use with faster storage media equipped with non-volatile memory, such as flash devices. NVMe storage can be directly attached to a host using a PCIe interface or indirectly through different fabric transport (NVMe-oF).

In a NVMe storage array, a namespace represents a storage volume. A NVMe namespace is analogous to a storage device (LUN) in other storage arrays. In the vSphere Client, NVMe namespaces appear in the list of storage devices. You can use the device to create a VMFS datastore.

### **Requirements for NVMe over PCIe**

NVMe over PCIe requires the following.

- Local NVMe storage devices.
- Compatible ESXi host.
- Hardware NVMe over PCIe adapter.

### **Requirements for NVMe over RDMA (RoCE v2)**

NVMe over PCIe requires the following.

- NVMe storage array with NVMe over RDMA (RoCE v2) transport support
- Compatible ESXi host.
- Ethernet switches supporting a lossless network.
- Network adapter that supports RDMA over Converged Ethernet (RoCE v2).
- Software NVMe over RDMA adapter.
- NVMe controller.

### **Requirements for NVMe over Fibre Channel**

NVMe over PCIe requires the following.

- Fibre Channel storage array that supports NVMe.
- Compatible ESXi host.
- Hardware NVMe adapter. (A Fibre Channel HBA that supports NVMe)
- NVMe controller.

### **VMware High Performance Plug-in (HPP)**

VMware provides the High-Performance Plug-in (HPP) to improve the performance of NVMe devices on your ESXi host. HPP replaces NMP for high-speed devices, such as NVMe.

HPP is the default plug-in that claims NVMe-oF targets. Within ESXi, the NVMe-oF targets are emulated and

presented to users as SCSI targets. The HPP supports only active/active and implicit ALUA targets.

NMP is the default plug-in for local NVMe devices, but you can replace it with HPP. NMP cannot be used to claim the NVMe-oF targets. High-Performance Plug-in (HPP) should be used for NVMe-oF.

Table 2-5 describes the vSphere 7.0 Support for HPP

**Table 2-5** vSphere 7.0 HPP Support

HPP Support	vSphere 7.0
Storage devices	Local NVMe PCIe  Shared NVMe-oF (active/active and implicit ALUA targets only)
Multipathing	Yes
Second-level plug-ins	No
SCSI-3 persistent reservations	No
4Kn devices with software emulation	No
vSAN	No

Table 2-6 describes the Path Selection Schemes (PSS) used by HPP when selecting physical paths for I/O requests.

**Table 2-6** HPP Path Selection Schemes (PSS)

PSS	Description
FIXED	Uses a designated preferred path is used for I/O requests
LB-RR (Load Balance - Round Robin)	(The default HPP scheme). After transferring a specified number of bytes or I/Os on a current path, the scheme selects the path using the round robin algorithm. You can configure the IOPS and Bytes properties to indicate the criteria for path switching.
LB-IOPS (Load Balance - IOPs)	After transferring a specified number (default 1000) of I/Os on a current path, the scheme selects an optimal path based on the least number of outstanding bytes.
LB-BYTES (Load Balance - Bytes)	After transferring a specified amount of data (default 10 MB) on a current path, the scheme selects an optimal path based on the least number of outstanding I/Os
Load Balance – Latency (LB-Latency)	The scheme selects an optimal path by considering the latency evaluation time and the sampling I/Os per path.

HPP best practices include the following.

- Use a vSphere version that supports HPP.
- Use HPP for NVMe local and networked devices.

- Do not use HPP with HDDs or any flash devices that cannot sustain 200,000 IOPS.
- If you use NVMe with Fibre Channel devices, follow your vendor recommendations.
- If you use NVMe-oF, do not mix transport types to access the same namespace.
- When using NVMe-oF namespaces, make sure that active paths are presented to the host.
- Configure VMs to use VMware Paravirtual controllers.
- Set the latency sensitive threshold for virtual machines.
- If a single VM drives a significant share of the device's I/O workload, consider spreading the I/O across multiple virtual disks, attached to separate virtual controllers in the VM (or you risk that the I/O may saturate a CPU core).

## VSAN CONCEPTS

vSAN virtualizes the local, physical storage resources of ESXi hosts by turning them into pools of storage that can be used by virtual machines based on their quality-of-service requirements. You can configure vSAN as a hybrid or an all-flash cluster. Hybrid clusters use flash devices for the cache layer and magnetic disks for the storage capacity layer. All Flash clusters use flash devices for both cache and capacity.

You can enable vSAN on existing host clusters as well as new clusters. You can expand the datastore by adding hosts with capacity devices to the cluster or by adding local drives to the existing hosts in the cluster. vSAN works best when all ESXi hosts in the cluster are configured similarly, including similar or identical

storage configurations. A consistent configuration enables vSAN to balance virtual machine storage components across all devices and hosts in the cluster. Hosts without any local devices also can participate and run their virtual machines on the vSAN datastore.

If a host contributes some of its local storage to a VSAN cluster, then it must contribute at least one device for cache. The drives contributed by a host form one or more disk groups. Each disk group contains a flash cache device and at least one capacity devices. Each host can be configured to use multiple disk groups.

vSAN offers many features of a traditional SAN. Its main limitations are that each vSAN instance can only support one cluster. It has the following benefits over traditional storage.

- vSAN does not require dedicated, storage network, such as on a Fibre Channel (FC) or Storage Area Network (SAN).
- With vSAN, you do not have to pre-allocate and pre-configure storage volumes (LUNs).
- vSAN does not behave like traditional storage volumes based on LUNs or NFS shares. You do not have to apply standard storage protocols, such as FC, and you do not need to format the storage directly.
- You can deploy, manage, and monitor vSAN by using the vSphere Client, rather than other storage management tools.
- A vSphere administrator, rather than storage administrator, can manage a vSAN environment.
- When deploying virtual machines, you can use automatically assigned storage policies with vSAN.

## vSAN Characteristics

vSAN is like a network distributed RAID for local disks, transforming them into shared storage. vSAN uses of copies of VM data, where one copy is local and another copy is on one of the other nodes in the cluster. The number of copies is configurable. Here are some of the features of vSAN:

- Shared storage support: The VMware features which require shared storage (HA, vMotion, DRS) are available with vSAN.
- On-disk format: highly scalable snapshot and clone management on a vSAN cluster.
- All-flash and hybrid configurations: vSAN can be used on hosts with all-flash storage, or with hybrid storage (combination SSD and traditional HDDs)
- Fault domains: Fault domains can be configured to protect against rack or chassis failures, preventing all copies of VM disk data from residing on the same rack or chassis.
- iSCSI target service: This allows the vSAN datastore to be visible and usable by ESXi hosts outside of the cluster and by physical bare-metal systems.
- Stretched cluster: vSAN supports stretching a cluster across physical geographic locations.
- Support for Windows Failover Clusters (WSFC): SCSI-3 Persistent Reservations (SCSI3-PR) are supported on virtual disks, which are required for shared disks and WSFC. MS SQL 2012 or later is supported on vSAN. The following limitations apply:
  - Maximum of 6 application nodes in each vSAN cluster.
  - Maximum of 64 shared disks per ESXi host.

- vSAN health service: This includes health checks for monitoring and troubleshooting purposes.
- VSAN performance service: This service includes statistics for monitoring vSAN performance metrics. This can be monitored at the cluster level, ESXi host, disk group, disk, or VMs.
- Integration with vSphere storage features: Snapshots, linked clones, and vSphere Replication are all supported on vSAN datastores.
- Virtual Machine Storage Policies: Policies can be defined for VMs on vSAN. If no policies are defined, a default vSAN policy is applied.
- Rapid provisioning: This provides fast storage provisioning for VM creation and deployment from templates.
- Deduplication and compression: Block-level deduplication and compression are available space-saving mechanisms on vSAN, which can be configured at the cluster level, and applied to each disk group.
- Data at rest encryption: Data at rest encryption is data that is not in transit, and no processes are being done, for example, deduplication or compression. If drives are removed, the data on those drives is encrypted.
- SDK support: This is an extension (written in Java) of the VMware vSphere Management SDK. It has libraries, code examples, and documentation for assistance in automating and troubleshooting vSAN deployments.

## vSAN Terminology

- Disk Group: a group of local disks on an ESXi host contributing to the vSAN datastore. This must

include one cache device and one capacity device. In a hybrid cluster, a flash disk is the cache device, and magnetic disks are used for capacity devices. In all-flash clusters, flash storage is used for both cache and capacity.

- Consumed Capacity: the amount of physical space used up by virtual machines at any point in time.
- Object-Based Storage: data is stored in vSAN by way of objects, which are flexible data containers. Objects are logical volumes with data and metadata spread among nodes in the cluster. Virtual disks are objects, as are snapshots. For object creation and placement, vSAN takes the following into account:
  - Virtual disk policy and requirements are verified
  - The number of copies (replicas) is verified; the amount of flash read cache allocated for replicas, number of stripes for replica as well as location is determined.
  - Policy compliance of virtual disks.
  - Mirrors and witnesses placed on different hosts or fault domains.
- vSAN Datastore: Like other datastores, a vSAN datastore which will appear in the Storage Inventory view in vSphere. vSAN clusters provide a single datastore to be available for every host in the cluster, even if they do not contribute storage to vSAN. An ESX hosts can mount VMFS and NFS datastores in addition to the vSAN datastore. Storage vMotion can be utilized to migrate VMs between any datastore type.
- Objects and Components:
  - VM Home Namespace: The VM home directory where all of the VM files are stored.

- VMDK: virtual disks for VMs.
- VM Swap Object: allows memory to be swapped to disk during periods of contention. This is created at VM power on.
- Snapshot Delta VMDKs: these are change files created when a snapshot is taken of a VM.
- Memory object: This is created when a VM is snapshotted (and choosing to retain the VM's memory) or suspended.
- Virtual Machine Compliance Status: Can be Compliant and Noncompliant, depending on whether each of the virtual machine's objects meet the requirements of the assigned storage policy. The status is available on the **Virtual Disks Page** on the **Physical Disk Placement** tab.
- Component State: Degraded and Absent States:
  - Degraded: vSAN detects a permanent failure of a component.
  - Absent: vSAN detects a temporary component failure.
- Object State: Healthy and Unhealthy:
  - Healthy: At least one RAID 1 mirror is available, or enough segments are available for RAID 5 or 6.
  - Unhealthy: no full mirror is available, or not enough segments are available for RAID 5 or 6.
- Witness: A component only consisting of metadata. It is used as a tiebreaker. Witnesses consume about 2 MB of space for metadata on a vSAN datastore when on-disk format 1.0 is used, and 4 MB when on-disk format 2.0 or later is used.
- Storage Policy-Based Management (SPBM): VM storage requirements are defined as a policy and

vSAN ensures these policies are met when placing objects. If you don't apply a storage policy when creating or deploying VMs, the default vSAN policy with **Primary level of failures to tolerate** is set to 1 with a single stripe per object, and thin provisioned disk.

- Ruby vSphere Console (RVC): This is a command-line interface used for managing and troubleshooting vSAN. RVC provides a cluster-wide view and is included with the vCenter Server deployment.
- VMware PowerCLI: vSAN cmdlets are included with PowerCLI to allow administration of vSAN.
- vSAN Observer: this is a web-based utility, built on top of RVC, used for performance analysis and monitoring. This can display performance statistics on the capacity tier, disk group statistics, CPU load, memory consumption, and vSAN objects in-memory and their distribution across the cluster.
- vSAN Ready Node: This is a preconfigured deployment which is provided by VMware partners. This is a validated design using certified hardware.
- User-Defined vSAN Cluster: This is a vSAN deployment making use of hardware selected by you.

**Note**

The capacity disks contribute to the advertised datastore capacity. The flash cache devices are not included as capacity

## What is New in VSAN 7.0

The following new features are available in vSAN 7.0

- **vSphere Lifecycle Manager.** vSphere Lifecycle Manager uses a desired-state model to enable

simple, consistent lifecycle management for your ESXi hosts, including drivers and firmware.

- **Integrated File Services.** The vSAN native File Service enables you to create and present NFS v4.1 and v3 file shares, effectively extending vSAN capabilities to files, such as availability, security, storage efficiency, and operations management.
- **Native support for NVMe hot plug.** The plugin provides a consistent way of servicing NVMe devices and provides operational efficiency.
- **I/O redirect based on capacity imbalance with stretched clusters.** This feature improves uptime of your VMs by redirecting all virtual machine I/O from a capacity-strained site to the other site.
- **Skyline integration with vSphere health and vSAN health.** Skyline Health for vSphere and vSAN are available, enabling a native, in-product health monitoring and consistent, proactive analysis.
- **Remove EZT for shared disk.** vSAN 7.0 eliminates the prerequisite that shared virtual disks using the multi-writer flag must also use the eager zero thick format.
- **Support vSAN memory as metric in performance service.** vSAN memory usage is now available in the Performance Charts (vSphere Client) and through the API.
- **Visibility of vSphere Replication objects.** vSphere replication objects are visible in vSAN capacity view.
- **Support for large capacity drives.** Support for 32TB physical capacity drives and up to 1PB logical

capacity when deduplication and compression is enabled.

- **Immediate repair after new witness is deployed.** vSAN immediately invokes a repair object operation after a witness has been added during a replace witness operation.
- **vSphere with Kubernetes integration.** CNS is the default storage platform for vSphere with Kubernetes. This integration enables various stateful containerized workloads to be deployed on vSphere with Kubernetes Supervisor and Guest clusters on vSAN, VMFS and NFS datastores.
- **File-based persistent volumes.** Kubernetes developers can dynamically create shared (Read/Write/Many) persistent volumes for applications. Multiple pods can share data. vSAN native File Services is the foundation that enables this capability.
- **vVol support for modern applications.** You can deploy modern Kubernetes applications to external storage arrays on vSphere using the CNS support added for vVols. vSphere now enables unified management for Persistent Volumes across vSAN, NFS, VMFS and vVols.
- **vSAN VCG notification service.** You can get notified through email about any changes to vSAN HCL components such as vSAN ReadyNode, I/O controller, drives (NVMe, SSD, HDD) and get notified through email about any changes.

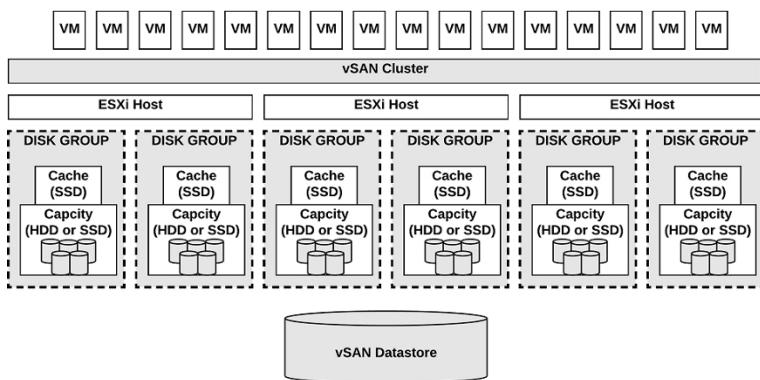
**Note**

In vCenter Server 7.0.0a, vSAN File Services and vSphere Lifecycle Manager can be enabled simultaneously on the same vSAN cluster.

## VSAN Deployment Options

## Standard Cluster

A standard vSAN cluster, which is illustrated in Figure 2-3, consists of a minimum of three hosts, typically residing at the same location, and connected on the same Layer 2 network. 10 Gb network connections are required for all-flash clusters and are recommended for hybrid configurations.

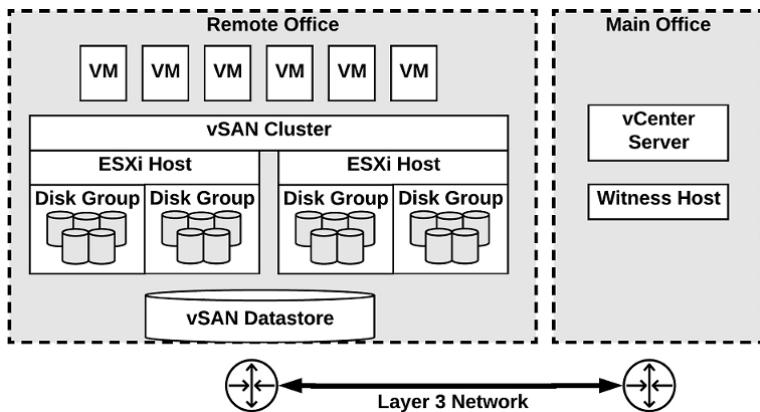


**Figure 2-3** A Standard vSAN cluster

## 2 Host vSAN Cluster

The main use case for a two host vSAN cluster is a remote office/branch office environment, where workloads require high availability. A two host vSAN cluster, which is illustrated in Figure 2-4, consists of two hosts at the same location, connected to the same network switch or directly connected. You can configure a two host vSAN cluster that uses a third host as a witness, which can be located separately from the remote office. Usually the witness resides at the main site, along with the vCenter Server. For more details on the Witness host, see the next section on *Stretched Clusters*.





**Figure 2-4** A Two-Node vSAN cluster

### Stretched Cluster



You can create a stretched vSAN cluster that spans two geographic sites and continues to function if a failure or scheduled maintenance occurs at one site. Stretched clusters, which are typically deployed in metropolitan or campus environments with short distances between sites, provide a higher level of availability and inter-site load balancing.

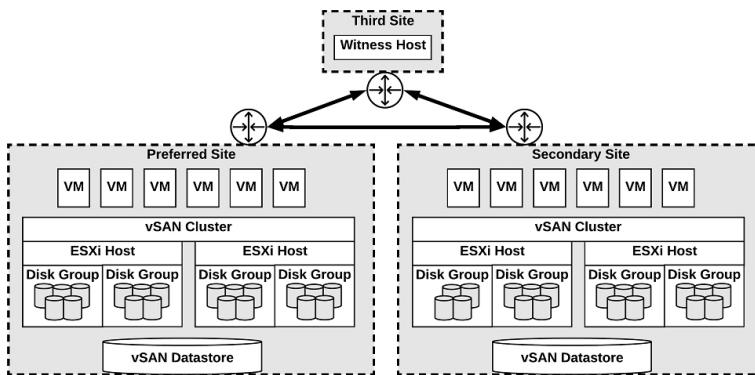
You can use stretched clusters for planned maintenance and disaster avoidance scenarios, where both data sites are active. If either site fails, vSAN uses the storage on the other site and vSphere HA can restart virtual machines on the remaining active site.

You should designate one site as the preferred site, which becomes the only used site in the event of a network connectivity loss between the two sites. A vSAN stretched cluster can tolerate one link failure at a time without data becoming unavailable. During a site failure or loss of network connection, vSAN automatically switches to fully functional sites.

**Note**

A link failure is a loss of network connection between the two sites or between one site and the witness host.

Each stretched cluster consists of two data sites and one witness host. The witness host resides at a third site and contains the witness components of virtual machine objects. It contains only metadata and does not participate in storage operations. Figure 2-5 shows an example of a stretched cluster, where the witness nodes resides at a third site along with vCenter Server.



**Figure 2-5** A Stretched vSAN cluster

The witness host acts as a tiebreaker for decisions regarding availability of datastore components. The witness host typically forms a vSAN cluster with the preferred site, but forms a cluster with secondary site, if the preferred site becomes isolated. When the preferred site is online again, data is resynchronized.

Characteristics of the witness host.

- It can use low bandwidth/high latency links.
- It cannot run VMs.
- It can support only one vSAN stretched cluster.
- It requires a VMkernel adapter enabled for vSAN traffic with connections to all hosts in the cluster. It can have only one VMkernel adapter dedicated to vSAN but can have another for management.

- It must be a standalone host. It cannot be added to any other cluster or moved in inventory through vCenter Server.
- It can be a physical ESXi host or a VM-based ESXi host.

**Note**

The witness virtual appliance is an ESXi host in a VM, packaged as an OVF or OVA, which is available in different options, based on the size of the deployment.

Each site in a stretched cluster resides in a separate fault domain. Three default domains are used: the preferred site, the secondary site, and a witness host.

Beginning with vSAN 6.6, you can provide an extra level of local fault protection for objects in stretched clusters using the following policy rules.

- **Primary level of failures to tolerate (PFTT)** defines the number of site failures that a virtual machine object can tolerate. For a stretched cluster, only a value of 0 or 1 is supported.
- **Secondary level of failures to tolerate (SFTT)** defines the number of additional host failures that the object can tolerate after the number of site failures (PFTT) is reached. For example, If PFTT = 1 and SFTT = 2, and one site is unavailable, then the cluster can tolerate two additional host failures. The default value is 0, and the maximum value is 3.
- **Data Locality** enables you to restrict virtual machine objects to a selected site in the stretched cluster. The default value is None, but you can change it to Preferred or Secondary. Data Locality is available only if PFTT = 0.

**Note**

If you set **SFTT** for a stretched cluster, the **Fault tolerance method** rule applies to the **SFTT**. The failure tolerance method used for the PFTT is set to RAID 1.

Consider the following guidelines and best practices for stretched clusters:

- DRS must be enabled on the cluster.
- Create two host groups, two virtual machines groups, and two VM-Host affinity rules to effectively control the placement of virtual machines between the preferred and the secondary sites.
- HA must be enabled on the cluster in a manner such that it respects the VM-Host affinity rules.
- Disable HA datastore heartbeats.
- On disk format 2.0 or later is required.
- Set **Failures to tolerate** to 1
- Symmetric Multiprocessing Fault Tolerance (SMP-FT) is supported when **PFFT** is set to 0 and **Data Locality** is set to Preferred or Secondary. SMP-FT is not supported if **PFFT** is set to 1.
- Using `esxcli` to add or remove hosts is not supported.
- If one of the three fault domains (preferred site, secondary site, or witness host) is inaccessible, new VMs can still be provisioned, but are non-compliant until the partitioned site rejoins the cluster. This implicit force provisioning is performed only when two of the three fault domains are available.
- If an entire site goes offline due to loss of power or network connection, restart the site immediately. Bring all hosts online approximately at the same

time to avoid resynchronizing a large amount of data across the sites.

- If a host is permanently unavailable, remove the host from the cluster before performing any reconfiguration tasks.
- To deploy witnesses for multiple clusters, do not clone a virtual machine that is already configured as a witness. Instead, you can first deploy a VM from OVF, then clone the VM, and configure each clone as a witness host for a different cluster

The stretched cluster network must meet the following requirements.

- The management network requires connectivity across all three sites, using a Layer 2 stretched network or a Layer 3 network.
- The vSAN network requires connectivity across all three sites using a Layer 2 stretched network between the two data sites and a Layer 3 network between the data sites and the witness host..
- The virtual machine network requires connectivity between the data sites, but not the witness host.  
Use a Layer 2 stretched network or Layer 3 network between the data sites. Virtual machines do not require a new IP address following failover to the other site.
- The vMotion network requires connectivity between the data sites, but not the witness host.  
Use a Layer 2 stretched or a Layer 3 network between data sites.

## VSAN Limitations



Limitations of vSAN include the following.

- No support for hosts participating in multiple vSAN clusters.
- No support for vSphere DPM and Storage I/O Control.
- No support for SE Sparse disks.
- No support for RDM, VMFS, diagnostic partition, and other device access features.

## vSAN Space Efficiency

You can use space efficiency techniques in vSAN to reduce the amount of space for storing data. These include the use of any or all of the following:

- Thin provisioning: only consuming the space on disk that is used (and not the total allocated virtual disk space).
- Deduplication: reduction of duplicated data blocks by using SHA-1 hashes for data blocks.
- Compression: compressing data using LZ4, which is a lightweight compression mechanism.
- Erasure Coding: creating a strip of data blocks with a parity block. This is similar to parity with RAID configurations, except it spans ESXi hosts in the cluster, instead of disks in the host.

## SCSI Unmap

SCSI UNMAP commands, which are supported in vSAN 6.7 Update 1 and later, enable you to reclaim storage space that is mapped to deleted vSAN objects. vSAN supports the SCSI UNMAP commands issued within a guest operating system to reclaim storage space. vSAN supports offline unmaps as well as inline unmaps. On Linux OS, offline unmaps are performed with the

`fstrim(8)` command, and inline unmaps are performed when the `mount -o discard` command is used. On Windows OS, NTFS performs inline unmaps by default.

## Deduplication and Compression

All-flash vSAN clusters support deduplication and compression. Deduplication removes redundant data blocks. Compression removes additional redundant data within each data block. Together, these techniques reduce the amount of space required to store data. As vSAN moves data from the cache tier to the capacity tier, it applies deduplication and then applies compression.

You can enable deduplication and compression as a cluster-wide setting, but they are applied on a disk group basis, where redundant data is reduced within each disk group.

When you enable or disable deduplication and compression, vSAN performs a rolling reformat of every disk group on every host, which may take a long time. You should first verify that enough physical capacity is available to place your data. You should minimize how frequently these operations are performed.

**Note**

Deduplication and compression might not be effective for encrypted VMs.

The amount of storage reduction achieved by deduplication and compression depends on many factors, such as the type of data stored and the number of duplicate blocks. Larger disk groups tend to provide a higher deduplication ratio.

## RAID 5 and RAID 6 Erasure Coding

In a vSAN cluster, you can use RAID 5 or RAID 6 erasure coding to protect against data loss while increasing storage efficiency when compared with RAID 1

(mirroring). You can configure RAID 5 on all-flash clusters with four or more fault domains. You can configure RAID 5 or RAID 6 on all-flash clusters with six or more fault domains.

RAID 5 or RAID 6 erasure coding requires less storage space to protect your data than RAID 1 mirroring. For example, if you protect a VM by setting the **Primary level of failures to tolerate (PFTT)** to 1, RAID 1 requires twice the virtual disk size and RAID 5 requires 1.33 times the virtual disk size. You can use [Table 2-7](#) to compare RAID 1 with RAID 5/6 for a 100 GB virtual disk.

**Table 2-7** RAID Configuration Comparison

RAID configuration	PFTT	Data Size	Required Capacity	Usable Capacity
RAID 1 (mirroring)	1	100 GB	200 GB	50%
RAID 5 or RAID 6 (erasure coding) with four fault domains	1	100 GB	133 GB	75%
RAID 1 (mirroring)	2	100 GB	300 GB	33%
RAID 5 or RAID 6 (erasure coding) with six fault domains	2	100 GB	150 GB	67%
RAID 1 (mirroring)	3	100 GB	400 GB	25%
RAID 5 or RAID 6 (erasure coding) with six fault domains	3	N/A	N/A	N/A

Before configuring RAID 5 or RAID 6 erasure coding in a vSAN cluster, you should consider the following.

- All-flash disk groups are required.
- On-disk format version 3.0 or later is required.
- A valid license supporting RAID 5/6 is required.
- You can enable deduplication and compression on the vSAN cluster to achieve additional space savings.
- PFTT must be set to less than 3.

## vSAN Encryption

You can use data at rest encryption in a vSAN cluster, where all data is encrypted after all other processing, such as deduplication, is performed. All files are encrypted, so all virtual machines and their data are protected. Only administrators with encryption privileges can perform encryption and decryption tasks. Data at rest encryption protects data on storage devices in case a device is removed from the cluster.

vSAN encryption requires an external Key Management Server (KMS), the vCenter Server system, and your ESXi hosts. vCenter Server requests encryption keys from an external KMS. The KMS generates and stores the keys, and vCenter Server obtains the key IDs from the KMS and distributes them to the ESXi hosts. The vCenter Server does not store the KMS keys, but keeps a list of key IDs.

vSAN uses encryption keys in the following manner:

- vCenter Server requests an AES-256 Key Encryption Key (KEK) from the KMS.
- vCenter Server stores only the ID of the KEK (not the key itself.)
- The host encrypts disk data using the industry standard AES-256 XTS mode.
- Each disk has a unique, randomly generated Data Encryption Key (DEK).
- A host key is used to encrypt core dumps, not data. All hosts in the same cluster use the same host key.
- When collecting support bundles, a random key is generated to re-encrypt the core dumps. You can specify a password to encrypt the random key.

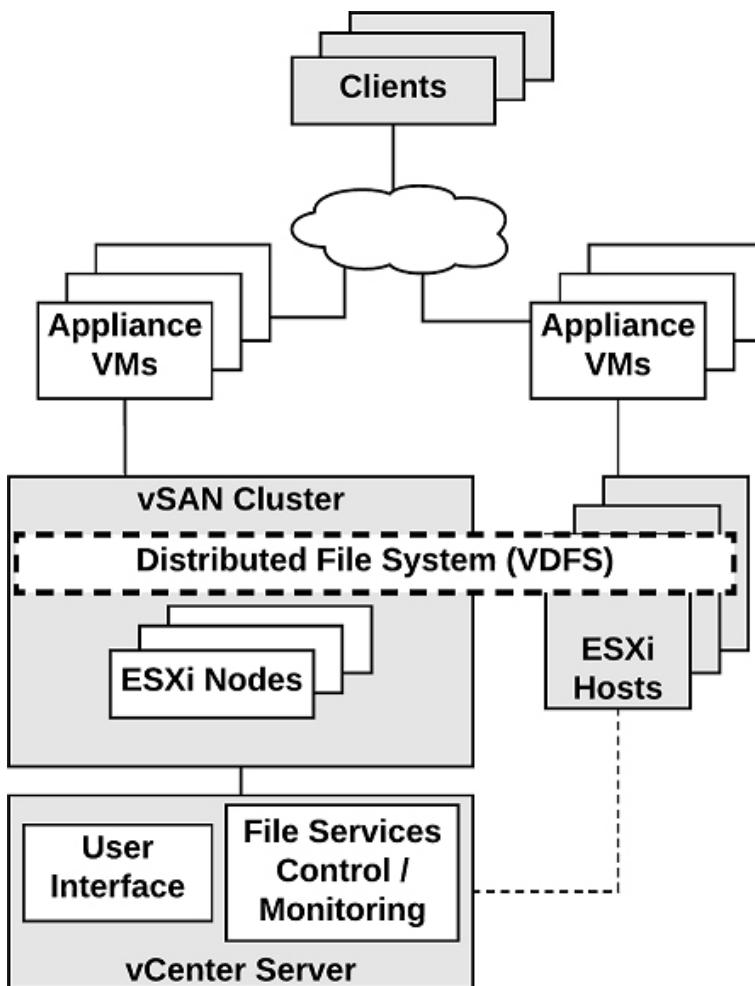
**Note**

Each ESXi host uses the KEK to encrypt its DEKs, and stores the encrypted DEKs on disk. The host does not store the KEK on disk. If a host reboots, it

requests the KEK with the corresponding ID from the KMS. The host can then decrypt its DEKs as needed

## vSAN File Service

You can use the vSAN file service to provide vSAN backed file shares that virtual machines can access as NFSv3 and NFSv4.1 file shares. It uses vSAN Distributed File System (vDFS), resilient file server end points, and a control plane, as illustrated in Figure 2-6. File shares are integrated into the existing vSAN Storage Policy Based Management, and on a per-share basis. The vSAN file service creates a single VDFS for the cluster and places a file service virtual machine (FSVM) on each host. The FSVMs manage file shares and act as NFS file servers using IP address from a static IP Address pool.



## Figure 2-6 vSAN File Service Architecture

The vSAN File Service is not supported on a vSAN stretched cluster.

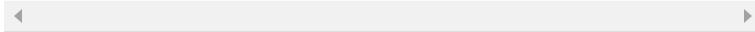
## VSAN Requirements

### VSAN Planning and Sizing

When you plan the capacity for a vSAN datastore, you should consider the PFTT and the failure tolerance method, as illustrated previously in [Table 2-7](#). For RAID-1, the required data store capacity can be calculated using the following formula.

---

Capacity = Expected Consumption Size \* (PFTT +1).



For example, assume you plan to use RAID-1 for a 500 GB virtual disk that you expect to be completely filled, then the required capacity is 1000 GB, 1500 GB, and 2000 GB for PFTT set to 1, 2, and 3, respectively.

The following list are guidelines for vSAN Capacity Sizing.

- Plan for some extra overhead is required depending on the on-disk format version. Version 1.0 adds approximately 1 GB overhead per capacity device. Versions 2.0 and 3.0 adds up to 2% overhead per capacity device. Version 3.0 adds 6.2% overhead for deduplication and compression checksums.
- Keep at least 30 percent unused space to avoid vSAN rebalancing.
- Plan spare capacity to handle potential failure or replacement of capacity devices, disk groups, and hosts.
- Reserve spare capacity to rebuild after a host failure or during maintenance. For example, with PFTT is

set to 1, at least four hosts should be placed in the cluster because at least 3 available hosts are required to rebuild components.

- Provide enough spare capacity to accommodate dynamically changing a VM storage policy, which may require vSAN to create a new RAID tree layout for the object and temporarily consume extra space.
- Plan for the space consumed by snapshots, which inherit the storage policy applied to the virtual disk.
- Plan for space consumed by the VM Home Namespace, which includes the virtual machine's swap file (in vSAN 6.7 and later).

When selecting devices to use for vSAN cache hardware (such as PCIe versus SDD flash devices), in addition to cost, compatibility, performance, and capacity, you should consider write endurance.

When selecting storage controllers for use in a vSAN cluster, in addition to compatibility, you should favorably consider adapters with higher queue depth to facilitate vSAN rebuilding operations. You should configure controllers for passthrough mode rather than RAID mode to simplify configuration and maintenance. You should disable caching on the controller or set it to 100% read.

When sizing the hosts, consider using at least 32-GB memory for full vSAN operations based on 5 disk groups per host and 7 capacity devices per disk group.

## Fault Domains Planning

If you span your vSAN cluster across multiple racks or blade server chassis, you can configure fault domains to protect against failures of a rack or chassis. A fault domain consists of one or more vSAN cluster member hosts sharing some physical characteristic, like being in the same rack or chassis. For example, you can configure

a fault domain to enable a vSAN cluster to tolerate the failures of an entire physical rack as well as the failure of a single host or other component (capacity devices, network link, or network switch) associated with the rack. When a virtual machine is configured with the Primary level of failures to tolerate set to 1 (PFTT=1), vSAN can tolerate a single failure of any kind and of any component in a fault domain, including the failure of an entire rack.

When you provision a new virtual machine, vSAN ensures that protection objects, such as replicas and witnesses, are placed in different fault domains. If you set a virtual machine's storage policy for PFTT=n, vSAN requires a minimum of  $2*n+1$  fault domains in the cluster. A minimum of three fault domains are required to support PFTT=1.

For best results, configure four or more fault domains in the cluster where PFTT=1 is used. A cluster with three fault domains has the same restrictions as a three-host cluster has, such as the inability to reprotect data after a failure and the inability to use the Full data migration mode.

Consider a scenario where you have a vSAN cluster where you plan to place four hosts per rack. To tolerate an entire rack failure, create a fault domain for each rack. To support PFTT=1 use a minimum of 12 hosts deployed to 3 racks. To support Full data migration mode and the ability to re-protect after a failure, deploy a minimum of 16 hosts to 4 racks. If you want the Primary level of failures to tolerate set to 2, configure five fault domains in the cluster.

When working with fault domains, you should consider the following best practices.

- At a minimum, configure three fault domains in the vSAN cluster. For best results, configure four or

more fault domains.

- Each host that is not directly added to a fault domain, resides in its own single-host fault domain.
- You can add any number of hosts to a fault domain. Each fault domain must contain at least one host.
- If you use fault domain, consider creating equal sized fault domains (same number of same-sized hosts).
- When moved to another cluster, vSAN hosts retain their fault domain assignments.

## **Hardware Requirements**

You should examine vSAN section of the *VMware Compatibility Guide* to verify that all the storage devices, drivers, and firmware versions are certified for the specific vSAN version you plan to use. Table 2-8 contains some of the vSAN storage device requirements.

**Table 2-8** vSAN Storage Device Requirements

---

Component	Requirements
Cache	<p>One SAS or SATA solid-state disk (SSD) or PCIe flash device.</p> <p>For a hybrid disk group, the cache device must provide at least 10 percent of the anticipated storage consumed on the capacity devices in a disk group, excluding replicas.</p> <p>The flash devices used for vSAN cache must be dedicated. They cannot be used for vSphere Flash Cache or for VMFS.</p>
Capacity (virtual machine) storage	<p>For a hybrid disk group, make sure that at least one SAS or NL-SAS magnetic disk is available.</p> <p>For an all-flash disk group, make sure at least one SAS or SATA solid-state disk (SSD) or at least one PCIe flash device is available.</p>
Storage controllers	<p>One SAS or SATA host bus adapter (HBA), or a RAID controller that is in passthrough mode or RAID 0 mode.</p> <p>In the scenario where the same storage controller is backing both vSAN and non-vSAN disks, you should apply the following VMware recommendations to avoid issues.</p> <p>Do not mix the controller mode for vSAN and non-vSAN disks. If the vSAN disks are in RAID mode, the non-vSAN disks should also be in RAID mode.</p> <p>If VMFS is used on the non-vSAN disks, then use the VMFS datastore only for scratch, logging, and core dumps.</p> <p>Do not run virtual machines from a disk or RAID group that shares its controller with vSAN disks or RAID groups.</p> <p>Do not pass through non-vSAN disks to virtual machine guests as Raw Device Mappings (RDMs).</p>

The memory requirements for vSAN depend on the number of disk groups and devices that the ESXi hypervisor must manage. Per VMware Knowledge Base (KB) article 2113954, the following formula can be used to calculate vSAN memory consumption.

---

```
vSANFootprint = HOST_FOOTPRINT + NumDiskGroups * Disk
```

where

---

```
DiskGroupFootprint = DISKGROUP_FIXED_FOOTPRINT + DISK
```

The ESXI Installer creates a coredump partition on the boot device, whose default size is typically adequate. If ESXi host memory is 512 GB or less, you can boot the host from a USB, SD, or SATADOM device. When you

boot a vSAN host from a USB device or SD card, the size of the boot device must be at least 4 GB. If ESXi host memory is more than 512 GB, consider the following guidelines.

- You can boot the host from a SATADOM or disk device with a size of at least 16 GB. When you use a SATADOM device, use a single-level cell (SLC) device.
- If you are using vSAN 6.5 or later, you must resize the coredump partition on ESXi hosts to boot from USB/SD devices.

Consider using at least 32-GB memory per host for full vSAN operations based on 5 disk groups per host and 7 capacity devices per disk group. Plan for 10% CPU overhead for vSAN.

## **Cluster Requirements**

You should verify that a host cluster contains a minimum of three hosts that contribute capacity to the cluster. A two host vSAN cluster consists of two data hosts and an external witness host. Ensure that each host that resides in a vSAN cluster does not participate in other clusters.

## **Software Requirements**

For full vSAN capabilities, the participating hosts must be version 6.7 Update 3 or later. vSAN 6.7.3 and later software supports all on-disk formats.

## **Network Requirements**

You should ensure the network infrastructure and configuration support vSAN as described in Table 2-9.

**Table 2-9** vSAN Networking Requirements

---

Component	Requirement
Host Bandwidth	For hybrid configuration, each host requires 1 Gbps (dedicated). For all-flash configuration, each host requires 10 Gbps (dedicated or shared).
Host network	Each vSAN cluster member host cluster (even those that do not contribute capacity) must have a vSAN enabled VMkernel network adapter connected to a Layer 2 or Layer 3 network.
IP version	vSAN supports IPv4 and IPv6.
Network Latency	<p>Maximum Round Trip Time (RTT) between all the member hosts in a standard vSAN clusters is 1 ms.</p> <p>Maximum RTT between the two main sites in a stretched vSAN cluster is 5 ms.</p> <p>Maximum RTT between each main site and the witness host in a stretched cluster is 200 ms.</p>

## License Requirements

You should ensure that you have a valid vSAN license that supports your required features. If you do not need advanced or enterprise features, then a standard license will suffice. An advanced (or enterprise) license is required for advanced features such as RAID 5/6 erasure coding, deduplication, and compression. An enterprise license is required for enterprise features such as encryption and stretched clusters.

The capacity of the license must cover the total number of CPUs in the cluster.

## Other vSAN Considerations

### VSAN Network Best Practices

- For hybrid configurations, use dedicated network adapters (at least 1 Gbps). For best performance use dedicated or shard 10 Gbps adapters.
- For all-flash configurations, use a dedicated or shared 10-GbE physical network adapter.
- Provision one additional physical NIC as a failover NIC.
- If you use a shared 10-GbE network adapter, place the vSAN traffic on a distributed switch with configure Network I/O Control.

## **Boot Devices and VSAN**

You can boot ESXi from a local VMFS on a disk that is not associated with vSAN.

You can boot a vSAN host from a USB/SD device, but you must use a high-quality, 4 GB or larger USB or SD flash drive. If the ESXi host memory is larger than 512 GB, for vSAN 6.5 or later, you must resize the coredump partition on ESXi hosts to boot from USB/SD devices.

You can boot a vSAN host from a SATADOM device, but you must use 16 GB or larger single-level cell (SLC) device.

## **Persistent Logging in a VSAN Cluster**

When you boot ESXi from a USB or SD device, log information and stack traces are lost on host reboot, because the scratch partition is on a RAM drive. You should consider using persistent storage other than vSAN for logs, stack traces, and memory dumps. You could use VMFS or NFS or you could configure the ESXi Dump Collector and vSphere Syslog Collector to send system logs to vCenter Server.

## **VSAN Policies**

Storage policies are used in vSAN to define storage requirements for your virtual machines. These policies determine how to provision and allocate storage objects within the datastore to guarantee the required level of service. You should assign at least one storage policy to each virtual machine in a vSAN datastore. Otherwise, vSAN assigns a default policy with **Primary level of failures to tolerate** set to 1, a single disk stripe per object, and a thin-provisioned virtual disks.

Storage policies, including those specific to vSAN, are covered later in this chapter.

# **VSPHERE STORAGE INTEGRATION**

In a vSphere 7.0 environment, you have several options for integrating with supported storage solutions, including Virtual Volumes (VVols), vSphere APIs for Storage Awareness (VASA), and vSphere API for Array Integration (VAAI).

## **VASA**

Storage vendors or VMware can make use of the vSphere APIs for Storage Awareness (VASA). This is done with a storage provider or VASA provider, which are software components that integrate with vSphere to provide information about the physical storage capabilities. Storage providers are utilized by either ESXi hosts or vCenter to gather information about the storage configuration and status and display it to administrators in the vSphere Client.

- Persistent Storage Providers: these are storage providers that manage storage arrays and handle abstraction of the physical storage. This is used by vVols and vSAN.
- Data Service Providers: This type of provider is used for host-based caching, compression, and encryption.
- Built-in Storage Providers: These are offered by VMware, and usually do not require registration. Examples of these are vSAN and I/O filters included in ESXi installations.
- Third-Party Storage Providers: If a third party is offering a storage provider, it must be registered.

The information that storage providers offer may include the following:

- Storage data services and capabilities. This is referenced when defining a storage policy.
- Storage status including alarms and events.
- Storage DRS information

Unless the storage provider is VMware, the vendor must provide the policy. There are other requirements to implementing storage providers as well:

- Contact your storage vendor for information about deploying the storage provider, and ensure it is deployed correctly.
- Ensure the storage provider is compatible by verifying it with the *VMware Compatibility Guide*.
- Do not install the VASA provider on the same system as vCenter.
- Upgrade storage providers to new versions to make use of new functionalities.
- Unregister and reregister the storage provider when upgrading.

Storage providers must be registered in the vSphere Client to be able to establish a connection between vCenter and the storage provider. VASA is essential when working with vVols, vSAN, vSphere APIs for I/O Filtering (VAIO), and storage VM policies.

**Note**

If vSAN is being used, service providers are registered automatically, and cannot be manually registered.

## VAAI

The vSphere API for Array Integration (VAAI), also known as hardware acceleration or hardware offload APIs, enable ESXi hosts to be able to communicate with storage arrays. They use functions called storage

primitives, which allow offloading of storage operations to the storage array itself. The goal is to reduce overhead and increase performance. This allows storage to be responsible for cloning operations and zeroing out disk files. Without VAAI hardware offloading, the VMkernel Data Mover service is utilized to copy data from the source datastore to the destination datastore, incurring physical network latencies and increasing overhead. The VMkernel will always attempt to offload to the storage array by way of VAAI, but if the offload fails, it will employ its Data Mover service.

The storage primitives were introduced in vSphere 4.1 and applied to Fibre Channel, iSCSI, and FCoE storage only. vSphere 5.0 added primitives for NAS storage and vSphere Thin Provisioning. The following storage primitives are available in vSphere 7.0

## **VAAI Block Primitives**

The following are the VAAI primitives for block storage.

- Atomic Test and Set (ATS): Replaces the use of SCSI reservations on VMFS datastores when updating metadata. With SCSI reservations, only one process can establish a lock on the LUN at a time, leading to contention and SCSI reservation errors. Metadata updates occur whenever a thin provisioned disk grows, a VM is provisioned, or when a vSphere administrator manually grows a virtual disk. With ATS, a lock is placed on a sector of the VMFS datastore when updating metadata. ATS allows larger datastores to be used without running into such contention issues. On storage arrays that do not support VAAI, SCSI reservations will still be used.
- ATS Only Flag: Can be set on VMFS datastores that were created as VMFS5 but cannot be enabled on VMFS5 datastores that were upgraded from

VMFS3. The ATS only flag forces ATS to be used as opposed to SCSI reservations for all metadata updates and operations. Manually enabling the ATS only flag is done via vmkfstools, using the following syntax.

```
vmkfstools -configATSOnly 1 [storage path]
```

- XCOPY (Extended Copy): Allows the VMkernel to offload cloning or Storage vMotion migrations to the storage array, avoiding use of the VMkernel Data Mover service.
- Write Same (Zero): Used with eager zeroed thick virtual disks, allowing the storage device to write the zeroes for this disk. This reduces overhead on the ESXi host in terms of CPU time, DMA buffers and use of the device queue. Write same is utilized whenever you clone a virtual machine with eager zeroed thick disks, whenever a thin-provisioned disk expands, or when lazy zeroed thick disks need to be zeroed out (at first write).

## VAAI NAS Primitives

The following are the VAAI primitives for NAS.

- Full File Clone: Works the same way as XCOPY but applies to NAS storage as opposed to block storage devices.
- Fast File Clone/Native Snapshot Support: Allows snapshot creation to be offloaded to the storage device for use in linked clones used in VMware Horizon View or in vCloud Director, which leverage reading from replica disks and writing to delta disks.
- Extended Statistics: Allows an ESXi host to have insight into space utilization on NAS storage. For example, when a NAS device is using thin

provisioning without the Extended Statistics primitive, the ESXi host would lack visibility of the actual storage usage leading you to run out of space.

- Reserve Space: Allows thick provisioning of virtual disks on NAS datastores. Prior to this primitive, only thin provisioning could be used on NAS storage devices.

### VAAI Thin Provisioning Primitives

If you are using thin-provisioning, and VMs are deleted or migrated off a datastore, the array may not be informed that blocks are no longer in use. Multiple primitives were added in vSphere 5.0 to add better support for Thin Provisioning.

- Thin Provisioning Stun: Prior to vSphere 5.0, if a thin-provisioned datastore reached 100% space utilization, all VMs on that datastore were paused. After the release of vSphere 5.0, only the VMs requiring extra space will be paused, other VMs are not affected.
- Thin Provisioning Space Threshold Warning: When a VM is migrated to a different datastore, or is deleted, the SCSI UNMAP command is used for the ESXi host to tell the storage array that space can be reclaimed. As of vSphere 5.1, this primitive is a manual one, due to performance and timing issues that arose when this was automatically invoked.

### Virtual Volumes (VVols)

With VVols, you have a similar storage operational module as vSAN, while leveraging SAN and NAS arrays. Like with vSAN, you can leverage storage policy-based management (SPBM) with VVols, allowing you to streamline storage operations. The VASA provider communicates with vCenter Server to report the

underlying characteristics of the storage container. You can leverage these characteristics as you create and apply storage policies to virtual machines to optimize the placement and enable the underlying services (such as caching or replication).

The main use case for vVols is to simplify the operational model for virtual machines and their storage. With vVols, the operational model changes from managing space inside datastores to managing abstract storage objects handled by storage arrays.

The major components in vVols are vVol Device, Protocol End Point, Storage Container, VASA Provider and Array. These components are illustrated in Figure 2-7.

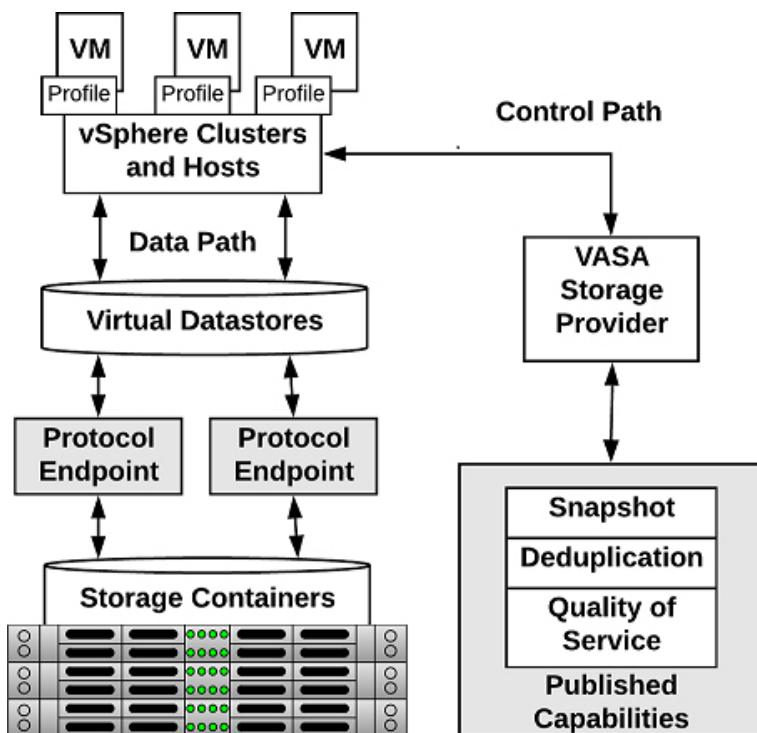


Figure 2-7 vVols Architecture

The following list contains the main characteristics of vVols.

- No File System.

- ESX manages the array through VASA.
- Arrays are logically partitioned into containers, called Storage Containers.
- Virtual Volume Objects are encapsulations of VM files and disks are stored natively on the Storage Containers.
- Storage Containers are pools of raw storage, or aggregations of storage capabilities, which a storage device can provide to vVols.
- I/O from ESXi host to the storage array is addressed through an access point called, Protocol Endpoint (PE).
- PEs are logical I/O proxies, used for communication for vVols and the virtual disk files. These endpoints are used to establish data paths on demand, by binding the ESXi hosts with the PEs.
- Bind requests must sent from ESXi hosts or vCenter Servers to before a vVol can be used.
- Data Services are offloaded to the array. Snapshot, Replication, Encryption.
- vVols are managed through storage policy-based management (SPBM) framework. VM Storage Policies are required for VMs to use vVols.

The following list provides the five type of vVols

- **Config-vVol:** Metadata
- **Data-vVol:** VMDKs
- **Mem-vVol:** Snapshots
- **Swap-vVol:** Swap files
- **Other-vVol:** Vendor solution specific

Limitations of vVols include the following.

- You cannot use vVols with a standalone ESXi host.
- vVols does not support Raw Device Mappings (RDMs).
- A vVols storage container cannot span across different physical arrays.
- Host profiles that contain virtual datastores are vCenter Server specific. A profile created by one vCenter Server cannot be applied by another vCenter Server.

## **STORAGE MULTIPATHING AND FAILOVER**

Multipathing is used for performance and failover. ESXi hosts can balance the storage workload across multiple paths for improved performance. In the event of a path, adapter, or storage processor failure, the ESXi host will failover to an alternate path.

During path failover, virtual machine I/O could be delayed for a maximum of 60 seconds. Active-passive type arrays could experience longer delays than active-active arrays.

- **Fibre Channel Failover:** For multipathing, hosts should have at least two HBAs. This is in addition to redundant fibre channel switches (the switch fabric) and redundant storage processors. If a host has two HBAs, attached to two fibre channel switches, connected to two storage processors, then the datastores attached to the SAN can withstand the loss of any single storage processor, fibre channel switch, or HBA.
- **Host-based Failover with iSCSI:** Similar to Fibre Channel Failover above, hosts should have at least two hardware iSCSI initiators or two NIC

ports used with the software iSCSI initiator. This is in addition to at least two physical switches, and at least two storage processors.

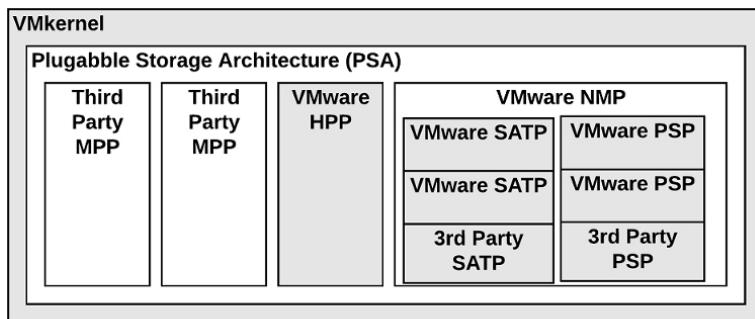
- **Array-based Failover with iSCSI:** On some storage systems, the storage device abstracts the physical ports from the ESXi hosts, and the ESXi hosts only see a single virtual port. This is used by the storage system for load balancing and path failover. If the physical port where the ESXi host is attached should be disconnected, the ESXi host will automatically attempt to reconnect to the virtual port, and the storage device will redirect it to an available port.
- **Path Failover and Virtual Machines:** When a path failover occurs, disk I/O could pause for 30 to 60 seconds. During this time, viewing storage in the vSphere client or virtual machines may appear stalled until the I/O fails over to the new path. In some cases, Windows VMs could fail if the failover is taking too long. VMware recommends increasing the disk timeout inside the guest OS registry to 60 seconds at least to prevent this.

## Pluggable Storage Architecture (PSA)

Pluggable Storage Architecture was introduced in vSphere 4 as a way for storage vendors to provide their own multipathing policies which you can install on ESXi hosts. PSA is based on a modular framework that can make use of third-party multipathing plugins, or MPPs, or utilize the VMware provided native multipathing plugin (NMP), as illustrated in [Figure 2-8](#).

VMware provides generic native multipathing modules, called VMware NMP and VMware HPP. In addition, the PSA offers a collection of VMkernel APIs that third-party developers can use. The software developers can create their own load balancing and failover modules for a

particular storage array. These third-party multipathing modules (MPPs) can be installed on the ESXi host and run in addition to the VMware native modules, or as their replacement. When installed, the third-party MPPs can replace the behavior of the native modules and can take control of the path failover and the load-balancing operations for the specified storage devices.



**Figure 2-8** Pluggable Storage Architecture

### VMware Native Multipathing Plugin



The VMware NMP supports all storage arrays listed on the VMware storage HCL and provides a default path selection algorithm based on the array type. It associates a set of physical paths with a specific storage device (LUN). NMP uses submodules, called Storage Array Type Plug-ins (SATPs) and Path Selection Plug-ins (PSPs).

The NMP performs the following operations.

- Manages physical path claiming and unclaiming.
- Registers and unregisters logical devices.
- Maps physical paths with logical devices.
- Supports path failure detection and remediation.
- Processes I/O requests to logical devices:

- Selects an optimal physical path.
- Performs actions necessary to handle path failures and I/O command retries.
- Supports management tasks, such as reset of logical devices

### **Storage Array Type Plug-ins (SATPs)**

Storage Array Type Plug-ins (SATPs) are submodules of the VMware NMP and are responsible for array-specific operations. The SATP handles path failover for the device. ESXi offers an SATP for every type of array that VMware supports. ESXi also provides default SATPs that support non-specific active-active, active-passive, ALUA, and local devices.

Each SATP performs the array-specific operations required to detect path state and to activate an inactive path. This allows the NMP module to work with multiple storage arrays without being aware of the storage device specifics.

The NMP determines which SATP to use for a specific storage device and maps the SATP with the storage device's physical paths. The SATP implements the following tasks:

- Monitors the health of each physical path.
- Reports changes in the state of each physical path.
- Performs array-specific actions necessary for storage failover. For example, for active-passive devices, it activates passive paths.

Table 2-10 provides details on the native SATP modules.

---

**Table 2-10** SATP Details

SATP	Description
VMW_SATP_LOCAL	SATP for local direct-attached devices.  Supports VMW_PSP_MRU and VMW_PSP_FIXED but not VMW_PSP_RR
VMW_SATP_DEFAULT_AA	Generic SATP for active-active arrays.
VMW_SATP_DEFAULT_AP	Generic SATP for active-passive arrays.
VMW_SATP_ALUA	SATP for ALUA-compliant arrays.

**Note**

You do not need to obtain or download any SATPs. ESXi automatically installs an appropriate SATP for an array you use. Beginning with vSphere 6.5 Update 2, VMW\_SATP\_LOCAL provides multipathing support for the local devices, except the devices in 4K native format. You are no longer required to use other SATPs to claim multiple paths to the local devices.

## Path Selection Plug-ins

VMware Path Selection Plug-ins (PSPs) are submodules of the NMP. PSPs handle path selection for I/O requests for associated storage devices. The NMP assigns a default PSP for each logical device based on the device type. You can override the default PSP.

Each PSP enables and enforces a corresponding path selection policy.

Table 2-11 provides details on the native path selection policies

**Table 2-11** VMware Path Selection Policies

PSP - Policy	Description
VMW_PSP_MRУ - Most Recently Used (VMware)	<p>Initially, MRU selects the first discovered, working path.</p> <p>If the path fails, MRU selects an alternative path and does not revert to the original path when that path becomes available.</p> <p>MRU is default for most active-passive storage devices</p>
VMW_PSP_FIXED - Fixed (VMware)	<p>FIXED uses the designated preferred path, if it is working. If the preferred path fails, FIXED selects an alternative available path, but reverts to the preferred path when it becomes available again.</p> <p>FIXED is the default policy for most active-active storage devices.</p>
VMW_PSP_RR - Round Robin (VMware)	<p>RR uses an automatic path selection algorithm rotating through the configured paths. RR sends a set of I/O down the first path, sends the next I/O set down the next path, and continues sending the next I/O set down the next path, until all paths are used, and the pattern repeats beginning with the first path. Effectively, this allows all the I/O from a specific host to use the aggregated bandwidth of multiple paths to a specific storage device.</p> <p>Both active-active and active-passive arrays use RR. With active-passive arrays, RR uses active paths. With active-active arrays, RR uses available paths.</p> <p>The latency mechanism that is activated for the policy by default makes it more adaptive. To achieve better load balancing results, the mechanism dynamically selects an optimal path by considering the I/O bandwidth and latency for the path.</p> <p>RR is the default policy for many arrays.</p>

## PSA Summary

To summarize, the PSA performs the following tasks:

- Loads and unloads multipathing plug-ins.
- Hides virtual machine specifics from a particular plug-in.
- Routes I/O requests for a specific logical device to the MPP managing that device.
- Handles I/O queueing to the logical devices.
- Implements logical device bandwidth sharing between virtual machines.
- Handles I/O queueing to the physical storage HBAs.
- Handles physical path discovery and removal.

- Provides logical device and physical path I/O statistics.

The following process occurs when VMware NMP receives an I/O request for one of its managed storage devices.

1. The NMP calls the appropriate PSP
2. The PSP selects an appropriate physical path.
3. The NMP issues the I/O request on the select path.
4. If the I/O operation is successful, the NMP reports its completion.
5. If the I/O operation reports an error, the NMP calls the appropriate SATP.
6. The SATP interprets the errors and, when appropriate, activates the inactive paths.
7. The PSP selects a new path for the I/O.

When coordinating the VMware native modules and any installed third-party MPPs, the PSA performs the following tasks:

- Loading and unloading MPPs.
- Hides virtual machine specifics from MPPs.
- Routes I/O requests for a specific logical device to the appropriate MPP.
- Handles I/O queueing to the logical devices.
- Shares logical device bandwidth between virtual machines.
- Handles I/O queueing to the physical storage HBAs.

## STORAGE POLICIES

Storage policies can be used to define which datastores to use when placing virtual machines disk. The following storage policies can be created:

- VM Storage Policy for Host-Based Data Services:  
These policies are rules for services which are offered by the ESXi hosts, such as encryption.
- VM Storage Policy for vVols: These policies allow you to set rules for VMs that apply to vVols datastores. This can include storage devices that are replicated for disaster recovery purposes or have specific performance characteristics.
- VM Storage Policy for Tag-Based Placement: You can create custom policies for VMs and custom tags for storage devices. This is helpful for storage arrays that do not support VASA and their storage characteristics are not visible to the vSphere client. For example, you could create a tag named Gold that you use to identify your best performing storage.

## **Storage Policy Based Management**

You can define a required policy for a VM, such as requiring it to reside on fast storage. You can then utilize the vSphere API for Storage Awareness (VASA) or define storage tags manually. Then a VM can only be placed on a storage device matching the requirements.

## **Virtual Disk Types**

When creating a virtual disk, you need to determine how you are going to allocate space to that virtual disk. The way space is allocated to a virtual disk is through writing zeroes, typically referred to as zeroing out the file. For example, if you wanted to create a 20 GB virtual disk and allocate all of the space up front, a VMDK file is created, and 20 GB worth of zeroes are written to that file. You can determine when the zeroes get written:

- Eager zeroed thick: The disk space for the virtual disk files is allocated and erased (zeroed) out at time of creation. If the storage device supports VAAI, this operation can be offloaded to the storage array. Otherwise, the VMkernel writes the zeroes, which could be slow. This method is the slowest for virtual disk creation, but the best for guest performance.
- Lazy zeroed thick: The disk space for the virtual disk files is allocated at the time of creation, but not zeroed. Each block is zeroed, on demand at run time, prior to presenting it to the guest OS for the first time. This increases the time required for disk format operations and software installations in the guest OS..
- Thin provisioned: The disk space for the virtual disk files is not allocated or zeroed at creation time. The space is allocated and zeroed on demand. This method is the fastest for virtual disk creation, but the worst for guest performance.

## vSAN Specific Storage Policies

vSAN storage policies define how VM objects are placed and allocated on vSAN to meet performance and redundancy requirements. [Table 2-12](#) defines the vSAN storage policies and their definitions.

**Table 2-12** vSAN Storage Policies

---

<b>Policy</b>	<b>Description</b>
Primary level of failures to tolerate (PFTT)	<p>This setting defines how many host and device failures a VM object can withstand. For <math>n</math> failures tolerated, data is stored in <math>n+1</math> location. This includes parity copies in the event of RAID 5 or 6. If no storage policy is selected at time of provisioning a VM, this policy is assigned by default. In the event of fault domains being used, <math>2n+1</math> fault domains, each with hosts adding to the capacity, are required. If an ESXi host isn't in a fault domain, it is considered to be in a single-host fault domain.</p> <p>Default = 1 Maximum = 3</p>
Secondary level of failures to tolerate (SFTT)	<p>In stretched clusters, this policy defines how many additional host failures can be tolerated after a site failure's PFTT has been reached. IN the event of PFTT = 1 and SFTT = 2, and one site is inaccessible, then two more host failures can be tolerated.</p> <p>Default = 1 Maximum = 3</p>
Data Locality	<p>If Primary level of failures to tolerate is set to 0, this option is available. The options for this policy are: None, Preferred, or Secondary. This allows objects to be limited to one site, or one host in stretched clusters.</p> <p>Default = None</p>
Failure tolerance method	<p>Defines if the data replication mechanism is optimized for performance or capacity. If RAID-1 (Mirroring) - Performance is selected, there will be more space consumed in the object placement, but better performance for accessing them. If RAID-5/6 (Erasure Coding) - Capacity is selected, there will be less disk utilization, but performance will be reduced.</p>
Number of disk stripes per object	<p>This policy determines the number of capacity devices where each VM object replica is striped. Setting this above 1 can improve performance but consumes more resources.</p> <p>Default = 1 Maximum = 12</p>
Flash read cache reservation	<p>The amount of flash capacity which is reserved for read caching of VM objects. This is defined as a percentage of the size of the VMDK. This is only supported in hybrid vSAN clusters.</p> <p>Default = 0% Maximum = 100%</p>
Force provisioning	<p>If set to yes, this policy forces provisioning of objects, even when policies cannot be met.</p> <p>Default = no</p>
Object space reservation	<p>Percentage of VMDK object that must be thick provisioned on deployment. The options are as follows:</p> <ul style="list-style-type: none"> <li>Thin provisioning (default value)</li> <li>25% reservation</li> <li>50% reservation</li> <li>75% reservation</li> <li>Thick provisioning</li> </ul>
Disable object checksum	<p>Checksum is used end-to-end in validating the integrity of the data to ensure data copies are the same as the original. In the event of a mismatch, incorrect data is overwritten. If set to yes, checksum is not calculated.</p> <p>Default = no</p>
IOPS limit for object	Sets a limit for IOPs of an object. If set to 0, there is no limit.

## STORAGE DRS (SDRS)

You can use vSphere Storage DRS (SDRS) to manage the storage resources of a datastore cluster. A datastore cluster is a collection of datastores with shared resources and a shared management interface. SDRS provides the following capabilities for a datastore cluster.

## **Initial Placement and Ongoing Balancing**

SDRS provides recommendations for initial virtual machine placement and ongoing balancing operations in a datastore cluster. Optionally, SDRS can automatically perform the recommended placements and balancing operations. Initial placements occur when the virtual machine is being created or cloned, when a virtual machine disk is being migrated to another datastore cluster, or when you add a disk to an existing virtual machine. SDRS makes initial placement recommendations (or automatically performs the placement) based on space constraints and SDRS settings (such as space and I/O thresholds).

## **Space Utilization Load Balancing**

You can set a threshold for space usage to avoid filling a datastore to its full capacity. When space usage on a datastore exceeds the threshold, SDRS generates recommendations or automatically performs Storage vMotion migrations to balance space usage across the datastore cluster.

## **I/O Latency Load Balancing**

You can set an I/O latency threshold to avoid bottlenecks. When I/O latency on a datastore exceeds the threshold, SDRS generates recommendations or automatically performs Storage vMotion migrations to balance I/O across the datastore cluster.

SDRS is invoked at the configured frequency (by default, every eight hours) or when one or more datastores in a datastore cluster exceeds the user-configurable space utilization thresholds. When Storage DRS is invoked, it checks each datastore's space utilization and I/O latency values against the threshold. For I/O latency, Storage DRS uses the 90th percentile I/O latency measured over the course of a day to compare against the threshold.

## SDRS Automation Level

Table 2-13 describes the available SDRS automation levels.

**Table 2-13** SDRS Automation Levels

Option	Description
No Automation (Manual Mode)	Placement and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Partially Automated	Placement recommendations run automatically, and migration recommendations are displayed, but do not run until you manually apply the recommendation.
Fully Automated	Placement and migration recommendations run automatically.

## SDRS Thresholds and Behavior



You can control the behavior of SDRS by specifying thresholds. You can use the following standard thresholds to set the aggressiveness level for Storage DRS.

- **Space Utilization:** SDRS generates recommendations or performs migrations when the percentage of space utilization on the datastore is greater than the threshold you set in the vSphere Client.
- **I/O Latency:** SDRS generates recommendations or performs migrations when the 90th percentile

I/O latency measured over a day for the datastore is greater than the threshold.

- **Space utilization difference:** SDRS can use this threshold to ensure that there is some minimum difference between the space utilization of the source and the destination, prior to making a recommendation. For example, if the space used on datastore A is 82% and datastore B is 79%, the difference is 3. If the threshold is 5, Storage DRS will not make migration recommendations from datastore A to datastore B.
- **I/O load balancing invocation interval:** After this interval, SDRS runs to balance I/O load.
- **I/O imbalance threshold:** Lowering this value makes I/O load balancing less aggressive. Storage DRS computes an I/O fairness metric between 0 and 1, with 1 being the fairest distribution. I/O load balancing runs only if the computed metric is less than  $1 - (\text{I/O imbalance threshold} / 100)$ .

## SDRS Recommendations

For datastore clusters, where SDRS automation is set to manual mode (no automation), SDRS makes as many recommendations as necessary to enforce SDRS rules, balance the space, and balance the I/O resources of the datastore cluster. Each recommendation includes the virtual machine name, the virtual disk name, the datastore cluster name, the source datastore, the destination datastore, and a reason for the recommendation.

SDRS makes mandatory recommendations when the datastore is out of space, anti-affinity or affinity rules are being violated, or the datastore is entering maintenance mode. SDRS makes optional recommendations are made when a datastore is close to running out of space or when

adjustments should be made for space and I/O load balancing.

SDRS considers moving powered on and powered off virtual machines for space balancing. Storage DRS considers moving powered-off virtual machines with snapshots for space balancing.

## **Anti-affinity Rules**

If you want to ensure a set of virtual machines are stored on separate datastores, you could create anti-affinity rules for the virtual machines. Alternatively, you can use an affinity rule to place a group of virtual machines on the same datastore.

By default, all virtual disks belonging to the same virtual machine are placed on the same datastore. If you want to separate the virtual disks of a specific virtual machine on separate datastores, you can do so with an anti-affinity rule

## **Datastore Cluster Requirements**

Datastore clusters can contain a mix of datastores having different sizes, I/O capacities, and storage array backing. However, the following types of datastores cannot coexist in a datastore cluster.

- NFS and VMFS datastores cannot be combined in the same datastore cluster.
- Replicated datastores cannot be combined with non-replicated datastores in the same Storage-DRS-enabled datastore cluster.
- All hosts attached to the datastores in a datastore cluster must be ESXi 5.0 and later. If datastores in the datastore cluster are connected to ESX/ESXi 4.x and earlier hosts, Storage DRS does not run.

- Datastores shared across multiple data centers cannot be included in a datastore cluster.
- As a best practice, all datastores in a datastore cluster should have identical hardware acceleration (enabled or disabled) settings.

## NIOC, SIOC, and SDRS

In vSphere, you can use Network I/O Control (NIOC), Storage I/O Control (SIOC) and Storage Distributed Resource Scheduler (SDRS) to manage I/O. These features are often confused by people in the VMware community. [Table 2-14](#) contains a brief description of each feature along with the chapter in this book where you can find more detail.

**Table 2-14** Comparing NIOC, SIOC, and SDRS

Feature	Description	Chapter
NIOC	Allows you to allocate network bandwidth to business-critical applications and to resolve situations where several types of traffic compete for common resources.	9
SIOC	Allows you to control the amount of storage I/O that is allocated to virtual machines during periods of I/O congestion by implementing shares and limits.	11
SDRS	Allows you to control the balance the usage of storage space and I/O resources across the datastores in a datastore cluster.	11

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, Chapter X, "Final Preparation," and the exam simulation questions on the CD-ROM.

## Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page.

**Table 2-15** lists a reference of these key topics and the page numbers on which each is found.

**Table 2-15** Key Topics

Key Topic Element	Description	Page Number
Paragraph	Paragraph Raw Device Mapping	
Figure 2-5	A Two-Node vSAN cluster	
Paragraph	Paragraph vSAN Stretched Cluster	
List	List vSAN Limitations	
Paragraph	Paragraph Native Multipathing Plugin	
Figure 2-7	vVols Architecture	
Paragraph	Paragraph SDRS Thresholds and Behavior	

## DEFINITIONS OF KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary:

RDM

I/O Filter

Disk Group

Witness Host

vSAN File Service

vVols

Virtual Volume

## Glossary

**RDM:** An RDM is a mapping file containing metadata that resides in a VMFS datastore and acts as a proxy for a physical storage device (LUN), allowing a virtual machine to access the storage device directly.

**I/O Filter:** I/O filters are software components that can be installed on ESXi hosts and can offer additional data services to virtual machines.

Disk Group: A disk group is a group of local disks on an ESXi host contributing to the vSAN datastore.

Witness Host: A witness host is a stretched vSAN component that consists only of metadata and serves as a tiebreaker.

vSAN File Service: The vSAN File service provides vSAN backed file shares that virtual machines can access as NFSv3 and NFSv4.1 file shares.

vVOLs: vVOLs is an integration and management framework that virtualizes SAN/NAS arrays, enabling a more efficient operational model,

Virtual Volume: Virtual volumes are encapsulations of virtual machine files, virtual disks, and their derivatives that are stored natively inside a storage system.

## **COMPLETE THE TABLES AND LISTS FROM MEMORY**

Print a copy of Appendix B, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

## **REVIEW QUESTIONS**

- 1.** You are deploying datastores in a vSphere environment and want to use the latest VMFS version that supports ESXi 6.5 and ESXi 7.0. Which version should you use?
  - a.** VMFS 3
  - b.** VMFS 4
  - c.** VMFS 5

**d. VMFS 6**

- 2.** You are preparing to manage and troubleshoot a vSAN environment. Which of the following is a command-line interface that provides a cluster-wide view and is included with the vCenter Server deployment?
- a.** VMware PowerCLI
  - b.** vSAN Observer
  - c.** Ruby vSphere Console
  - d.** ESXCLI
- 3.** You want to integrate vSphere with your storage system. Which of the following provides software components that integrate with vSphere to provide information about the physical storage capabilities?
- a.** VASA
  - b.** VAAI
  - c.** SATP
  - d.** NMP
- 4.** Which of the following is the default path selection policy for most active-passive storage devices?
- a.** VMW\_PSP\_MRU
  - b.** VMW\_PSP\_FIXED
  - c.** VMW\_PSP\_RR
  - d.** VMW\_PSP\_AP
- 5.** You are deploying virtual machines in a vSphere environment. Which virtual disk configuration provides the best performance for the guest OS?
- a.** Thin provisioned

- b.** Thick eager zeroed
- c.** Thick lazy zeroed
- d.** Thin eager zeroed

# **Chapter 3. Network Infrastructure [This content is currently in development.]**

**This content is currently in development.**

# Chapter 4. Clusters and High Availability

This chapter covers the following topics:

- Cluster Concepts / Overview
- Distributed Resources Scheduler (DRS)
- vSphere High Availability (HA)
- Other Resource Management and Availability Features

This chapter contains information related to VMware 2V0-21.20 exam objectives 1.6, 1.6.1, 1.6.2, 1.6.3, 1.6.4, 1.6.4.1, 4.5, 4.6, 5.1, 5.1.1, 5.2, 7.5, 7.11.5

This chapter introduces vSphere 6.7, describes its major components, and identifies its requirements.

## “DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section.

Regardless, the authors recommend that you read the entire chapter at least once. Table 4-1 outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 4-1** “Do I Know This Already?” Section-to-Question Mapping

---

Foundation Topics Section	Questions
Cluster Concepts and Overview	1
Distributed Resource Scheduler (DRS)	2,3,4
vSphere High Availability (HA)	5,6,7
Other Resource Management and Availability Features	8,9,10

**Caution**

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** You are configuring EVC mode in a vSphere cluster that uses Intel hardware. Which of the following values should you choose to set the EVC mode to the lowest level that includes the SSE4.2 instruction set?
  - a.** Merom
  - b.** Penryn
  - c.** Nehalem
  - d.** Westmere
  
- 2.** In vSphere 7.0, you want to configure the DRS Migration Threshold such that it is at the minimum level at which the virtual machine happiness is considered. Which of the following values should you choose?
  - a.** Level 1
  - b.** Level 2
  - c.** Level 3
  - d.** Level 4
  - e.** Level 5
  
- 3.** Which of the following is not a good use for Resource Pools in DRS?

- a.** To delegate control and management
  - b.** To impact the use of network resources
  - c.** To impact the use of CPU resources
  - d.** To impact the use of memory resources
- 4.** You need your resource pool to use a two-pass algorithm to divvy reservations. In the second pass, excess pool reservation is divvied proportionally to virtual machines (limited by virtual machine size). Which step should you take?
  - a.** Ensure vSphere 6.7 or higher is used
  - b.** Ensure vSphere 7.0 or higher is used
  - c.** Enable scalable shares
  - d.** Enable expandable reservations
- 5.** You are configuring vSphere HA in a cluster. You want to configure the cluster to use a specific host as a target for failovers. Which setting should you use?
  - a. Host failures cluster tolerates**
  - b. Define host failover capacity by > Cluster resource percentage**
  - c. Define host failover capacity by > Slot Policy (powered-on VMs)**
  - d. Define host failover capacity by > Dedicated failover hosts**
  - e. Define host failover capacity by > Disabled**
- 6.** You are enabling VM Monitoring in your vSphere HA cluster. You want to set the monitoring level such that its failure interval is

60 seconds. Which of the following options should you choose?

**a.** High

**b.** Medium

**c.** Low

**d.** Normal

**7.** You are configuring Virtual Machine Component Protection (VMCP) in a vSphere HA cluster. Which of the following statements are true?

**a.** For PDL and APD failures, you can control the restart policy for virtual machines, by setting it to conservative or aggressive.

**b.** For PDL failures, you can control the restart policy for virtual machines, by setting it to conservative or aggressive.

**c.** For APD failures, you can control the restart policy for virtual machines, by setting it to conservative or aggressive.

**d.** For PDL and APD failures, you cannot control the restart policy for virtual machines

**8.** You want to use Predictive DRS. What is the minimum vSphere Version you need?

**a.** vSphere 6.0

**b.** vSphere 6.5

**c.** vSphere 6.7

**d.** vSphere 7.0

**9.** You are configuring vSphere Fault Tolerance (FT) in your vSphere 7.0 environment. What is the maximum number for virtual CPUs you can use with FT-protected virtual machine?

**a. 1**

**b. 2**

**c. 4**

**d. 8**

**10.** You are concerned about service availability for your vCenter Server. Which of the following statements are true?

- a.** If a vCenter service fails, VMware Service Lifecycle Manager restarts it.
- b.** If a vCenter service fails, VMware Lifecycle Manager restarts it.
- c.** If a vCenter service fails, vCenter Server HA restarts it.
- d.** VMware Service Lifecycle Manager is a part of the PSC.

## **CLUSTER CONCEPTS AND OVERVIEW**

A vSphere cluster is a set of ESXi hosts that are intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit. In addition to creating a cluster, assigning a name, and adding ESXi objects, you can enable and configure features on a cluster, such as vSphere Distributed Resource Scheduler (DRS), VMware Enhanced vMotion Compatibility (EVC), Distributed Power Management (DPM), vSphere High Availability (HA), and vSAN.

In the vSphere Client, you can manage and monitor the resources in a cluster as a single object. You can easily monitor and manage the hosts and virtual machines in the DRS cluster.

If you enable VMware EVC on a cluster, you can ensure that migrations with vMotion do not fail because of CPU compatibility errors. If you enable vSphere DRS on a cluster, you can allow automatic resource balancing using the pooled host resources in the cluster. If you enable vSphere HA on a cluster, you can allow rapid virtual machine recovery from host hardware failures using the cluster's available host resource capacity. If you enable DPM on a cluster, you can provide automated power management in the cluster. If you enable vSAN on a cluster, you utilize a logical SAN that is built upon a pool of drives attached locally to the ESXi hosts in the cluster.

You can use the Quickstart workflow in the vSphere Client to create or configure a cluster. The Quickstart page provides three cards, Cluster Basics, Add Hosts, and Configure Cluster. For an existing cluster, you can use Cluster Basics to change the cluster name and enable cluster services, such as DRS and vSphere HA. You can use the Add Hosts card to add hosts to the cluster. You can use the Configure Cluster card to configure networking and other settings on the hosts in the cluster.

Additionally, in vSphere 7.0 you can configure a few general settings for the cluster. For example, when you create a cluster you, even if you do not enable DRS, vSphere, HA or vSAN, you can choose an option to manage all hosts in the cluster with a single image. With this option, all hosts in a cluster inherit the same image, which reduces variability between hosts, improves your ability to ensure hardware compatibility, and simplifies upgrades. This feature requires hosts to already be ESXi

7.0 or above. It replaces baselines. Once enabled, baselines cannot be used in this cluster.

**Note**

Do not confuse a vSphere cluster with a datastore cluster. In vSphere, datastore clusters and vSphere (host) clusters are separate objects. Although you can directly enable a vSphere cluster for vSAN, DRS and vSphere HA, you cannot directly enable it for datastore clustering. You create datastore clusters separately. See [Chapter 2, "Storage Infrastructure,"](#) for details on datastore clusters.

## Enhanced vMotion Compatibility (EVC)

Enhanced vMotion Compatibility (EVC) is a cluster setting that can improve CPU compatibility between hosts for supporting vMotion. vMotion migrations are live migrations that require compatible instruction sets for source and target processors used by the virtual machine. The source and target processors must come from the same vendor class (AMD or Intel) to be vMotion compatible. Clock speed, cache size, and number of cores can differ between source and target processors. When you start a vMotion migration, or a migration of a suspended virtual machine, the wizard checks the destination host for compatibility and displays an error message if problems exist. Using EVC, you can allow vMotion between some processors that would normally be incompatible.

The CPU instruction set that is available to virtual machine guest OS is determined when the virtual machine is powered on. This CPU feature set is based on the following items:

- Host CPU family and model
- Settings in the BIOS that might disable CPU features
- ESX/ESXi version running on the host
- The virtual machine's compatibility setting

- The virtual machine's guest operating system

EVC ensures that all hosts in a cluster present the same CPU feature set to virtual machines, even if the actual CPUs on the hosts differ. EVC is a cluster setting that you can enable and configure the EVC Mode with a baseline CPU feature set. EVC ensures that hosts in cluster uses the baseline feature set when presenting an instruction set to a guest OS. EVC uses AMD-V Extended Migration technology (for AMD hosts) and Intel FlexMigration technology (for Intel hosts) to mask processor features, allowing hosts to present the feature set of an earlier generation of processor. You should configure the EVC mode to accommodate the host with the smallest feature set in the cluster.

The EVC requirements for hosts include the following.

- ESXi 6.5 or later
- Hosts must be attached to a vCenter Server
- CPUs must be from a single vendor, either Intel or AMD.
- If the AMD-V, Intel-VT, AMD NX, or Intel XD features are available in the BIOS, enable them.
- Supported CPUs for EVC Mode per the VMware Compatibility Guide.

**Note**

You can apply a custom CPU compatibility mask to hide host CPU features from a virtual machine, but this is not recommended by VMware.

You can configure the EVC settings using the **Quickstart > Configure Cluster** workflow in the vSphere Client. You can also configure EVC directly in the cluster settings. The options for **VMware EVC** are **Disable EVC**, **Enable EVC for AMD Hosts**, and **Enable EVC for Intel Hosts**.

If you choose **Enable EVC for Intel Hosts**, then you can set the **EVC Mode** to one of the options described in [Table 4-2](#).

**Table 4-2** EVC Modes for Intel

Level	EVC Mode	Description
L0	Intel "Merom"	Smallest Intel feature set for EVC mode.
L1	Intel "Penryn"	Includes the Intel "Merom" feature set and exposes additional CPU features including SSE4.1.
L2	Intel "Nehalem"	Includes the Intel "Penryn" feature set and exposes additional CPU features including SSE4.2 and POPCOUNT.
L3	Intel "Westmere"	Includes the Intel " Nehalem " feature set and exposes additional CPU features including AES and PCLMULQDQ.
L4	Intel "Sandy Bridge"	Includes the Intel " Westmere " feature set and exposes additional CPU features including AVX and XSAVE.
L5	Intel "Ivy Bridge"	Includes the Intel " Sandy Bridge" feature set and exposes additional CPU features including RDRAND, ENFSTRG, FSGSBASE, SMEP, and F16C..
L6	Intel "Haswell"	Includes the Intel " Ivy Bridge" feature set and exposes additional CPU features including ABMX2,AVX2, MOVBE, FMA, PERMD, RORX/MULX, INVPCID, VMFUNC.
L7	Intel "Broadwell"	Includes the Intel " Haswell" feature set and exposes additional CPU features including Transactional Synchronization Extensions, Supervisor Mode Access Prevention, Multi-Precision Add-Carry Instruction Extensions, PREFETCHW and RDSEED
L8	Intel "Skylake"	Includes the Intel " Broadwell" feature set and exposes additional CPU features including Advanced Vector Extensions 512, Persistent Memory Support Instructions, Protection Key Rights, Save Processor Extended States with Compaction, and Save Processor Extended States Supervisor
L9	Intel "Cascade Lake"	Includes the Intel " Skylake" feature set and exposes additional CPU features including VNNI and XGETBV with ECX = 1.

If you choose **Enable EVC for AMD Hosts**, then you can set the **EVC Mode** to one of the options described in [Table 4-3](#).

**Table 4-3** EVC Modes for AMD

Level	EVC Mode	Description
A0	AMD Opteron Generation 1	Smallest AMD feature set for EVC mode.
A1	AMD Opteron Generation 2	Includes the AMD "Generation 1" feature set and exposes additional CPU features including CPMXCHG16B and RDTSCP.
A3	AMD Opteron Generation 3	Includes the AMD "Generation 2" feature set and exposes additional CPU features including SSE4A, MisAlignSSE, POPCOUNT and ABM (LZCNT).
A2, B0	AMD Opteron Generation 3 (no 3DNow!)	Includes the AMD "Generation 3" feature set without 3DNow support.
B1	AMD Opteron Generation 4	Includes the AMD "Generation 3 no3DNow" feature set and exposes additional CPU features including SSSE3, SSE4.1, AES, AVX, XSAVE, XOP, and FMA4.
B2	AMD Opteron "Piledriver"	Includes the AMD "Generation 4" feature set and exposes additional CPU features including FMA, TBM, BMI1, and F16C.
B3	AMD Opteron "Steamroller"	Includes the AMD "Piledriver" feature set and exposes additional CPU features including XSAVEOPT RDFSBASE, RDGSBASE, WRFSBASE, WRGSBAS and FSGSBASE.
B4	AMD "Zen"	Includes the AMD "Steamroller" feature set and exposes additional CPU features including RDRAND, SMEP, AVX2, BMI2, MOVBE, ADX, RDSEED, SMAP, CLFLUSHOPT, XSAVES, XSAVEC, SHA, and CLZERO
B5	AMD "Zen 2"	Includes the AMD "Zen" feature set and exposes additional CPU features including CLWB, UMP, RDPID, XGETBV with ECX = 1, WBNOINV, and GMET.

## vSAN Services

You can enable DRS, vSphere HA, and vSAN at the cluster level. The following sections provide details on DRS and vSphere HA. For details on vSAN, see [Chapter 2](#).

## DISTRIBUTED RESOURCE SCHEDULER (DRS)

Distributed Resource Scheduler (DRS) distributes compute workload in a cluster, by strategically placing virtual machines during power on operations and live migrating (vMotion) virtual machines (VMs) when necessary. DRS provides many features and settings that enable you to control its behavior.

You can set the DRS Automation Mode for a cluster to one of the following.

- **Manual:** DRS does not automatically place or migrate virtual machines. It only makes recommendations.
- **Partially Automated:** DRS automatically places virtual machines as they power on. It makes recommendations for virtual machine migrations.
- **Fully Automated:** DRS automatically places and migrates virtual machines.

You can override the automation mode at the virtual machine level.

## Recent DRS Enhancements

Beginning in vSphere 6.5, VMware has added many improvements to DRS. For example, in vSphere 7.0, DRS runs once every minute rather than every 5 minutes in older DRS versions. The new DRS tends to recommend smaller (memory) virtual machines for migration to facilitate faster vMotion migrations, where the old DRS tends to recommend large virtual machines to minimize the number of migrations. The old DRS uses an imbalance metric that is derived from the standard deviation of load across the hosts in the cluster. The new DRS focuses on virtual machine happiness. The new DRS is much lighter and faster than the old DRS.

The new DRS recognizes vMotion has an expensive operation and accounts for it in its recommendations. In a cluster where virtual machines are frequently powered on the workload is volatile, avoids continuously migrating virtual machines. To this, DRS calculates the gain duration for live migrating a virtual machine and considers the gain duration when making recommendations.

The following sections provide details on other recent DRS enhancements.

## Network-Aware DRS



In vSphere 6.5, DRS considers the utilization of host network adapters during initial placements and load balancing, but it does not balance the network load. Instead, its goal is to ensure that the target host has sufficient available network resources. It works by eliminating hosts with saturated networks from the list of possible migration hosts. The threshold used by DRS for network saturation is 80% by default. When DRS cannot migrate VMs due to network saturation, the result may be an imbalanced cluster.

In vSphere 7.0, DRS uses a new cost modeling algorithm, which is flexible and now balances network bandwidth along with CPU and memory usage.

## Virtual Machine Distribution

Starting in vSphere 6.5, you can enable an option to distribute a more even number of virtual machines across hosts. The main use case is to improve availability. The primary goal of DRS remains unchanged, which is to ensure that all VMs are getting the resources they need and that the load is balanced in the cluster. But with this new option enabled, DRS will also try to ensure that the number of virtual machines per host is balanced in the cluster.

## Memory Metric for Load Balancing

Historically, vSphere uses the Active Memory metric for load balancing decisions. In vSphere 6.5 and 6.7, you have the option to set DRS to load balance based on Consumed Memory. In vSphere 7.0, the Granted Memory metric is used for load balancing and no cluster option is available to change the behavior.

## **Virtual Machine Initial Placement**

Starting with vSphere 6.5, DRS uses a new initial placement algorithm that is faster, lighter, and more effective than the previous algorithm. In earlier versions, DRS takes a snapshot of the cluster state when making virtual machine placement recommendations. In the algorithm, DRS does not snapshot the cluster state, allowing faster and more accurate recommendations. With the new algorithm, DRS powers on virtual machines much faster. In vSphere 6.5, the new placement feature is not supported for the following configurations.

- Clusters where DPM, Proactive HA, or HA Admission Control is enabled
- Clusters with DRS configured in manual mode
- Virtual machines with manual DRS override setting
- Virtual machines that are FT-enabled
- Virtual machines that are part of a vApp

In vSphere 6.7, the new placement is available for all configurations.

## **Enhancements to the Evacuation Workflow**

Prior to vSphere 6.5, when evacuating a host that is entering maintenance mode, DRS waited to migrate templates and powered-off virtual machines until after the completion of vMotion migrations, leaving those objects unavailable for use for a long time. Starting in vSphere 6.5, DRS prioritizes the migration of virtual machine templates and powered-off virtual machines over powered-on virtual machines, making those objects available for use without waiting on vMotion migrations.

Prior to vSphere 6.5, the evacuation of powered off virtual machines was inefficient. Starting in vSphere 6.5, these evacuations occur in parallel, making use of up to

100 re-register threads per vCenter Server. This means that you may see only a small difference when evacuating up to 100 virtual machines.

Starting in vSphere 6.7, DRS is more efficient in evacuating powered-on virtual machines from a host that is entering maintenance mode. Instead of simultaneously initiating vMotion for all the powered-on VMs on the host as in previous versions, DRS initiates vMotion migrations in batches of 8 at a time. Each vMotion batch of vMotion is issued after the previous batch completes. The vMotion batching makes the entire workflow more controlled and predictable.

### **DRS Support for NVM**

Starting in vSphere 6.7, DRS supports virtual machines running on next generation persistent memory devices, known as Non-Volatile Memory (NVM) devices. NVM is exposed as a datastore that is local to the host. Virtual machines can use the datastore as an NVM device exposed to the guest (Virtual Persistent Memory or vPMem) or as a location for a virtual machine disk (Virtual Persistent Memory Disk or vPMemDisk). DRS is aware of the NVM devices used by virtual machines and guarantees the destination ESXi host has enough free persistent memory to accommodate placements and migrations.

### **How DRS scores VMs**



Historically, DRS balanced the workload in a cluster based on host compute resource usage. In vSphere 7.0, DRS balances the workload based on virtual machine happiness. A virtual machine's DRS score is a measure of its happiness, which is a measure of the resources available for consumption by the virtual machine. The

higher the DRS score for a VM, the better its resource availability. DRS moves virtual machines to improve their DRS scores. DRS also calculates a DRS score for the cluster, which is a weighted sum of the DRS scores of all the cluster's virtual machines.

In Sphere 7.0, DRS calculates the core for each virtual machine on each ESXi host in the cluster every minute. Simply put, DRS logic computes an ideal throughput (demand) and an actual throughput (goodness) for each resource (CPU, memory, and network) for each virtual machine. The virtual machine's efficiency for a particular resource is ratio of the goodness over the demand. A virtual machine's DRS score (total efficiency) is the product of its CPU, memory, and network efficiencies.

When calculating the efficiency, DRS applies resource costs. For CPU resources, DRS includes costs for CPU cache, CPU ready, and CPU tax. For memory resources, DRS includes costs for memory burstiness, memory reclamation, and memory tax. For network resources, DRS includes a network utilization cost.

DRS compares a virtual machine's DRS score for the current host on which it runs. DRS determines if another host can provide a better DRS score for the virtual machine. If so, DRS calculates the cost for migrating the virtual machine to the host and factors that score into its load balancing decision.

## DRS Rules

You can configure rules to control the behavior of DRS.

A **VM-Host affinity rule** specifies whether the members of a selected virtual machine DRS group can run on the members of a specific host DRS group. Unlike a virtual machine to virtual machine affinity rule, which specifies affinity (or anti-affinity) between individual virtual machines, a VM-Host affinity rule specifies an

affinity relationship between a group of virtual machines and a group of hosts. There are *required* rules (designated by "must") and *preferential* rules (designated by "should".)

A VM-Host affinity rule includes the following components.

- One virtual machine DRS group.
- One host DRS group.
- A designation of whether the rule is a requirement ("must") or a preference ("should") and whether it is affinity ("run on") or anti-affinity ("not run on").

**A VM-VM affinity rule** specifies whether selected individual virtual machines should run on the same host or be kept on separate hosts. This type of rule is used to create affinity or anti-affinity between individual virtual machines. When an affinity rule is created, DRS tries to keep the specified virtual machines together on the same host. You might want to do this, for example, for performance reasons.

**With an anti-affinity rule**, DRS tries to keep the specified virtual machines apart. You could use such a rule if you want to guarantee that certain virtual machines are always on different physical hosts. In that case, if a problem occurs with one host, not all virtual machines would be at risk. You can create VM-VM affinity rules to specify whether selected individual virtual machines should run on the same host or be kept on separate hosts.

**VM-VM Affinity Rule Conflicts** can occur when you use multiple VM-VM affinity and VM-VM anti-affinity rules. If two VM-VM affinity rules are in conflict, you cannot enable both. For example, if one rule keeps two virtual machines together and another rule keeps the same two virtual machines apart, you cannot enable both

rules. Select one of the rules to apply and disable or remove the conflicting rule. When two VM-VM affinity rules conflict, the older one takes precedence and the newer rule is disabled. DRS only tries to satisfy enabled rules and disabled rules are ignored. DRS gives higher precedence to preventing violations of anti-affinity rules than violations of affinity rules.

**Note**

A VM-VM rule does not allow the “should” qualifier. You should consider these as “must” rules.

## DRS Migration Sensitivity

Prior to vSphere 7.0, DRS used a Migration Threshold to determine when virtual machines should be migrated to balance the cluster workload. In vSphere 7.0, DRS does not consider cluster standard deviation for load balancing. Instead, it is designed to be more virtual machine centric and workload centric, rather than cluster centric. You can set the DRS Migration Sensitivity to one of the following values.



- **Level 1** – DRS only makes recommendations to fix rule violations or to facilitate a host entering maintenance mode.
- **Level 2** - DRS expands on Level 1 by making recommendations in situations that are at, or close to, resource contention. It does not make recommendations just to improve virtual machine happiness or cluster load distribution.
- **Level 3** – (Default Level) DRS expands on Level 2 by making recommendations to improve VM happiness and cluster load distribution.

- **Level 4** - DRS expands on Level 3 by making recommendations for occasional bursts in the workload and reacts to the sudden load changes.
- **Level 5** - DRS expands on Level 4 by making recommendations dynamic, greatly varying workloads. DRS reacts to the workload changes every time.

## Resource Pools

Resource pools are container objects in the vSphere inventory that are used to compartmentalize the CPU and memory resources of a host, a cluster, or a parent resource pool. Virtual machines run in and draw resources from resource pools. You can create multiple resource pools as direct children of a standalone host or a DRS cluster. You cannot create child resource pools on host that has been added to a cluster or on a cluster that is not enabled for DRS.

You can use resource pools much like a folder to organize virtual machines. You can delegate control over each resource pool to specific individuals and groups. You can monitor resources and set alarms on resource pools. If you need a container just for organization and permission purposes, consider using a folder. If you also need resource management, then consider using a resource pool. You can assign resource settings, such as shares, reservations, and limits to resource pools.

## Use Cases

You can use resource pools to compartmentalize a cluster's resources and then use the resource pools to delegate control to individuals or organizations. Table 4-4 provides some use cases for resource pools.

**Table 4-4** Resource Pool Use Cases

---

Use Case	Details
Flexible hierarchical organization	Add, remove, modify, and reorganize resource pools as needed.
Resource isolation	Cluster administrators can use resource pools to allocate resources to separate departments, in a manner where changes in a pool do not unfairly impact other departments.
Access control and delegation	A cluster administrator can use permissions to delegate activities, such as virtual machine creation and management, to other administrators
Separation of resources from hardware	In a DRS cluster, administrators can perform resource management independently of the actual hosts.
Managing multi-tier applications.	You can manage the resources for a group of virtual machines (in a specific resource pool), which is easier than managing resources per virtual machine.

## Shares, Limits, and Reservations

You can configure CPU and Memory shares, reservations, and limits on resource pools, as explained in [Table 4-5](#).

**Table 4-5** Shares, Limits, and Reservations

Option	Description
Shares	<p>Shares specify the relative importance of a virtual machine or a resource pool. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources. Shares can be thought of as priority under contention.</p> <p>Shares are typically set to <b>High</b>, <b>Normal</b>, or <b>Low</b> and these values specify share values with a 4:2:1 ratio, respectively. You can also select Custom and assign a specific number of shares (which expresses a proportional weight).</p> <p>The resource pool uses its shares to compete for the parent's resources and is allocated a portion based on the ratio of the pool's shares compared with its siblings. Siblings share the parent's resources according to their relative share values, bounded by the reservation and limit.</p> <p>For example, consider a scenario where a cluster has two child resource pools with normal CPU shares, another child resource pool with high CPU shares, and no other child objects. During periods of contention, each of the pools with normal shares would get access to 25 % of cluster's CPU resources and the pool with high shares would get access to 50%.</p>
Reservation	<p>A reservation specifies the guaranteed minimum allocation for a virtual machine or a resource pool. A CPU reservation is expressed in MHz and a memory reservation is expressed in MB. You can power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine. If the virtual machine starts, then it is guaranteed that amount even when the physical server is heavily loaded.</p> <p>For example, if you configure the CPU reservation for each virtual machine as 1 GHz, you will be able to start 8 VMs in a resource pool where the CPU reservation is set for 8 GHz and expandable reservations are disabled. But you will not be able to start additional virtual machines in the pool.</p> <p>You can use reservations to guarantee a specific amount of resources for a resource pool. The default value for a resource pool's CPU or memory reservation is 0. If you change this value, it is subtracted from the unreserved resources of the parent. The resources are considered reserved, regardless of whether virtual machines are associated with the resource pool.</p>
Expandable Reservation	<p>You can enable expandable reservations to effectively allow a child resource pool to borrow from its parent. When enabled (which is the default setting), expandable reservations are considered during admission control. When powering on a virtual machine, if the resource pool does not have sufficient unreserved resources, the resource pool can use resources from its parent or ancestors.</p> <p>For example, in a resource pool where 8 GHz is reserved and expandable reservations is disabled, you try to start 9 virtual machines each with 1 GHz, but the last virtual machine does not start. If you enable expandable reservation in the resource pool and its parent pool (or cluster) has sufficient unreserved CPU resources, you can start the ninth virtual machine.</p>
Limit	<p>A limit specifies an upper bound for CPU or memory resources that can be allocated to a virtual machine or a resource pool.</p> <p>You can set a limit on the amount of CPU and memory allocated to a resource pool. The default is unlimited.</p> <p>For example, if you power on multiple, CPU intensive virtual machines in a resource pool, where the CPU Limit is 10 GHz, then collectively, the virtual machines will not be able to utilize more than 10 GHz CPU resources, regardless of the pool's reservation settings, the pool's share settings, or the amount of available resources in the parent.</p>

Table 4-6 provides the CPU and memory share values for virtual machines when using the High, Normal, and Low settings. The corresponding share values for a resource pool are equivalent to a virtual machine with four vCPUs and 16 GB memory.

**Table 4-6** Virtual Machine Shares

Setting	CPU Share Value	Memory Share Value
High	2000 per vCPU	20 per MB
Normal	1000 per vCPU	10 per MB
Low	500 per vCPU	5 per MB

**Note**

For example, the share values for a resource pool configured with Normal CPU Shares and High Memory Shares are  $(4 \times 1000)$  4000 CPU shares and  $(16 * 1024 * 20)$  327,680 Memory shares

**Note**

The relative priority represented by each share changes with the addition and removal of virtual machines in a resource pool or cluster. It also changes as you increase or decrease the Shares on a specific virtual machine or resource pool.

## Enhanced Resource Pool Reservation

Starting in vSphere 6.7, DRS uses a new two-pass algorithm to divvy resource reservations to its children. In the old divvying model will not reserve more resources than the current demand, even when the resource pool is configured with a higher reservation. When a spike in virtual machine demand occurs after resource divvying is completed, DRS does not make the remaining pool reservation available to the virtual machine, until the next divvying operation occurs. As a result, a virtual machine's performance may be temporarily impacted. In the new divvying model, each divvying operation uses two passes. In the first pass, the resource pool reservation is divvied based on virtual machine demand. In the second pass, excess pool reservation is divvied proportionally, limited by the virtual machine's

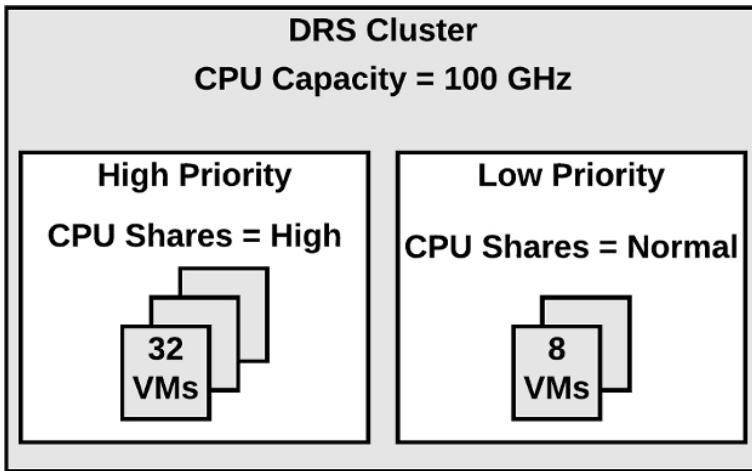
configured size, which reduces the performance impact due to virtual machine spikes.

## Scalable Shares



Another new DRS feature in vSphere 7.0 is scalable shares. Its main use case is the scenario where you want to use shares to give high priority resource access to a set of virtual machines in a resource pool, without concern for the relative number of objects in the pool compared to other pools. With standard shares, each pool in a cluster competes for resource allocation with its siblings based on the share ratio. With scalable shares, the allocation for each pool factors in the number of objects in the pool.

For example, consider a scenario where a cluster with 100 GHz CPU capacity has High Priority resource pool and a Low Priority resource pool with CPU Shares set to High and Normal, respectively as shown in [Figure 4-1](#). This means that the share ratio between the pools is 2:1, so the High Priority pool is effectively allocated twice the CPU resources as the Low Priority pool, whenever CPU contention exists in the cluster. The High Priority Pool is allocated 66.7 GHz and the Low Priority Pool is effectively allocated 33.3 GHz. 40 virtual machines of equal size are running in the cluster, with 32 in the High Priority pool and 8 in the Low Priority pool. The virtual machines are all demanding CPU resources causing CPU contention in the cluster. In the High Priority pool, each virtual machine is allocated 2.1 GHz. In the Low Priority pool, each virtual machine is allocated 4.2 GHz.



**Figure 4-1** Scalable Shares Example

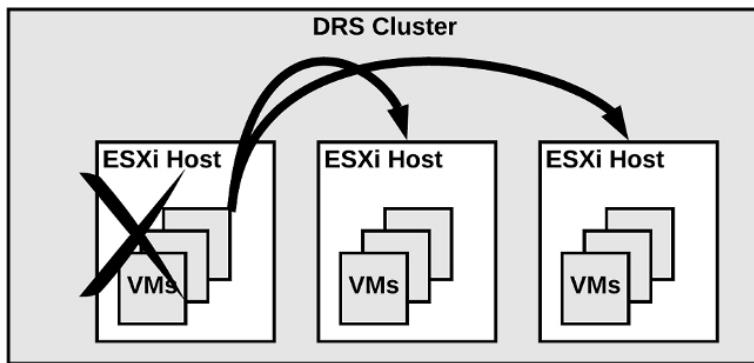
If you want to change the resource allocation such that each virtual machine in the High Priority pool is effectively allocated more resource than the virtual machines in the Low Priority Pool, then you can use scalable shares. If you enable scalable shares in the cluster, then DRS effectively allocates resources to the pools based on the Shares settings and the number of virtual machines in the pool. In this example, the CPU Shares for the pools provide a 2:1 ratio. Factoring this with the number of virtual machines in each pool, the allocation ratio between the High Priority pool and Low Priority pool is 2 times 32 to 1 times 8, or simply 8:1, respectively. The High Priority Pool is allocated 88.9 GHz and the Low Priority pool is allocated 11.1 GHz. Each virtual machine in the High Priority pool is allocated 2.8 GHz. Each virtual machine in the Low Priority pool is allocated 1.4GHz.

## VSPHERE HIGH AVAILABILITY (HA)

vSphere HA is a cluster service that provides high availability for the virtual machines running in the cluster. You can enable vSphere High Availability (HA) on a vSphere cluster to provide rapid recovery from

outages and cost-effective high availability for applications running in virtual machines. vSphere HA provide application availability in the following ways:

- It protects against a server failure by restarting the virtual machines on other hosts within the cluster when a host failure is detected, as illustrated in [Figure 4-2](#).
- It protects against application failure by continuously monitoring a virtual machine and resetting it if a failure is detected.
- It protects against datastore accessibility failures by restarting affected virtual machines on other hosts which still have access to their datastores.
- It protects virtual machines against network isolation by restarting them if their host becomes isolated on the management or vSAN network. This protection is provided even if the network has become partitioned.



**Figure 4-2** vSphere HA Host Failover

Benefits of vSphere HA over traditional failover solutions include:

- Minimal configuration
- Reduced hardware cost
- Increased application availability

- DRS and vMotion integration

vSphere HA can detect the following types of host issues.

- Failure: A host stops functioning
- Isolation: A host cannot communicate with any other hosts in the cluster.
- Partition: A host loses network connectivity with the master host.

When you enable vSphere HA on a cluster, the cluster elects one of the hosts to act as the master host. The master host communicates with vCenter Server to report cluster health. It monitors the state of all protected virtual machines and subordinate hosts. It uses network and datastore heartbeating to detect failed hosts, isolation, and network partitions. vSphere HA takes appropriate actions to respond to host failures, host isolation, and network partitions. For host failures, the typical reaction is to restart the failed virtual machines on surviving hosts in the cluster. If a network partition occurs, a master is elected in each partition. If a specific host is isolated, vSphere HA takes the predefined host isolation action, which may be to shut down or power down the host's virtual machines. If the master fails, the surviving hosts elect a new master. You can configure vSphere to monitor and respond to virtual machine failures, such as guest OS failures, by monitoring heartbeats from VMware Tools.

**Note**

Although vCenter Server is required to implement vSphere HA, the health of the HA cluster is not dependent on vCenter Server. If vCenter Server fails, vSphere HA still functions. If vCenter Server is offline when a host fails, vSphere HA can failover the impacted virtual machines.

## vSphere HA Requirements

## Key Topic

- The cluster must have at least two hosts, licensed for vSphere HA.
- Hosts must use static IP addresses, or guarantee that IP addresses assigned by DHCP persist across host reboots.
- Each host must have at least one, preferably two, management networks in common.
- To ensure that virtual machines can run any host in the cluster, the hosts must access the networks and datastores.
- To use VM Monitoring, install VMware Tools in each virtual machine.
- IPv4 or IPv6 can be used.

### Note

The Virtual Machine Startup and Shutdown (automatic startup) feature is disabled and unsupported for all virtual machines residing in a vSphere HA cluster.

## vSphere HA Response to Failures

You can configure how a vSphere HA cluster should respond to different types of failures, as described in [Table 4-7](#).

## Key Topic

**Table 4-7** vSphere HA Response to Failure Settings

Option	Description
<b>Host Failure Response &gt; Failure Response</b>	If <b>Enabled</b> , the cluster responds to host failures by restarting virtual machines. If <b>Disabled</b> , host monitoring is turned off and the cluster does not respond to host failures.
<b>Host Failure Response &gt; Default VM Restart Priority</b>	Provides the order in which virtual machines are restarted when the host fails. (Higher priority machines first)
<b>Host Failure Response &gt; VM Restart Priority Condition</b>	A condition that must be met before HA restarts the next priority group.
<b>Response for Host Isolation</b>	Provides the action that you want to occur if a host becomes isolation. You can choose <b>Disabled</b> , <b>Shutdown and restart VMs</b> , or <b>Power off and restart VMs</b> .
<b>VM Monitoring</b>	Provides the sensitivity ( <b>Low</b> , <b>High</b> , or <b>Custom</b> ) to which vSphere HA responds to lost VMware Tools Heartbeats.
<b>Application Monitoring</b>	Provides the sensitivity ( <b>Low</b> , <b>High</b> , or <b>Custom</b> ) to which vSphere HA responds to lost VMware Tools Heartbeats.

**Note**

If multiple hosts fail, the virtual machines one failed host migrate first in order of priority, followed by virtual machines from the next host.

## Heartbeats

The master host and subordinate hosts exchange network heartbeats every second. When the master host stops receiving these heartbeats from a subordinate host, it checks for ping responses or the presences of datastore heartbeats from the subordinate host. If the master host does not receive a response after checking for a subordinate host's network heartbeat, ping, or datastore heartbeats, it declares that the subordinate host has failed. If the master host detects datastore heartbeats for a subordinate host, but no network heartbeats or ping responses, it assumes the subordinate host is isolated or in a network partition.

If any host is running, but no longer observes network heartbeats, it attempts to ping the set of cluster isolation addresses. If those pings also fail, the host declares itself to be isolated from the network.

## vSphere HA Admission Control

Admission control is used by vSphere when you power on a virtual machine. It checks the amount of unreserved compute resources and determines whether it can

guarantee any reservation that is configured for the virtual machine is configured. If so, it allows the virtual machine to power on. Otherwise, it generates an **Insufficient Resources** warning.

vSphere HA Admission Control is a setting that you can use to specify whether virtual machines can be started if they violate availability constraints. The cluster reserves resources so that failover can occur for all running virtual machines on the specified number of hosts. When you configure vSphere HA Admission Control, you can set options described in Table 4-8.

**Table 4-8** vSphere HA Admission Control Options

Option	Description
<b>Host failures cluster tolerates</b>	The maximum number of host failures for which the cluster guarantees failover.
<b>Define host failover capacity by &gt; Cluster resource percentage</b>	The percentage of the cluster's compute resources to reserve as spare capacity to support failovers
<b>Define host failover capacity by &gt; Slot Policy (powered-on VMs)</b>	A slot size policy that covers all powered on VMs
<b>Define host failover capacity by &gt; Dedicated failover hosts</b>	Designated hosts to use for failover actions.
<b>Define host failover capacity by &gt; Disabled</b>	Disable admission control.
<b>Performance degradation VMs tolerate</b>	The percentage of performance degradation the VMs in the cluster are allowed to tolerate during a failure

If you disable vSphere HA Admission control, then you enable the cluster to allow virtual machines to power on regardless of whether they violate availability constraints. In the event of a host failover, you may discover that vSphere HA cannot start some virtual machines.

In vSphere 6.5, the default admission control setting is changed to **Cluster Resource Percentage**, which reserves a percentage of the total available CPU and memory resources in the cluster. For simplicity, the percentage is now calculated automatically by defining the number of host failures to tolerate (FTT). The

percentage is dynamically changed as hosts are added or removed from the cluster. Another new enhancement is the **Performance Degradation VMs Tolerate** setting, which controls the amount of performance reduction that is tolerated after a failure. A value of 0% indicates that no performance degradation is tolerated.

With the slot policy option, vSphere HA admission control ensures that a specified number of hosts can fail, leaving sufficient resources in the cluster to accommodate the failover of the impacted virtual machines. Using the slot policy, when you perform certain operations, such as powering on a virtual machine, vSphere HA applies admission control in the following manner

- HA calculates the slot size, which is a logical representation of memory and CPU resources. By default, it is sized to satisfy the requirements for any powered-on virtual machine in the cluster. For example, it is sized to accommodate the virtual machine with the greatest CPU reservation and the virtual machine with the greatest memory reservation.
- HA determines how many slots each host in the cluster can hold.
- HA determines the Current Failover Capacity of the cluster, which is the number of hosts that can fail and still leave enough slots to satisfy all the powered-on virtual machines.
- HA determines whether the Current Failover Capacity is less than the Configured Failover Capacity (provided by the user).
- If it is, admission control disallows the operation.

If your cluster has a few virtual machines with much larger reservations than the others, they will distort slot

size calculation. To remediate this, you can specify an upper bound for the CPU or memory component of the slot size by using advanced options. You can also set a specific slot size (CPU size and memory size). See the next section for advanced options that impact the slot size.

## vSphere HA Advanced Options

You can set vSphere HA advanced options using the vSphere Client or in the `fdm.cfg` file on the hosts. Table 4-9 provides some of the available vSphere HA advanced options.

**Table 4-9** vSphere HA Advanced Options

Option	Description
<code>das.isolationaddressX</code>	Provides the addresses to use to test for host isolation, when no heartbeats are received from other hosts in the cluster. If this option is not specified (default setting), the management network default gateway is used to test for isolation. To specify multiple addresses, you can set <code>das.isolationAddressX</code> , where X is a number between 0 and 9.
<code>das.usedefaultisolationaddress</code>	Specifies whether to use the default gateway IP address for isolation tests.
<code>das.isolationshutdowntimeout</code>	For scenarios where the host's isolation response is Shut down, this setting specifies the period of time that the virtual machine is permitted to shut down before the system powers it off.
<code>das.slotmeminmb</code>	Defines the maximum bound on the memory slot size.
<code>das.slotcpuinmhz</code>	Defines the maximum bound on the CPU slot size.
<code>das.vmmemoryminmb</code>	Defines the default memory resource value assigned to a virtual machine whose memory reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy.
<code>das.vmcpuminmhz</code>	Defines the default CPU resource value assigned to a virtual machine whose CPU reservation is not specified or zero. This is used for the Host Failures Cluster Tolerates admission control policy. If no value is specified, the default is 32MHz.
<code>das.heartbeatdsperhost</code>	Changes the required number (2 to 5) of heartbeat datastores required per host. Default is 2.
<code>das.config.fdm.isolationPolicyDelaySec</code>	The number of seconds the system delays before executing the isolation policy after determining that a host is isolated. The minimum is 30. Lower values result in 30 seconds delay.
<code>das.respectvmvmanitaffinityrules</code>	Determines if vSphere HA should enforce VM-VM anti-affinity rules, even when DRS is not enabled.

## Virtual Machine Settings

To use the **Host Isolation Response > Shutdown and restart VMs** setting, you must install VMware Tools in the virtual machine. If a guest OS fails to shutdown 300 seconds (or value specified by `das.isolationshutdowntimeout`), the virtual machine is powered off.

You can override the cluster's settings for **Restart Priority** and **Isolation Response** per virtual machine. For example, you may want to prioritize virtual machines providing infrastructure services like DNS or DHCP.

At the cluster level, you can create dependencies between groups of virtual machines. You can create VM groups, Host Groups, and dependency rules between the groups. In the rules, you can specify that one VM group cannot be restarted another specific VM group is started.

## VM Component Protection (VMCP)

Virtual Machine Component Protection (VMCP) is a vSphere HA feature that can detect datastore accessibility issues and provide remediation for impacted virtual machines. When a failure occurs, such that a host can no longer access the storage path for a specific datastore, vSphere HA can respond by taking actions such as creating event alarms or restarting virtual machine on other hosts. The main requirements are that vSphere HA is enabled in the cluster and that ESX 6.0 or later is used on all hosts in the cluster.

The types of failure detected by VMCP are Permanent Device Loss (PDL) and All Paths Down (APD). PDL is an unrecoverable loss of accessibility to the storage device that cannot be fixed without powering down the virtual machines. APD is a transient accessibility loss or other issue that is recoverable.

For PDL and APD failures, you can set VMCP to either issue event alerts or to power off and restart virtual

machines. For APD failures only, you can additionally control the restart policy for virtual machines, by setting it to conservative or aggressive. With the conservative setting, the virtual machine will only be powered off if HA determines that it can be restarted on another host.

## Virtual Machine and Application Monitoring

VM Monitoring restarts specific virtual machines if their VMware Tools heartbeats are not received within a specified time. Likewise, Application Monitoring can restart a virtual machine if the heartbeats from a specific application in the virtual machine are not received. If you enable these features, you can configure the monitoring settings to control the failure interval and reset period.

The settings are described in [Table 4-10](#).

**Table 4-10** VM Monitoring Settings

Setting	Failure Interval	Reset Period
High	30 seconds	1 hour
Medium	60 seconds	24 hours
Low	120 seconds	7 days

The **Maximum per-VM resets** setting can be used to configure the maximum number of times vSphere HA will attempt to restart a specific failing virtual machine within the reset period.

## vSphere HA Best Practices

You should provide network path redundancy between cluster nodes. To do so, you can use NIC Teaming for the virtual switch. You can also create a second management network connection using a separate virtual switch.

When performing disruptive network maintenance operations on the network used by clustered ESXi host,

you should suspend the Host Monitoring feature to ensure vSphere HA does not falsely detect network isolation or host failures. You can re-enable host monitoring after completing the work.

To keep vSphere HA agent traffic on specified network, you should ensure the VMkernel virtual network adapters used for HA heartbeats (enabled for **Management traffic**) do not share the same subnet as VMkernel adapters used for vMotion and other purposes.

Use the `das.isolationaddressX` advanced option to add an isolation addresses for each management network.

## Proactive HA

Proactive HA integrates with select hardware partners to detect degraded components and evacuate VMs from affected vSphere hosts before an incident causes a service interruption. Hardware partners offer a vCenter Server plug-in to provide the health status of the system memory, local storage, power supplies, cooling fans, and network adapters. As hardware components become degraded, Proactive HA determines which hosts are at risk and places them into either Quarantine or Maintenance mode. When a host enters Maintenance mode, DRS evacuates its virtual machines to healthy hosts and the host is not used to run virtual machines. When a host enters Quarantine mode, DRS leaves the current virtual machines running on the host but avoids placing or migrating virtual machines to the host. If you prefer that Proactive HA simply makes evacuation recommendations rather than automatic migrations, you can set the **Automation Level** to **Manual**.

The vendor provided health providers read sensor data in the server and provide the health state to vCenter

Server. The health states are Healthy, Moderate Degradation, Severe Degradation, and Unknown.

## **OTHER RESOURCE MANAGEMENT AND AVAILABILITY FEATURES**

### **Predictive DRS**

Since vSphere 6.5, Predictive DRS is a feature that leverages the predictive analytics of vRealize Operations (vROps) Manager and vSphere DRS. Together, these two products can provide workload balancing prior to the occurrence of resource utilization spikes and resource contention. Nightly, vROps calculates dynamic thresholds, which are used to create forecasted metrics for the future utilization of virtual machines. vROps passes the predictive metrics to vSphere DRS to determine the best placement and balance of virtual machines before resource utilization spikes occur. Predictive DRS helps prevent resource contention on hosts that run virtual machines with predictable utilization patterns.

Prerequisites include the following:

- vCenter Server 6.5 or later.
- Predictive DRS must be configured and enabled in both vCenter Server and vROps.
- The vCenter Server and vROps clocks must be synchronized.

### **Distributed Power Management (DPM)**

The vSphere Distributed Power Management (DPM) feature enables a DRS cluster to reduce its power consumption by powering hosts on and off, as needed,

based on cluster resource utilization. DPM monitors the cumulative virtual machine demand for memory and CPU resources in the cluster and compares this to the available resources in the cluster. If sufficient excess capacity is found, vSphere DPM directs the host to enter standby mode. When DRS detects a host is entering standby mode, it evacuates the virtual machines. Once the host is evacuated, DPM powers it off and the host is in standby mode. When DPM determines that capacity is inadequate to meet the resource demand, DPM brings a host out of standby mode by powering it on. Once the host exits standby mode, DRS migrates virtual machines to it.

To power on a host, DPM can use one of three power management protocols, which are Intelligent Platform Management Interface (IPMI), Hewlett-Packard Integrated Lights-Out (iLO), or Wake-On-LAN (WOL). If a host supports multiple protocols, they are used in the following order: IPMI, iLO, WOL. If a host does not support one of these protocols, then DPM cannot automatically bring a host out of standby mode.

DPM is very configurable. Like DRS, you can set its automation to be manual or automatic.

**Note**

Do not disconnect a host in standby mode or remove it from the DRS cluster without first powering it on. Otherwise, vCenter Server is not able to power the host back on.

To configure IPMI or iLO settings for a host, you can edit the host's Power Management settings. You should provide credentials for the BMC account, the IP address of the appropriate NIC, and the MAC address of the NIC.

To use WOL with DPM, you must meet the following prerequisites.

- ESXi 3.5 or later

- vMotion is configured
- The vMotion NIC must support WOL
- The physical switch port must be set to auto negotiate the link speed.

Before enabling DPM, use the vSphere Client to request the host to enter Standby Mode. After the host powers down, right-click the host and attempt to power on. If this is successful, you can allow the host to participate in DPM. Otherwise, you should disable the power management for the host.

You can enable DPM in the DRS Cluster's settings. You can set its **Automation Level** to **Off**, **Manual** or **Automatic**. When set to off, DPM is disabled. When set to manual, DPM makes recommendations only. When set to automatic, DPM automatically performs host power operations as needed.

Much like DRS you can control the aggressiveness of DPM (DPM threshold) with a slider bar in the vSphere Client. The DRS threshold and the DPM threshold are independent. You can override automation settings per host. For example, for a 16 host cluster, perhaps you would feel more comfortable if you set DPM Automation to Automatic on only 8 of the hosts.

## Fault Tolerance (FT)

If you have virtual machines that require continuous availability as opposed to high availability, you can consider protecting the virtual machines with vSphere Fault Tolerance (FT). FT provides continuous availability for a virtual machine (the Primary VM) by ensuring that the state of a Secondary VM is identical at any point in the instruction execution of the virtual machine.

If the host running the Primary VM fails, an immediate and transparent failover occurs. The Secondary VM

becomes the Primary VM host without losing network connections or in-progress transactions. With transparent failover, there is no data loss and network connections are maintained. The failover is fully automated and occurs even if vCenter Server is unavailable. Following the failover, FT spawns a new Secondary VM and re-establishes redundancy and protection, assuming that a host with sufficient resources is available in the cluster. Likewise, if the host running the Secondary VM fails, a new Secondary VM is deployed. vSphere Fault Tolerance can accommodate symmetric multiprocessor (SMP) virtual machines with up to 8 vCPUs.

Use cases for FT include the following.

- Applications that require continuous availability, especially those with long-lasting client connections that need to be maintained during hardware failure.
- Custom applications that have no other way of being clustering.
- Cases where other clustering solutions are available but are too complicated or expensive to configure and maintain.

Before implementing FT, consider the following requirements.



- CPUs must be vMotion compatible
- CPUs support Hardware MMU virtualization.
- Low latency, 10 Gbps network for FT logging

- VMware recommends a minimum of two physical NICs.
- Virtual machine files, other than VMDK files, must be stored on shared storage
- vSphere Standard License for FT protection of virtual machines with up to two virtual CPUs
- vSphere Enterprise Plus License for FT protection of virtual machines with up to eight virtual CPUs
- Hardware Virtualization (HV) must be enabled in the host BIOS.
- Hosts must be certified for FT.
- VMware recommends that the host BIOS power management settings are set to "Maximum performance" or "OS-managed performance".
- The virtual memory reservation should be set to match the memory size
- You should have at 3 hosts in the cluster to accommodate a new Secondary VM following a failover.
- vSphere HA must be enabled on the cluster
- SSL certificate checking must be enabled in the vCenter Server settings.
- The hosts must use ESXi 6.x or later

The following vSphere features are not supported for FT protected virtual machines.

- Snapshots. (Exception: Disk-only snapshots created for vStorage APIs - Data Protection (VADP) backups are supported for FT, but not for legacy FT)
- Storage vMotion.

- Linked clones.
- Virtual Volume datastores.
- Storage-based policy management. (Exception: vSAN storage policies are supported.)
- I/O filters.
- Disk encryption.
- Trusted Platform Module (TPM).
- Virtual Based Security (VBS) enabled VMs.
- Universal Point in Time snapshots (a NextGen feature for vSAN)
- Physical Raw Device Mappings (RDMs) (Note: virtual RDMs are supported for legacy FT)
- Virtual CD-ROM for floppy drive backed by physical device.
- USB, sound devices, serial ports, parallel ports.
- N\_Port ID Virtualization (NPIV)
- Network adapter passthrough
- Hot plugging devices (Note: the hot plug feature is automatically disabled when you enable FT on a virtual machine.)
- Changing the network where a virtual NIC is connected.
- Virtual Machine Communication Interface (VMCI)
- Virtual disk files larger than 2 TB.
- Video device with 3D enabled.

You should apply the following best practices for FT.

- Use similar CPU frequencies in the hosts.
- Use active / standby NIC teaming settings.

- Ensure the FT Logging network is secure (FT data is not encrypted).
- Enable jumbo frames and 10 GBps for the FT network. Optionally, configure multiple NICs for FT Logging.
- Place ISO files on shared storage.
- You can use vSAN for Primary or Secondary VMs, but do not also connect those virtual machines to other storage types. Also, place the Primary and Secondary VMs in separate vSAN fault domains.
- Keep vSAN and FT Logging on separate networks.

In vSphere 6.5, FT is supported with DRS only when EVC is enabled. You can assign a DRS automation to the Primary VM and let the Secondary VM assume the same setting. If you enable FT for a virtual machine in a cluster where EVC is disabled, the virtual machine DRS automation level is automatically set to disabled. Starting in vSphere 6.7, EVC is not required for FT to support DRS.

To enable FT, you first create a VMkernel virtual network adapter on each host and connect to the FT logging network. You should enable vMotion on a separate VMkernel adapter and network.

When you enable FT protection for a virtual machine, the following events occur.

- If the Primary VM is powered on, validation tests occur. If validation is passed, then the entire state of the Primary VM is copied and used to create the Secondary VM on a separate host. The Secondary VM is powered on. The virtual machine's FT status is **Protected**.
- If the Primary VM is powered off, the Secondary VM is created and registered to a host in the

cluster, but not powered on. The virtual machine FT Status is **Not Protected, VM not Running**.

When power on the Primary VM, the validation checks occur and Secondary VM is powered on.

Then the FT Status changes to **Protected**.

Legacy FT VMs can exist only on ESXi hosts running on vSphere versions earlier than 6.5. If you require Legacy FT, you should configure a separate vSphere 6.0 cluster.

## vCenter Server High Availability

vCenter Server High Availability (vCenter HA) is described in [Chapter 1, "vSphere Overview, Components, and Requirements."](#) vCenter HA implementation is covered in [Chapter 8, "vSphere Installation."](#) vCenter HA management is covered in [Chapter 13, "Manage vSphere and vCenter Server."](#)

## VMware Service Lifecycle Manager

If a vCenter service fails, VMware Service Lifecycle Manager restarts it. VMware Service Lifecycle Manager is a service running in vCenter server that monitors the health of services and takes preconfigured remediation action when it detects a failure. If multiple attempts to restart a service fails, then the service is considered failed.

**Note**

Do not confuse VMware Service Lifecycle Manager with VMware vSphere Lifecycle Manager, which provides simple, centralized lifecycle management for ESXi hosts through the use of images and baselines.

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, [Chapter 15, "Final](#)

"Preparation," and the exam simulation questions on the CD-ROM.

## REVIEW ALL KEY TOPICS

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. **Table 4-11** lists a reference of these key topics and the page numbers on which each is found.

**Table 4-11** Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Section	Network-Aware DRS	
Section	How DRS scores VMs	
List	DRS Migration Sensitivity	
Section	Scalable Shares	
List	vSphere HA Requirements	
Table 4-7	vSphere HA Response to Failure Settings	
List	vSphere FT requirements	

## DEFINE KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary:

VMware Service Lifecycle Manager

vSphere FT

Predictive DRS

Proactive HA

Virtual Machine Component Protection (VMCP)

## Glossary

**VMware Service Lifecycle Manager:** VMware Service Lifecycle Manager is a service running in vCenter server that monitors the health of services and takes

preconfigured remediation action when it detects a failure.

**vSphere FT:** vSphere Fault Tolerance (FT) provides continuous availability for a virtual machine (the Primary VM) by ensuring that the state of a Secondary VM is identical at any point in the instruction execution of the virtual machine.

**Predictive DRS:** Predictive DRS is a feature that leverages the predictive analytics of vRealize Operations (vROps) Manager and vSphere DRS to provide workload balancing prior to the occurrence of resource utilization spikes and resource contention

**Proactive HA:** Proactive High Availability (Proactive HA) integrates with select hardware partners to detect degraded components and evacuate VMs from affected vSphere hosts before an incident causes a service interruption.

**VCMP:** Virtual Machine Component Protection (VMCP) is a vSphere HA feature that can detect datastore accessibility issues and provide remediation for impacted virtual machines.

## REVIEW QUESTIONS

- 1.** You are configuring EVC. Which of the following is not a requirement?
  - a.** A vSphere Cluster
  - b.** A DRS cluster
  - c.** CPUs in the same family
  - d.** CPUs with the same base instruction set
- 2.** In vSphere 7.0, you want to configure the DRS Migration Threshold such that it is at the maximum level at which resource contention is

considered, but not virtual machine happiness.

Which of the following values should you choose?

- a.** Level 1
  - b.** Level 2
  - c.** Level 3
  - d.** Level 4
  - e.** Level 5
- 3.** In a vSphere Cluster, which of the following statements is true, if the master host detects datastore heartbeats for a subordinate host, but no network heartbeats or ping responses?
- a.** The master host declares the subordinate host is isolated
  - b.** The master host assumes the subordinate host is isolated or in a network partition
  - c.** The master host takes the host isolation response action
  - d.** The master host restarts the virtual machines on the failed subordinate host.
- 4.** You want to configure vSphere HA. Which of the following is a requirement?
- a.** Use IPv4 for all host management interfaces
  - b.** Enable vMotion on each host
  - c.** Ensure the Virtual Machine Startup and Shutdown (automatic startup) feature is enabled on each virtual machine.
  - d.** Host IP addresses must persist across reboots.

**5.** You are configuring vSphere Distributed Power Management (DPM) in your vSphere 7.0 environment. Which of the following is not a requirement for using Wake on LAN (WOL) in DPM?

- a.** The management NIC must support WOL
- b.** vMotion is configured
- c.** The vMotion NIC must support WOL
- d.** The physical switch port must be set to auto negotiate the link speed

# **Chapter 5. vCenter Server Features and Virtual Machines**

**This chapter covers the following topics:**

- vCenter Server and vSphere
- Virtual Machine File Structure
- Virtual Machine Snapshots
- Virtual Machine Settings
- Virtual Machine Migration
- Virtual Machine Cloning

This chapter contains information related to VMware 2V0-21.20 exam objectives 1.2, 1.5, 2.3, 5.6, 7.1, 7.2, 7.3, 7.6, 7.9, 7.11.4

This chapter provides details on vCenter Server features that have not been covered in previous chapters. It details for virtual machines, such as file structure, migrations, and cloning. Chapters 13 and 14 provides details for managing vCenter Server, vSphere, and virtual machines.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section. Regardless, the authors recommend that you read the

entire chapter at least once. [Table 5-1](#) outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 5-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
vCenter Server and vSphere	1, 2
Virtual Machine File Structure	3
Virtual Machine Snapshots	4
Virtual Machine Settings	5, 6
Virtual Machine Migration	7, 8, 9
Virtual Machine Cloning	10

- 1.** You just installed a new vCenter Server. Using the vSphere Client, what is the first object that you can create in the inventory pane? (pick two)
  - a.** A cluster
  - b.** A host
  - c.** A virtual machine
  - d.** A data center
  - e.** A datastore
  - f.** A folder
  
- 2.** You want to create a content library for your vCenter Server. Which type of content library cannot be modified directly?
  - a.** A library backed by vSAN
  - b.** A local library
  - c.** A published library
  - d.** A subscribed library

- 3.** You are providing support for a virtual machine named Server01 in a vSphere 7.0 environment. Which of the following is the virtual disk data file?
- a. Server01.vmdk**
  - b. Server01-flat.vmdk**
  - c. Server01.vmx**
  - d. Server01-data.vmdk**
- 4.** You have taken multiple snapshots for a virtual machine. In the vSphere Client Snapshot Manager, what is the location of the location of the **You Are Here** icon?
- a.** Under the parent snapshot.
  - b.** Under the child snapshot
  - c.** Under the latest snapshot.
  - d.** Under the associate delta file.
- 5.** You are configuring a virtual machine in vSphere 7.0. Which of the following devices cannot be configured or removed?
- a.** SIO Controller
  - b.** SCSI Controller
  - c.** Parallel Port
  - d.** PCI Device
- 6.** You are using the vSphere Client to edit a virtual machine in vSphere 7.0. Which of the following is not available on the VM Options tab?
- a.** General Options
  - b.** Encryption Options
  - c.** Snapshot Options

**d. vApp Options**

7. You want to perform a cross vCenter Server migration in vSphere 7.0. Which of the following statements is true?
  - a. If separate SSO domains are used, you must use the APIs to perform the migration.
  - b. If separate SSO domains are used, you can use the vSphere Client to perform the migration
  - c. If separate SSO domains are used, you cannot perform the migration.
  - d. The vSphere and vCenter Server Enterprise licenses are required.
8. You want to perform multiple, simultaneous virtual machine migrations for a 4 node DRS cluster with a 10 GigE vMotion network and multiple datastores. Which of the following operations are allowed without any queuing?
  - a. 9 simultaneous vMotion migrations
  - b. 9 simultaneous vMotion without Shared Storage migrations.
  - c. One Storage vMotion and 4 vMotion operations
  - d. 4 simultaneous vMotion and 5 provisioning operations involving the same host.
9. You are optimizing your vSphere environment. Which of the following is not helpful for improving vMotion performance?
  - a. Use NIOC to increase shares for vMotion traffic
  - b. Use traffic shaping to limit the bandwidth that is available to vMotion traffic.

- c.** Use Multi NIC vMotion
    - d.** Use jumbo frames
- 10.** You want to use Instant Clones in vSphere.  
Which of the following statements are true?
  - a.** You can use the Host Client to perform an instant clone.
  - b.** You can use the vSphere Client to perform an instant clone.
  - c.** A sample, major use case for Instant Clones are large scale deployments in a VMware Horizon VDI
  - d.** vSphere 6.5 supports Instant Clones

## VCENTER SERVER AND VSphere

Previous chapters provide detail for the vSphere topology, storage infrastructure, network infrastructure and vSphere clusters. This section provides details for other features, such as the vSphere inventory, host profiles, and the content library.

### vSphere Managed Inventory Objects

This section describes the vSphere inventory and object types, which should be planned prior to implementing vSphere. It provides information on creating and configuring inventory objects during the vSphere implementation.

In vSphere, the inventory is a collection of managed virtual and physical objects. Depending on the object type, you can configure each object and perform operations, such as set permissions, monitor tasks,

monitor events, and set alarms. You can organize many of these objects by placing them into folders, making them easier to manage.

All inventory objects, except for hosts, can be renamed to represent their purposes. For example, they can be named after company departments, locations, or functions.

**Note**

Inventory object names cannot exceed 214 bytes (UTF-8 encoded).

## Data Centers

A data center is a container object in the vSphere inventory that is an aggregation of all the different types of objects used to work in virtual infrastructure. The first object that you must create in a vSphere inventory is a data center (except for a folder to contain data centers). You cannot add any ESXi hosts, virtual machines, or other objects in the inventory until you create a data center.

Data centers are often used to contain all the objects in a physical data center. For example, if you use a single vCenter Server to manage vSphere assets in San Francisco and Chicago, you may wish to use corresponding virtual data centers to organize each city's assets. You could create data center objects named San Francisco and Chicago and place each ESXi host, virtual machine, and other objects in the appropriate data center.

Within each data center, there are four separate hierarchies.

- Virtual machines (and templates)
- Hosts (and clusters)
- Networks

- Datastores

The data center the is the namespace for networks and datastores. The names for these objects must be unique within a data center. You cannot use identical datastore names within the same data center, but you can use identical datastore names within in two different data centers. Virtual machines, templates, and clusters need not to have unique names within the data center but must have unique names within their folder.

## **Folders**

Folders are container objects in the vSphere inventory that allow you to group objects of a single type. A folder can contain data centers, clusters, datastores, networks, virtual machines, templates, or hosts. For example, one folder can contain hosts and a folder containing hosts, but it cannot contain hosts and a folder containing virtual machines.

You can create data center folders directly under the root vCenter Server and use them to organize your data centers. Within each data center is one hierarchy of folders for virtual machines and templates, one for hosts and clusters, one for datastores, and one for networks.

The only setting that is available for you to set on a folder is its name. Additionally, you can assign permissions and alarms.

## **Clusters**

A cluster is a set of ESXi hosts that are intended to work together as a unit. When you add a host to a cluster, the host's resources become part of the cluster's resources. vCenter Server manages the resources of all hosts in a cluster as one unit. In addition to creating a cluster, assigning a name, and adding ESXi objects, you can enable and configure features on a cluster, such as VMware EVC, vSphere DRS, and vSphere HA.

If you enable VMware EVC on a cluster, you can ensure that migrations with vMotion do not fail because of CPU compatibility errors. If you enable vSphere DRS on a cluster, you can allow automatic resource balancing using the pooled host resources in the cluster. If you enable vSphere HA on a cluster, you can allow rapid virtual machine recovery from host hardware failures using the cluster's available host resource capacity.

Cluster features are covered in detail in [Chapter 4](#).

## **Resource Pools**

Resource pools are container objects in the vSphere inventory that are used to compartmentalize the CPU and memory resources of a host or cluster. Virtual machines run in resource pools, using resources provided by the resource pools. You can create multiple resource pools as direct children of a standalone host or cluster.

You can use resource pools much like a folder to organize VMs. You can delegate control over each resource pool to specific individuals and groups. You can monitor resources and set alarms on resource pools. If you need a container for strictly organization and permission purposes, consider using a folder. If you also need resource management, then consider using a resource pool.

If DRS is enabled, you can use the vSphere Client to create resource pools in the cluster and assign resource settings, such as reservations and limits. Otherwise, you can create resource pools directly on specific ESXi hosts.

You can configure resource settings for resource pools, such as reservations, limits, and shares. See [Chapter 4](#) for more detail on resource pools.

## **Hosts**

Hosts are objects in the vSphere inventory that represent your actual ESXi servers. After installing an ESXi host, you can choose to add it to the vSphere inventory, which requires you to provide credentials for a user that is assigned the `Administrator` role directly on the host.

The `vpxa` agent in the ESXi server maintains communication with vCenter Server. It is an interface between the vCenter Server and the ESXi `hostd` service, which drives the main operations on the host, such as powering on a virtual machine.

For maintenance and troubleshooting activities, you can disconnect a host from the vCenter Server, which does not remove it from vCenter Server, but suspends related vCenter Server monitoring activities. You can connect hosts that are disconnected. If you choose to remove a host from inventory, the host and all its associated virtual machines will be removed.

If the SSL certificate used by vCenter Server is replaced or changed, the vCenter Server will be unable to decrypt the host passwords. You will need to reconnect and resupply the host credentials.

To remove a host from the vSphere inventory, you must first enter maintenance mode.

## **Networks**

Networks are objects in the vSphere inventory that are used to connect a set of virtual network adapters. Each ESXi host may have multiple VMkernel virtual network adapters. Each virtual machine may have multiple virtual network adapters. Each virtual network adapter may be connected to a port group (on a standard virtual switch) or a distributed port group (on a vSphere distributed switch). All virtual machines that connect to the same port group belong to the same network in the virtual environment, even if they are on different physical

servers. You can manage networks by monitoring, setting permissions, and setting alarms on port groups and distributed port groups.

[Chapter 3](#) provides details on networks.

## **Datastores**

Datastores are objects in the vSphere inventory that represent physical storage resources in the data center. A datastore is the storage location for virtual machine files. The physical storage resources can come from local SCSI disks of the ESXi host, Fibre Channel SAN disk arrays, iSCSI SAN disk arrays, or Network Attached Storage (NAS) arrays. VMFS datastores can be backed by local SCSI, Fibre Channel, or iSCSI. NFS data stores can be backed by NAS. vSAN datastores can be built in VSAN clusters.

[Chapter 2](#) provides details on datastores.

## **Virtual Machines**

Virtual machines are represented in the vSphere inventory in a manner that reflects the current inventory view. For example, in the Hosts and Clusters view, each virtual machine is descendent of the ESXi host on which it runs. In the Networks view, each virtual machine is descendent of the network to which it connects.

## **Templates**

Templates are objects in the vSphere inventory that effectively are non-executable virtual machines. A template is a master copy of a virtual machine that can be used to create and provision new virtual machines. Templates can have a guest operating system and application software installed. They are often customized during deployment to ensure that each new virtual machine has a unique name and network settings.

You can convert a virtual machine to a template and vice versa. But the main use case for templates is for rapid deployment of new, similar virtual machines from a single template. In this case, you are effectively cloning the template again and again, allowing the template to remain unchanged and ready for future use. To update a template, such as to install the most recent guest OS updates, you can temporarily convert the template to a virtual machine, apply the updates, and convert back to template.

For more details on templates see the [Virtual Machine Cloning](#) section in this chapter.

### vApps

A vApp is a container object in vSphere that provides a format for packaging and managing applications.

Typically, a vApp is a set of virtual machines that runs a single application and allows you to manage the application as a single unit. You can specify a unique boot order for the virtual machines in a vApp, which allows you to graceful start an application that spans multiple virtual machines. You can apply resource management settings to a vApp in a similar manner as you would to a resource pool.

## Host Profiles

A Host Profile is a feature that enables you to encapsulate the configuration of one host and apply it to other hosts. It is especially helpful in environments administrators manage multiple hosts and clusters with vCenter Server. The following list are characteristics of host profiles.

- Host Profiles are an automated and centrally managed mechanism.
- Host Profiles are used for host configuration and configuration compliance.

- Host Profiles can improve efficiency by reducing the use of repetitive, manual tasks.
- Host Profiles capture the configuration of a reference host and store the configuration as a managed object.
- Host Profiles provide parameters for configure networking, storage, security, and other host-level settings.
- Host Profiles can be applied to individual hosts, a cluster, or a set of hosts and clusters.
- Host Profiles make it easy to ensure that all hosts in the cluster have a consistent configuration.

You can use the following workflow to leverage a host profile to apply a consistent host configuration in your vSphere environment. Set up and configure a reference host.



1. Create a host profile from the reference host.
2. Attach hosts or clusters to the host profile.
3. Check the compliance of the hosts with the host profile. If all hosts are compliant with the reference host, then you do not need to take additional steps.
4. If the hosts are not fully compliant, then you apply (remediate) the hosts with the host profile.

**Note**

If you want a Host Profile to use directory services for authentication, the reference host must be configured to use a directory service.

In previous releases, vSphere requires that the reference host be available for certain tasks, such as editing, importing, and exporting the host profile. Starting with

vSphere 6.0, a dedicated reference host is no longer required for these tasks.

Auto Deploy uses host profiles to configure ESXi.

## **Content Library**

A content library is a repository that can be used to share files such as virtual machine templates, vApps, and image files among a set of vCenter Servers. The content library, which was introduced in vSphere 6.0, addresses the fact that multiple vCenter Servers do not directly share associated files such as Open Virtualization Format (OVF) and image (ISO) files. A great use case is companies having multiple sites, each managed by a dedicated vCenter Server, where the OVF files and ISO files that are used at one site are not directly available for use at other sites. In this case, you can create a content library at one site and publish it to serve the other sites. At the other sites you can create subscribed libraries that automatically synchronize with the published library. For example, you can create a local content library using the main office vCenter Server, publish it, and subscribe to it from branch office vCenter Servers.

A subscribed content library can be configured to only download metadata whenever it receives notification of a change. In this case, the subscribing library reflects the most recent changes, but it is not burdened with supplying the storage space for every published file. Instead, the administrator can choose whether to download the actual data for the entire item or per item.

Three types of content libraries can be used local, published, and subscribed. A local content library is the simplest form. It allows the administrator to allow, modify and delete content. A published library is a local library, where content is published for subscription. A subscribed library is a library, whose content you cannot

change or publish. It receives its content from a published library.

Each content library is built upon a single storage entity, which may be a VMFS datastore, an NFS datastore, a CIFS share, a local disk, or a vSAN datastore. In vSphere 7.0, the following maximum limitations apply.



- 1000 libraries per vCenter Server
- 1000 items per library
- 16 concurrent synchronization operations per published library
- 9 virtual disk files per OVA/OVF template

After one library is set to subscribe to another library, synchronization occurs. Automatic synchronization occurs every 24 hours by default, can be modified using an API. The content library service, which is named `vmware-vdcs`, is installed as part of the vCenter Server installation and uses the same database as vCenter Server.

Simple versioning is used to keep the libraries synchronized. Version numbers are assigned to each library and to each item in the library. These numbers are incremented whenever content is added or modified. The library does not store previous versions or provide rollback.

The following sequence occurs between a subscribed and published library

1. The library service on the subscriber connects to the library services on the publisher using the

VMware Content Subscription Protocol (vCSP) and checks for updates

2. The subscriber pulls the **lib.json** file from the publisher and each library's lib.json files are examined to determine if discrepancies exist between the publisher and subscriber.
3. Using vCSP, the library service determines what data has changed and sends a request to the transfer service to copy the required files.
4. The subscriber updates the versioning information in the database.

Beginning with vSphere 6.5, you can mount an ISO directly from the Content Library, apply a guest OS customization specification during VM deployment, and update existing templates. The Content Library performance is improved. The new Optimized HTTP Sync option stores content in a compressed format, which reduces the synchronization time. The Content Library leverages new features in vCenter Server 6.5, including vCenter HA and backup / restore.

In previous versions of vSphere, content libraries supported only OVF templates. As a result, virtual machine templates and vApp templates were converted to OVF files when you uploaded them to a content library. Starting with vSphere 6.7 Update 1, content libraries support virtual machine templates. So, templates in the content library can either be of the OVF Template type, or the VM Template type. vApp templates are still converted to OVF files when you upload them to a content library. The distribution of VM templates requires that the respective vCenter Server instances be in Enhanced Linked Mode or Hybrid Linked Mode and that the respective hosts are connected through a network.

To allow a user to manage a content library and its items, you can assign the **Content Library Administrator**

role, which is a sample role, to that user as a global permission. Users who are assigned the Administrator at a vCenter Server level cannot see the libraries unless they have a **Read-Only** role as a global permission.

## vSphere with Kubernetes

By using vSphere with Kubernetes, you can use a vSphere cluster as a platform for running Kubernetes workloads in dedicated resource pools. Once enabled on a vSphere cluster, vSphere with Kubernetes creates a Kubernetes control plane directly in the hypervisor layer, enabling you to deploy vSphere Pods and run your applications inside these clusters.

A vSphere Pod, which is the equivalent of a Kubernetes pod, is a small virtual machine that runs one or more Linux containers. The storage and compute for each vSphere Pod is sized precisely for its workload with explicit resource reservations.

To use vSphere with Kubernetes, you must use the VMware vSphere 7 Enterprise Plus with Add-on for Kubernetes license for all ESXi hosts that you want to use in a Supervisor Cluster. You must assign an NSX-T Data Center Advanced or higher license to NSX Manager.

## VIRTUAL MACHINE FILE STRUCTURE

A virtual machine consists of several files that are stored in a datastore. The key files are the configuration file, virtual disk file, NVRAM setting file, and log file. [Table 5-2](#) provides details for virtual machine files. You can configure virtual machine settings through the vSphere Client, ESXCLI, or the vSphere Web Services SDK.

**Note**

Do not directly change, move, or delete virtual machine files without guidance from a VMware Technical Support representative

**Table 5-2** Virtual Machine Files

File	Description
vmname.vmx	Virtual machine configuration file
vmname.vmxf	Additional virtual machine configuration file
vmname.vmdk	Virtual disk characteristics (metadata) file.
vmname-flat.vmdk	Virtual disk data file. (commonly called the Flat file)
vmname.nvram or nvram	Virtual machine BIOS or EFI configuration file
vmname.vmsd	Virtual machine snapshots file
vmname.vmsn	Virtual machine snapshot data file
vmname.vswp	Virtual machine swap file
vmname.vmss	Virtual machine suspend file
vmware.log	Current virtual machine log file
vmware-#.log	Old virtual machine log files, where # is a number starting with 1

Additional files may be created when you perform specific operations, such as creating snapshots. If you convert a virtual machine to a template the .vmtx file replaces the virtual machine configuration file (.vmx file).

By default, when creating a virtual machine, the system creates a folder in the datastore and assigns a folder name that is similar to the virtual machine name. In cases where the default folder name is already in use, the system appends a number to the new folder to make it unique.

## Configuration File

A virtual machine's configuration file is a text file that contains all the virtual machine's settings, including a description of the virtual hardware. For example, a portion of the contents of a VMX file for a CentOS virtual machine named `server1` could include the following text.

```
displayName = "server1"
guestOS = "centos-64"
nvram = "server1.nvram"
scsi0:0.fileName = "server1.vmdk"
```

If that virtual machine is sized with two virtual CPUs and 1024 GB memory, then the contents of the VMX file may also include the following text.

```
numvcpus = "2"
memSize = "1024"
```

## Virtual Disk Files

The name of the VMDK file that contains metadata for a virtual disk is included in the VMX file as shown in the previous example (`scsi0:0.fileName = "server1.vmdk"`). The VMDK metadata file is a text file that contains details about the virtual disk, such as its number of cylinders, heads, and sectors, as shown in the following sample content.

```
ddb.geometry.cylinders = "1305"
ddb.geometry.heads = "255"
ddb.geometry.sectors = "63"
```

The VMDK metadata file also contains the names of other files associated with the virtual disk, such as data (extent) files as shown in the following sample content.

```
# Extent description  
RW 20971520 VMFS "server1-flat.vmdk"
```

## Snapshot Files

When you take a snapshot of a virtual machine, the system creates a few files. For example, if you take a snapshot for a powered off virtual machine named `server1` that has only one virtual disk and no previous snapshots, the resulting files may be created.



- **server1-000001-sesparse.vmdk:** A delta data disk that store changes made since the creation of the snapshot.
- **server1-000001.vmdk:** A VMDK metadata file for the delta disk.
- **server1-Snapshot1.vmsn:** Snapshot data.

The following section provides more details on virtual machine snapshots.

## VIRTUAL MACHINE SNAPSHOTS

Snapshots capture the state of a virtual machine and the data in the virtual machine at a specific point in time. Snapshots are useful when you want to return the state of a virtual machine to a point that was previously captured. For example, you can create a snapshot of a virtual machine just prior to installing and testing software in the virtual machine. This enables you to revert the virtual machine back to its original state when you finish testing.

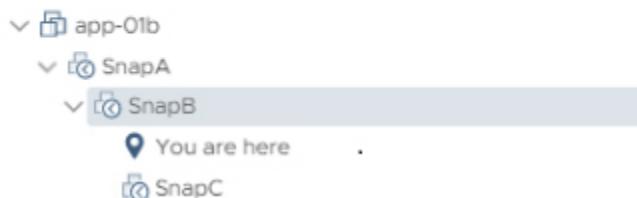
You can take multiple snapshots of a virtual machine. If you take multiple snapshots without reverting the virtual machine, then the snapshots are created in a linear fashion as shown in [Figure 5.1](#). The vSphere Client represents the snapshot hierarchy of a virtual machine as a tree with the root node being the virtual machine and nodes being each snapshot. If you revert the virtual machine to a snapshot, the state of your virtual machine is associated with that snapshot as shown in [Figure 5.2](#). If you create another snapshot, you add branches to the snapshot tree, as shown in [Figure 5.3](#).

## Manage Snapshots | app-01b



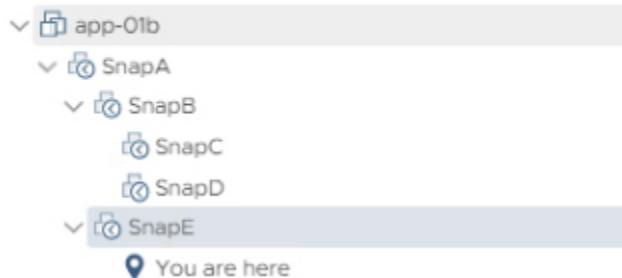
**Figure 5-1** Linear Snapshots

## Manage Snapshots | app-01b



**Figure 5-2** Post-Revert Snapshot Tree

## Manage Snapshots | app-01b



### Figure 5-3 New Branch in Snapshot Tree

Each branch in a snapshot tree can have up to 32 snapshots.

In the vSphere Client, you can perform several snapshot operations, including taking a snapshot, reverting to a snapshot, and deleting a snapshot. When taking a snapshot, you can choose whether to snap the memory and whether to quiesce the guest OS. In cases where no snapshot exists, but delta files exist, you can choose to consolidate the disks.

**Note**

You cannot quiesce virtual machines that have large capacity disks.

## Use Cases

The following list contains some common use cases for snapshots.



- **Rollback changes:** Prior to upgrading or making a configuration change to an application, you can take a virtual machine snapshot to provide a rollback option.
- **Rollback guest OS upgrade:** Prior to upgrading the guest OS, you can take a virtual machine snapshot to provide a rollback option.
- **Training and Development Labs:** You can take snapshots of a set of virtual machines used in a lab environment prior to allowing user access. When the user finishes their experiments, you can revert the state of the environment back to the original state for the next user.

- **Backups:** A backup utility may first trigger a virtual machine snapshot and then copy the virtual machine files without needing to deal with open files. Following the backup, the utility will delete the snapshot.
- **Troubleshooting and triage:** You can take a snapshot of a troubled virtual machine to allow you an option to later choose to return the virtual machine to the exact state when it experienced an issue.
- **Linked Clones:** Automation and virtual desktop software, such as vRealize Automation and Horizon, may leverage virtual machine snapshots to allow you to use fast provisioning (linked clone) methods where new virtual machines share a base virtual disk. For example, to use a linked clone in a vRealize Automation blueprint you need to identify a virtual machine snapshot.

## What a Snapshot Preserves

A snapshot preserves the following information:

- Virtual machine settings. The virtual machine directory, which includes the disks added or changed after you take the snapshot.
- Disk state. State of each virtual disks.
- (Optional) Memory state. The contents of the virtual machine's memory
- Power state. The virtual machine can be powered on, powered off, or suspended when you take the snapshot. If you revert to a snapshot that includes the memory state, the virtual machine is returned to its preserved power state.

## Parent Snapshots

The first virtual machine snapshot that you create is the base snapshot. Taking a snapshot creates a delta disk file for each disk attached to the virtual machine and optionally, a memory file. The delta disk files and memory file are stored with the base VMDK file. The parent (current) snapshot is always the snapshot that appears immediately above the **You are here** icon in the Snapshot Manager. If you revert to a snapshot, that snapshot becomes the parent of the **You are here** current state. When you have multiple snapshots, each child snapshot has a parent snapshot.

**Note**

The parent snapshot is not always the snapshot that you took most recently.

## Snapshot Behavior

Taking a snapshot preserves the disk state by creating a series of delta disks for each attached virtual disk or virtual raw device mapping (RDM). Taking a snapshot creates a snapshot object in the Snapshot Manager that represents the virtual machine state and settings. Each snapshot creates a delta disk for each virtual disk. When you take a snapshot, the system prevents the virtual machine from writing to the current data (VMDK) file and instead directs all writes to the delta disk. The delta disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the parent snapshot. Delta disk files can expand quickly and become as large as the configured size of the virtual disk if the guest operating system writes to every block of the virtual disk.

When you take a snapshot, the state of the virtual machine, virtual disks and (optionally) the virtual memory are captured in a set of files, such as the delta, database, and memory files. By default, the delta disks are stored with the corresponding virtual disk files and

the memory and database files are stored in the virtual machine directory.

### **Flat File**

A virtual disk involves a metadata file and a data file each with the `vmdk` extension. The metadata VMDK file contains information about the virtual disk, such as geometry and child-parent relationship information. The data VMDK file is called the flat file. Its name contains the work `flat`. Only the names of the metadata files appear in the vSphere Client Datastore Browser. In normal circumstances, the virtual machines guest OS and applications write to the flat file.

### **Delta Disk Files**

When you create a snapshot, you create a delta disk for each virtual disk. The delta (child) disk represents the difference between the current state of the virtual disk and the state that existed at the time that you took the parent snapshot. A delta disk has two VMDK files. One is a small metadata file and the other is a data file. Delta disk data files are also called redo logs.

### **Database File**

The database file is a file with the `vmsd` extension that contains snapshot details required by the Snapshot Manager. It contains details on the relationships between snapshots and child disks.

### **Memory File**

The memory file is a file with the `vmsn` extension that includes the active state of the virtual machine's memory. Capturing the memory state of the virtual machine lets you revert to a powered-on state. Memory snapshots take longer to create than nonmemory snapshots. The size of the memory impacts the amount of time required to create the snapshot.

## Limitations

The use of snapshots can impact the virtual machine performance and can be limited in some scenarios, as summarized in the following list.

- Snapshots are not supported for RDM physical mode disks or for iSCSI initiators in a guest OS.
- Snapshots of powered-on or suspended virtual machines with independent disks are not supported.
- A quiesced snapshots requires a supported guest operating system and active VMware Tools services.
- Snapshots are not supported with PCI vSphere DirectPath I/O devices.
- Snapshots are not supported for virtual machines configured for bus sharing.
- Although snapshots may be a useful step for a backup utility, a snapshot is not a backup by itself. A snapshot does not provide a redundant copy of data. If the base flat file is lost or corrupt, you cannot restore the virtual machine by reverting to a snapshot.
- Snapshots can negatively affect the performance of a virtual machine. The performance degradation is impacted by factors such as the age of the snapshot, the depth of the snapshot tree, and the amount of data in the delta files.
- Snapshot operations can take much longer to finish when they involve virtual disks larger than 2 TB.
- Deleting a large snapshot that is part of the current path (as indicated by **You are here** in the Snapshot Manager) can negatively impact the performance and the health of the virtual machine.

To minimize risk, you can shut down the virtual machine prior to deleting the snapshot.

## VIRTUAL MACHINE SETTINGS

### VM Hardware / Compatibility

You can configure a virtual machine's compatibility setting to control which ESXi host versions can be used to run the virtual machine. In the vSphere Client, you can set the **Compatible with** option for a virtual machine to a compatible ESXi version, such as **ESXi 7.0 and later** or **ESXi 6.7 Update 2 and later**. The compatibility setting determines which ESXi host versions the virtual machine can run on and the hardware features available to the virtual machine. At the host, cluster, or datacenter level you can set the **Default VM Compatibility** setting. See [Chapter 14](#) for more details.

Virtual hardware devices perform the same function for the virtual machines as physical hardware devices do for traditional servers. Each virtual machine has CPU, memory, and disk resources. All modern operating systems provide support for virtual memory, allowing software to use more memory than is present in the server hardware. Similarly, ESXi can provide virtual machine memory to its virtual machines totaling more than the capacity of the host's physical memory.

You can add virtual hardware devices to a virtual machine by editing the virtual machine's settings in the vSphere Client. Not all devices are configurable. For example, the PCI and SIO virtual hardware devices are part of the virtual motherboard, but cannot be configured or removed. You can enable the **Memory hotplug** or **CPU hotplug** settings to allow you to add memory or CPU resources to a running virtual. Memory hotplug is supported on all 64 bit operating systems, but

some guest operating systems may not be able to make use of the added memory without restarting. The ESXi license and other factors for the host where the virtual machine runs may impact the available devices for the virtual machine. For a list of hardware devices and their functions, see **Table 5-3**.

**Table 5-3** Virtual Machine Hardware Devices

Device	Description
CPU	At least one vCPU, but not more than the number of logical CPUs in the host.  You can set advanced CPU features, such as the CPU Identification Mask and hyperthreaded core sharing.
Chipset	The virtual motherboard consists of VMware proprietary virtual devices based on the following chips: <ul style="list-style-type: none"> <li>Intel 440BX AGPset 82443BX Host Bridge/Controller</li> <li>Intel 82371AB (PIX4) PCI ISA IDE Xcelerator</li> <li>National Semiconductor PC87338 ACPI 1.0 and PC98/99 Compliant SuperI/O</li> <li>Intel 82093AA I/O Advanced Programmable Interrupt Controller</li> </ul>
DVD/CD-ROM Drive	One by default. You can configure the virtual DVD/CD-ROM device to connect to client devices, host devices, or datastore ISO files.  You can add and remove virtual DVD/CD-ROM devices.
Hard Disk	A virtual disk is backed by a set of files as previously discussed in this chapter.
IDE 0, IDE 1	Two virtual Integrated Drive Electronics (IDE) interfaces are present by default.
Keyboard	The virtual keyboard is mapped to the user keyboard when you connect to the virtual machine console.
Memory	The size of the virtual memory becomes the size of memory that the guest OS perceives to be physical memory.
Network Adapter	You can configure the number of virtual network adapters (NICs) and the adapter type used by each virtual machine.
Parallel port	You can add, remove, and configure virtual parallel ports.
PCI controller	One PCI controller, which is located on the virtual motherboard, is presented to the virtual machine. It cannot be removed or modified.
PCI Device	If you configured devices to be reserved for PCI passthrough on the host, then you can add (up to 16) PCI vSphere DirectPath devices to a virtual machine.
Pointing device	The virtual pointing device is mapped to the user pointing device when you connect to the virtual machine console.
Serial Port	You can configure a virtual machine with up to 32 virtual serial ports. You can add, remove, or configure virtual serial ports.
SATA controller	Provides access to virtual disks and DVD/CD-ROM devices. The SATA virtual controller appears to the guest OS as an AHCI SATA Controller.
SCSI controller	Provides access to virtual disks. The SCSI virtual controller appears to the guest OS as different types of controllers, including LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual.
SIO controller	Provides serial and parallel ports, floppy devices, and performs system management activities. One SIO controller is available to the virtual machine, but it cannot be configured or removed.
USB controller	The virtual USB Controller is the software virtualization of the USB host controller function in the virtual machine.
USB device	You can add multiple virtual USB devices to a virtual machine that you map to USB

	devices connected to an ESXi host or a client computer.
VMCI	The Virtual Machine Communication Interface (VMCI) device provides a high-speed communication channel between a virtual machine and the hypervisor. You cannot add or remove VMCI devices.
NVMe controller	NVM Express controller. NVMe is a logical device interface specification for accessing nonvolatile storage media attached through a PCI Express (PCIe) bus in real and virtual hardware.
NVDIMM controller	Provides access to the non-volatile memory resources of the host.
NVDIMM device	You can add up to 64 virtual Non-Volatile Dual In-Line Memory Module (NVDIMM) devices to a virtual machine.
TPM device	You can add a virtual Trusted Platform Module (TPM) 2.0 device to a virtual machine to allow the guest OS to store sensitive information, perform cryptographic tasks, or attest the integrity of the guest platform.

## Virtual Machine -Virtual Disk Provisioning

You can configure the provisioning type for a virtual disk to thin provisioned, lazy zeroed thick provisioned, or eager zeroed thick provisioned as described in the *Virtual Disk Type* section in [Chapter 2](#). With thin provisioning, storage blocks are not allocated during disk creation, which allows fast provisioning, but requires allocation and zeroing during runtime. With thick eager zeroed, storage blocks are allocated and zeroed during provisioning, which allows fast runtime. With thick lazy zeroed provisioning, storage blocks are pre-allocated but not pre-zeroed. Your choice for the provisioning type depends on each virtual machine's use case. For example, if you want to minimize the virtual machine startup time and minimize its risk, you may choose thick provision lazy zeroed.

## VMware Tools

VMware Tools is a set of software modules and services, including services that can communicate with the VMkernel. This communication allows integration with vSphere for activities such as customizing the guest OS, running scripts in the guest OS, and synchronizing time. If you use guest operating systems without VMware Tools, many VMware features will not be available. VMware Tools enhances the guest OS performance by enabling the latest drivers for virtual devices, enabling memory functions (like ballooning), and more. It

includes drivers, such as SVGA, Paravirtual SCSI, VMXNet NIC, mouse, audio, guest introspection, memory control, and more. Prior to upgrading the hardware for a virtual machine, you should upgrade VMware Tools.

VMware Tools includes the VMware user process named `vmtoolsd` that enables copy and paste, mouse control, and automatically sets screen resolution for some non-Windows guests. It enhances the performance of the virtual machine's guest operating system and improves management of the virtual machine. It includes device drivers and other software that is essential for your VM. With VMware Tools, you have more control over the virtual machine interface.

## Virtual Machine Options

When you edit a virtual machine setting, you can navigate to and manipulate settings on the **VM Options** tab. Many of these options have dependencies with the ESXi hosts, datacenters, clusters, or resource pools on which the virtual machine resides. **Table 5-4** describes the available virtual machine options.

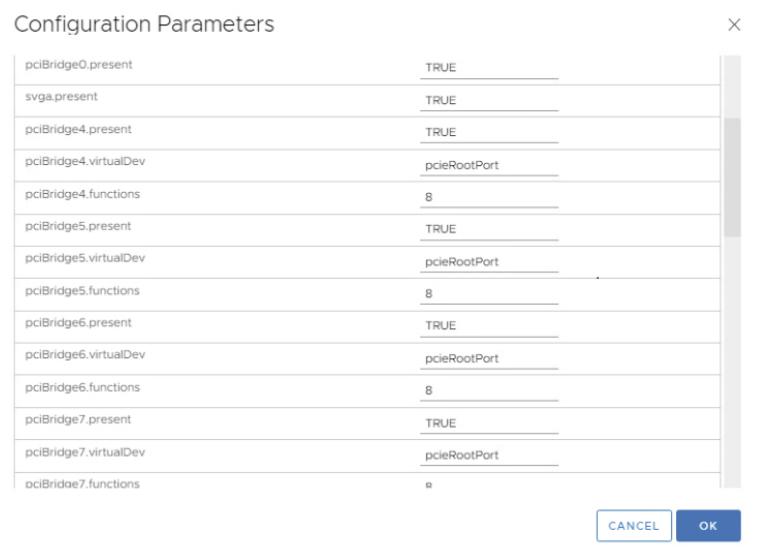
**Table 5-4** Virtual Machine Options

Category	Description
General Options	Settings include virtual machine name, configuration file location, and the working directory location.
Encryption Options	Settings allow you to enable or disable virtual machine encryption or vMotion encryption.
Power Management	Settings allow you to choose how to respond when the guest OS is placed on standby. The choices are to suspend the virtual machine or put the guest OS into standby mode.
VMware Tools	Settings allow you to choose how to respond to specific power operations. For example, choose whether to power off the virtual machine or shutdown the guest when the red power-off button is clicked.
Virtualization Based Security (VBS)	For virtual machines running the modern Windows OS versions, you can enable VBS to add an extra level of protection.
Boot Options	Settings include firmware, boot delay, and failed boot recovery.
Advanced Options	Settings include logging, debugging, swap file location, and configuration parameters.
Fibre Channel NPIV	Settings that allow the virtual machine to use N-port ID virtualization (NPIV), including whether to generate new world wide names (WWNs).
vApp Options	Settings to control vApp functionality for the virtual machine, such as enable / disable and IP allocation policy. vApp settings that are made directly to a virtual machine override setting made on the vApp.

## Virtual Machine Advanced Settings

As mentioned in the previous table, you can use the vSphere Client to edit the **Advanced Settings** for a virtual machine in its **VM Options** tab. You can set a virtual machine's advanced settings to enable or disable logging. You can enable or disable hardware acceleration. You can set debugging and statistics to **Run Normally, Record Debugging Information, Record Statistics, or Record Statistics and Debugging**. For applications that are highly sensitive to latency, you can set **Latency Sensitivity** to **High**.

In the Advanced Settings, you can select **Configuration Parameters**, where you can directly manipulate the virtual machine low level settings, as illustrated in [Figure 5.4](#).



**Figure 5-4** Sample Virtual Machine Configuration Parameters

## VIRTUAL MACHINE MIGRATION

This chapter provides information such as concepts, prerequisites, and data flow details for each migration

type. Chapter 14 provides information for performing the migrations.

## Virtual Machine Migration

### VM Migration Overview

You can migrate virtual machines from one compute resource or storage location to another while the virtual machine is stopped (cold) or running (hot). For example, if you want to balance the workload, you can migrate some virtual machines from busy ESXi hosts or datastores (or both) to other hosts and datastores. For another example, if you want to perform maintenance (such as an upgrade), you could first migrate all virtual machines from an ESXi host or datastore, perform the maintenance, and optionally migrate virtual machines back to the original location.

Moving a virtual machine between inventory folder or resource pools in the same data center is not considered a migration. Cloning and copying a virtual machine are also not forms of migration.

Each migration type involves a unique set of requirements, such as minimum privileges required to perform the operation.

**Note**

To migrate virtual machines with disks larger than 2 TB, the source and destination ESXi hosts must be version 6.0 and later.

### Cold Migrations

Moving a powered off or suspended virtual machine to a new host, new datastore, or both is considered a cold migration. The required privilege is **Resource.Migrate powered off virtual machine**.

### Hot Migrations

Moving a powered on virtual machine to a new host, new datastore, or both is considered a hot migration. During the migration, vCenter Server must take steps to ensure that active connections and services of the virtual machine are not interrupted.

### **Cross Host Migrations**

Moving a virtual machine, whether hot or cold, to a new host is considered a cross host migration. In vSphere Client wizards that involve cross host migrations, you can choose a destination host. Alternatively, when available and properly configured, you can choose a DRS cluster, resource pool, or vApp as the destination.

The cross-host migration wizards include a **Compatibility** panel to identify any compatibility issues or warnings. If the panel displays the message Compatibility checks succeeded, then you can proceed with no concern. If the panel display an error, the migration is disabled for the associated hosts. If it displays a warning message, the migration is not disabled and you can proceed, bearing in mind the warning. For hot migrations, the compatibility check accommodates vMotion CPU compatibility checking.

For a virtual machine using a NVDIMM device and PMem storage, the destination host or cluster must have available PMem resources to pass the compatibility check. For a cold migration involving a virtual machine that does not have an NVDIMM device but uses PMem storage, you can choose a target host or cluster without available PMem resources. The hard disks will use the storage policy and datastore selected for the virtual machine's configuration files.

### **Cross Datastore Migrations**

Moving a virtual machine, whether hot or cold, to a new datastore is considered a cross datastore migration.

## Cross vCenter Server Migrations

Moving a virtual machine, whether hot or cold, to a new vCenter Server is considered a cross vCenter Server migration. To perform a cross vCenter Server migration, you must meet the following requirements.



- The associated vCenter Servers and ESXi hosts must be 6.0 or later.
- The cross vCenter Server and long-distance vMotion features require an Enterprise Plus license.
- Both vCenter Server instances must be time-synchronized with each other for correct vCenter Single Sign-On token verification.
- For migration of compute resources only, both vCenter Server instances must be connected to the shared virtual machine storage.
- When using the vSphere Client, both vCenter Server instances must be in Enhanced Linked Mode and must be in the same vCenter Single Sign-On domain.

**Note**

If the vCenter Server instances exist in separate vCenter Single Sign-On domains, you can use vSphere APIs/SDK to migrate virtual machines.

## Virtual Machine Migration Limitations



vCenter Server limits the number of simultaneous virtual machine migration and provisioning operations that

occur per host, network, and datastore. Each of the network, datastore, and host limits must be satisfied for the operation to proceed. vCenter Server uses a costing method, where each migration and provisioning operation is assigned a cost per resource. Any operation whose cost causes a resource to exceed its limit is queued until other operations complete.

Limits depend on the resource type, ESXi version, migration type, and other factors, like network type. ESXi versions 5.0 to 7.0 have consistent limits.

- **Network Limits:** Network limits apply only to vMotion migrations. Each vMotion has a network resource cost of 1. The Network Limit is dependent on the network bandwidth for the VMkernel adapter enabled for vMotion. For 1 GigE the limit is 4 and for 10 GigE it is 8.
- **Datastore Limits:** Datastore limits apply to vMotion and Storage vMotion migrations. Each vMotion migration has a resource cost of 1 against the shared datastore. Each Storage vMotion migration has a resource cost of 16 against both the source and destination datastores. The Datastore Limit per datastore is 128.
- **Host Limits:** Host Limits apply to vMotion, Storage vMotion, and cold migrations. They also apply to virtual machine provisioning operations, including new deployments, and cloning. Provisioning and vMotion operations have a host cost of 1. Storage vMotion operations have a host cost of 4. The Host Limit per host is 8.

For costing purposes, a hot migration that is both cross host and cross data store (vMotion without shared storage) is considered to be a combination of vMotion and Storage vMotion and applies the associated network, host, and datastore costs. vMotion without shared

storage is equivalent to a Storage vMotion with a network cost of 1.

Consider the following examples, for a 4 node DRS cluster with a 10 GigE vMotion network.

- If you perform 9 simultaneous vMotion migrations, the 9<sup>th</sup> migration is queued due to the network limit, even if different hosts are involved.
- If you perform 9 simultaneous hot cross host and cross data store migrations involving the same datastore, the 9<sup>th</sup> migration is queued due to the datastore limit, even if the migrations are split as to whether the datastore is the source or the target.
- You can simultaneously perform one Storage vMotion and 4 vMotion operations involving a specific host.

### **TCP/IP Stacks**

You can use the vMotion TCP/IP stack to isolate vMotion traffic and assign it to a dedicated default gateway, routing table, and DNS configuration. To use the vMotion TCP/IP stack, select **vMotion** from the **TCP/IP stack** drop-down menu when configuring the associated VMkernel virtual network adapter. When you assign a VMkernel virtual network adapter to the vMotion stack, you cannot use the adapter for purposes other than vMotion.

Likewise, you can use the provisioning TCP/IP stack to isolate traffic for cold migration, cloning, and snapshots. To use the provisioning TCP/IP stack, select **Provisioning** from the **TCP/IP stack** drop-down menu when configuring the associated VMkernel virtual network adapter. When you assign a VMkernel virtual network adapter to the provisioning stack, you cannot use the adapter for purposes other than provisioning.

## vMotion Details

This section provides details on the vMotion feature in vSphere.

### vMotion Overview

A hot cross host migration is called vMotion. A hot migration across hosts and datastores is often called a vMotion without shared storage. A hot cross vCenter Server migration is often called a cross vCenter Server vMotion. Although the term vMotion may be used to describe any hot cross host migration, this section provides details on just the traditional vMotion, where shard storage is used and cross datastore migration does not occur.

During a vMotion migration, the entire state of the virtual machine is moved to the new host. The state includes the current memory content and all the information that defines and identifies the virtual machine. The memory content includes the components of the operating system, applications, and transaction data that are in the memory. The state includes all the data that maps to the virtual machine hardware elements, such as BIOS, devices, CPU, MAC addresses for the Ethernet cards, chipset states, and registers. The associated virtual disk remains in the original location on storage that is shared between the source and destination hosts. After the virtual machine state is migrated to the destination host, the virtual machine continues execution on the destination host.

### vMotion Requirements



As explained in the *Enhanced vMotion Compatibility (EVC)* section in Chapter 4, vMotion requires that the

destination host's processors be compatible with the source host's processors to support live migration. Specifically, the destination processors must come from the same family and provide the same instruction set as the source processors. You can enable EVC in the cluster to broaden the vMotion compatibility.

Before using vMotion, you must address its host configuration requirements. Each host must meet the licensing, shared storage, and networking requirements for vMotion.

For standard vMotion, you must configure the source and destination hosts with shared storage to enable the migrated virtual machines to remain in the same datastore throughout the migration. Shared storage may be implemented with Fibre Channel, iSCSI, or NAS storage. The datastore may be VMFS or NFS. You can also leverage a vSAN datastore to meet the shared storage requirement for vMotion migrations between cluster members.

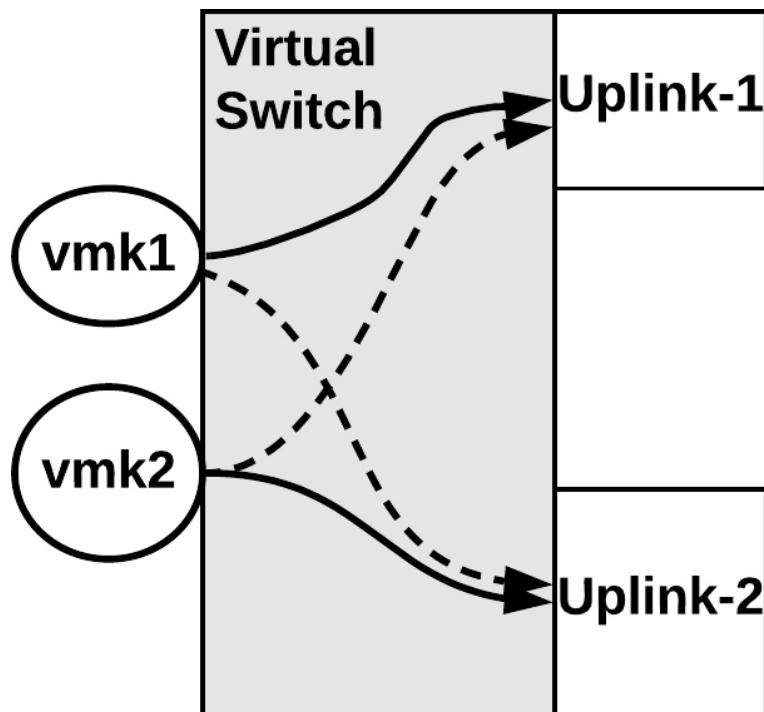
**Note**

Hot migrations that are cross host and cross datastore, which are often called vMotion without shared storage, do not require shared storage.

For vMotion, you must configure each host with a VMkernel virtual network interface connected to a virtual switch with an uplink that uses at least one physical network interface card (NIC). VMware recommends the network connection is made to a secured network. The vMotion network must provide at least 250 Mbps of dedicated bandwidth per concurrent vMotion session. For long-distance migrations, the maximum supported network round-trip time for vMotion migrations is 150 milliseconds. For faster vMotion migrations, consider using 10 Gbps NICs instead of 1 Gbps NICs.

To improve vMotion migration times even further, consider implementing multi-NIC vMotion. With multi-NIC vMotion, multiple paths are used simultaneously to carry the vMotion workload. To configure multi-NIC vMotion, you can enable vMotion traffic for two VMkernel virtual network adapters that are configured to use separate paths. For example, you can apply the following steps to enable multi-NIC vMotion, as illustrated in [Figure 5-5](#).

1. On a virtual switch, attach two uplink adapters connected to the vMotion network.
2. Connect two VMkernel adapters enabled for vMotion
3. For the first VMkernel adapter, set the first uplink path to Active and the second uplink path to Standby.
4. For the second VMkernel adapter, set the first uplink path to Standby and the second uplink path to Active.



**Figure 5-5** Multi-NIC vMotion

For more vMotion performance improvements, you can use Network I/O Control (NIOC) to guarantee network bandwidth to vMotion traffic. You can also use jumbo frames. To avoid network saturation, you can use traffic shaping to limit the average and peak bandwidth that is available to vMotion traffic.

By default, you cannot use vMotion to migrate a virtual machine that is attached to a standard switch with no physical uplinks. To change this behavior, you can set the **config.migrate.test.CompatibleNetworks.VMOnVirtualIntranet** advanced settings of vCenter Server to **false**.

**Note**

During a vMotion without shared storage migration the virtual disk data is transferred over the vMotion network.

## vMotion Migration and Data flow details

During a vMotion migration, the state of the running virtual machines is copied to the destination host over the designated vMotion network, the virtual machine is stopped on the source ESXi host, and it is resumed on the target ESXi host. The process involves the following steps.

- **Compatibility Check:** Intended to ensure that requirements are met and that the destination host can run the virtual machine.
- **Pre-copy:** Briefly stuns the source memory and starts memory trackers. Copies memory page from source to target. Tracks which source pages are modified after the pre-copy, so these pages (dirty pages) can be re-sent later.
- **Iterations of Pre-copy:** If dirty pages exist, repeat the pre-copy of just the dirty pages, while scanning for new dirtied pages. Continue iteration until no dirty pages exist or until vMotion

determines that the final page copy can be completed in less than 500 ms.

- **Switchover:** Quiesces and suspends the virtual machine execution on the source host, transfers checkpoint data, and starts the execution of the virtual machine using the checkpoint data on the target host.

The stun time (the time at which the virtual machine is not running anywhere) is typically between 100 ms and 200 ms.

## Encrypted vMotion

When migrating encrypted virtual machines, vSphere vMotion always uses encryption. For non-encrypted virtual machines, you can select one of the following encrypted vMotion options.

- **disabled:** Do not use encryption.
- **Opportunistic:** Use encryption if the source and destination hosts support it.
- **Required:** If the source or destination host does not support Encrypted vMotion, then do allow the migration.

**Note**

Only ESXi versions 6.5 and later use encrypted vSphere vMotion. To use vMotion to migrate encrypted virtual machines across vCenter Server instances, you must use the vSphere API.

## Storage vMotion Details

This section provides details on the Storage vMotion feature in vSphere.

### Storage vMotion Overview

Storage vMotion is a hot cross datastore migration. Storage vMotion enables you to migrate a virtual

machine and its disk files from one datastore to another while the virtual machine is running. Use cases for Storage vMotion include preparing for datastore maintenance (such as upgrading the underlying storage array), optimizing performance (redistribution of storage load), and transforming the virtual disk provisioning type. When you use Storage vMotion on a virtual machine, you can migrate all the virtual machine files to a single location, migrate individual virtual disks, or separate virtual disks from other virtual machine files.

**Note**

Migration with Storage vMotion changes virtual machine files on the destination datastore to match the inventory name of the virtual machine. The migration renames all virtual disk, configuration, snapshot, and NVRAM files. If the new names exceed the maximum filename length, the migration fails.

## Storage vMotion Requirements and Limitations

- Virtual disks in non-persistent mode are not supported for Storage vMotion. For virtual compatibility mode RDMs, you can migrate just the mapping file or include the migration of the data to a virtual disk file. For physical compatibility mode RDMs, you can only migrate the mapping file.
- Storage vMotion migration is not supported during VMware Tools installation.
- You cannot use Storage vMotion to migrate virtual disks larger than 2 TB from a VMFS5 datastore to a VMFS3 datastore.
- The source host running must have a license that includes Storage vMotion.
- ESXi 4.0 and later hosts do not require vMotion configuration to perform Storage vMotion migrations.
- The host on which the virtual machine is running must have access to both the source and target datastores.

## **Storage vMotion data flow details**

- The virtual machine home directory is copied to the destination datastore.
- A hidden (shadow) virtual machine starts using the copied files. The underlying processes (worlds) are visible to the ESXTOP utility. The virtual machine continues to run in pre-existing worlds.
- An initial copy of the source virtual disk is made to the destination datastore, while leveraging change block tracking (CBT) to track blocks that are changed after they are copied.
- The previous step is repeated until the amount of changed blocks is small enough to support a fast switch over.
- The system invokes a fast suspend and resume operation that transfers the running virtual machine to the idling hidden virtual machine. The virtual machine now runs in the new worlds. The pre-existing worlds that were associated with the virtual machine are removed.

# **VIRTUAL MACHINE CLONING**

In vSphere, you have many cloning options as described in this section.

## **Clone**

When you clone a virtual machine, vCenter Server creates a virtual machine that is a copy of the original virtual machine. The virtual disk files, configuration file, and other files are copied from the original virtual machine to the new virtual machine. The new virtual machine is commonly referred to as a clone. The new virtual machine files are named and stored based on parameters you provide during the deployment. You can

choose to make some configuration changes and customizations during the cloning process. The content of some of the files, such as the configuration file are modified. At the end of the operation, you can manage both the original virtual machine as well as the new virtual machine as inventory objects in vCenter Server.

### **Cold clone**

A cold clone occurs if when the source virtual machine is powered down prior to starting the clone operation. In this case, vCenter Server does not have to worry with interrupting the execution of the source virtual machine.

### **Hot Clone**

A hot clone occurs if when the source virtual machine is running during a clone operation. In this case, the vCenter Server must act not to disrupt the execution of the source virtual machine. To do so, it takes a virtual machine snapshot prior to copying data and removes the snapshot at the end of the operation.

### **Linked Clone**

A linked clone is a virtual machine that was cloned in a manner that it shares its virtual disk files with the original virtual machine (parent). The shared files are static. Much like a virtual machine that has a snapshot, a linked clone writes its virtual disk changes to separate data files. In comparison to full clones, the linked clone operation is faster and conserves disk space. You cannot use the vSphere Client to directly create linked clones. You can use PowerCLI (using the `-LinkedClone` parameter in the `New-VM` command) or other VMware products to create linked clones. For example, in VMware Horizon, you can create desktop pools based on linked clones and in vCloud Director, you can use Fast Provisioning.

### **Template**

Templates are objects in the vSphere inventory that effectively are non-executable virtual machines. A template is a master copy of a virtual machine that can be used to create and provision new virtual machines. Templates typically have a guest operating system and application software installed. They are often customized during deployment to ensure that each new virtual machine has a unique name and network settings.

You can convert a virtual machine to a template and vice versa. But the main use case for templates is for rapid deployment of new, similar virtual machines from a single template. In this case, you are effectively cloning the template again and again, allowing the template to remain unchanged and ready for future use. To update a template, such as to install the most recent guest OS updates, you can temporarily convert the template to a virtual machine, apply the updates, and convert back to template.

When you deploy a virtual machine from a template, vCenter Server creates a virtual machine that is a copy of the original template. The virtual disk files, configuration file, and other files are copied from the template to the new virtual machine. The new virtual machine files are named and stored based on parameters you provide during the deployment. You can choose to make some configuration changes and customizations during the cloning process. The content of some of the files, such as the configuration file are modified. At the end of the operation, you can manage both the original template as well as the new virtual machine as inventory objects in vCenter Server.

Deploying a virtual machine from a template is much like cloning a virtual machine. In either case, a new virtual machine is created by copying a source object. For template deployments, the source object is a template.

For virtual machine cloning, the source object is a virtual machine.

## Instant Clone



Starting with vSphere 6.7, you can use the Instant Clone technology to hot clone a running virtual machine using technology that is much like a combination of vMotion and Linked Clone technology. The result of an Instant Clone operation is a new virtual machine (destination virtual machine) that is identical to the source virtual machine. The processor state, virtual device state, memory state, and disk state of the destination virtual machine matches the source virtual machine. To avoid network conflicts, you can customize the virtual NICs' MAC addresses, but the guest customization feature is not supported for instant clones. You cannot use the vSphere Client to perform an instant clone operation.

The main use case for instant clone is just in time deployment in virtual desktop infrastructure (VDI). Instant clones enable you to perform large scale deployments by creating virtual machines from a controlled point in time. For example, VMware Horizon uses Instant Clone to improve the provisioning process for virtual desktops. In comparison to View Composer, which uses Linked clones, Instant Clone eliminates some steps (such as reconfigure and checkpoints) and replaces other steps to greatly reduce the provisioning time. Other use cases are large deployments of identical virtual servers in the cloud and situations where you want to reduce boot storms and provisioning times.

During an Instant Clone (vmFork) operation, the system quiesces and stuns the source virtual machine, creates and transfers a checkpoint, customizes the destination

MAC address and UUID, and forks the memory and disk. The destination virtual machine shares the parent virtual machine's disk and memory for reads. For writes, the destination machine uses copy on write (COW) to direct disk and memory changes to delta files and private memory space.

The requirements for instant clones may depend on the software applications that use the API to perform the cloning operations. For example, VMware Horizon 7.1 requires static port binding, ESXi 6.0 U1 or later, and a distributed virtual switch

Instant Cloned virtual machines are fully independent vCenter Server inventory objects. You can manage Instant Clone destination virtual machines like regular virtual machines without any restrictions.

## REVIEW ALL KEY TOPICS

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 5-5](#) lists a reference of these key topics and the page numbers on which each is found.



**Table 5-5** Key Topics for Chapter 5

---

Key Topic Element	Description	Page Number
Procedure	Host Profile Workflow	
List	Content Library limitations	
List	Files in a virtual machine snapshot	
List	Use Cases for snapshots	
List	Requirements for Cross vCenter Server Migrations	
Section	Virtual Machine Migration Limitations	
Section	vMotion Requirements	
Section	Instant Clone	

## DEFINE KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary:

**vSphere Inventory:** The vSphere inventory is a collection of managed virtual and physical objects.

**Data Center:** A data center is a container object in the vSphere inventory that is an aggregation of all the different types of objects used to work in virtual infrastructure.

**Cluster:** A cluster is a set of ESXi hosts that are intended to work together as a unit.

**Resource Pool:** Resource pools are container objects in the vSphere inventory that are used to compartmentalize the CPU and memory resources of a host or cluster.

**Templates:** Templates are objects in the vSphere inventory that effectively are non-executable virtual machines.

**vApp:** A vApp is a container object in vSphere that provides a format for packaging and managing applications.

**Host Profile:** A Host Profile is a feature that enables you to encapsulate the configuration of one host and apply it to other hosts.

**Content Library:** A content library is a repository that can be used to share files such as virtual machine templates, vApps, and image files among a set of vCenter Servers.

**Virtual Machine Snapshot:** Virtual Machine Snapshots capture the state of a virtual machine and the data in the virtual machine at a specific point in time.

**VMware Tools:** VMware Tools is a set of software modules and services, including services that can communicate with the VMkernel.

**vMotion:** vMotion is the hot, cross host migration of a virtual machine.

**Storage vMotion:** Storage vMotion is the hot, cross dataastpre migration of a virutal machine.

## REVIEW QUESTIONS

- 1.** Which of the following is not a valid use case for virtual machine snapshots?
  - a.** Rollback guest OS changes.
  - b.** Recover from the accidental deletion of a flat file.
  - c.** Troubleshooting
  - d.** Linked clone in a vRA blueprint
  
- 2.** You are troubleshooting a virtual machine using the vSphere Client. Which if the following is not a valid debugging and statistics Advanced setting?
  - a.** Record Trivial
  - b.** Record Debugging
  - c.** Run Normal

**d. Record Statistics**

- 3.** You want to migrate a virtual machine with a 2.5 TB virtual disk. What is the minimum ESXi version that supports this?
- a. 6.0**
  - b. 6.5**
  - c. 6.7**
  - d. 7.0**
- 4.** You want to hot-migrate a virtual machine from one ESXi host and VMFS datastore to another ESXi host and VMFS datastore. Which of the following statements are true?
- a. This operation is not supported in vSphere 7.0**
  - b. The virtual disk data is transferred over the management network.**
  - c. The virtual disk data is transferred over the vMotion network.**
  - d. You must perform the operation in two separate steps (vMotion and Storage vMotion)**
- 5.** You are supporting thousands of virtual machines in a vSphere environment. Which of the following features are associated with vmFork?
- a. Instant Clone**
  - b. Linked Clone**
  - c. Snapshot**
  - d. Cross-vCenter vMotion**

# **Chapter 6. VMWare Product Integration [This content is currently in development.]**

**This content is currently in development.**

# Chapter 7. vSphere Security

**This chapter covers the following subjects:**

- vSphere Certificates
- vSphere Permissions
- ESXi and vCenter Server Security
- vSphere Network Security
- Virtual Machine Security
- Available Add-on Security

This chapter contains information related to VMware 2V0-21.20 exam objectives 1.10, 1.11, 4.10, 4.11, 4.11.1, 4.13, 7.7, 7.8

## “Do I Know This Already?” Quiz

### vSphere Certificates

#### vSphere Certificates Overview

#### Certificate Requirements

#### ESXi Host Certificates

### vSphere Permissions

#### Authentication and Authorization

#### Inventory Hierarchy and Objects

#### Privileges and Roles

#### Permissions

#### Global Permissions

#### Best Practices for Roles and Permissions

#### Required Privileges for Common Tasks

## How Permissions are Applied by vCenter Server.

### ESXi and vCenter Server Security

#### Built-in Security Features

#### Security Profiles

#### ESXi Password Hardening

#### Join an ESXi Host to a Directory Service

#### vSphere Authentication Proxy

#### ESXi Host Access

#### Control MOB Access

#### ESXi Secure Boot and TPM

#### vSphere Trust Authority (vTA)

#### vCenter Server Security

##### User Access

##### vCenter SSO Password Policy

##### Restrict Administrative Privileges

##### Restrict vCenter Server Access

##### Control Datastore Browser Access

##### vCenter Server and Client Certificates

##### Time Synchronization

### vSphere Network Security

#### Firewalls

#### Segmentation and Isolation

#### Internet Protocol Security

#### General Networking Security

#### Recommendations

#### Network Security Policies

### Virtual Machine Security

#### Virtual Machine Hardening Best Practices

#### Configure UEFI Boot

Disable Unexposed Features

Other Common Settings

Virtual Machine Risk Profiles

Protect Virtual Machine Against Denial-of-Service Attacks

Control VM Device Connections

Virtual Machine Encryption

Encrypted vSphere vMotion

Virtual Trusted Platform Module (vTPM)

Virtual Intel Software Guard Extension (vSGX)

Available Add-on Security

Compliance using vRealize Operations Manager

VMware NSX

AppDefense

Summary

Review All the Key Topics

Complete the Tables and Lists from Memory

Definitions of Key Terms

This chapter covers exam topics related to hardening a vSphere Environment.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section.

Regardless, the authors recommend that you read the entire chapter at least once. Table 7-1 outlines the major headings in this chapter and the corresponding “Do I

“Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 7-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions Covered in This Section
vSphere Certificates	1, 2
vSphere Permissions	3, 4
ESXi and vCenter Server Security	5, 6
vSphere Network Security	7
Virtual Machine Security	8, 9
Available Add-on Security	10

- 1.** You are preparing to import certificates for your vSphere environment. Which of the following is not a requirement?
  - a.** x509 version 3
  - b.** PEM format: PKCS8 and PKCS1
  - c.** Key Usage: Digital Signature, Key Encipherment.
  - d.** Key size: 1024 bits to 16384 bits
- 2.** You are making plans for ESXi host certificates. Which of the following is not a valid certificate mode?
  - a.** VMware Endpoint Certificate Store
  - b.** VMware Certificate Authority
  - c.** Custom Certificate Authority
  - d.** Thumbprint Mode
- 3.** You are preparing to apply permissions in vCenter Server. Which of the following is a system role?
  - a.** Read Only

- b. Virtual Machine User**
  - c. Datastore Consumer**
  - d. Content Library Administrator**
- 4.** You are configuring permissions in vCenter Server. Which privilege is required for a user to use Storage vMotion to migrate a virtual machine?
  - a. Resource.Migrate Powered On Virtual Machine**
  - b. Resource.Migrate Powered Off Virtual Machine**
  - c. Resource.Assign Virtual Machine to Resource Pool on the cluster**
  - d. Resource.Assign Virtual Machine to Resource Pool on the VM folder**
- 5.** You are hardening your ESXi hosts. Which of the following is true concerning normal lockdown mode?
  - a. All users with administrator privileges on the host can access the DCUI**
  - b. All users in the Exception Users list can access the DCUI**
  - c. No one can access the DCUI**
  - d. Users identified in the host's DCUI.Access advanced option can access the DCUI**
- 6.** You are creating user accounts in the vCenter SSO domain. With default settings, which of the following is a valid password?
  - a. VMware1!**
  - b. VMworld!**

**c. VMwareRocks**

**d. VMwarerocks!!**

**7.** You are configuring IPsec on your ESXi hosts.

Which of the following commands can you use to list the available security associations on an ESXi host?

**a. esxcli network ipsec sa list**

**b. esxcli network ip ipsec sa list**

**c. esxcli network ip ipsec list**

**d. esxcli network ip sa list**

**8.** You want to migrate virtual machines across

vCenter Instances. Concerning vMotion migration across vCenter Server instances, which of the following statements is true? (pick two)

**a. For encrypted vMotion, you can use the vSphere Client**

**b. For encrypted vMotion, you must use the vSphere APIs.**

**c. vMotion of encrypted virtual machines is not supported**

**d. Encrypted vMotion of non-encrypted virtual machines is not supported.**

**9.** You are hardening virtual machines in your

vSphere 7 environment. Which of the following options can be set to TRUE because it disables an unexposed feature?

**a. tools.guestlib.enableHostInfo**

**b. tools.setInfo.sizeLimit**

**c. vmx.log.keepOld**

**d. isolation.tools.ghi.launchmenu.change**

**10.** You want to use micro-segmentation to protect the applications and data in your vSphere environment. What should you implement?

- a.** VMware AppDense
- b.** VMware NSX
- c.** VMware vRealize Automation
- d.** VMware vRealize Log Insight

## VSPHERE CERTIFICATES

This section describes the use of certificates in a vSphere environment.

### vSphere Certificates Overview

In vSphere 7.0, you can use the default approach to provision vCenter Server components and ESXi hosts with VMware Certificate Authority (VMCA) certificates. You can also use custom certificates which you store in the VMware Endpoint Certificate Store (VECS). vCenter Server supports custom certificates that are generated and signed from your own enterprise Public Key Infrastructure (PKI). vCenter Server also supports custom certificates that are generated and signed trusted third-party Certificate Authorities (CAs), such as VeriSign or GoDaddy. vSphere uses certificates to do the following.

- Encrypt communications nodes, such as a vCenter Server and ESXi hosts.
- Authenticate vSphere services.
- Perform internal actions such as signing tokens.

**Table 7-2** identifies the core identity services in vSphere.

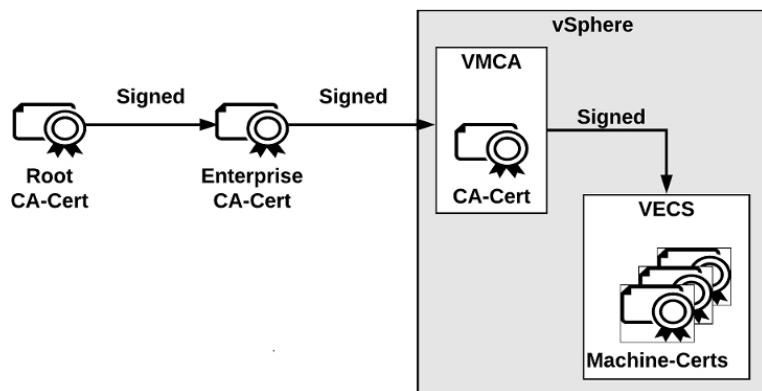
**Table 7-2** Core Identity Services in vSphere

Service	Description
VMware Directory Service (vmdir)	Identity source that handles SAML certificate management for authentication with vCenter Single Sign-On.
VMware Certificate Authority (VMCA)	Issues certificates for VMware solution users, machine certificates for machines on which services are running, and ESXi host certificates. VMCA can be used as is, or as an intermediary certificate authority.
VMware Authentication Framework Daemon (VMAFD)	Includes the VMware Endpoint Certificate Store (VECS) and several internal authentication services.

VECS is the local (client-side) repository for certificates, private keys, and other certificate information that can be stored in a keystore. You can choose not to use VMCA as your certificate authority and certificate signer, but you must use VECS to store all vCenter certificates and keys. ESXi certificates are stored locally on each host and not in VECS. The stores included in VECS are described in the *vCenter Server Components* section in [Chapter 8](#) in [Table 8-9](#).

The VMware Certificate Authority (VMCA), which runs in every vCenter Server Appliance, is vSphere's internal certificate authority. It provides all the required certificates for vCenter Server and ESXi. VMCA's default configuration provides the lowest operational overhead for certificate management and immediately secures the solution without any other modification. vSphere provides mechanism to renew expired certificates and to replace specific certificates with your own certificates.

You can replace the VMCA root certificate with a certificate that is signed by an enterprise CA or third-party CA. IN this case, VMCA signs the custom root certificate each time it provisions certificates, making VMCA an intermediate CA, as illustrated in [Figure 7-1](#).



**Figure 7-1**

You can replace the existing VMCA-signed certificates with custom certificates, bypassing VMCA and making you responsible for all certificate provisioning and monitoring.

VMware recommends that you replace only the SSL certificate that provides encryption between nodes. VMware does not recommend replacing either solution user certificates or STS certificates. VMware does not recommend using a subordinate CA in place of the VMCA. If you fail to follow these recommendations, you might encounter significant complexity and an increase in your operational risk. VMware recommendations for managing certificates are summarized in Table 7-3.

**Table 7-3** Recommended Modes for Managing Certificates

Mode	Description	Advantages
VMCA Default Certificates	VMCA provides all the certificates for vCenter Server and ESXi hosts.	Lowest overhead option. VMCA manages the certificate life cycle for vCenter Server and ESXi host
VMCA Default Certificates with External SSL Certificates (Hybrid Mode)	You replace the vCenter Server SSL certificates and allow VMCA to manage certificates for solution users and ESXi hosts. Optionally, for high-security conscious deployments, you can replace the ESXi host SSL certificates as well.	VMCA manages internal certificates but you get the benefit of using your corporate-approved, trusted SSL certificates.

## Certificate Requirements

The following is required for all imported certificates.

- Key size: 2048 bits to 16384 bits
- PEM format. VMware supports PKCS8 and PKCS1 (RSA keys). When you add keys to VECS, they are converted to PKCS8.
- x509 version 3
- SubjectAltName must contain DNS Name=machine\_FQDN
- CRT format
- Contains the following Key Usages: Digital Signature, Key Encipherment.
- Enhanced Key Usage can be either empty or contain Server Authentication.

VMCA does not support the following certificates.

- Certificates with wildcards.
- The algorithms md2WithRSAEncryption 1.2.840.113549.1.1.2, md5WithRSAEncryption 1.2.840.113549.1.1.4, and sha1WithRSAEncryption 1.2.840.113549.1.1.5 are not recommended.
- The algorithm RSASSA-PSS with OID 1.2.840.113549.1.1.10 is not supported.

If you do not generate Certificate Signing Requests (CSRs) using Certificate Manager, ensure that the CSR includes the fields listed in [Table 7-4](#).

**Table 7-4** Required Fields for the CSR

---

<b>String</b>	<b>X.500 Attribute Type</b>
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

If you use VMCA as an intermediate CA, you can use the vSphere Certificate Manager to create the CSR or you can create the CSR manually. When creating the CSR manually, in addition to the previously stated requirements, you should consider the requirements in [Table 7-5](#), which are based on the specific certificate types.

**Note**

Do not use CRL Distribution Points, Authority Information Access, or Certificate Template Information in any custom certificates.

**Table 7-5** Requirements for Certificates when VMCA is an Intermediate CA

---

Certificate Type	Additional Requirements
Root certificate	Set CA extension to true and include “cert sign”. For example, use the following in the CSR.  <pre>basicConstraints = critical, CA:true keyUsage = critical, digitalSignature, keyCertSign</pre>
Machine SSL certificate	No additional requirements
Solution user certificate	Use a different <b>Name</b> value for each solution user, which may appear as <b>CN</b> under <b>Subject</b> depending on your tool.

VMCA provisions your environment with certificates that are described in [Table 7-6](#), including machine SSL certificates for secure connections, solution user certificates for service authentication with vCenter Single Sign-On, and ESXi host certificates.

**Table 7-6** Certificates in vSphere

---

Certificate	Provisioned	Details
ESXi certificates	VMCA (default)	Stored locally on ESXi host in the <code>/etc/vmware/ssl</code> directory when the host is first added to vCenter Server and when it reconnects.
Machine SSL certificates	VMCA (default)	<p>Stored in VECS.</p> <p>Used to create an SSL socket on for SSL client connections, for server verification, and for secure communication such as HTTPS and LDAPS.</p> <p>Used by the reverse proxy service, the vCenter Server services (vpxd), and the VMware Directory Service (vmdir).</p> <p>Uses standard X.509 version 3 certificates to encrypt session information.</p>
Solution user certificates	VMCA (default)	<p>Stored in VECS.</p> <p>Used by solution users to authenticate to vCenter Single Sign-On through SAML token exchange.</p>
vCenter Single Sign-On SSL signing certificate	Provisioned during installation.	<p>Used throughout vSphere for authentication, where a SAML token represents the user's identity and contains group membership information.</p> <p>You can manage this certificate from the command line. Do not change this certificate in the filesystem or unpredictable behavior results.</p>
VMware Directory Service (VMDIR) SSL certificate	Provisioned during installation.	Starting with vSphere 6.5, the machine SSL certificate is used as the vmdir certificate.
vSphere Virtual Machine Encryption Certificates	Depends	<p>Used for virtual machine encryption, which relies on an external Key Management Server (KMS).</p> <p>Depending on how the solution authenticates to the KMS, it might generate certificates and store them in VECS.</p>

A solution user presents the certificate to vCenter Single Sign-On when it first authenticates, after a reboot, and after a timeout has elapsed. The timeout (Holder-of-Key Timeout) can be set from the vSphere Client and defaults to 2592000 seconds (30 days).

The following solution user certificate stores are included in VECS:

- **Machine:** Used by the license server and the logging service.
- **vpxd:** Used by the vCenter service (vpxd) to authenticate to vCenter Single Sign-On.
- **vpxd-extension:** Used by the Auto Deploy service, inventory service, and other services that

are not part of other solution users.

- **vsphere-webclient:** Use by the vSphere Client and some additional services such as the performance chart service.
- **wcp:** Used by vSphere with Kubernetes.

**Note**

Do not confuse the machine solution user certificate with the machine SSL certificate. The machine solution user certificate is used for the SAML token exchange. The machine SSL certificate is used for secure SSL connections for a machine.

## ESXi Host Certificates

In vSphere 6.0 and later, vCenter Server supports the certificate modes for ESXi hosts that are described in **Table 7-7**.

**Table 7-7** Certificate Modes for ESXi Hosts

Certificate Mode	Description
VMware Certificate Authority (default)	Use this mode when VMCA provisions all ESXi hosts, either as the top-level CA or as an intermediate CA. In this mode, you can refresh and renew certificates from the vSphere Client.
Custom Certificate Authority (CA)	Use this mode with custom certificates signed by a third-party or an enterprise CA. In this mode, you cannot refresh and renew certificates from the vSphere Client.
Thumbprint Mode	Use this legacy (vSphere 5.5) mode only for troubleshooting. In this mode, vCenter Server checks the certificate format, not the certificate's validity. For example, expired certificates are accepted. Some vCenter 6.x and later services might not work correctly in thumbprint mode.

**Note**

If you apply custom certificates to the hosts but do not change the certificate mode to Custom Certificate Authority, VMCA might replace custom certificates, when you select **Renew** in the vSphere Client.

You can use the vSphere Client to view expiration data for certificates, whether it is signed by VMCA or a third party. The vCenter Server raises yellow alarms for hosts

where certificates expire shortly (less than 8 months) and red alarms where certificates in the Expiration Imminent state (expire in less than 2 months).

ESXi hosts that boot from installation media, have an autogenerated certificate. When a host is added to the vCenter Server system, it is provisioned with a certificate that is signed by VMCA as the root CA.

## VSPHERE PERMISSIONS

This section describes the permission model in vSphere.

### Authentication and Authorization

vCenter Single Sign-On (SSO) is responsible for authenticating vCenter Server users. The user accounts may be defined directly in the SSO domain or in a supported identity source. vCenter Server uses permissions and roles to provide authorization, which controls what an authenticated user can do. It allows you to assign a permission to an object in the vCenter Server inventory, by specifying which privileges a specific user or group has on that object.

The default SSO domain name is `vsphere.local`, but you can change it during the domain creation. Initially, only the SSO domain administrator is authorized to log into vCenter Server. By default, the SSO domain administrator is `administrator@vsphere.local`. You can create additional users in the SSO domain. You can add supported identity sources to SSO, including Active Directory over LDAP, a native Active Directory (Integrated Windows Authentication) domain, or an OpenLDAP directory service.

Starting in vSphere 7.0, vCenter Server supports federated authentication, where you configure a connection to an external identity provider to replace

vCenter Server as the identity provider. Currently, vCenter Server supports only Active Directory Federation Services (AD FS) as an external identity provider.

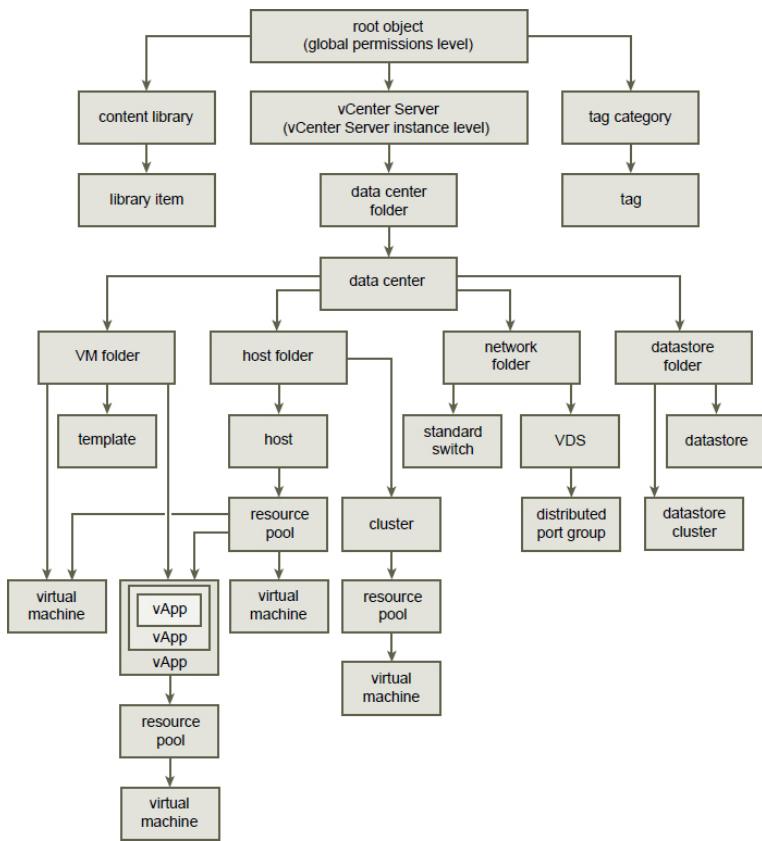
The permission model for vCenter Server systems relies on assigning permissions to objects in the object hierarchy. A permission is the assignment of a user (or group) and a role to an inventory object.

When you add a new identity source to SSO, all users can be authenticated, but will effectively have the `No Access` role to the vCenter Server inventory.

## Inventory Hierarchy and Objects

You can assign permissions to objects at different levels of the inventory hierarchy, such as ESXi hosts, clusters, virtual machines, folders, resource pools, datastores and networks. You can also assign permissions to a global root object to apply the permissions to all object in all solutions. You can apply permissions to container objects and optionally allow the permissions to propagate to its descendent objects. Most objects inherit permissions from its parents via a single path, but virtual machines inherit permissions from virtual machine folders, hosts, resource pools, etc., as you can see in [Figure 7-2](#). If an object inherits permissions from two parent objects, then its inherited permissions are determined by the union of the permissions. [Figure 7-2](#) is a diagram from the *VMware vSphere 7.0 Security Guide* that shows the vSphere Inventory Hierarchy.





**Figure 7-2** vSphere Inventory Hierarchy

Objects might have multiple permissions, but only one permission for each user or group. In other words, you cannot assign two permissions on a specific object that specify the same group. If multiple permissions are applied to a specific object using multiple groups and if a specific user belongs to more than one of these groups, then the effective permissions for that user on that object is the union of the privileges in applicable roles.

Privileged users can define permissions on managed objects.

- Clusters
- Data centers
- Datastores
- Datastore clusters

- Folders
- Hosts
- Networks (except vSphere Distributed Switches)
- Distributed port groups
- Resource pools
- Templates
- Virtual machines
- vSphere vApps

## Privileges and Roles

Privileges are the lowest-level access controls, which can be used to define the actions that a user can take on an object in the vSphere inventory. [Table 7-8](#) describes a few of the available privilege categories and a few sample privileges in each category.

**Table 7-8** Sample Privileges

---

Category	Sample privileges
Virtual Machine Configuration	Virtual machine.Configuration.Add existing disk
	Virtual machine.Configuration.Add new disk
	Virtual machine.Configuration.Change CPU count
Datastore	Datastore.Allocate space
	Datastore.Browse datastore
	Datastore.Remove file
Virtual machine Snapshot	Virtual machine .Snapshot management.Create snapshot
	Virtual machine .Snapshot management.Rename Snapshot
	Virtual machine .Snapshot management.Revert to snapshot

A role is a set of privileges. The vCenter Server provides many roles out of the box. You cannot modify the vCenter Server System Roles, which are described in [Table 7-9](#). You can modify the Sample Roles, but VMware recommends that you do not modify these roles directly, but instead clone the roles and modify the clones to suit your case.

**Note**

Changes to roles take effect immediately even for users who are currently logged into vCenter Server. One exception is using searches where the change is not realized until the next time the user logs into vCenter Server.

**Table 7-9** System Roles in vCenter Server 7.0

System Role	Details
Read Only	Allows the user to view the state of an object and details about the object. For example, users with this role can view virtual machine attributes, but cannot open the VM console.
Administrator	Includes all privileges of the Read Only role plus allows the user to view and perform all actions on the object. If you have the Administrator role on an object, you can assign privileges to individual users and groups. If you have the Administrator role in vCenter Server, you can assign privileges to users and groups in the default SSO identity source. By default, the administrator@vsphere.local user has the Administrator role on both vCenter Single Sign-On and vCenter Server.
No Access	Prevents users from viewing or interacting with the object. New users and groups are effectively assigned this role by default.
No Cryptography Administrator	Includes all privileges of the Administrator role, except for Cryptographic operations privileges. This role allows administrators to designate users who can perform all administrative tasks, except encrypting or decrypting virtual machines or accessing encrypted data.
Trusted Infrastructure Administrator Role	Allows users to perform VMware vSphere Trust Authority operations on some objects. Membership in the TrustedAdmins group is required for full vSphere Trust Authority capabilities.

The sample roles in vCenter Server 7.0 are:



- Resource Pool Administrator (sample)
- Virtual Machine User (sample)
- VMware Consolidated Backup User (sample)
- Datastore Consumer (sample)
- Network Administrator (sample)
- Virtual Machine Power User (sample)
- Content Library Administrator (sample)
- Content Library Registry administrator (sample)

To get familiar with the privileges in a sample role, you can edit the role and explore the privileges that are included in the role. For example, if you edit the Virtual Machine Console User role, you will see that it only includes some privileges in the Virtual Machine >

Interaction category and no other privileges.

Specifically, it includes only these privileges:

- Answer Question
- Configure CD media
- Configure floppy media
- Connect devices
- Console interaction
- Install VMware Tools
- Power off
- Power on
- Reset
- Suspend

**Note**

If you create a role, it does not inherit privileges from any of the system roles.

## Permissions

The permission model for vCenter Server systems relies on assigning permissions to objects in the object hierarchy. A permission is the assignment of a user (or group) and a role to an inventory object. A permission is set on an object in the vCenter object inventory. Each permission associates the object with a group (or user) and a role, as illustrated in [Figure 7-3](#). For example, you can select a virtual machine object, add one permission that gives the `ReadOnly` role to `Group 1`, and add a second permission that gives the `Administrator` role to `User 2`.

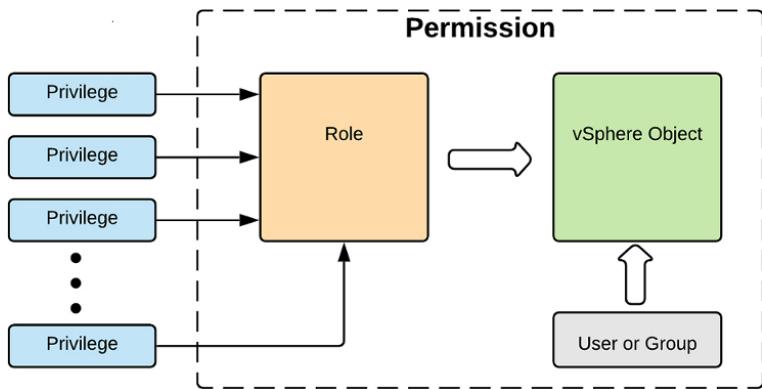


Figure 7-3

## Global Permissions

Most entities that appear in the vCenter Server inventory are managed objects, whose access can be controlled using permissions. You cannot modify permissions on entities that derive permissions from the root vCenter Server system, such as the following.

- Custom fields
- Licenses
- Roles
- Statistics intervals
- Sessions

The global root object is used to assign permissions across solutions. The vCenter Server is an example of a solution and it is attached as a child to the global root object in the hierarchy. The Content Library and Tag Category objects are also attached as children to the global root object. Global permissions are permissions that are applied to the global root object and span solutions. For example, a global permission can be applied to both vCenter Server and vRealize Orchestrator. Each solution has its own root object in the hierarchy, whose parent is the global root object. You can give a group of users Read permissions to all objects in both object hierarchies.

## Best Practices for Roles and Permissions

VMware recommends the following best practices when configuring roles and permissions in your vCenter Server environment:

- Where possible, assign roles to groups rather than to individual users.
- Grant permissions to users (groups) only on the objects where they are required. Use the minimum number of permissions to meet the required functionality.
- If you assign a restrictive role to a group, check that the group does not contain the Administrator user or other users who require administrative privileges.
- Use folders to group objects. For example, to grant modify permission on one set of hosts and view permission on another set of hosts, place each set of hosts in a folder.
- Use caution when adding a permission to the root vCenter Server objects. Users with privileges at the root level have access to global data on vCenter Server, such as roles, custom attributes, and vCenter Server settings.
- Consider enabling propagation when you assign permissions to an object. Propagation ensures that new objects in the object hierarchy inherit permissions. For example, you can assign a permission to a virtual machine folder and enable propagation to ensure the permission applies to all VMs in the folder.
- Use the `No Access` role to mask specific areas of the hierarchy. The `No Access` role restricts access for the users or groups with that role.

**Note**

Changes to licenses propagate to all linked vCenter Server systems in the same vCenter Single Sign-On domain.

## Required Privileges for Common Tasks

Many tasks require permissions on multiple objects in the inventory. Consider the following:

- To perform any operation that consumes storage space, such taking a snapshot, you must have the **Datastore.Allocate Space** privilege on the target datastore in addition to having the directly required privileges on the major object.
- Moving an object in the inventory hierarchy requires appropriate privileges on the object itself, the source parent object (such as a folder or cluster), and the destination parent object.
- Deploying a virtual machine directly to a host or cluster requires the **Resource.Assign Virtual Machine to Resource Pool** privilege, because each host or cluster has its own implicit resource pool.

Table 7-10 shows the required privileges for a few common tasks.

**Table 7-10** Required permissions for common tasks

Task	Required Privileges
Create a virtual machine	<p>On the destination folder or datacenter:</p> <p><b>Virtual Machine.Inventory.Create new</b></p> <p><b>Virtual Machine.Configuration.Add New Disk</b></p> <p><b>Virtual Machine .Configuration.Add Existing Disk</b></p> <p><b>Virtual Machine.Configuration.Raw Device</b></p> <p>On the destination host, cluster, or resource pool:</p> <p><b>Resource.Assign Virtual Machine to Resource Pool</b></p> <p>On the destination datastore or datastore folder:</p> <p><b>Datastore.Allocate Space</b></p> <p>On the network</p> <p><b>Network.Assign Network</b></p>
Deploy a virtual machine from a template	<p>On the destination folder or datacenter:</p> <p><b>Virtual Machine.Inventory.Create from existing</b></p> <p><b>Virtual Machine.Configuration.Add New Disk</b></p> <p>On a template or template folder:</p> <p><b>Virtual Machine.Provisioning.Deploy Template</b></p> <p>On the destination host, cluster or resource pool:</p> <p><b>Resource.Assign Virtual Machine to Resource Pool</b></p>

	<p>On the destination datastore or folder of datastores:  <b>Datastore.Allocate Space</b></p> <p>On the network that the virtual machine will be assigned to:  <b>Network.Assign Network</b></p>
Take a virtual machine snapshot	<p>On the virtual machine or a folder of virtual machines:  <b>Virtual Machine.Snapshot Management.Create Snapshot</b></p> <p>On the destination datastore or folder of datastores:  <b>Datastore.Allocate Space</b></p>
Move a virtual machine into a resource pool	<p>On the virtual machine or folder of virtual machines:  <b>Resource.Assign Virtual Machine to Resource Pool</b>  <b>Virtual Machine.Inventory.Move</b></p> <p>On the destination resource pool:  <b>Resource.Assign Virtual Machine to Resource Pool</b></p>
Install a guest operating system on a virtual machine	<p>On the virtual machine or folder of virtual machines:  <b>Virtual Machine.Interaction.Answer Question</b>  <b>Virtual Machine.Interaction.Console Interaction</b>  <b>Virtual Machine.Interaction.Device Connection</b>  <b>Virtual Machine.Interaction.Power Off</b>  <b>Virtual Machine.Interaction.Power On</b>  <b>Virtual Machine.Interaction.Reset</b>  <b>Virtual Machine.Interaction.Configure CD Media</b>  <b>Virtual Machine.Interaction.Configure Floppy Media</b>  <b>Virtual Machine.Interaction.Tools Install</b></p> <p>On a datastore containing the installation media ISO image:  <b>Datastore.Browse Datastore</b></p> <p>On the datastore to which you upload the installation media ISO image:  <b>Datastore.Browse Datastore</b></p>

	<b>Datastore.Low Level File Operations</b>
Migrate a virtual machine with vMotion	<p>On the virtual machine or folder of virtual machines:</p> <p><b>Resource.Migrate Powered on Virtual Machine</b></p> <p><b>Resource.Assign Virtual Machine to Resource Pool</b></p> <p>On the destination host, cluster, or resource pool:</p> <p><b>Resource.Assign Virtual Machine to Resource Pool</b></p>
Cold migrate (relocate) a virtual machine	<p>On the virtual machine or folder of virtual machines:</p> <p><b>Resource.Migrate Powered Off Virtual Machine</b></p> <p><b>Resource.Assign Virtual Machine to Resource Pool</b></p> <p>On the destination host, cluster, or resource pool:</p> <p><b>Resource.Assign Virtual Machine to Resource Pool</b></p> <p>On the destination datastore:</p> <p><b>Datastore.Allocate Space</b></p>
Migrate a Virtual Machine with Storage vMotion	<p>On the virtual machine or folder of virtual machines:</p> <p><b>Resource.Migrate Powered On Virtual Machine</b></p> <p>On the destination datastore:</p> <p><b>Datastore.Allocate Space</b></p>
Move a host into a cluster	<p>On the host:</p> <p><b>Host.Inventory.Add Host to Cluster</b></p> <p>On the destination cluster:</p> <p><b>Host.Inventory.Add Host to Cluster</b></p> <p><b>Host.Inventory.Modify.cluster</b></p>

## How Permissions are Applied by vCenter Server.

As you assign each permission, you can choose whether to allow the permission to propagate to child objects.

This setting is made per permission and cannot be universally applied. The default setting is to allow propagation to child objects. The propagation is applied to the vSphere Inventory Hierarchy as shown in Figure

7-2.



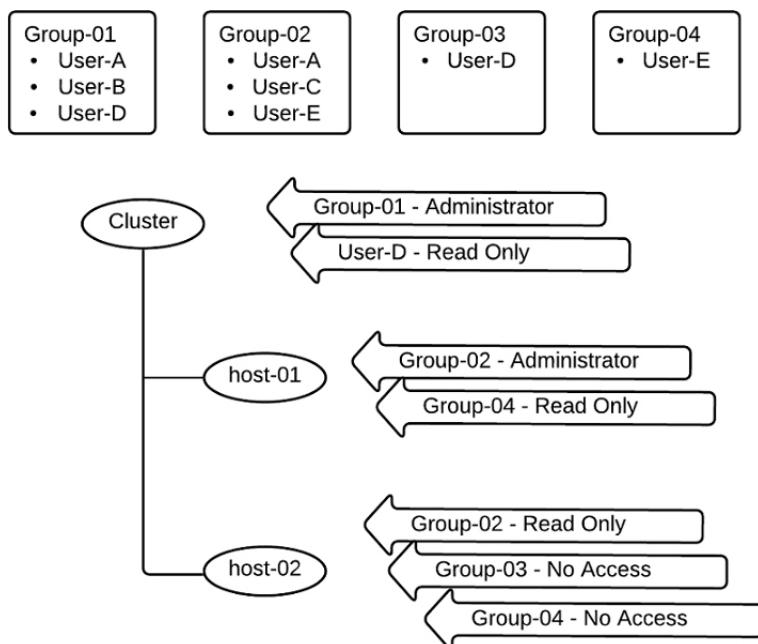
In the case where conflicting permissions are applied to an object and to its ancestors, the permissions that are assigned at a lower level object in the inventory hierarchy override permissions assigned at a higher level object. In the case where multiple permissions are assigned to the same object to different groups that contain a specific user, then that user's effective permissions are the union of the associated privileges. Permissions assigned to a user override permissions assigned to groups containing the user, when the permissions are applied to the same object. The No Access permission is given precedence over all other roles. For example, consider the following scenario, which is illustrated in [Figure 7-4](#).

- One cluster exists in the inventory, which contains host-o1 and host-o2.
- The user account User-A is a member of groups Group-o1 and Group-o2
- The user account User-B is a member of group Group-o1
- The user account User-C is a member of group Group-o2
- The user account User-D is a member of groups Group-o1 and Group-o3
- The user account User-E is a member of groups Group-o2 and Group-o4

**Propagate to Child Objects** is enabled for each of the following permissions

- A permission assigns Group-o1 the Administrator role on the Cluster
- A permission assigns Group-o2 the Administrator role on host-o1
- A permission assigns Group-o2 the Read Only role on host-o2

- A permission assigns User-D the Read Only role on the cluster
- A permission assigns Group-03 the No Access role on host-02
- A permission assigns Group-04 the Read Only role on host-01
- A permission assigns Group-04 the No Access role on host-02



**Figure 7-4**

In this scenario, the following effective permissions apply

- User-A:
  - Can perform all tasks on the cluster object
  - Can perform all tasks on the host-01 object
  - Can only view the host-02 object
- User-B:
  - Can perform all tasks on the cluster object

- Can perform all tasks on the host-o1 object
- Can perform all tasks on the host-o2 object
- User-C:
  - Cannot view or perform any task on the cluster object
  - Can perform all tasks on the host-o1 object
  - Can only view the host-o2 object
- User-D
  - Can only view the cluster object
  - Can only view the host-o1 object
  - Cannot view or perform any task on the host-o2 object
- User-E
  - Cannot view or perform any task on the cluster object
  - Can perform all tasks on the host-o1 object
  - Cannot view or perform any task on the host-o2 object

## **ESXI AND VCENTER SERVER SECURITY**

ESXi has many built-in security features such as CPU isolation, memory isolation, and device isolation. An ESXi host is protected with a firewall that is intended to only permit required network traffic. Starting with vSphere 6.0, ESXi hosts participate in the certificate infrastructure and, by default, are provisioned with certificates that are signed by the VMware Certificate Authority (VMCA).

Optionally, you can further harden ESXi by configuring features such as lockdown mode, certificate replacement, and smart card authentication for enhanced security.

You should consider limiting direct access to ESXi hosts, using security profiles, using host profiles, and managing certificates. Additionally, you can take other security measures, such as using multiple networks to segregate ESXi network functions, configuring Smart Card Authentication, and implementing UEFI Secure Boot for ESXi hosts

## Built-in Security Features



- ESXi Shell and SSH are disabled by default.
- By default, ESXi runs only services that are essential to managing its functions.
- By default, all ports that are not required for management access to the host are closed.
- By default, weak ciphers are disabled and communications from clients are secured by SSL. Default certificates created on ESXi use PKCS#1 SHA-256 with RSA encryption as the signature algorithm.
- A Tomcat Web service is used internally by ESXi to support access by Web clients. ESXi is not vulnerable to the Tomcat security issues reported in other use cases, because the service has been modified to run only functions that a Web client requires for administration and monitoring
- VMware monitors all security alerts that can affect ESXi security and issues security patches when needed.

- Secure services such as SSH and SFTP are available and should be used instead of insecure counterparts, like Telnet and FTP.
- ESXi provides the option of using UEFI Secure Boot
- When a TPM 2.0 chip is available in the hardware and configured in the system BIOS, ESXi works with Secure Boot to enhance security and trust assurance rooted in hardware

## Security Profiles

You can customize many of the essential security settings for your host through the Security Profile panel available in the vSphere Client. You can use Security Profiles to customize services and configure the ESXi firewall. [Table 7-11](#) identifies the services and that are available to you to view and manage using the vSphere Client for a default vSphere installation. For each service, the default state and description are provided. You can use the vSphere client to start, stop, and restart individual services.

**Table 7-11** ESXi Services in the Security Profile

---

Service	Default State	Description
Direct Console UI	Running	The Direct Console User Interface (DCUI) service allows you to interact with an ESXi host from the local console host using text-based menus.
ESXi Shell	Stopped	The ESXi Shell is available from the Direct Console User Interface or from SSH.
SSH	Stopped	The host's SSH service that allows remote connections through Secure Shell.
Load-Based Teaming Daemon	Running	Load-Based Teaming service
attestd	Stopped	vSphere Trust Authority Attestation Service.
kmxsd	Stopped	vSphere Trust Authority Key Provider Service.
Active Directory Service	Stopped	Started on hosts after you configure ESXi for Active Directory, this service is started.
NTP Daemon	Stopped	Network Time Protocol daemon.
PC/SC Smart Card Daemon	Stopped	Started on hosts after you enable the host for smart card authentication.
CIM Server	Running	Service that can be used by Common Information Model (CIM) applications.
SNMP Server	Stopped	SNMP daemon.
Syslog Server	Stopped	Syslog daemon.
VMware vCenter Agent	Running	vCenter Server agent (vpxa) running in ESXi that connects the host to vCenter Server.
X.Org Server	Stopped	Internally used for virtual machine 3D graphics.

Table 7-12 lists the firewall ports that are installed by default in ESXi 7.0. On a specific host, the list of actual services and firewall ports can be impacted by the currently installed VMware Installation Bundles (VIBs).

**Table 7-12** Incoming and Outgoing

<b>Firewall Service</b>	<b>Incoming Port(s)</b>	<b>Outgoing Port(s)</b>
CIM Server	5988 (TCP)	
CIM Secure Server	5989 (TCP)	
CIM SLP	427 (TCP,UDP)	427 (TCP,UDP)
DHCPv6	546 (TCP,UDP)	547 (TCP,UDP)
DVSSync	8301,8302 (UDP)	8301,8302 (UDP)
HBR		44046,31031 (TCP)
NFC	902 (TCP)	902 (TCP)
WOL		9 (UDP)
Virtual SAN Clustering Service	12345,23451 (UDP)	12345,23451 (UDP)
DCHP Client	68 (UDP)	68 (UDP)
DNS Client	53 (UDP)	53 (TCP,UDP)
Fault Tolerance	8100,8200,8300 (TCP,UDP)	80,8100,8200,8300 (TCP,UDP)
NSX Distributed Logical Router Service	6999 (UDP)	6999 (UDP)
Software iSCSI Client		3260 (TCP)
rabbitmqproxy		5671 (TCP)
Virtual SAN Transport	2233 (TCP)	2233 (TCP)
SNMP Server	161 (UDP)	
SSH Server	22 (TCP)	
vMotion	8000 (TCP)	8000 (TCP)
VMware vCenter Agent		902 (UDP)
vSphere Web Access	80 (TCP)	
vsanvp	8080 (TCP)	8080 (TCP)
RFB Protocol	5900-5964 (TCP)	
vSphere Life Cycle Manager	80, 9000 (TCP)	80, 9000 (TCP)
I/O Filter Service	9080 (TCP)	

The RFB Protocol (TCP 5900-5964) and OpenWSMAN Daemon (TCP 8889) are firewall ports for services that are not visible in the vSphere Client by default.

## ESXi Password Hardening

One step for hardening an ESXi host is to harden the password required to use its predefined, local administrator account, which is called root. By default, the ESXi host enforces passwords for its local user accounts, which may be used to access the host via the Direct Console User Interface (DCUI), the ESXi Shell, Secure Shell (SSH) or the vSphere Client. You can modify

the ESXi password requirements by setting the `Security.PasswordQualityControl` advanced option for the host. For example, you can set `Security.PasswordQualityControl` to configure the ESXi host to accept pass phrases, which it does not accept by default.

## Join an ESXi Host to a Directory Service

You can join an ESXi host to a directory service, such as an Active Directory, and configure permissions to allow the associated users to connect directly to the ESX host using DCUI, ESXi Shell, SSH, or the vSphere Host Client. The main reason for this is to reduce the number of local ESXi user accounts that you must create and manage. Another reason is to provide users with the means to access ESXi directly with an existing user account whose password is already hardened.

## vSphere Authentication Proxy

You can add ESXi hosts to an Active Directory domain by using vSphere Authentication Proxy instead of adding the hosts explicitly to the Active Directory domain. To do this, you can add the host's IP address to the vSphere Authentication Proxy access control list. By default, the vSphere Authentication Proxy will authorize the host based on its IP address. You can enable client authentication to have vSphere Authentication Proxy check the host's certificate. If you are using Auto Deploy, you can configure a reference host to point to the Authentication Proxy, setup a rule that applies the reference host's profile to others hosts provisioned by Auto Deploy, let Auto Deploy store the host's IP address in the access control list, and join the host to the AD domain.

## ESXi Host Access

You can implement lockdown mode to force operations to be performed through vCenter Server. You can choose to use strict lockdown mode, which disables the Direct Console User Interface (DCUI) service or normal lockdown mode, which allows DCUI access for some users. In normal lockdown mode, user accounts that are in the `Exception Users` list and have administrator privileges on the host can access the DCUI. A common use case is to provide access to service accounts, such as backup agents. Also, in normal lockdown mode, users identified in the host's `DCUI.Access` advanced option can access the DCUI. If the ESXi Shell or SSH is enabled and the host is placed in lockdown mode, accounts in the `Exception Users` list who have administrator privileges can use these services. For all other users, ESXi Shell or SSH access is disabled. The main use case is to provide user access in the event of catastrophic failure. Starting with vSphere 6.0, ESXi or SSH sessions for users who do not have administrator privileges are terminated.

## Control MOB Access

The vCenter Server Managed Object Browser (MOB) provides a means to explore the vCenter Server object model. Its primary use is for debugging. It provides the ability to make some configuration changes, so it may be considered a vulnerability for malicious attacks. The MOB is disabled by default. You should only enable it for debugging or for tasks that require it, like extracting the old certificate from a system. To enable MOB, you can use the vSphere Client to set the host's advanced system setting

```
Config.HostAgent.plugins.solo.enableMob.  
You should not use the vim-cmd in the ESXi Shell for  
this purpose.
```

## ESXi Secure Boot and TPM

UEFI Secure Boot is a mechanism that ensures that only trusted code is loaded by the EFI firmware prior to OS handoff. When Secure Boot is enabled, the UEFI firmware validates the digitally signed kernel of an OS against a digital certificate stored in the UEFI firmware. Starting with vSphere 6.5, ESXi supports secure boot if it is enabled in the hardware. ESXi version 6.5 and later supports UEFI secure boot at each level of the boot stack.

ESXi is composed of digitally signed packages called vSphere installation bundles (VIBs). These packages are never broken open. At boot time, the ESXi file system maps to the content of those packages. By leveraging the same digital certificate in the host UEFI firmware used to validate the signed ESXi kernel, the kernel then validates each VIB using the Secure Boot verifier against the firmware-based certificate, ensuring a cryptographically “clean” boot.

When Secure Boot is enabled, ESXi will prevent the installation of unsigned code on ESXi. To install unsigned code such as beta drivers, you must disable Secure Boot. When Secure Boot is enabled, the Secure Boot verifier will run, detect the unsigned VIB, and crash the system, which produces the Purple Screen of Death (PSOD) event that identifies the VIB that must be removed. To remediate, boot the ESXi host with Secure Boot disabled, remove the VIB, and reboot with Secure Boot enabled.

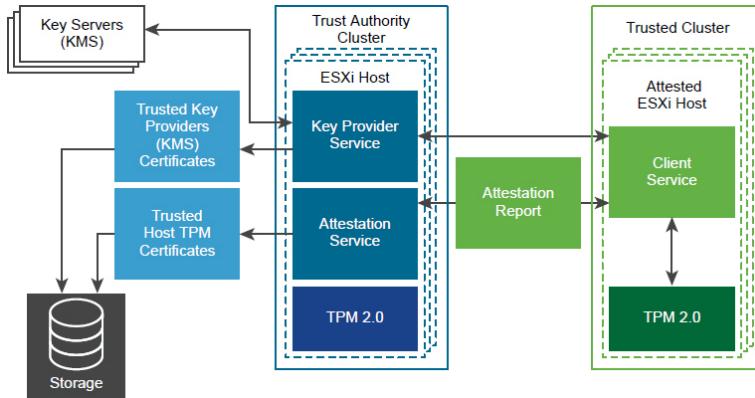
ESXi can use Trusted Platform Modules (TPM) chips, which are secure cryptoprocessors that enhance host security by providing a trust assurance rooted in hardware as opposed to software. TPM is an industry-wide standard for secure cryptoprocessors. TPM chips are found in most of today's computers, from laptops, to desktops, to servers. vSphere 7.0 supports TPM version 2.0. A TPM 2.0 chip attests to an ESXi host's identity. Host attestation is the process of authenticating and

attesting to the state of the host's software at a given point in time. UEFI secure boot, which ensures that only signed software is loaded at boot time, is a requirement for successful attestation.

## vSphere Trust Authority (vTA)



In an environment where TPM attestation is used, you can implement Configure vSphere Trust Authority (vTA), which uses its own management cluster to serve as a hardware root of trust. Ideally the vTA trusted hosts cluster is small, separate from all other clusters, and has very few administrators. In vSphere 6.7, you could leverage TPM and vCenter Server to identify hosts that failed attestation, but you could not automatically prevent secured workloads from migrating to those hosts. Also, you could not encrypt vCenter Server. In vSphere 7.0 with vTA, you can enable the trusted hosts cluster to handle the attestation of other hosts and to take over the distribution of the encryption keys from the Key Management Servers (KMS). This removes vCenter Server from the critical path for key distribution and enables you to encrypt vCenter Server. A Trusted Infrastructure consists of at least one vSphere Trust Authority Cluster, at least one Trusted Cluster, and at least one external KMIP-compliant key management server, as illustrated in [Figure 7-5](#), which is a diagram from the *VMware vSphere 7.0 Security Guide*.



**Figure 7-5**

## vCenter Server Security

You should follow VMware guidelines to ensure security of the vCenter Server environment.

### User Access

The user accounts defined in the local operating system (localos) of the Linux based vCenter Server Appliance have no permissions defined in the vCenter Server environment. The localos user accounts, like root, sshd, and vdtc are not members of any SSO domain (vsphere.local) group to which permissions are applied. No one should attempt to use these accounts to login to the vSphere Client. You should not use these accounts when configuring permissions or group memberships. Do not allow users to login directly to the localos of the vCenter Server appliance. Only login locally when required.

By default, the only accessible user account in the SSO domain is Administrator, which has full control of the environment. If you use the default SSO domain name, then the user account is

`Administrator@vsphere.local`. Ideally, you should integrate vSphere with a supported enterprise directory service, like Active Directory, to allow users seamless access without requiring additional user accounts.

Alternatively, you can create other user accounts in the

SSO domain for your users. You should ensure each user access the environment with a unique account that is assigned the minimally required privileges.

**Note**

Do not confuse the administrator (root) of the localos with the SSO administrator (administrator@vsphere.local by default). By default, no localos user account has full administrator privileges in vCenter Server.

For users who require the Administrator role, you should assign the role to the appropriate user accounts or group accounts to avoid using the SSO administrator account.

The vCenter Server connects to each ESXi host with the vpxuser account defined on the host. By default, vCenter Server changes the vpxuser password automatically every 30 days on each connected ESXi host. To change this behavior, you can change the value of the vCenter Server advanced setting

VimPasswordExpirationInDays.

## vCenter SSO Password Policy

The password for the SSO administrator account and other SSO domain user accounts is controlled by the SSO password policy. By default, this password must meet the following requirements:

- At least eight characters
- At least one lowercase character
- At least one numeric character
- At least one special character

Additionally, the password cannot use more than 20 characters and cannot contain non-ASCII characters. SSO administrators can change the default password policy.

## Restrict Administrative Privileges

You should use permissions to assign the Administrator role to just the specific users and group, who truly require it. You should create and use custom roles with only the required privileges when creating permissions. In other words, you should apply the principle of least privileges when configuring permissions in vCenter Server.

By default, a user with the Administrator role can interact with files and applications within a virtual machine's guest operating system. If your administrators do not require this interaction, consider applying a role without the Guest Operations privilege.

### **Restrict vCenter Server Access**

You should minimize users who can log directly in to the vCenter Server localos, as they could intentionally or unintentionally cause harm by altering settings and modifying processes. Allow only users with legitimate purposes to log in to the system and ensure the login events are audited.

You should secure the network where vCenter Server is connected by applying the information in the *vSphere Network Security* section in this chapter.

### **Control Datastore Browser Access**

Assign the **Datastore.Browser** datastore privilege only to users and user groups who truly require the privilege.

### **vCenter Server and Client Certificates**

You should ensure that vSphere Client users and other client applications heed certificate verification warnings to avoid Man in the Middle (MiTM) attacks.

You should remove any expired or revoked certificates from the vCenter Server to avoid MiTM attacks.

### **Time Synchronization**

You should ensure that all systems, such as vCenter Server, ESXi, and supporting services, use the same relative time source. The time source must be in sync with an acceptable time standard, such as Coordinated Universal Time (UTC). Time synchronization is critical for many vSphere features, such as vSphere HA. It is also critical for securing vSphere.

Time synchronization is essential for certificate validation. Time synchronization simplifies troubleshooting and auditing. Incorrect time settings make it difficult to analyze and correlate log files related to detecting attacks and conducting security audits.

## VSPHERE NETWORK SECURITY

You can use firewalls, segmentation, VLANs, and other measures to secure the networks used by your virtual machines and the vSphere environment. Put vCenter Server on the management network only. Avoid putting the vCenter Server system on other networks such as your production network or storage network, or on any network with access to the Internet. vCenter Server does not need access to the network where vMotion operates.

### **Firewalls**

You can use traditional (physical) firewalls, virtual machine-based firewalls, and hypervisor based firewalls (like NSX distributed firewall) to protect inbound and outbound traffic to the vCenter Server, ESXi hosts, virtual machines, and other vSphere components.

Ideally, you could use firewalls to allow only the required traffic between specific vSphere components, virtual machines, and network segments.

### **Segmentation and Isolation**

You should keep different virtual machine zones within a host on different network segments to reduce the risk of

data leakage and threats. Such threats include Address Resolution Protocol (ARP) spoofing, where an attacker manipulates the ARP table to remap MAC and IP addresses, and gains access to network traffic to and from a host. Attackers use ARP spoofing to generate man in the middle (MITM) attacks, perform denial of service (DoS) attacks, and hijack the systems. You can implement segmentation by using one of two approaches.

- Use separate physical network adapters for virtual machine zones, which may be the most secure method.
- Set up virtual local area networks (VLANs) for virtual machine zones, which may be the most cost-effective method.

You should isolate the vSphere management network, which provides access to the management interface on each component. In most cases, you should place the vSphere management port group in a dedicated VLAN and ensure that the network segment is not routed, except to other management-related networks. Likewise, you should isolate IP-based storage traffic and vMotion traffic.

## **Internet Protocol Security**

You can configure Internet Protocol Security (IPsec) on ESXi hosts to enable authentication and encryption of incoming and outgoing packets. You can configure security associations to control *how* the system encrypts the traffic. For each association, you configure a name, source, destination, and encryption parameters. You can configure security policies to determine *when* the system should encrypt traffic. Security policies include information such as source, destination, protocol, direction, mode, and a security association.

To list the available security associations, you can use this command in ESXi.

```
esxcli network ip ipsec sa list
```

To add a security association, you can use the `esxcli network ip ipsec sa add` with one or more options from [Table 7-13](#).

**Table 7-13** IPsec Options

Option	Description
<code>--sa-source= <i>source address</i></code>	Required. Specify the source address.
<code>--sa-destination= <i>destination Address</i></code>	Required. Specify the destination address.
<code>--sa-mode= <i>mode</i></code>	Required. Specify the mode, either transport or tunnel
<code>--sa-spi= <i>security parameter index</i></code>	Required. Specify the security parameter index as a hexadecimal
<code>--encryption-algorithm= <i>encryption algorithm</i></code>	Required. Specify the algorithm as one of the following parameters. <ul style="list-style-type: none"><li>• 3des-cbc</li><li>• aes128-cbc</li><li>• null (no encryption)</li></ul>
<code>--integrity-algorithm= <i>authentication algorithm</i></code>	Required. Specify the authentication algorithm, either hmac-sha1 or hmac-sha2-256.
<code>--integrity-key= <i>authentication key</i></code>	Required. Specify the authentication key. You can enter keys as ASCII text or as a hexadecimal.
<code>--sa-name= <i>name</i></code>	Required. Provide a name for the security association.

## General Networking Security Recommendations

Here are other general networking security recommendations.



- If spanning tree is enabled, ensure that physical switch ports are configured with Portfast.
- Ensure that Netflow traffic for a Distributed Virtual Switch is only sent to authorized collector IP addresses.
- Ensure that only authorized administrators have access to virtual networking components by using the role-based access controls.
- Ensure that port groups are not configured to the value of the native VLAN.
- Ensure that port groups are not configured to VLAN values reserved by upstream physical switches.
- Ensure that port groups are not configured to VLAN 4095 except for Virtual Guest Tagging (VGT).
- On distributed virtual switches, restrict port-level configuration overrides. The port-level override option is disabled by default.
- Ensure that distributed virtual switch port mirror traffic is sent only to authorized collector ports or VLANs.

## **Network Security Policies**

You should connect virtual machines to standard virtual switch port group or distributed virtual switch port group that are configured with an appropriate security policy. The network security policy provides three options, which may be set to Reject or Accept, as described in [Table 7-14](#).

**Table 7-14** Network Security Policies

---

Option	Setting	Description
Promiscuous Mode	Accept	The virtual switch forwards all frames to the virtual network adapter.
	Reject	The virtual switch forwards only the frames that are address to the virtual network adapter.
MAC address changes	Accept	If the guest operating system changes the effective MAC address of the virtual adapter to a value that differs from the MAC address assigned to the adapter in the VMX file, the virtual switch allows the inbound frame to pass.
	Reject	If the guest operating system changes the effective MAC address of the virtual adapter to a value that differs from the MAC address assigned to the adapter in the VMX file, the virtual switch drops all inbound frames to the adapter. If the guest OS changes the MAC address back to its original value, then the virtual switch will stop dropping the frames and allow inbound traffic to the adapter.
Forged Transmits	Accept	The virtual switch does not filter outbound frames. It permits all outbound frames, regardless of source MAC address.
	Reject	The virtual switch drops any outbound frame from a virtual machine virtual adapter that uses a source MAC address that differs from the MAC address assigned to the virtual adapter in the VMX file.

On a distributed virtual switch, you can override the security policy per virtual port.

## VIRTUAL MACHINE SECURITY

To harden a virtual machine, you could follow best practices, configure UEFI, implement security policies, protect against denial of service attacks, and implement encryption.

### Virtual Machine Hardening Best Practices



- **General Protection** – In most respects, treat the virtual machine as you would a physical server when it comes to applying security measures. For example, be sure to install guest operating systems

patches, protect with anti-virus software and disable unused serial ports.

- **Templates** – Carefully harden the first virtual machine deployment of each guest O/S and verify hardening completeness. Convert the virtual machine into a template and use the template to deploy virtual machines as needed.
- **Virtual machine console** – Minimize the use of this console. Only use it when required. Use remote tools, such as SSH and Remote Desktop to access virtual machines. Consider limiting the number of console connections to just one.
- **Virtual machine resource usage** – Prevent virtual machines from taking over resources on the ESXi host to minimize the risk of Denial of Service to other virtual machines. Configure each virtual machine with enough virtual hardware, but not more virtual hardware resources than needed. For example, configure each virtual machine with enough virtual memory to handle its workload and meet application vendor recommendations, but do not provide much more memory than you expect it will need. Consider setting reservations or shares to ensure that critical virtual machines have access to enough CPU and memory.
- **Disable unnecessary services** – Disable or uninstall any function for the guest O/S that is not required to reduce the number of components that can be attacked and to reduce its resource demand. For example, turn off screen savers, disable unneeded guest operating system services, and disconnect the CD/DVD drive.
- **Disable Unnecessary Hardware Devices** – To minimize potential attack channels, disable any hardware devices that are not required, such as

floppy drives, serial ports, parallel ports, USB controllers, and CD-ROM drives.

## Configure UEFI Boot



Starting with vSphere 6.5, If the operating system supports secure UEFI boot, you can configure your VM to use UEFI boot. Prerequisites are UEFI firmware, Virtual hardware version 13 or later, VMware Tools version 10.1 or later, an operating system that supports UEFI secure boot. For Linux virtual machines, VMware Host-Guest Filesystem is not supported in secure boot mode and should be removed from VMware Tools before you enable secure boot. If you turn on secure boot for a virtual machine, you can load only signed drivers into that virtual machine.

In guest operating system that supports UEFI secure boot, each piece of boot software is signed, including the bootloader, the operating system kernel, and operating system drivers. The default configuration includes several code-signing certificates, including a Microsoft certificate for booting Windows, a Microsoft certificate for third party code, and a VMware certificate for booting ESXi inside a virtual machine. The virtual machine default configuration includes one certificate, which is the Microsoft Key Exchange Key (KEK) certificate.

If you turn on secure boot for a virtual machine, you can only load signed drivers in the guest OS.

## Disable Unexposed Features

Some virtual machine settings, which are useful for other platforms (such as VMware Workstation and VMware Fusion) can be disabled in a vSphere environment. To

reduce potential risk, consider setting the following advanced virtual machine options to TRUE.

- isolation.tools.unity.push.update.disable
- isolation.tools.ghi.launchmenu.change
- isolation.tools.memSchedFakeSampleStats.disable
- isolation.tools.getCreds.disable
- isolation.tools.ghi.autologon.disable
- isolation.bios.bbs.disable
- isolation.tools.hgfsServerSet.disable

## Other Common Settings

You should consider the following setting, which are commonly set to address specific, potential security threats.

- **Disk shrinking:** Because disk shrinking, which reclaims unused disk space from a virtual machine, can take considerable time to complete and its invocation can result in a temporary denial of service, disable disk shrinking using the following lines in the VMX file

---

```
isolation.tools.diskWiper.disable = "TRUE"
isolation.tools.diskShrink.disable =
"TRUE"
```

---

- **Copy and paste:** This ability is disabled by default in new virtual machines. In most cases, retain this default setting to ensure that one user of the virtual machine console cannot paste data that was originally copied from a previous user. Ensure that the following lines remain in the VMX files

```
isolation.tools.copy.disable = "TRUE"  
isolation.tools.paste.disable = "TRUE"
```

- **Connecting devices:** By default, the ability to connect and disconnect devices is disabled. One reason is to prevent one user from accessing a sensitive CD-ROM device that was left in the drive. Another reason is to prevent users from disconnecting the network adapter, which could produce a denial of service. Ensure that the following lines remain in the VMX file.

```
isolation.device.connectable.disable =  
"TRUE"  
isolation.device.edit.disable = "TRUE"
```

- **Logging:** Uncontrolled virtual machine logging could lead to denial of service if the associated datastore runs out of disk space. VMware recommends keeping 10 log files. To set this on a virtual machine, set the following in the VMX file

```
vmx.log.keepOld = "10"
```

Alternatively, to limit the number of log files for virtual machines on an ESXi host, add the previous line to the host's /etc/vmware/config file. A more aggressive measure is to disable virtual machine logging with the following statement in the VMX file

```
logging = "FALSE"
```

- **VMX file size:** By default, the size of each VMX file is 1 MB, because uncontrolled file sizes can lead to a denial of service if the datastore runs out of disk space. Occasionally, *setinfo* messages that define virtual machine characteristics or identifiers are sent as name-value pairs from the virtual

machine to the VMX file. If needed, you can increase the size of the VMX file limit by using the following statement in the VMX file but replacing the numeric value with a larger value. In most cases, keep the default setting as a security measure.

---

```
tools.setInfo.sizeLimit = "1048576". If  
tools.setInfo.sizeLimit is not set in the  
virtual machine's advanced options, then  
the default size applies.
```

---

- **Performance counters:** VMware Tools provides performance counters on CPU and memory from the ESXi host into the virtual machine for use by PerfMon. This feature is disabled by default, because an adversary could potentially make use of this information to attack the host. Ensure the following line remains in the VMX files, which blocks some, but not all performance metrics.

---

```
tools.guestlib.enableHostInfo = "FALSE"
```

---

## Virtual Machine Risk Profiles

VMware provides the *vSphere 6.0 Hardening Guide* that provides guidelines for address vulnerabilities based on risk profiles. When you can apply the hardening guide to your environment, the first step is to apply the appropriate risk profile based on the sensitivity of your environment and data. The hardening guide offers three risk profiles:

- **Risk Profile 1:** Intended to be implemented in just the most secure environments, such as top-secret government environments.
- **Risk Profile 2:** Intended to be implemented in sensitive environments to protect sensitive data

such as those that must adhere to strict compliance rules.

- **Risk Profile 3:** Intended to be implemented in all production environments.

For vSphere 6.7, the *vSphere Hardening Guide* is replaced with the *vSphere 6.7 Update 1 Security Configuration Guide*. The risk profiles are removed, primarily because only the only remaining Risk Profile 1 setting is `ESXi.enable-strict-lockdown-mode`. Instead of identifying risk profiles, the new guide simply lists the current 50 Guideline IDs alphabetically and includes a Vulnerability Discussion for each guideline. As of July 2020, no *vSphere 7.0 Security Configuration Guide* is available.

## Protect Virtual Machine Against Denial-of-Service Attacks

As previously stated, the virtual machine configuration file (VMX file) size limit is 1 MB by default, but you can change it using the `tools.setInfo.sizeLimit` parameter to avoid filling the datastore and causing a Denial of Service (DoS).

Virtual Machine Communication Interface (VMCI) is a high-speed communication mechanism for virtual machine to ESXi host communication. In some VMware products, including ESXi 4.x, VMCI also provides high-speed communication between virtual machines on the same ESXi host. In ESXi 5.1, the guest to guest VMCI is removed. In a VMX file, the `vmcio.unrestricted` parameter is used to control VMCI isolation for virtual machines running on ESX/ESXi 4.x and ESXi 5.0, but has no effect on virtual machines running on ESXi 5.1 and later. Any DoS concerns related to VMCI in previous vSphere versions do not apply to vSphere 7.0.

Non-administrative users in the guest operating system can shrink virtual disks to reclaim the disk's unused space. However, if you shrink a virtual disk repeatedly, the disk can become unavailable and cause a denial of service. To prevent this, you could disable the ability to shrink virtual disks using the following steps.

1. Shutdown the virtual machine
2. Modify the advanced settings in the virtual machine options.
3. Set **isolation.tools.diskWiper.disable** and **isolation.tools.diskShrink.disable** to TRUE

## Control VM Device Connections

As previously stated, the ability to connect and disconnect devices is disabled by default for new virtual machines. In most cases, you should not change this behavior. You should verify that the following setting exist in your VMX files, especially if the virtual machines were deployed from a non-hardened template or were originally built on older ESXi hosts.

```
isolation.device.connectable.disable = "TRUE"  
isolation.device.edit.disable = "TRUE"
```

If these parameters are set to FALSE, then in a guest operating system, any user or process, with or without root or administrator privileges, could use VMware Tools to change device connectivity and settings. They could connect or disconnect devices, such as network adaptors and CD-ROM drives. They could modify device settings. This functionality could allow them to connect a CD-ROM with sensitive data. It could allow them to disconnect a network adapter, which could cause a denial of service to other users.

## Virtual Machine Encryption

Starting with vSphere 6.5, you can protect your virtual machines, virtual disks, and other virtual machines files using virtual machine encryption. In vSphere 6.5 and 6.7, you must set up a trusted connection between vCenter Server and a key management server (KMS). The KMS generates and stores keys. It passes the keys to vCenter Server for distribution. Starting in vSphere 7.0, you can remove the need for vCenter to request keys from the KMS by configuring vSphere Trust Authority (vTA) and making encryption keys conditional to cluster attestation.

You can use the vSphere Client or the vSphere API to add key provider instances to the vCenter Server system.

vCenter Server uses the Key Management Interoperability Protocol (KMIP) to allow flexibility in choosing a KMS. If you use multiple key provider instances, all instances must be from the same vendor and must replicate keys. If you use different KMS vendors in different environments, you can add a key provider for each KMS and specify a default key provider. The first key provider that you add becomes the default key provider, but you can change it.

Only vCenter Servers (not the ESXi hosts) have the credentials for logging in to the KMS. vCenter Server obtains keys from the KMS and pushes them to the hosts. Two types of keys are used for virtual machine encryption.

- Data encryption keys (DEKs) are internal keys generated by the ESXi host and used to encrypt virtual machines and disks. DEKs are XTS-AES-256 keys.
- Key encryption key (KEKs) are the keys that vCenter Server requests from the KMS. KEKs are AES-256 keys. vCenter Server stores only the ID of each KEK, but not the key itself.

You can encrypt an existing virtual machine or virtual disk by changing its storage policy. Encryption works with any guest OS because encryption occurs at the hypervisor level. Encryption keys and configuration are not contained in the VM guest OS. Encryption works with any supported storage type, including VMware vSAN

You can encrypt virtual disks only for encrypted virtual machines. You cannot encrypt the virtual disk of an unencrypted VM. You can encrypt virtual machine files (NVRAM, VSWP, and VMSN files), virtual disk files, and core dump files. Log files, virtual machine configuration files, and virtual disk descriptor files are not encrypted. Per virtual machine, you can use the vSphere Client to encrypt and decrypt the virtual disks independently.

Core dumps are always encrypted on ESXi hosts where encryption mode is enabled. Core dumps on the vCenter Server system are not encrypted. To perform cryptographic operations, you must be assigned the Cryptographic Operations privileges.

ESXi uses KEKs to encrypt the internal keys and stores the encrypted internal keys on disk. ESXi does not store the KEK on disk. If a host reboots, vCenter Server requests the KEK with the corresponding ID from the KMS and makes it available to ESXi, who decrypts the internal keys as needed. In addition to VMDK files, most virtual machine files that contain guest data are encrypted, such as the NVRAM, VSWP, and VMSN files. The key that vCenter Server retrieves from the KMS unlocks an encrypted bundle in the VMX file that contains internal keys and other secrets.

**Note**

Encryption keys and configuration are not contained in the VM guest OS.

VM encryption uses vSphere APIs for I/O filtering (VAIO), which is typically called the IOFilter. The IOFilter is an ESXi framework that allows for the interception of virtual machine I/O in the virtual SCSI emulation (vSCSI) layer, which is just below the virtual machine and above the file system. It enables VMware and third-party developers to develop services using virtual machine I/O, such as encryption, caching, and replication. It is implemented entirely in user space, which cleanly isolates it from the core architecture and core functionality of the hypervisor. In case of any failure, only the virtual machine in question would be impacted. Multiple filters can be enabled for a particular virtual machine or a virtual disk, which are typically chained in a manner so that I/O is processed serially by each of these filters before the I/O is passed down to VMFS or completed within one of the filters.

The default Administrator system role includes all Cryptographic Operations privileges. A new default role, the `No Cryptography Administrator`, supports all Administrator privileges except for the Cryptographic Operations privileges. You can create a custom role that contains granular Cryptographic Operations privileges such as **Cryptographic operations > Encrypt** (allows a user to encrypt a virtual machine or virtual disk) and **Cryptographic operations > Add disk** (allows a user to add a disk to an encrypted virtual machine).

The vSphere Client can be used to encrypt and decrypt virtual machines. To recrypt a virtual machine, you must use the API. You can use the API to perform a deep recrypt (replacing the DEK and KEK) or a shallow recrypt (replacing just the KEK) of a virtual machine. The deep recrypt requires that the virtual machine be powered off and be free from snapshots. The shallow recrypt is permitted on a virtual machine with one (not multiple) snapshots. The **crypto-util** command line

utility can be used to decrypt core dumps, check for file encryption, and perform management tasks on the ESXi host.

When a user performs an encryption task, such as creating an encrypted virtual machine, the following events occur.

- The vCenter Server requests a new key from the default KMS to use as the KEK.
- The vCenter Server stores the key ID and passes the key to the ESXi host. If the host is part of a cluster, vCenter Server sends the KEK to each host in the cluster.
- The key itself is not stored on the vCenter Server system. Only the key ID is known.
- The ESXi host generates internal keys (DEKs) for the virtual machine and its disks. It uses the KEKs to encrypt internal keys and keeps the internal keys in memory only (never on disk). Only encrypted data is stored on disk.
- The ESXi host uses the encrypted internal keys to encrypt the virtual machine.
- Any hosts that can access the encrypted key file and the KEK can perform operations on the encrypted virtual machine or disk.

## **Encrypted vSphere vMotion**

Encrypted vSphere vMotion provides confidentiality, integrity, and authenticity of the data that is transferred with vSphere vMotion. Starting with vSphere 6.5, vSphere vMotion always uses encryption when migrating encrypted virtual machines. You cannot turn off encrypted vSphere vMotion for encrypted virtual machines. For virtual machines that are not encrypted,

you can set **Encrypted vMotion** to one of the following states. The default is **Opportunistic**.

- **Disabled:** Do not use encrypted vSphere vMotion.
- **Opportunistic:** use encrypted vSphere vMotion if source and target hosts support it.
- **Required:** If the source or destination host does not support encrypted vSphere vMotion, migration with vSphere vMotion is not allowed.



The following rules apply concerning encrypted vMotion across vCenter Server instances.

- You must use the vSphere APIs.
- Encrypted vMotion of unencrypted virtual machines is supported.
- vMotion of encrypted virtual machines is not supported
- The source and destination vCenter Server instances must share the KMS cluster that was used to encrypt the virtual machine.
- The name of the shared KMS cluster must be the same on each vCenter Server instance.
- You must have the **Cryptographic operations.Migrate** privilege on the virtual machine.
- You must have the **Cryptographic operations.EncryptNew** privilege on the destination vCenter Server.
- If the destination ESXi host is not in "safe" mode, then you also need the **Cryptographic**

**operations.RegisterHost** privilege on the destination vCenter Server

- You cannot change the virtual machine storage policy or perform a key change

**Note**

Only ESXi versions 6.5 and later use encrypted vSphere vMotion.

When using vSphere Trust Authority (vTA), the following requirements apply.

- The destination host must be configured with vTA and must be attested.
- Encryption cannot change on migration.
- You can migrate a standard encrypted virtual machine onto a Trusted Host.
- You cannot migrate a vTA encrypted virtual machine onto a non-Trusted Host.

## Virtual Trusted Platform Module (vTPM)

A virtual Trusted Platform Module (vTPM) is a software-based representation of a physical Trusted Platform Module (TPM) 2.0 chip. A vTPM uses software to perform the same functions that a TPM performs in hardware. A vTPM uses the `.nvram` file, which is encrypted using virtual machine encryption, as its secure storage. A hardware TPM includes a preloaded key called the Endorsement Key (EK), which has a private and public key. For vTPM, the EK is provided either by the VMware Certificate Authority (VMCA) or by a third-party Certificate Authority (CA).

You can add a vTPM to either a new virtual machine or an existing virtual machine, which enables the guest operating system to create and store keys that are private. The keys are not exposed to the guest operating

system itself, even if the guest operating system is compromised. The keys can be used only by the guest operating system for encryption or signing. With an attached vTPM, a third party can remotely attest to (validate) the identity of the firmware and the guest operating system.

When you configure a vTPM, VM encryption automatically encrypts the virtual machine files but not the disks. The backup of a VM with a vTPM must include all virtual machine data, including the \*.nvram file. In order to successfully restore the VM, the backup must include the \*.nvram file and you must ensure that the encryption keys are available.

To use a vTPM, you must meet the following requirements.

- Virtual machine hardware version 14 using EFI firmware
- vCenter Server 6.7 or greater
- Virtual machine encryption (for home files) and Key Management Server (KMS)
- Windows Server 2016 (64 bit) or Windows 10 (64 bit)

You can add a vTPM as you create a virtual machine, by selecting **Customize Hardware > Add New Device > Trusted Platform Module**. Likewise, you can add a vTPM to an existing, powered down virtual machine. In the vSphere Client, you can identify which virtual machines are enabled with vTPM by using **Show / Hide Column** in the **VMs** tab for a selected object, such as a host or cluster.

## **Virtual Intel Software Guard Extension (vSGX)**

Intel Software Guard Extension (SGX) is a processor-specific technology for application developers to protect code and data from disclosure or modification. It allows user-level code to define enclaves, which are private regions of memory. It prevents code running outside the enclave from accessing content in the enclave.

If Intel SGX technology is available on your hardware, then your virtual machines can use Virtual Intel SGX (vSGX). To enable vSGX for a virtual machine, you must meet the following requirements.

- Virtual machine hardware version 17 and EFI firmware
- vCenter Server 7.0 and ESXi 7.0
- Linux, Windows Server 2016 (64 bit) or later, or Windows 10 (64 bit) guest OS
- Intel Coffee Lake CPU or later

When vSGX is enabled on a virtual machine, the following features are not supported for that machine.

- vMotion / DRS Migration
- Virtual machine suspend and resume
- Memory snapshots (Virtual machine snapshots are supported without snapshotting the memory.)
- Fault Tolerance
- Guest Integrity (GI) (The platform foundation for VMware AppDefense 10)

## AVAILABLE ADD-ON SECURITY

You can further secure your environment by procuring and implementing additional measures that are not provided natively in vSphere. Such measures include

additional VMware products, such as vRealize Operations Manager, NSX, and AppDefense.

## Compliance using vRealize Operations Manager

You can implement vRealize Operations Manager (vROps) to provide a single pane of glass monitoring solution for your virtual infrastructure, applications, storage, and network devices. vROps provides an open and extensible platform supported by third-party management packs. It monitors performance and availability metrics, performs predictive analysis of the data, and enables pro-active remediation of emerging issues. Additionally, you can use vROps to monitor objects in your vSphere environment, such as vCenter Servers, hosts, virtual machines, distributed port groups, and datastores to ensure compliance with the appropriate standards. You can use vROps to define and analyze compliance standards.

You can customize vROps policies to enable vSphere Security Configuration Guide which enables vSphere alerts for ESXi hosts, vCenter Server, and virtual machines that are in violation with the guide.

Additionally, hardening guides for regulatory standards are delivered as management packs (PAK files) that you can upload, license, and install. For example, you can install management packs for the following regulatory standards:

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS) compliance standards
- CIS Security Standards
- Defense Information Systems Agency (DISA) Security Standards

- The Federal Information Security Management Act (FISMA) Security Standards
- International Organization for Standardization Security Standards

vROps collects compliance data from your vSphere objects, generates compliance alerts, and creates reports of the compliance results.

## VMware NSX

You can implement VMware NSX Data Center for vSphere (NSX) to add a distributed logical firewall, micro segmentation, and additional security measures to your vSphere environment.

NSX provides a Distributed Firewall (DFW) that runs in the VMkernel as a VIB package on all NSX-prepared ESXi hosts. The DFW offers near line rate performance, virtualization, identity awareness, automated policy creation, advanced service insertion, and other network security features. The DFW enhances your physical security by removing unnecessary hair-pinning from the physical firewalls and reduces the amount of traffic on the network. It enables micro-segmentation, where effectively, you can place a firewall on each VM network connection.

Micro-segmentation decreases the level of risk and increases the security posture of your vSphere environment. Micro-segmentation utilizes the following capabilities.

- Distributed stateful firewalling
- Topology agnostic segmentation
- Centralized policy control
- Granular controls

- Network based isolation

With NSX, isolation can be achieved by leveraging VXLAN technology and virtual networks (i.e., Logical Switches). Isolation can also be achieved with traditional networking methods, such as ACLs, firewall rules, and routing policies. For example, in a brownfield environment, you could choose to keep existing VLAN segmentation to isolate VMkernel traffic and VM zones while using the NSX DFW to implement application segmentation.

With NSX, you can implement virtual machine to virtual machine protection, which is commonly referred to as east-west protection, in more than one manner. For example, you could implement multiple L2 segments with L3 isolation (see Figure 7-6) or implement a single L2 segment and use DFW rules for isolation (see Figure 7-7).

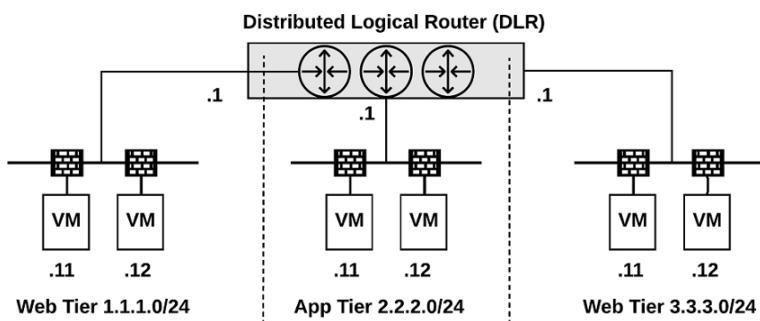


Figure 7-6

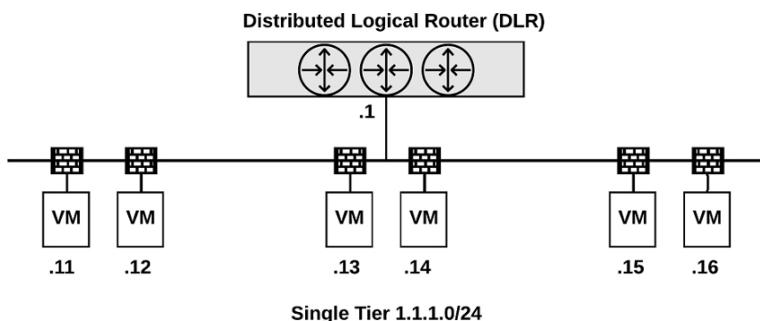


Figure 7-7

NSX provides other security features, such as Service Composer, which you can use to configure security groups and security policies. Security policies are a collection of firewall rules, endpoint services, and network introspection services. Security groups may be populated statically or dynamically based on containers (such as folders and clusters), security tags, Active Directory groups, and regular expressions. You map a security policy to a security group.

NSX includes other security features, such as SpoofGuard, Edge Firewall, and Virtual Private Network (VPN).

## **AppDefense**

You can secure your vSphere environment further by using VMware AppDefense. AppDefense is a data center endpoint security product that protects applications running in vSphere. AppDefense understands an application's intended state and behavior, then monitors for changes to that intended state that indicate a threat. When a threat is detected, AppDefense automatically responds based on your policies. You can use AppDefense to define "good behavior" and to trigger automated, custom actions when other behavior is detected. For vSphere 7.0, AppDefense is available only as a separate product. For vSphere 6.7, AppDefense is included in the vSphere Platinum edition.

Key features of AppDefense are:

- It understands the intended state of each application and runs inside the hypervisor where it has an authoritative understanding of how data center endpoints are meant to behave. This means it is the first to know when changes are made.
- Being hypervisor based, it runs in an isolated, protected environment, reducing the chance that

AppDefense itself will be compromised.

- When a threat is detected, it takes the action that you pre-configure, leveraging vSphere and NSX, such as:
  - Block VM network communication
  - Snapshot a VM
  - Suspend or shutdown a VM

## SUMMARY

You completed reading this chapter on vSphere Security. You can use the remain sections in the chapter to prepare for associated exam questions

## REVIEW ALL THE KEY TOPICS

Table 7-15 provides a reference to each of the key topics identified in this chapter. Take a few moments to review each of these specific items.

**Table 7-15** Key Topics

---

<b>Key Topic Element</b>	<b>Description</b>	<b>Pages</b>
Figure 7-2	vSphere Inventory Hierarchy	
List	vCenter Server 7.0 Sample roles	
Paragraph	How Permissions are applied by vCenter Server	
List	Built-in Security Features	
Paragraph	vSphere Trust Authority (vTA)	
List	General Networking Security Recommendations	
List	Virtual Machine Hardening Best Practices	
Paragraph	Configure UEFI Boot	
List	Rules for encrypted vMotion across vCenter Server instances	

## COMPLETE THE TABLES AND LISTS FROM MEMORY

Print a copy of Appendix B, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

## DEFINITIONS OF KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary.

Trusted Platform Modules (TPM)

vmdir

VMware Certificate Authority (VMCA)

VMware Endpoint Certificate Store (VECS)

Virtual Trusted Platform Module (vTPM)

Intel Software Guard Extension (SGX)

Micro-segmentation

AppDefense

## Glossary

**TPM:** Trusted Platform Modules (TPM) chips are secure cryptoprocessors that enhance host security by providing a trust assurance rooted in hardware as opposed to software

**vmdir:** VMware Directory Service (vmdir) is an identity source that handles SAML certificate management for authentication with vCenter Single Sign-On.

**VMCA:** VMware Certificate Authority (VMCA) provisions each ESXi host, each machine in the environment, and each solution user with a certificate signed by VMCA

**VECS:** VMware Endpoint Certificate Store (VECS) is the local (client-side) repository for certificates, private keys, and other certificate information that can be stored in a keystore.

**vTPM:** Virtual Trusted Platform Module (vTPM) is a software-based representation of a physical Trusted Platform Module (TPM) 2.0 chip

**SGX:** Intel Software Guard Extension (SGX) is a processor-specific technology for application developers to protect code and data from disclosure or modification

**Micro-segmentation:** Micro-segmentation is a type of network segmentation that decreases the level of risk and increases the security posture of the modern data center by providing granular control and distributed stateful firewalling. Effectively, it allows you to place a firewall on each VM network connection.

**AppDefense:** AppDefense is a data center endpoint security product that protects applications running in vSphere.

- 1.** You are preparing to implement certificates in your vSphere environment. Which of the following is supported in custom certificates by VMCA when it is used as a subordinate CA?

  - a.** CRL Distribution Points
  - b.** Authority Information Access
  - c.** CRT format
  - d.** Certificate Template Information
- 2.** On which of the following items can you set permissions in vCenter Server.

  - a.** Licenses
  - b.** Datastores
  - c.** Roles
  - d.** Sessions
- 3.** You are examining the default security profile in your vSphere environment. Which of the following services are stopped by default?

  - a.** DCUI
  - b.** Load-based Teaming Daemon
  - c.** CIM Server
  - d.** SNMP Server
- 4.** You are hardening a vCenter Server and see that it contains some expired certificates. What is the main purpose for removing expired and revoked certificates from vCenter Server.

  - a.** Avoid DoS attacks
  - b.** Avoid MiTM attacks
  - c.** Avoid automatic virtual machine shutdown due to expired certificates

- d.** Avoid ARP spoofing
- 5.** You want to enable UEFI boot for your virtual machines. Which of the following is a requirement?
  - a.** Virtual hardware version 11 or later
  - b.** VMware Tools 11 or later
  - c.** Virtual hardware version 12 or later
  - d.** VMware Tools 10.1 or later

# Chapter 8. vSphere Installation

This chapter covers the following subjects:

- Install ESXi hosts
- Deploy vCenter Server Components
- Configure Single Sign-On (SSO)
- Initial vSphere Configuration

This chapter contains information related to VMware  
2V0-21.20 exam objectives 1.1, 1.2, 1.8, 4.1.1, 4.1.2, 4.3,  
4.3.1, 4.3.2, 4.3.3, 4.4, 4.6, 4.12, 4.15, 4.16, 7.9, 7.10, 7.11,  
7.11.1, 7.11.2

## “Do I Know This Already?” Quiz

### Install ESXi hosts

Install ESXi Interactively

Scripted ESXi Installation

Auto Deploy

### Deploy vCenter Server Components

vCenter Server Database

Platform Services Controller (PSC)

vCenter Server Appliance

Deploy VCSA Using the GUI Installer

CLI Deployment

Post Installation

Configure/Manage VMware Certificate Authority (VMCA)

## Configure Single Sign-On (SSO)

SSO and Identity Sources Overview

Add/Edit/Remove SSO Identity Sources

How to Add an Active Directory Identity Source

How to Add an LDAP Authentication Source

Enable/Disable Single Sign-On (SSO) Users

Configure SSO Policies

Configure Identity Federation

## Initial vSphere Configuration

vSphere Client Implementation

VMware vSphere Lifecycle Manager Implementation

Configure the vCenter Server Inventory

Implement vCenter HA

Configure ESXi Using Host Profiles

Host Profile Overview

Edit Host Profiles

Apply Permissions to ESXi Hosts Using Host Profiles

VMware Tools

Advanced ESXi Host Options

ESXi Advanced System Settings

ESXi Kernel options

## Summary

Review All the Key Topics

Complete the Tables and Lists from Memory

Definitions of Key Terms

Answer Review Questions

This chapter covers the procedures for installing and configuring a vSphere 7.0 environment.

## “DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section.

Regardless, the authors recommend that you read the entire chapter at least once. **Table 8-1** outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 8-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions Covered in This Section
Install ESXi hosts	1,2
Deploy vCenter Server Components	3,4
Configure Single Sign-On (SSO)	5,6, 7
Initial vSphere Configuration	8, 9,10

- 1.** You are preparing to deploy vSphere 7.0. Which of the following is a prerequisite for installing ESXi interactively?
  - a.** Download the ESX Installer ISO
  - b.** Download the ESX Installer OVF
  - c.** Download the GUI Installer for Windows or Mac.
  - d.** Download the ESXi MSI.
  
- 2.** You are preparing to do a scripted installation of ESXi 7.0. Where is the location of the default installation script?

- a. /etc/vmware/weasel/ks.py**
  - b. /etc/vmware/weasel/ks.cfg**
  - c. /etc/vmware//ks.cfg**
  - d. /etc/vmware/ks.py**
- 3.** You are preparing to install vCenter Server 7.0 using a deployment command. To perform a pre-deployment check, which command should you use?
- a. vcsa-deploy-precheck *path-to-JSON-file***
  - b. vcsa-deploy install --precheck *path-to-JSON-file***
  - c. vcsa-deploy install --verify-only *path-to-JSON-file***
  - d. vcsa-deploy precheck *path-to-JSON-file***
- 4.** You are installing vSphere 7.0 and want to document the location of certificates. Where are the ESXi certificates stored?
- a. Locally on the ESXi hosts**
  - b. In the VECS**
  - c. In the vCenter Server database.**
  - d. In the VMCA**
- 5.** You are adding a OpenLDAP authentication source for your recently deployed vCenter Server. Which of the following is Not a requirement.
- a. All users have an objectClass of  
inetOrgPerson**
  - b. All groups have an objectClass of  
groupOfUniqueNames**

- c.** All groups have a group membership attribute of uniqueMember
    - d.** All users must be members of the OpenLDAP group
- 6.** You are deploying a new vSphere environment and need to control which users can manage certificates. Which vCenter Server Single Sign On domain group membership should you manipulate?
  - a.** DCAdmins
  - b.** SolutionUsers
  - c.** CAAdmins
  - d.** SystemConfiguration\_Administrators
- 7.** You are adding an Active Directory (Integrated Windows Authentication) identity source and want to ensure future machine name changes do not cause issues. Which settings should you use?
  - a.** Select **Use Service Principle Name (SPN)** and provide a **UPN**
  - b.** Select **Use Machine Account** and provide a **UPN**
  - c.** Select **Use Service Principle Name (SPN)** and provide a **Base DN for Users**
  - d.** Select **Use Machine Account** and provide a **Base DN for Users**
- 8.** You are deploying vCenter Server in a secured network with no Internet access. What do you need to install to download updates?
  - a.** Update Manager Download Service
  - b.** Update Manager Proxy Service
  - c.** Lifecycle Manager Download Service

- d. Lifecycle Manager Proxy Service**
- 9.** You are implementing vCenter HA. How will you connect the nodes to vCenter HA network?
  - a.** Connect NIC 1 on the Active and Passive nodes and NIC 0 to the vCenter HA network.  
Do not connect the Witness node to the vCenter HA network.
  - b.** Connect NIC 1 on the Active and Passive nodes and NIC 0 on the Witness Nodes to the vCenter HA network.
  - c.** Connect NIC 0 on the Active, Passive and Witness Nodes to the vCenter HA network.
  - d.** Connect NIC 1 on the Active, Passive and Witness Nodes to the vCenter HA network.
- 10.** You are installing new ESXi hosts and want to configure boot options. Which of the following **kernelopt** options are deprecated in ESXi 7.0?
  - a. autoCreateDumpFile**
  - b.**  
**autoPartitionCreateUSBCoreDumpPartition**
  - c. skipPartitioningSsds**
  - d. autoPartitionOnlyOnceAndSkipSsd**

## INSTALL ESXI HOSTS

To begin your vSphere deployment, you should install and configure at least one ESXi host using the information in this section. Optionally, you can apply the information here to install and configure additional ESXi

hosts. In many cases, administrators choose to deploy the first ESXi host, then deploy vCenter Server, and use vCenter Server along with other tools, such as host profiles, to facilitate the deployment and configuration of the remaining ESXi hosts.

You have several choices for installing ESXi, such as using the interactive wizard, using scripts, and using Auto Deploy. These choices are covered in this section. Using host profiles to configure ESXi hosts after installation is covered in a separate section later in this chapter.

## Install ESXi Interactively

You can use the following procedure to install ESXi interactively, which is very useful in small environments with fewer than five ESXi hosts.



Preparation:

**Step 1.** Verify all of the target machine hardware is supported and meets minimum requirements

**Step 2.** Gather and record the information that will be required during the installation as shown in [table 8-2](#)

**Step 3.** Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.

**Step 4.** Download the ESXi Installer ISO and prepare the hardware system to boot from it.

Procedure:

**Step 1.** Start the machine so that it boots from the ESXi Installer

**Step 2.** On the Select a Disk page, select the drive on which to install ESXi and press Enter.

**Step 3.** Select the keyboard type for the host.

**Step 4.** Enter a password to be used by the root account.

**Step 5.** When prompted, remove the bootable media and press Enter to reboot the host.

**Table 8-2** Required Information for ESXi Installation

Information	Required or Optional	Details
Keyboard layout	Required	Default: US English
VLAN ID	Optional	Range: 0-4094 Default: None
IP address	Optional	Default: DHCP
Subnet mask	Optional	Default: Based on the configured IP address
Gateway	Optional	Default: Based on the configured IP address and subnet mask
Primary DNS	Optional	Default: Based on the configured IP address and subnet mask
Secondary DNS	Optional	Default: None
Host name	Required for static IP settings	Default: None
Install location	Required	Must be at least 5 GB if you install on a single disk.  Default: None
Migrate existing ESXi settings. Preserve VMFS datastore.	Required if you are installing ESXi on a drive with an existing ESXi installation.	Default: None
Root password	Required	Must contain at least 8 to 40 characters in addition to other requirements.  Default: None

The default behavior is to configure the ESXi management network using DHCP. You can override the default behavior and use static IP settings for the management network after the installation is completed.

If your host is not yet assigned an IP address or if you wish to change it, you can use the following procedure to select the appropriate network adapter, configure the VLAN, and configure the IP configuration for the host's management network interface.

Procedure:

**Step 1.** Logon to the Direct Console User Interface (DCUI), which appears on the host's monitor

**Step 2.** If needed, use the DCUI to change the network adapter used for management

- a.** Select **Configure Management Network** and press **Enter**.
- b.** Select **Network Adapters** and press **Enter**.
- c.** Select a **network adapter** and press **Enter**.

**Step 3.** If needed, use the DCUI to change the VLAN used for management

- a.** Select **Configure Management Network** and press **Enter**.
- b.** Select **VLAN** and press **Enter**.
- c.** Enter the appropriate VLAN ID number for your network connection.

**Step 4.** If needed, use the DCUI to change the IP configuration used for management

- a.** Select **Configure Management Network** and press **Enter**.
- b.** Select **IP Configuration** and press **Enter**.

- c. Select Set static IP address and network configuration.**
- d. Enter the IP address, subnet mask, and default gateway and press Enter.**

You can use the DCUI to configure DNS following this procedure.

**Step 1.** Select Configure Management Network and press Enter.

**Step 2.** Select **DNS Configuration** and press Enter.

**Step 3.** Select Use the following DNS server addresses and hostname.

**Step 4.** Enter the primary server, an alternative server (optional), and the host name.

After ESXi is installed and the management network is configured, you can manage the host and make other configuration changes using the vSphere Host Client.

## Scripted ESXi Installation

Installation scripts provide an efficient way to deploy multiple hosts and/or to deploy hosts remotely.

The installation script includes the settings for installing ESXi. The script can be applied to all of the hosts that need to have the same configuration. Only supported commands can be used in the installation script. This can be modified for settings which need to be unique for each host. The installation script location can be one of the following:

- FTP server
- HTTP/HTTPS server
- NFS server

- USB flash drive
- CD-ROM drive

To start the installation script, you can enter boot options at the ESXi installer boot command line. At boot time you can press Shift+O in the boot loader (see [Figure 8-1](#)) to specify boot options and access the kickstart file. If you are installing using PXE boot, options can be passed through the `kernelopts` line of the `boot.cfg` file. The location of the installation script is defined by setting the `ks=filepath` option, where `filepath` is where the kickstart file is located. If `ks=filepath` is not included in the script, the text installer runs.



**Figure 8-1** ESXi Installer

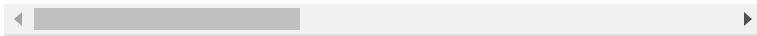
Procedure:

**Step 1.** Start the host.

**Step 2.** When the **Loading ESXi installer** window appears (see [Figure 8-1](#)), press Shift+O to define the options.

**Step 3.** At the **runweasel** command prompt, enter **ks=** along with the path to the installation script and the command line options. For example, you could enter the following options to boot the host from a script named `ks-script-01` residing on the server `192.168.1010.10` and to set the host's IP address to `192.168.100.101`

```
ks=http://192.168.100.10/kickstart/ks-script-01.cfg n
```



To successfully perform a scripted installation, you may need to enter boot options to access the script file. **Table 8-3** shows some of these options.

**Table 8-3** Boot Options for ESXi Scripted Installation

Boot Option	Description
BOOTIF= <i>hwtype-MAC address</i>	Similar to the <code>netdevice</code> option, except in the PXELINUX format
gateway= <i>ip address</i>	Gateway used for downloading the installation script.
ip= <i>ip address</i>	IP address used for downloading the installation script.
ks=cdrom:/ <i>path</i>	Performs a scripted installation with the script at <i>path</i> , which resides on the CD in the CD-ROM drive.
ks=file:// <i>path</i>	Performs a scripted installation with the script at <i>path</i> .
ks= <i>protocol://serverpath</i>	Performs a scripted installation with a script located on the network at the given URL. The <i>protocol</i> can be <code>http</code> , <code>https</code> , <code>ftp</code> , or <code>nfs</code> , as in this example, <code>ks=nfs://host/porturl-path</code> .
ks=usb	Performs a scripted installation, accessing the script from an attached USB drive
ks=usb:/ <i>path</i>	Performs a scripted installation with the script file at the specified <i>path</i> , which resides on USB.
ksdevice= <i>device</i> or	Tries to use a network adapter <i>device</i> when looking for an

<code>netdevice=device</code>	installation script and installation media. Specify as a MAC address, for example, 00:50:56:C0:00:01. This location can also be a vmnic## name.
<code>nameserver=ip address</code>	Specifies a domain name server to be used for downloading the installation script and installation media.
<code>netmask=subnet mask</code>	Subnet mask used for downloading the installation script.
<code>vlanid=vlanid</code>	VLAN used for downloading the installation script.

There is a default installation script included with the ESXi Installer. This can be used to install ESXi to the first disk that is detected. The default **ks.cfg** installation script is in the initial RAM disk at **/etc/vmware/weasel/ks.cfg**. The location of the default ks.cfg file can be defined with the **ks=file:///etc/vmware/weasel/ks.cfg** boot option. When using the ks.cfg script for the install, the default root password is **myp@ssword**. The installation script on the installation media can't be modified. After the ESXi host has been installed, the Host Client or the vSphere Web Client logged into the vCenter Server that manages the ESXi host can be used to change any of the default settings.

Example 8-1 shows the contents of the default script.

### Example 8-1

```

#
# Sample scripted installation file
#
# Accept the VMware End User License Agreement
vmaccepteula
# Set the root password for the DCUI and Tech

```

```

Support Mode

rootpw myp@ssw0rd

# Install on the first local disk available on
machine

install --firstdisk --overwritevmfss

# Set the network to DHCP on the first network
adapter

network --bootproto=dhcp --device=vmnic0

# A sample post-install script

%post --interpreter=python --ignorefailure=true
import time

stampFile = open('/finished.stamp',

```

In the default script, you can see it sets the root password to **myp@ssword**, installs on the first disk, overwrites any existing VMFS datastore, and sets the network interface to use DHCP. When creating your own script, you can specify many options, a few are shown in [Table 8-4](#).

**Table 8-4** Sample Options for ESXi Installation Script.

Command	Options	Description
Clearpart (Optional )	-- ignoredrives=	Removes partitions on all drives except those specified
	-- overwritevmf s	Allows overwriting of VMFS partitions on the specified drives.
dryrun	N/A	Parses and checks the installation script, but does not perform the installation.

install	--disk=	<p>Specifies the disk to partition. Acceptable values can use various forms, like these examples.</p> <p><b>Path:</b></p> <pre>--disk=/vmfs/devices/disks/mpx.vmhba1:C0:T0:L0</pre> <p><b>MPX name:</b></p> <pre>--disk=mpx.vmhba1:C0:T0:L0</pre> <p><b>VML name:</b></p> <pre>--disk=vml.000000034211234</pre> <p><b>vmkLUN UID:</b></p> <pre>--disk=vmkLUN_UID</pre>
	--ignoressd	Excludes solid-state disks from eligibility for partitioning
	--overwritevsan	You must use the --overwritevsan option when you install ESXi on a disk, either SSD or HDD (magnetic), that is already in a vSAN disk group.
network	--bootproto=	Specifies if the IP address should be set statically or via DHCP.
	--ip=	Sets an IP address for the machine to be installed, in the form xxx.xxx.xxx.xxx. Required with the <code>bootproto=static</code> option and ignored otherwise
	--nameserver	Designates the primary name server as an IP address. Used with the <code>bootproto=static</code> option. You can omit this option if you do not intend to use DNS.

## Auto Deploy

vSphere Auto Deploy provides the functionality to install ESXi on hundreds of physical hosts. Large environments can be deployed and managed efficiently by experienced administrators utilizing Auto Deploy. Hosts utilize network booting to boot from a central Auto Deploy server. Hosts can be configured with a host profile of a reference host, if desired. This host profile could be created to prompt for input. After the hosts boot and are configured, they are then managed by vCenter Server like other ESXi hosts. Auto Deploy can also be configured for stateless caching or stateful installations.

With stateless caching, which is the default setting, Auto Deploy does not store ESXi configuration or state data within the host. Instead, Auto Deploy uses image profiles and host profiles to maintain the host configuration. During subsequent boots, the host must connect to the Auto Deploy server to retrieve its configuration.

With stateful installs, Auto Deploy is used to boot the host but the installation and configuration is written to a local disk. On subsequent boots, the host boots from the local disk where this host configuration is stored.

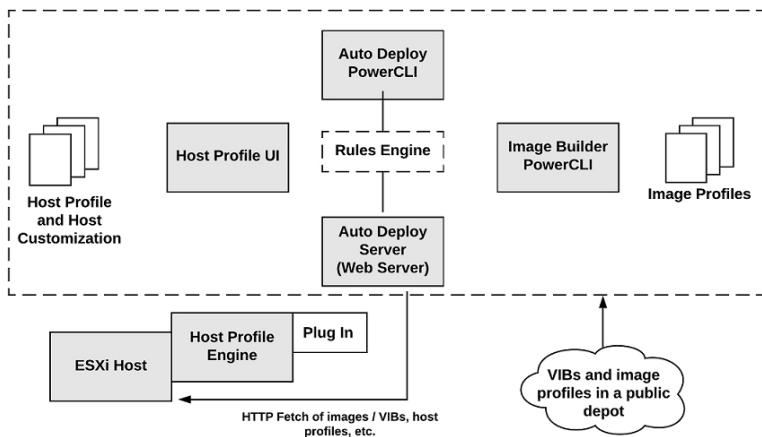
Auto Deploy can be configured and managed using a graphical user interface (GUI) in vSphere 6.5 and later. The PowerCLI method is still available, but the GUI provides an easier-to-use option. For the Auto Deploy GUI to be visible in the vSphere Web Client, both the Image Builder and Auto Deploy services must be running when you're logging in to vCenter Server. The Image Builder feature in the GUI enables you to download ESXi images from the VMware public repository or to upload ZIP files containing ESXi images or drivers. You can customize the images by adding or removing components and optionally export images to ISO or ZIP for use elsewhere. You can compare two images to see how their contents differ.

You can use the Deployed Hosts tab to view hosts that are provisioned with Auto Deploy and to perform tests and remediations.

The architecture for Auto Deploy includes many components as described in [Table 8-5](#) and illustrated in [Figure 8-2](#).

**Table 8-5** Auto Deploy Components

Component	Description / Purpose
Auto Deploy Server	Uses a rules engine, a set of images, a set of host profiles, and required infrastructure to manage ESXi deployments.
Rules Engine	Assigns image profiles and host profiles to each host.
Host Profiles	Defines host-specific configurations, such as networking, NTP, and host permissions. You can use host customization in conjunction with host profiles to provide details that are unique to each host, such as IP address.
Auto Deploy PowerCLI	Command line engine for driving Auto Deploy.
Image Builder PowerCLI	Command line engine for building images.
vCenter Server	Manages the vSphere inventory and provides host profiles.
DHCP Server	Provides IP configuration to the host and redirects the host to the PXE server.
PXE server	Boots the host and directs it to the TFTP server.
TFTP server	Provides the appropriate boot image.
Software Depot	A collection of VIBs either online (accessible via HTTP) or offline (accessible via a USB drive or CD/DVD).
Image Profiles	A collection of VIBs used to install the ESXi server and saved as ZIP files or ISO images. You can obtain image profiles from VMware and VMware partners and you can create custom image profiles using ESXi Image Builder.
vSphere Installation Bundle (VIB)	This is a collection of files (such as drivers) that are packaged into an archive similar to a ZIP file. These are the acceptance levels, from highest to lowest: <ul style="list-style-type: none"><li>• VMwareCertified</li><li>• VMwareAccepted</li><li>• PartnerSupported</li><li>• CommunitySupported</li></ul>



**Figure 8-2** Auto Deploy Architecture

You control the behavior of the vSphere Auto Deploy server by using rules. The rules engine checks the rule set for matching host patterns to decide which items (image profile, host profile, vCenter Server location, or script object) to use to provision each host. Rules can assign image profiles and host profiles to a set of hosts. A rule can identify target hosts by boot MAC address, SMBIOS information, BIOS UUID, Vendor, Model, or fixed DHCP IP address. You can create rules by using the vSphere Web Client or vSphere Auto Deploy cmdlets in a PowerCLI.

For example, to create a new deployment rule named **Rule-01** that places all hosts in a folder named **Auto-deployed Hosts**, you can use the following command.

```
New-DeployRule -Name Rule-01 -Item "Auto-deployed Hos
```

If you wish to modify the rule so that it only applies to a set of hosts in a specific IP range, you can do so using the Set-DeployRule cmdlet.

```
Set-DeployRule -DeployRule Rule-01 -Pattern "ipv4=192
```

**Table 8-6** describes some of common AutoDeploy PowerCLI cmdlets.

**Table 8-6** Sample of AutoDeploy PowerCLI cmdlets.

<b>Command</b>	<b>Description</b>
<b>Get-DeployCommand</b>	Returns a list of Auto Deploy cmdlets.
<b>New-DeployRule</b>	Creates a new rule with the specified items and patterns.
<b>Set-DeployRule</b>	Updates an existing rule with the specified items and patterns. You cannot update a rule that is part of a rule set.
<b>Get-DeployRule</b>	Retrieves the rules with the specified names.
<b>Copy-DeployRule</b>	Clones and updates an existing rule.
<b>Add-DeployRule</b>	Adds one or more rules to the working rule set and, by default, also to the active rule set. Use the NoActivate parameter to add a rule only to the working rule set.
<b>Remove-DeployRule</b>	Removes one or more rules from the working rule set and from the active rule set. Run this command with the -Delete parameter to completely delete the rule.
<b>Set-DeployRuleSet</b>	Explicitly sets the list of rules in the working rule set.
<b>Get-DeployRuleSet</b>	Retrieves the current working rule set or the current active rule set.
<b>Switch-ActiveDeployRuleSet</b>	Activates a rule set so that any new requests are evaluated through the rule set.
<b>Get-VMHostMatchingRules</b>	Retrieves rules matching a pattern. For example, you can retrieve all rules that apply to a host or hosts. Use this cmdlet primarily for debugging.
<b>Test-DeployRulesetCompliance</b>	Checks whether the items associated with a specified host are in compliance with the active rule set.

<b>Repair-DeployRulesetCompliance</b>	Given the output of Test-DeployRulesetCompliance, this cmdlet updates the image profile, host profile, and location for each host in the vCenter Server inventory. The cmdlet might apply image profiles, apply host profiles, or move hosts to the prespecified folders or clusters on the vCenter Server system.
<b>Apply-EsxImageProfile</b>	Associates the specified image profile with the specified host.
<b>Get-VMHostImageProfile</b>	Retrieves the image profile in use by a specified host. This cmdlet differs from the Get-EsximageProfile cmdlet in the Image Builder PowerCLI.
<b>Repair-DeployImageCache</b>	Use this cmdlet only if the Auto Deploy image cache is accidentally deleted.
<b>Get-VMHostAttributes</b>	Retrieves the attributes for a host that are used when the Auto Deploy server evaluates the rules.
<b>Get-DeployMachineIdentity</b>	Returns a string value that Auto Deploy uses to logically link an ESXi Host in vCenter to a physical machine.
<b>Set-DeployMachineIdentity</b>	Logically links a host object in the vCenter Server database to a physical machine. Use this cmdlet to add hosts without specifying rules.
<b>Get-DeployOption</b>	Retrieves the Auto Deploy global configuration options. This cmdlet currently supports the vlan-id option, which specifies the default VLAN ID for the ESXi Management Network of a host provisioned with Auto Deploy. Auto Deploy uses the value only if the host boots without a host profile.
<b>Set-DeployOption</b>	Sets the value of a global configuration option. Currently supports the vlan-id option for setting the default VLAN ID for the ESXi Management Network.



The first time a host boots using Auto Deploy, the following sequence of events occurs.

1. The host starts a PXE boot sequence. The DHCP Server assigns an IP address and redirects the host to the TFTP server.
2. The host downloads and executes the iPXE file and applies the associated configuration file.
3. The host makes an HTTP boot request to the vSphere Auto Deploy server. The HTTP request includes hardware and network information.
4. The vSphere Auto Deploy server performs these tasks:

- Queries the rules engine.
  - Streams data from the image profile and the host profile.
5. The host boots using the image profile. If the vSphere Auto Deploy server provided a host profile, the host profile is applied to the host.
  6. vSphere Auto Deploy adds the host to the proper location in the vCenter Server system.
  7. If the host is part of a DRS cluster, virtual machines from other hosts might be migrated to the host.

**Note**

If the host profile requires the user to specify certain information, such as a static IP address, the host is placed in maintenance mode when the host is added to the vCenter Server system. You must reapply the host profile and update the host customization to have the host exit maintenance mode.

## DEPLOY VCENTER SERVER COMPONENTS

VMware vCenter 7.0 is only available as a pre-built Linux-based virtual appliance. It is no longer available to be installed on Windows systems.

### vCenter Server Database

As of vCenter 7.0, there is only one database that can be used: an included version of the VMware specific distribution of PostgreSQL for vSphere and vCloud.

**Note**

The vCenter installation program allows migration from a Windows-based vCenter server to the vCenter appliance, as with prior versions and includes migrating from Oracle or MSSQL to PostgresSQL.

### Platform Services Controller (PSC)

In vSphere 6.x, the Platform Services Controller (PSC) was a component that could be deployed externally from

vCenter Server. Beginning with vSphere 7.0, the services that PSC provided in vSphere 6.x, such as SSO, VMCA and License Service, are consolidated into vCenter Server. These services cannot be deployed as a separate virtual appliance. Since the services are now part of vCenter, they are no longer listed as part of the PSC. For example, in vSphere 7.0, the *vSphere Authentication* publication replaces the *Platform Services Controller Administration* publication.

## vCenter Server Appliance

As of vSphere 7.0, the vCenter Server is only available as a pre-built virtual appliance. This appliance consists of:

- Photon OS 3.0
- vSphere Authentication Services
- PostgreSQL
- VMware vSphere Lifecycle Manager Extension
- VMware vCenter Lifecycle Manager

vCenter version 7.0 deploys with VM hardware version 10, supporting up to 64 virtual CPUs per VM. The deployment wizard allows you to determine the resource allocation of the virtual appliance based on the size of your environment.

To prepare for a vCenter Server Appliance deployment, you should download the vCenter Server Appliance installer ISO file and mount it to a virtual machine or physical machine from which you want to perform the deployment. To use the vCenter Server Appliance GUI (or CLI) installer, you can use a machine that is running a supported version of Windows, Linux, or Mac operating system, as shown in [Table 8-7](#)

---

**Table 8-7** Requirements for GUI / CLI installers

OS	Supported Versions	Minimal Hardware Configuration
Windows	<ul style="list-style-type: none"> <li>Windows 8, 8.1, 10</li> <li>Windows 2012 x64 bit</li> <li>Windows 2012 R2 x64 bit</li> <li>Windows 2016 x64 bit</li> </ul>	4 GB RAM, 2 CPU having 4 cores with 2.3 GHz, 32 GB hard disk, 1 NIC
Linux	<ul style="list-style-type: none"> <li>SUSE 15</li> <li>Ubuntu 16.04 and 18.04</li> </ul>	4 GB RAM, 1 CPU having 2 cores with 2.3 GHz, 16 GB hard disk, 1 NIC  CLI Installer requires 64 bit OS.
Mac	<ul style="list-style-type: none"> <li>MacOS v10.13, 10.14, 10.15</li> <li>MacOS High Sierra, Mojave, Catalina</li> </ul>	

Using the GUI or CLI Installers, you can:

- Deploy and upgrade the vCenter Server Appliance.
- Converge prior vCenter installations with external Platform Services Controller(s) to the current vCenter Server version.
- Restore a vCenter Server Appliance from a file-based backup.

### Deploy VCSA Using the GUI Installer

You can use the GUI installer to deploy a vCenter Server Appliance. To perform a GUI based deployment, you download the vCenter Server Appliance installer on a network client machine, run the deployment wizard from the client machine, and provide the required information.

**Note**

vCenter 7 incorporates all services that were part of the Platform Services Controller to a single vCenter VM.

Using the GUI Installer involves two stages. In the first stage, you navigate through the installation wizard, choose the deployment type, provide the appliance settings, and deploy the OVA. Alternatively, you could

use the vSphere Web Client or the vSphere Host Client to deploy the OVA.

In the second stage using the GUI Installer, you use a wizard to configure the appliance time synchronization, configure vCenter Single Sign-On (SSO), and start the services in the newly deployed appliance. Alternatively, you can use a web browser to access the appliance's VMware Appliance Management Interface (VAMI) at <https://FQDN:5480>. If you use the alternative approach in the first stage, then you must use it in the second stage. To use the GUI Installer to deploy the VCSA, you can follow these steps.



**Step 1.** In the vCenter Server Appliance installer, navigate to the appropriate subdirectory in the **vcsa-ui-installer** directory and run the installer executable file.

- a. For Windows OS, use the **win32** subdirectory the **installer.exe** file.
- b. For Linux OS, use the **lin64** subdirectory and the **installer** file.
- c. For Mac OS, use the **mac** subdirectory and the **Installer.app** file.

**Step 2.** On the Home page, click **Install**.

**Step 3.** On the next page, click **Next**.

**Step 4.** Read and accept the license agreement and click **Next**.

**Step 5.** Connect to the target server, where you want to deploy the appliance. You have two choices.

- a. Provide the FQDN (or IP address) and credentials for the target ESXi host and provide the appropriate certificate.
- b. Provide the FQDN (or IP address) and credentials for the target vCenter Server (that is managing the hosts on which this new vCenter Server will be deployed), provide the appropriate certificate, and specify the appropriate location in the vSphere Inventory.

**Step 6.** On the next page, set the appliance's name and root user password, following these rules.

- a. The appliance name must not contain a percent sign (%), backslash (\), or forward slash (/) and must be no more than 80 characters in length.
- b. The password must contain only lower ASCII characters without spaces, at least eight characters, a number, uppercase and lowercase letters, and a special character, for example, an exclamation mark (!), hash key (#), at sign (@), or brackets (()).

**Step 7.** Select the deployment size. Choose Tiny, Small, Medium, Large, X-Large as explained in [Chapter 1](#).

**Step 8.** Select the storage size for the appliance as explained in [Chapter 1](#).

**Step 9.** Select an available datastore. (Enable Thin Disk Mode will allow the vCenter VM virtual disks to be thin provisioned. NFS datastores are thin provisioned by default).

**Step 10.** On the Configure Network settings page, setup the network settings, such as virtual switch port

group, IP configuration, and communication ports.

**Step 11.** On the Ready to complete page, select **Finish**.

**Step 12.** Wait for the OVA to deploy, then click **Continue** to proceed with Stage 2.

**Step 13.** In Stage 2, click **Next** on the Introduction page.

**Step 14.** For time configuration, choose an option.

- a. Synchronize time with the ESXi host.
- b. Synchronize time with NTP Servers

**Step 15.** Optionally, enable SSH connections into the appliance.

**Step 16.** Create a new SSO domain or join an existing domain.

- a. Create new: enter domain (such as vsphere.local), set the SSO Administrator (administrator@vsphere.local by default) account password, provide a SSO site name, and confirm the password.
- b. Join an existing SSO domain: enter the PSC FQDN containing the SSO Server, provide the HTTPS port that PSC will use, provide the target SSO domain name (such as vsphere.local), and enter the SSO Administrator account password.

**Step 17.** Optionally, choose the option to join the VMware Customer Experience Improvement Program (CEIP)

**Step 18.** On the Ready to complete page, click **Finish** and **OK**.

## CLI Deployment

You can use the CLI installer to perform a silent deployment of a VCSA appliance. The CLI deployment process includes downloading the installer, preparing a JSON configuration file with the deployment information, and running the deployment command. The VCSA Installer contains JSON templates for all deployment types. This enables you to deploy an appliance with minimum effort by copying the appropriate JSON template, changing a few values, and using it with the CLI Installer. The steps are:

**Step 1.** In the vCenter Server Appliance installer, navigate to one of the following directories:

- a. If you are running Windows: **/vcsa-cli-installer/win32**
- b. If you are running Linux: **/vcsa-cli-installer/lin64**
- c. If you are running MacOS: **/vcsa-cli-installer/mac**

**Step 2.** Copy the templates from the **install** subfolder to your desktop.

**Step 3.** Use a text editor to modify the JSON template for your use case. Modify the default parameter values with your appropriate values and add additional parameters as necessary. For example, to use an IPv4 DHCP assignment, in the `network` subsection of the template, change the value of the `mode` parameter to `dhcp` and remove the default configuration parameters that are used for a static assignment, as shown here.

---

```
"network": {  
  "ip_family": "ipv4",
```

```

        "mode": "dhcp"
    },

```

**Step 4.** Save the file in UTF-8 format.

Table 8-8 shows some of the available JSON templates.

**Table 8-8** JSON Templates Sample.

Template	Description
PSC_replication_on_ESXi.json	Contains the minimum configuration parameters that are required for deployment of a Platform Services Controller appliance joining an existing vCenter Single Sign-On domain on an ESXi host.
PSC_replication_on_VC.json	Contains the minimum configuration parameters that are required for deployment of a Platform Services Controller appliance joining an existing vCenter Single Sign-On domain on a vCenter Server instance.
vCSA_on_ESXi.json	Contains the minimum configuration parameters that are required for deployment of a vCenter Server Appliance with an external Platform Services Controller on an ESXi host.
vCSA_on_VC.json	Contains the minimum configuration parameters that are required for deployment of a vCenter Server Appliance with an external Platform Services Controller on a vCenter Server instance.

**Note**

When using the CLI Installer, you must strictly use only ASCII characters for the command line and JSON configuration file values, including usernames and passwords.

Prior to running the deployment command, you can run the pre-deployment check using this command.

```
vcsa-deploy install --verify-only path-to-JSON-file
```

When ready, you can run the deploy command.

```
vcsa-deploy install --accept-eula --acknowledge-ceip
```

## Post Installation

After installing vCenter Server, you should be able to access the vSphere Client at

`https://vcenter_server_ip_address_or_fqdn/ui` and the vSphere Web Client at  
`https://vcenter_server_ip_address_or_fqdn/vsphere-client.`

The VMware Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality. In the vSphere 6.5 release, the VMware Enhanced Authentication Plug-in replaced the Client Integration Plug-in.

To install the VMware Enhanced Authentication Plug-in you can use the following procedure. If you install the plug-in from an Internet Explorer browser, you must first disable Protected Mode and enable pop-up windows on your Web browser.

**Step 1.** In a Web browser, open the vSphere Web Client.

**Step 2.** At the bottom of the vSphere Web Client login page, click **Download Enhanced Authentication Plug-in**.

**Step 3.** Save the plug-in to your computer and run the executable.

**Step 4.** Follow the wizard for both the VMware Enhanced Authentication Plug-in and the VMware Plug-in Service which are run in succession.

**Step 5.** When the installations are complete, refresh the browser.

**Step 6.** On the External Protocol Request dialog box, click **Launch Application**

## Configure/Manage VMware Certificate Authority (VMCA)

The VMware Certificate Authority (VMCA), which runs in the vCenter Server Appliance, is responsible for issuing certificates for VMware solution users, certificates for machines running required services, and certificates for ESXi hosts. The VMware End Point Certificate Service (VECS) is a local repository for certificates and private keys. VECS is a mandatory component that will be used when VMCA is not signing certificates. The VECS includes a set of keystores including machine SSL certificates, trusted roots, CRLs, and solution users (machine, vpxd, vpx-extension, vSphere-webclient). VECS does not store ESXi Certificates. ESXi certificates are stored locally on the ESXi hosts in the `/etc/vmware/ssl` directory. Table 8-9 describes the stores included in VECS.

**Table 8-9** VECS stores.

---

<b>Store</b>	<b>Description</b>
Machine SSL store (MACHINE_SSL_CERT)	Used by the reverse proxy service on each ESXi host and by the vmdir service
Trusted root store (TRUSTED_ROOTS)	Contains all trusted root certificates.
Solution user stores <ul style="list-style-type: none"><li>• Machine</li><li>• Vpxd</li><li>• vpxd-extension</li><li>• vsphere-webclient</li></ul>	VECS includes one store for each solution user.
vSphere Certificate Manager Utility backup store (BACKUP_STORE)	Used by VMCA (VMware Certificate Manager) to support certificate revert.
Other stores	Other stores might be added by solutions. For example, the Virtual Volumes solution adds an SMS store.

With VMCA, you can deal with certificates in three different manners. You can let VMCA operate in a default manner, where it uses a self-signed root certificate, issues certificates to the vSphere components, and serves as the certificate authority (CA) to vSphere. You can configure VMCA to operate as a subordinate CA on behalf of the enterprise's CA and to use a subordinate CA signing certificate. You can bypass VMCA and use only 3<sup>rd</sup> party certificates, which you will need to store in the VECS, except for ESXi hosts certificates. When necessary, you can use `vecs-cli` commands to explicitly manage certificates and keys.

**Note**

The VMCA in vSphere 7.x does NOT support the use of CRLs nor does it have the concept of certificate revocation. If you suspect one certificate was compromised, you should remove it and consider replacing all certificates.

Using VMCA in the default manner, where it acts as the CA for vSphere, no real configuration is required, other than to configure web browsers to trust VMCA. The VMCA can handle all certificate management in vSphere environments, where historically the administrator has elected not to replace certificates. During an upgrade to vSphere 6.0, all self-signed certificates are replaced with certificates signed by VMCA.

Using VMCA in a subordinate CA manner requires you to replace the VMCA root certificate with a certificate signed by a third party CA, making the VMCA certificate an intermediate certificate of the CA. To use VMCA in the subordinate CA manner, follow this procedure.



**Step 1.** Launch the vSphere 6.0 Certificate Manger.

**Step 2.** Select **Option 2**, which is to replace the VMCA root certificate with a custom signing certificate and replace all certificates.

**Step 3.** When prompted provide the password for the SSO domain administrator account.

**Step 4.** Select **Option 1**, to generate a Certificate Signing Request (CSR) and key. When prompted, provide a directory to save the CSR and key.

**Step 5.** Provide the CSR (`root_signing_cert.csr`) to your CA to generate the subordinate signing certificate.

**Step 6.** Use a text editor to copy content of intermediate CA certificates and the root CA certificate into a single file (`root_signing_chain.cer`).

**Step 7.** In the Certificate Manger, select **Option 1**, to continue to the step to import custom certificates.

**Step 8.** Import the root signing certificate (`root_signing_chain.cer`) and root signing key (`root_signing_cert.key`).

**Step 9.** When prompted, provide a value for each item, such as country, name, and organization.

**Step 10.** After completing these steps, the VMCA root certificate is replaced with a custom signing certificate.

For more details on this procedure see VMware KB 2112016.

## CONFIGURE SINGLE SIGN-ON (SSO)

In addition to deploying one or more VCSAs and creating a vCenter Single Sign-on (SSO) domain in a new vSphere environment, you need to configure SSO. Configuring SSO includes adding and editing SSO identity sources, configuring SSO users, and configuring SSO policies.

### SSO and Identity Sources Overview

To access vCenter Server, users must login using SSO domain user accounts or user accounts from identity sources registered in SSO. The acceptable identity sources are Active Directory (Integrated Windows Authentication), Active Directory as a LDAP Server, Open LDAP and Local OS.

The Local OS identity source is available immediately following the installation of SSO. Local operating system users are local to the operating system where the vCenter Single Sign-On server is running. The local operating system identity source exists only in basic vCenter Single Sign-On server deployments and is not available in deployments with multiple vCenter Single Sign-On instances. Only one local operating system identity source is allowed.

The SSO domain is also available immediately as an identity source. This domain was called vsphere.local in vSphere 5.5, but in vSphere 6.x and higher, you may assign the SSO domain name during installation.

## Add/Edit/Remove SSO Identity Sources

You can use the vSphere Client to add SSO identity sources using the following procedure

**Step 1.** Log in with the vSphere Client to the vCenter Server using administrator@vsphere.local or another member of the SSO Administrators group.

**Step 2.** Navigate to **Home > Administration > Single Sign On > Configuration**

**Step 3.** Click **Identity Sources** and click **Add Identity Source**

**Step 4.** Select one of the following available identity sources and enter the appropriate settings

- Active Directory (Integrated Windows Authentication)
- Active Directory over LDAP
- OpenLDAP
- Local operating system of SSO server.

**Step 5.** Click **Add**.

To remove an SSO identity source, you can use the vSphere Web Client to select the identity source on the **Identity Sources** tab at **Administrator > Single Sign-On > Configuration** and click the **Delete Identity Source** icon. When prompted, click **Yes** to confirm.

You can configure a default domain for SSO. The default SSO domain allows users to authenticate without identifying a domain name. Users from other identity sources must identify the domain name during authentication. To configure a default domain using the vSphere Client, you can use these steps.

**Step 1.** Navigate to **Home > Administration > Single Sign On > Configuration**

**Step 2.** Click **Identity Sources** and click **Add Identity Source**

**Step 3.** Select an identity source and click **Set as Default**.

## **How to Add an Active Directory Identity Source**

To permit Active Directory authentication in vSphere, add one or more Active Directory domains as identity sources in SSO. In scenarios, where the SSO server is a member of an Active Directory domain, that domain may be added as **Active Directory (Integrated Windows Authentication)** identity source. You can add other Active Directory domains to SSO as **Active Directory LDAP Server** identity sources.

As a requirement to add an integrated Active Directory identity source, you need to ensure the server where SSO is installed is in the domain. The vCenter Server appliance can be added to the domain using the following procedure.

**Step 1.** Logon to the vSphere Web Client using the SSO domain administrator account, such as administrator@vsphere.local.

**Step 2.** In the left pane, select **Administration > System Configuration > Nodes**.

**Step 3.** Select the appropriate node and click the **Manage** tab.

**Step 4.** Select **Active Directory** and click **Join**.

**Step 5.** Enter the Active Directory details such as **Domain, Organizational Unit, User Name, and Password**.

**Step 6.** Click **OK**.

**Step 7.** Right-click the node and select **Reboot**.

After the appliance reboots, you add it as an Active Directory (Integrated Windows Authentication) identity source

When adding an Active Directory (Integrated Windows Authentication) identity source, provide the following information

- **Domain Name:** FQDN of the domain
- **Use Machine Account:** Select this option to use the local machine account as the Server Principal Name (SPN). Do not use this option if you plan to rename the machine.
- **Use Service Principal Name (SPN):** Select this option, instead of Use Machine Account, if you prefer to specify a unique SPN, instead of using the machine name as the SPN. If you choose this option, then you must also provide the SPN, UPN, and password as follows.
- **Service Principal Name (SPN):** If you selected the Use Service Principal Name option, then provide a unique name that includes the domain name, such as STS/domain.com.
- **User Principal Name (UPN):** If you selected the Use Service Principal Name option, then

provide a user name that can authenticate to the Active Directory domain.

- **Password:** If you selected the Use Service Principal Name option, then provide a password that is associated with the UPN.

**Note**

The user account must have read access to the OUs containing users and group. If the user account does not have sufficient permission or is locked or disabled, then authentications and searches in the Active Directory domain fail

When adding an Active Directory over LDAP identity source, provide the following information



- **Name:** Logical name for the identify source
- **Base DN for users:** Base Distinguished Name for users.
- **Base DN for groups:** Base Distinguished Name for groups.
- **Domain Name:** FDQN of the domain
- **Domain Alias:** The Domain's NetBIOS name.
- **Username:** User name in the domain that has at least read access to the specified user and group base DNs.
- **Password:** Password that is associated with the user name.
- **Connect to:** Domain controller which to connect.
- **Primary Server URL:** The primary domain controller's URL in the form of `ldap://hostname:port`, or `ldaps://hostname:port`.

- **Secondary Server URL:** The secondary domain controller's URL in the form of `ldap://hostname:port`, or `ldaps://hostname:port`.
- **SSL certificate:** When using LDAPS in the URL parameters, specify the certificate.

You can add additional user accounts from other Identity Sources to the SSO Administrators group. To add additional user accounts from other Identity Sources to the Administrators group in the SSO domain, you can follow these steps:

**Step 1.** Login to vSphere Web Client with the SSO domain administrator account.

**Step 2.** Select **Administration > Users / Groups**

**Step 3.** Select the **Group tab > Administrators > Add Member** icon from the Group Members section

**Step 4.** Select the additional Identity Source from the **Domain** drop down menu.

**Step 5.** Select the account you would like to add

**Step 6.** Click **OK**

## How to Add an LDAP Authentication Source

To use OpenLDAP for authentication, one or more LDAP authentication sources have to be added in vCenter. In order to utilize OpenLDAP for authentication, the following requirements must be met.

- OpenLDAP schema is RFC4519 compliant
- All users have an objectClass of `inetOrgPerson`

- All groups have an objectClass of groupOfUniqueNames
- All groups have a group membership attribute of uniqueMember
- All users and group objects have entryUUID configured

When configuring OpenLDAP, the following information needs to be provided.

- **Name:** Logical name for the identify source
- **Base DN for users:** Base Distinguished Name for users.
- **Base DN for groups:** Base Distinguished Name for groups.
- **Domain Name:** FDQN of the domain
- **Domain Alias:** The domain name in capital letters is added if no alias is defined
- **Username:** User name in the domain that has at least read access to the specified user and group base DNs.
- **Password:** Password that is associated with the user name.
- **Primary Server URL:** The primary server's URL in the form of ldap://*hostname*:*port*, or ldaps://*hostname*:*port*.
- **Secondary Server URL:** The secondary server's URL in the form of ldap://*hostname*:*port*, or ldaps://*hostname*:*port*.
- **SSL certificate:** When using LDAPS in the URL parameters, specify the certificate.

## **Enable/Disable Single Sign-On (SSO) Users**

To manage SSO users, you could use the vSphere Client. For example, to add a SSO user, follow these steps.

**Step 1.** Logon to the vCenter Server connected using administrator@vsphere.local or another user in the SSO Administrators group.

**Step 2.** Navigate to Home > Administration > Single Sign-On > Users and Groups

**Step 3.** Select the **Users** tab and click **Add User**.

**Step 4.** Provide the **User Name** and **Password**.  
Optionally provide values for the other fields.

**Step 5.** Click **OK**.

In a similar manner, you can create an SSO group by selecting **Users** tab in Step 3 and providing details in Step 4. You can also use the **Groups** tab to select a group and use the **Add Member** icon (in the details section) to add users to the group. When adding a user to a group, use the **Domain** dropdown to select the SSO domain or another identity source and select a user account from the provided list.

To disable or enable an SSO user account, select the user account in **Users and Groups**, click the ellipsis icon, and click **Disable** or **Enable**.

The SSO domain (vsphere.local in vSphere 5.5, but may be named differently in vSphere 6.0) provides several pre-defined groups. You can add users from Active Directory domains or other identity sources to these pre-defined groups. Some SSO privileges are determined solely by the membership of these groups. For example, a user who is a member of the CAAdmins group can manage VMCA and a user who is a member of

the `LicenseService.Administrators` group can manage licenses.

The SSO domain contains many pre-defined groups, including the following:

- `Users`: Contains all users in the SSO domain
- `DCAdmins`: Members can perform Domain Controller Administrator actions on the VMware Directory Service.
- `SolutionUsers`: Each solution user authenticates individually to vCenter Single Sign-On with a certificate. By default, VMCA provisions solution users with certificates. Do not add members to this group explicitly.
- `CAAdmins`: Members have administrator privileges for VMCA. Adding members to these groups is not usually recommended, but a user must be a member of this group to perform most certificate management operations, such as using the `certool` command.
- `SystemConfiguration.BashShellAdministrators`: Members can enable and disable access to the BASH Shell.
- `SystemConfiguration.Administrators`: Members can view and manage the system configuration and perform tasks such as restarting services.
- `LicenseService.Administrators`: Members have full write access to all licensing related data and can add, remove, assign, and un-assign serial keys for all product assets registered in licensing service.
- `Administrators`: Members can perform SSO administration tasks for the VMware Directory Service (`vmdir`)

## Configure SSO Policies

SSO provides policies that enforce security rules in the environment. You can configure SSO password policies, SSO lockout policies, and SSO token policies. To configure these policies, you can use the vSphere Client to select **Administration > Single Sign-On > Configuration**, then select **Password Policy**, **Lockout Policy**, or **Token Policy** and click **Edit**. For each set of policies, set the appropriate password policy parameters as described in Table 8-10.

**Table 8-10** SSO Policies and Parameters

SSO Policy Type	Policy Parameter	Details
Password Policy	Description	Password policy description.
	Maximum lifetime	Maximum number of days that a password can exist before the user must change it.
	Restrict reuse	Number of the user's previous passwords that cannot be selected.
	Maximum length	Maximum number of characters that are allowed in the password
	Minimum length	Minimum number of characters that are allowed in the password, which must be no less than the combined minimum of alphabetic, numeric, and special character requirements.
	Character requirements	Minimum number of different character types that are required in the password. The types include special, alphabetic, uppercase, lowercase and numeric.
	Identical adjacent characters	The number of identical adjacent characters that are supported in a password. The value must be greater than 0.
Lockout Policy	Description	Description of the lockout policy
	Max number of failed login attempts	Maximum number of failed login attempts that are allowed before the account is locked
	Time interval between failures	Time period in which failed login attempts must occur to trigger a lockout
	Unlock time	The amount of time the account stays locked. The value 0 specifies that an administrator must explicitly unlock the account.
Token Policy	Clock tolerance	Time difference in milliseconds that SSO tolerates between a client clock and a domain controller clock. If the time difference is greater than the specified value, SSO declares the token to be invalid.
	Maximum token renewal count	Maximum number of times a token may be renewed, before a new security token is required.
	Maximum token delegation count	Maximum number of times a single holder-of-key token can be delegated.
	Maximum bearer token lifetime	The lifetime value of a bearer token before the token must be reissued.
	Maximum holder-of-key token lifetime	The lifetime value of a holder-of-key token before the token is marked invalid.

## Configure Identity Federation

When added to an identity provider, the vSphere Client will redirect a user's login attempt to that provider's login page. Corporate credentials (including multifactor authentication) can then be used to log in. After authentication, the identify provider redirects the user back to the vSphere Client via a cryptographic token used for authorization.

Identity Federation utilizes OAuth2 and OIDC protocols for information exchange. Identity Federation replaces traditional Active Directory, Integrated Windows Authentication, and LDAP/LDAPS authentication for vCenter. vSphere Single Sign-on is not replaced, however, to allow additional administration or emergency access.



Active Directory Federation Services requirements:

- AD FS for Windows Server 2016 R2 or higher is deployed
- AD FS is connected to Active Directory
- Application Group for vCenter is created in AD FS for configuration.  
(<https://kb.vmware.com/s/article/78029>)
- AD FS server certificate signed by Certificate Authority.
  - If self-signed certificates are used, the root CA certificate has to be imported to the vCenter JRE truststore.

vSphere requirements:

- vSphere 7.0
- Communication possible between the vCenter server and AD FS endpoint, authorization, token, logout, JWKS, and other advertised endpoints
- `VcIdentityProviders.Manage` privilege in vCenter to create, update, or delete a vCenter Server Identity Provider required for federated authentication. If a user should be limited to view the Identity Provider configuration and not change it, use the `VcIdentityProviders.Read` privilege.

Procedure to enable Identity Federation:

**Step 1.** In the vSphere Client, navigate to Home > Administration > Configuration > Single Sign On

**Step 2.** Select the Identity Provider tab

**Step 3.** Click the “i” next to “Change identity provider”

**Step 4.** Copy the URIs in the pop-up (these will be needed to configure the AD FS server)

**Step 5.** Close the pop-up

**Step 6.** Create an OpenID Connect configuration in the AD FS and configure it for the vCenter Server.

a. A shared secret and identifying information must be established between the identity provider and vCenter. An OpenID Connect configuration is created in AD FS, which is known as an Application Group: a Server application and a Web API. These components define the information that vCenter uses to trust and communicate with the AD FS server. To create the AD FS

Application Group, the 2 Redirect URIs from step 5 are used. It is then important to copy or record the following information:

- i. Client identifier
- ii. Shared Secret
- iii. OpenID address of the AD FS server

**Step 7.** Go back to the **Identity Provider** tab

**Step 8.** Click **Change identity provider**

**Step 9.** Select **Microsoft ADFS**

**Step 10.** Click **Next**

**Step 11.** Enter the following information:

- a. Client identifier
- b. Shared Secret
- c. OpenID Address of the AD FS Server

**Step 12.** Click **Next**

**Step 13.** Enter the user and group information for Active Directory over LDAP to then search for users and groups.

**Step 14.** Click **Next**

**Step 15.** Review the configuration information and click **Finish**

**Step 16.** Go to **Home > Administration**

**Step 17.** Click on Users and Groups under Single Sign On

**Step 18.** Click the **Groups** tab

**Step 17.** Click **Administrators (group)** and click **Add Members**

**Step 18.** From the drop-down, select **Microsoft ADFS**

**Step 19.** In the text box under the drop-down menu, enter **vcenter** and wait for the drop-down to show a selection.

**Step 20.** Select **vCenter Admins** and then add it to the group.

**Step 21.** Click **Save**

**Step 22.** Log into vCenter with an AD user to verify functionality

## INITIAL VSHERE CONFIGURATION

This section covers other vSphere settings, components, and features that are typically configured in conjunction with a new vSphere deployment.

### vSphere Client Implementation

The vSphere Client is HTML5 based and uses the “Clarity” style user interface. You will use this as your primary GUI. The vSphere Client is a service that is installed automatically as you install vCenter Server.

### VMware vSphere Lifecycle Manager Implementation

In vSphere 7.0, vSphere Lifecycle Manager replaces VMware Update Manager from prior versions. Lifecycle Manager adds onto the functionality of Update Manager to include features and capabilities for ESXi lifecycle management at the cluster level. Lifecycle Manager operates as a service which runs on the vCenter Server.

This service is available via the vSphere Client immediately after the vCenter Server deployment. So, no special steps are required to install vSphere Lifecycle Manager, unless you need to install the optional module VMware vSphere Update Manager Download Service (UMDS),

In scenarios where vCenter Server is installed in a secured network with no Internet access, you can install UMDS and use it to download updates. You can use UMDS to export the updates to a portable media drive that you then present to vSphere Lifecycle Manager. Or, if network connectivity exists between the vCenter Server and UMDS, you can automate the export process by leveraging the Web server on the UMDS machine.

See *Update Manager Download Service* in Chapter 13, "Manage vSphere and vCenter Server" for more details.

## Configure the vCenter Server Inventory

You can use the following procedures to create an inventory hierarchy that includes data centers, folders, clusters, and resource pools.

To create a data center, you can use the following procedure

**Step 1.** Logon to the vSphere Client as a user with the **Datacenter.Create datacenter** privilege

**Step 2.** Right-click the vCenter Server in the inventory.

**Step 3.** Select New Datacenter.

**Step 4.** Provide a name for the data center and click **OK**.

To create a folder, you can use the following procedure.

**Step 1.** In the vSphere Client, right-click the appropriate parent object (a data center or another folder).

**Step 2.** Select **New Folder**.

- If the parent object is a folder, then new folder type is automatically set to match the parent
- Otherwise, specify the folder type as **Host and Cluster** folder, **Storage** folder, or **VM and Template** folder.

**Step 3.** Provide a name for the folder and click **OK**.

To add an ESXi host, you must address the following prerequisites.

- Ensure the appropriate data center and (optionally) folder objects are created in the vCenter Server inventory
- Obtain the root account credentials for the host.
- Verify the host and vCenter Server can communicate via port 902 or a custom port.
- Verify that any NFS mounts on the host are active.
- For a host with more than 512 LUNs and 2,048 paths, verify the vCenter Server instance is set to support a large or an x-large environment.

Then can use the following procedure.

**Step 1.** Logon to the vSphere Client as a user with the **Host.Inventory.Add standalone host** privilege

**Step 2.** Right-click the data center or folder in the inventory.

**Step 3.** Select **Add Host**.

**Step 4.** Provide the host's FQDN (or IP address) and credentials

**Step 5.** Provide licensing information (use a new or existing license)

**Step 6.** Optionally, set the lockdown mode, remote access, and virtual machine folder information and continue navigating to the final wizard page.

**Step 7.** click **OK**

## Implement vCenter HA



You can use the following procedure to configure vCenter HA.

**Step 1.** In the vSphere Client, select the vCenter Server in the inventory pane.

**Step 2.** Select Configure > Select vCenter HA > Set Up vCenter HA.

**Step 3.** If your vCenter server is managed by another vCenter server in a different SSO domain, do the following steps.

- Click **Management vCenter Server credentials**. Provide the FQDN and Single Sign-On credentials and click **Next**.
- You may see a Certificate warning displayed. Review the SHA1 thumbprint and select Yes to continue.

**Step 4.** In the **Resource settings** section, first select the vCenter HA network for the active node

from the drop-down menu.

**Step 5.** Click on the checkbox if you want to automatically create clones for Passive and Witness nodes.

**Step 6.** For the **Passive** node, click **Edit**.

- Provide details for the passive node virtual machine, such as name, compute resource, datastore
- Select the Management (NIC 0) and vCenter HA (NIC 1) networks.
- Complete the settings and click **Finish**.

**Step 7.** For the **Witness** node, click **Edit**.

- Provide details for the passive node virtual machine, such as name, compute resource, datastore
- Select the vCenter HA (NIC 1) networks.
- Complete the settings and click **Finish**.

**Step 8.** Click **Next**.

**Step 9.** In the **IP settings** section, provide the IP address details.

**Step 10.** Click **Finish**.

## Configure ESXi Using Host Profiles

### Host Profile Overview

During the implementation of vSphere, you can use Host Profiles to efficiently deploy a standard configuration to a set of ESXi hosts. To do so, you could configure a single ESXi host, create a host profile from that host, then apply the profile to other recently deployed hosts. This process reduces the time required to configure ESXi

hosts and minimizes the risk of misconfigured hosts. The host profile contains all the networking, storage, security, and other host-level settings. The host from which the profile is created is known as the reference host. You can attach a host profile to individual hosts, a cluster, or all the hosts and clusters managed by a vCenter Server. Applying a Host Profile. After attaching the profile, you can check compliance of the associated hosts and remediate as necessary.

You can use this procedure to create a host profile from a reference host.

**Step 1.** Navigate to the Host Profiles main view and click **Extract Host Profile**.

**Step 2.** Select the host that acts as the reference host and click **Next**.

**Step 3.** Enter the name and description for the new profile and click **Next**.

**Step 4.** Review the summary information for the new profile and click **Finish**.

You can use this procedure to attach a profile to ESXi hosts and clusters.

**Step 1.** From the Host Profiles main view, select the host profile to be applied to the host or cluster.

**Step 2.** Click **Attach/Detach** a host profile to hosts and clusters.

**Step 3.** Select the host or cluster from the expanded list and click **Attach**.

**Step 4.** Optionally, click **Attach All** to attach all listed hosts and clusters to the profile.

**Step 5.** If you **enable Skip Host Customization** you will not need to customize hosts during this

process.

**Step 6.** Click **Next**.

**Step 7.** Optionally, you can update or change the user input parameters for the Host Profiles policies by customizing the host.

**Step 8.** Click **Finish** to complete attaching the host or cluster to the profile.

You can use this procedure to remediate an ESXi host.

**Step 1.** Navigate to **Host Profiles** main view.

**Step 2.** Right-click the host profile and select **Remediate**.

**Step 3.** Select the host or hosts you want to remediate with the host profile.

**Step 4.** Optionally, enter the host customizations to specify host properties or browse to import a host customization file.

**Step 5.** Click **Pre-check Remediation** to check if the selected hosts are ready for remediation.

**Step 6.** Select the checkbox to reboot the host if it is required in order to complete the remediation process. If you wish to manually reboot the host after the process, do not select the checkbox.

**Step 7.** Review the tasks that are necessary to remediate the Host Profile and click **Finish**.

## Edit Host Profiles

To edit a host profile, you can use this procedure

**Step 1.** Navigate to **Host Profiles** main view.

**Step 2.** Select the host profile that you want to edit and click the **Configure** tab.

**Step 3.** Click **Edit Host Profile**.

**Step 4.** Optionally, click the **Name and description** tab to change the profile name and description.

**Step 5.** In the Edit host profile page expand each category to view or edit a specific policy or setting.

**Step 6.** View **All** host profile configurations or only **Favorites** configurations.

**Step 7.** Optionally, in the search field, filter the configuration names and values you want to view. For example, enter `SNMP`. All configurations that relate to `SNMP` are displayed.

**Step 8.** Optionally, customize the hosts. Make any changes to the available configuration values for this profile and click **Save**

## **Apply Permissions to ESXi Hosts Using Host Profiles**

You can use host profiles to apply ESXi host permissions to be used when users access the host directly. To configure the host profile with the appropriate permissions, you can use the vSphere Client (not the vSphere Web Client) and follow this procedure.

**Step 1.** Select **View > Management > Host Profiles**.

**Step 2.** Select an existing profile and click **Edit Profile**.

**Step 3.** In the profile tree, locate and expand **Security configuration**.

**Step 4.** Right click on the **Permission rules** folder and click **Add Profile**.

**Step 5.** Expand **Permissions rules** and select **Permission**.

**Step 6.** On the **Configuration Details** tab, click the **Configure permission** drop down menu and select **Require a Permission Rule**.

**Step 7.** Enter the name of a user or group. Use the format *domain\name*, where *domain* is the domain name and *name* is the user or group name.

**Step 8.** If a group name is used, select the **Name refers to a group of users** checkbox.

**Step 9.** Enter the assigned role name, which is case sensitive. This can be the name of a built-in role on the host or a custom role that you created on the host. For system roles, use the non-localized role name, such as `Admin` for the Administrator role or `ReadOnly` for the Read-only role.

**Step 10.** Optionally, select **Propagate permission**.

**Step 11.** Click **OK**.

After configuring the host profile, you can use it to apply the permissions to new or existing ESXi hosts.

## VMware Tools

Ideally, you should install VMware Tools in all your virtual machines. When deploying a new vSphere Environment, you should install VMware Tools in any virtual machines that you deployed as part of the virtual infrastructure and management. For example, if you use virtual machines to run Active Directory domain controllers, DNS servers, or DHCP servers, consider installing VMware Tools.

VMware Tools is a suite of utilities that you install in the operating system of a virtual machine. VMware Tools enhances the performance and management of the virtual machine. You can use the following procedure to install VMware Tools in a virtual machine using the VMware Host Client. This procedure is useful for installing VMware Tools in a DNS, Active Directory domain controller, database server, or other virtual machine that you may deploy prior to deploying vCenter Server.

**Step 1.** Click **Virtual Machines** in the VMware Host Client inventory.

**Step 2.** Select a powered-on virtual machine from the list. (The virtual machine must be powered on to install VMware Tools.)

**Step 3.** Open a console to the virtual machine and log in with administrator or root privileges.

**Step 4.** Click **Actions**, select **Guest OS** from the drop-down menu, and select **Install VMware Tools**.

**Step 5.** Use the guest OS to complete the installation.

## Advanced ESXi Host Options

### ESXi Advanced System Settings

You can use the VMware Host Client or the vSphere Client to set advanced attributes on ESXi hosts. You should change the advanced options only when you get specific instructions from VMware technical support or a knowledge base article.

To change a host's advanced settings using the VMware Host Client, you can navigate to **Manage > System > Advanced Settings**. To change a host's advanced settings using the vSphere Client, you can select the host

and navigate to **Configure > System > Advanced System Settings**.

### **ESXi Kernel options**

Disk partitioning in ESXi 7.0 boot devices has changed. These changes include the following:

- Larger system boot partition
- Larger boot banks
- Coredump, tools, and scratch has been consolidated to a single VMFS-L based ESX-OSData volume
- Coredumps default to a file in the ESX-OSData volume

Boot options have to be issued at time of boot, either by defining the `kernelopt` in the ESXi `boot.cfg` file, or by manually entering them after entering **Shift-O** in the ESXi boot loader.

Table 8-11 lists these boot options:

---

**Table 8-11** ESXi 7.0 Kernel Options.

Template	Description
autoPartition=TRUE/FALSE (default FALSE)	<p>This setting, if set to TRUE, defines automatic partitioning of the unused local storage devices at boot time. The boot disk will get partitioned with boot bands, ESXi-OSData, and, if the disk is larger than 128 GB, a VMFS partition. Any new empty device discovered will be autoPartitioned as well. Auto-partitioning can be defined to only the first unused device with the setting autoPartitionOnlyOnceAndSkipSsd=TRUE. On hosts with USB boot and VMFS-L ESX-OSData does not exist on other local disks.</p> <p>If there is a scratch partition and a coredump partition on the same storage device, the partition will be converted to ESX-OSData, otherwise the 1<sup>st</sup> unused disk identified will be partitioned with ESX-OSData as well.</p>
skipPartitioningSsds=TRUE/FALSE (default FALSE)	If set to TRUE, local SSDs are excluded from automatic partitioning.
autoPartitionOnlyOnceAndSkipSsd=TRUE/FALSE (default FALSE)	If set to TRUE, SSD/NVMe devices are excluded, and the ESXi host will automatically partition the first unused local disk if there is no VMFS-L ESX-OSData volume.
allowCoreDumpOnUSB=TRUE/FALSE (default FALSE)	If set to TRUE, this enables the ESXi to write kernel crash core dumps to the VMFS-L Locker volume on a USB boot device.
dumpSize (default:0 (automatically sized))	This option sets the size of the core dump file in MB created on the system VMFS-L volume. This is limited to ½ of the available space on the VMFS-L volume.
autoCreateDumpFile=TRUE/FALSE (default TRUE)	<p>This option, when set to TRUE, will automatically create a coredump file. This is attempted to be created in the following order:</p> <ul style="list-style-type: none"> <li>VMFS-L ESX-OSData</li> <li>USB VMFS-L</li> <li>Local VMFS</li> </ul>

#### Note

The following kernel boot options have been deprecated and are no longer supported in ESXi 7.0:

- --no-auto-partition
- autoPartitionCreateUSBCoreDumpPartition
- autoPartitionDiskDumpPartitionSize

## SUMMARY

You completed reading this chapter on vSphere installation and configuration. You can use the remaining sections in the chapter to prepare for associated exam questions.

## REVIEW ALL THE KEY TOPICS

Table 8-12 provides a reference to each of the key topics identified in this chapter. Take a few moments to review each of these specific items.

**Table 8-12** Key Topics

Key Topic Element	Description	Pages
Procedure	Install ESXi Interactively	
List	First Time boot sequence using Auto Deploy	
Procedure	Deploy VCSA using GUI installer	
Procedure	Use VMCA in a subordinate CA manner	
Procedure	Add an Active Directory over LDAP identity source	
Procedure	Enable Identity Federation	
Procedure	Implement vCenter HA	

## COMPLETE THE TABLES AND LISTS FROM MEMORY

Print a copy of Appendix B, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

## DEFINITIONS OF KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary.

VMware Lifecycle Manager

vSphere Client

VMware Enhanced Authentication Plug-in

VMware Certificate Authority (VMCA)

VECS

Stateless caching

## Glossary

**VMware Lifecycle Manager:** VMware Lifecycle Manager replaces VMware Update Manager from prior versions. Lifecycle Manager adds onto the functionality of Update Manager to include features and capabilities for ESXi lifecycle management at the cluster level.

**vSphere Client:** vSphere Client is the HTML5 based GUI used for vSphere administration.

**VMware Enhanced Authentication Plug-in:**

VMware Enhanced Authentication Plug-in provides Integrated Windows Authentication and Windows-based smart card functionality. In the vSphere 6.5 release, the VMware Enhanced Authentication Plug-in replaced the Client Integration Plug-in.

**VMware Certificate Authority (VMCA):** The VMCA is responsible for issuing certificates for VMware solution users, certificates for machines running required services, and certificates for ESXi hosts.

**VECS:** The VMware End Point Certificate Service (VECS) is a local repository for certificates and private keys. VECS is a mandatory component that will be used when VMCA is not signing certificates.

**Stateless caching:** With stateless caching, Auto Deploy does not store ESXi configuration or state data within the host. Instead, during subsequent boots, the host must connect to the Auto Deploy server to retrieve its configuration.

## ANSWER REVIEW QUESTIONS

The answers to the Review Questions can be found in Appendix A.

- 1.** You are using the GUI Installer for vCenter Server 7.0. Which of the following statements is true?

  - a.** In the first stage, choose the deployment type.  
In the second state, you navigate through the installation wizard.
  - b.** In the first stage, provide the appliance settings. In the second state, you navigate through the installation wizard.
  - c.** In the first stage, choose the deployment type.  
In the second state, you deploy the OVA.
  - d.** In the first stage, provide the appliance settings. In the second state, you configure SSO
- 2.** You are adding an Active Directory over LDAP identity source. Which setting must you provide?

  - a.** UPN
  - b.** SPN
  - c.** Use Machine Account
  - d.** Base DN for users
- 3.** You are implementing a new vSphere environment and want to install services for updating the ESXi hosts. What should you do?

  - a.** Deploy a VMware Update Manager appliance
  - b.** Deploy a vSphere Life Cycle Manager appliance
  - c.** Deploy vCenter Server with an embedded Update Manager
  - d.** Nothing. The software service is included in vCenter Server

- 4.** You are implementing Auto Deploy and want to control its behavior with rules. Which of the following is not a means by which a rule can identify target hosts?
- a.** MAC address
  - b.** Model
  - c.** Serial Number
  - d.** BIOS UUID
- 5.** You are using host profiles to deploy a standard configuration to ESXi hosts. Which of the following provides the proper order of operation?
- a.** Click **attach host profile**, click **pre-check remediation**, click **remediate**.
  - b.** Click **attach host profile**, click **remediate**, click **pre-check remediation**, click **Finish**
  - c.** Click **attach host profile**, click **pre-check remediation**, click **remediate**.
  - d.** Click **pre-check remediation**, click **remediate**, click **attach host profile**, click **Finish**

# **Chapter 9. Configure and Manage Virtual Networks**

**[This content is currently in development.]**

**This content is currently in development.**

# **Chapter 10. Managing and Monitoring Clusters and Resources**

This chapter covers the following topics:

- Create and Configure a vSphere cluster
- Create and Configure a vSphere DRS cluster
- Create and Configure a vSphere HA cluster
- Monitor and Manage vSphere Resources
- Events, Alarms, and Automated Actions
- Logging in vSphere

This chapter contains information related to VMware  
2V0-21.20 exam objectives **1.6, 1.6.2, 1.6.3, 1.6.4,**  
**1.6.4.1, 4.9, 5.1, 5.1.1, 5.2, 5.3, 7.5, 7.12**

This chapter introduces vSphere 6.7, describes its major components, and identifies its requirements.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section. Regardless, the authors recommend that you read the entire chapter at least once. Table 10-1 outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the

answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 10-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Create and Configure a vSphere cluster	1
Create and Configure a vSphere DRS cluster	2, 3
Create and Configure a vSphere HA cluster	4, 5
Monitor and Manage vSphere Resources	6, 7, 8
Events, Alarms, and Automated Actions	9
Logging in vSphere	10

**Caution**

The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

**1.** You want to add hosts to a cluster for which you previously chose the option **Configure network settings later**. Which of the following is a true statement?

- a.** You cannot use Quickstart to add more hosts to the cluster.
- b.** You can use Quickstart to add hosts to the cluster and configure the host networking.
- c.** You can use Quickstart to add hosts to the cluster but must manually configure the host networking
- d.** You can edit the cluster and change the **Configure networking settings later** option.

**1.** You are creating a resource pool in a DRS cluster. Which of the following statements is not true?

- a. When you create a child resource pool, the system applies admission control.

- b. If you choose Scale Descendant's Shares, then child pools will use scalable share
  - c. The default CPU Reservation is 0.
  - d. The default Memory Limit is 0.
2. You are configuring a vSphere HA cluster. Which of the following is not a valid setting for **Define host failover capacity?**
- a. Standby
  - b. Cluster Resource Percentage
  - c. Slot Policy
  - d. Dedicated Host Failures
3. You want to configure VMCP in a vSphere Cluster. Which of the following settings are valid?
- a. In the vSphere HA settings, set **Failures and Responses > Datastore with PDL** to **Power off and restart VMs - conservative restart policy**
  - b. In the vSphere HA settings, set **Failures and Responses > Datastore with PDL** to **Power off and restart VMs**
  - c. In the vSphere DRS settings, set **Failures and Responses > Datastore with APD** to **Power off and restart VMs - conservative restart policy**
  - d. In the vSphere DRS settings, set **Failures and Responses > Datastore with APD** to **Power off and restart VMs - conservative restart policy**
4. You are configuring a vSphere HA cluster and want to configure Proactive HA. Which of the following is not a requirement?

- a. Host.Config.Quarantine and Host.Config.Maintenance privileges
  - b. A vendor supplied vSphere Client plugin
  - c. A VMware supplied plugin
  - d. vSphere DRS is enabled.
5. You are experiencing poor performance for an application in a virtual machine. You learn from guest OS software and the vSphere Client Performance Charts that the guest OS is paging. Which of the following is likely to fix the problem?
- a. Increase memory in the ESXi host.
  - b. Increase the memory size of the virtual machine.
  - c. Migrate the virtual machine to a host with plenty of free memory.
  - d. Reserve all the virtual machine's memory.
6. You are configuring virtual disks for the virtual machines in your vSphere environment. Which provisioning type is the best choice when you care more about optimizing the disk usage and less about performance or availability risk?
- a. Thin provisioned
  - b. Thick Eager zeroed
  - c. Thick Lazy zeroed
  - d. Sparse provisioned.
7. You are using ESXTOP to analyze your vSphere performance. Which of the following statistics is the best indicator of some resource contention?
- a. %USED
  - b. %DRPTX

- c. OVHD
  - d. READ/s
8. You are configuring alarms in your vSphere environment. Which of the followings is not a valid event type?
- a. Error
  - b. Warning
  - c. Information
  - d. Audit
9. You are examining vSphere logs. Which of the following logs contain data about the agent that manages and configures the ESXi host?
- a. /var/log/vmkernel.log
  - b. /var/log/vpxa.log
  - c. /var/log/hostd.log
  - d. /var/log/vmksummary.log

## **CREATE AND CONFIGURE A VSPHERE CLUSTER**

Using the vSphere Client, you can create a vSphere cluster and use its Quickstart feature to configure the cluster. You can configure DRS, vSphere HA, and EVC on the cluster, as described in this chapter. You can also configure vSAN on the cluster, as described in Chapter 11.

### **Create a Cluster**

To create a vSphere cluster that you plan to configure using Quickstart, you should ensure that the hosts have the same ESXi version and patch level. If you are adding hosts to the vCenter Server inventory, you need the credentials for root user account for the hosts. You must have the **Host.Inventory.Create cluster** privilege. To create a cluster that you manage with a single image, verify that you have a supported ESXi 7.0 or later image available in the vSphere Lifecycle Manager depot. You can use the following procedure to create the cluster.

**Step 1.** In the vSphere Client, right-click a data center in the inventory pane

**Step 2.** Select **New Cluster**.

**Step 3.** Enter a name for the cluster.

**Step 4.** Optionally, for each of the following services, slide the switch to the right to enable the service (default is disabled).

- **DRS** (Default settings: **Fully Automated** using **Threshold Level 3**)
- **vSphere HA**
- **vSAN**

**Step 5.** Optionally, to create a cluster that you manage with a single image, select **Manage all hosts in the cluster with a single image**.

- Select an ESXi Version (Image) from the drop-down menu.
- Optionally, select an option from the **Vendor Addon** and **Vendor Addon version** drop-down menus.

**Step 6.** Click **OK**.

## Configure the Cluster with Quickstart

To modify an existing cluster, you can select the cluster in the inventory pane and click **Configure > Configuration > Quickstart**. On the Quickstart page you will see three cards, **Cluster Basics**, **Add Hosts**, and **Configure Cluster**. To change the name and the enabled cluster services, click **Cluster Basics > Edit**.

To add a host to a cluster, you can use the following procedure.



1. In the vSphere Client, select a cluster in the inventory pane.
2. Navigate to **Configure > Configuration > Quickstart > Add Hosts > Add**.
3. Click **New Hosts > Add** to and provide the name (or IP address) and credentials for each host that you want to add that is not already in the vCenter Server inventory.
4. Optionally, select the **Use the same credentials for all hosts** option
5. Click **Existing Hosts > Add** to and select each host that you want to add that is already in the vCenter Server inventory
6. Click **Next**.
7. On the Host summary page, click **Next**.
8. On the **Ready to complete** page, click **Finish**.
9. Monitor the progress in **Recent Tasks**, which will display any errors.
10. When complete, you can view the number of hosts and the health on the **Add Hosts card**.  
Optionally, select **Re-validate**.

11. You can use the inventory pane to verify the hosts are attached to the cluster and are in maintenance mode.

To configure cluster settings and host networking in a cluster, you can use the following procedure.

1. In the vSphere Client, select a cluster in the inventory pane.
2. Navigate to **Configure > Configuration > Quickstart**.
3. Optionally, if you want to configure the cluster manually, click **Skip quickstart**, which is irreversible. Otherwise continue with the following steps to use Quickstart to configure the cluster.
4. Click **Configure Cluster > Configure**.
5. On the **Distributed switches** page, you can either select the irreversible option **Configure networking settings later** or use the following steps to configure the cluster networking.
  - a. Specify the number of distributed switches to create (up to three).
  - b. Enter a unique name for each distributed switch. Alternatively, click **Use Existing** and select an existing compatible distributed switch and distributed port group.
  - c. To set up the vMotion network, select a distributed switch and assign a new port group to it.
  - d. In the **Physical adapters** section, for each physical network adapter, assign a distributed switch name from the drop-down menu. Ensure that each new distributed switch is assigned to at least one physical adapter. For any existing distributed switch, to avoid an

error, select the physical adapter that is currently mapped to the switch.

e. Click **Next**.

f. If you enabled the vSphere DRS feature during cluster creation, the **vMotion traffic** page appears. Provide the VLAN ID, protocol type, and IP configuration.

6. Click **Next**.

7. In the **Advanced options** page, configure the following options.

- a. If you enabled vSphere HA during cluster creation, use the options in the **High Availability** section to enable or disable host failure monitoring, virtual machine monitoring, and admission control. For admission control, you can specify the number of hosts for failover capacity.
- b. If you enabled vSphere DRS during cluster creation, use the options in the **Distributed Resource Scheduler** to set the automation level and migration threshold.
- c. In the **Host Options** section, set the **Lockdown mode** and enter an NTP server address.
- d. Optionally, in the **Enhanced vMotion Capability** section, use the options to enable EVC and select a mode.

8. Click **Next**.

9. The **Ready to complete** page appears.

10. Review the settings and select **Finish**.

You can extend a cluster by adding more hosts. If you initially selected the **Skip Quickstart** option, then you should add hosts manually. If you previously used

Quickstart, but selected **Configure networking settings later**, then you can add hosts using Quickstart, but must manually configure the host networking. To extend a cluster, you can use the following procedure.

1. In the vSphere Client select a configured cluster in the inventory pane
2. Right-click the cluster and select **Add Hosts**.
3. In the wizard, select hosts from the vCenter Server inventory and add new hosts (provide name and credentials) to include in the cluster.
4. On the **Ready to complete** page, click **Finish**.
5. The **Extend Cluster Guide** page appears.
6. In the **Configure hosts** card, select **Configure**.
  - a. If you previously used Quickstart to configure the host networking, then the **vMotion traffic** page appears. Provide the VLAN ID, protocol type, and IP configuration.
  - b. A pop-up window appears. It informs you that the configuration for the hosts that exist in the cluster is applied to the newly added hosts.
7. Select **Continue**.

After successful validation, the **Configure** button in the **Configure Hosts** card becomes inactive. The **Re-validate** button is available.

If you enable DRS, its default settings are **Automation Level** is Fully Automated using **Threshold** is 3). If you enable HA, the default values are (**Host Monitoring** and **Admission Control** are Enabled, **VM Monitoring** is Disabled). You can override the default values later in the workflow.

If you select an image to use to manage all the hosts in the cluster, you can later edit the image specification

later from the **Updates** tab. If you do not choose an image to manage hosts, you must manage the cluster by using baselines and baseline groups. You can switch from using baselines to using images later.

Starting with vSphere 7.0, you can use vSphere Lifecycle Manager to upgrade and update the hosts in your cluster. A vSphere Lifecycle Manager image is a combination of vSphere software, driver software, and desired firmware for specific host hardware. You can assign an image to a cluster uses to control the software set to be installed on the hosts including the ESXi version, additional VMware-provided software, and vendor software, such as firmware and drivers.

The image that you define during cluster creation is not immediately applied to the hosts. If you do not set up an image for the cluster, the cluster uses baselines and baseline groups. For more information about using images and baselines to manage hosts in clusters, see the Managing Host and Cluster Lifecycle documentation.

## EVC Mode

As previously described, you can configure EVC using **Quickstart > Configure Cluster**. You can also configure EVC directly in the cluster settings. You can set **VMware EVC to Disable EVC, Enable EVC for AMD Hosts, or Enable EVC for Intel Hosts**.

If you choose **Enable EVC for AMD Hosts**, then you can set the mode to one of the options in [Chapter 4 Table 4-3](#).

If you choose **Enable EVC for Intel Hosts**, then you can set the mode to one of the options in [Chapter 4 Table 4-2](#).

To view the EVC mode for all the cluster's virtual machines in the vSphere Client, you can select a cluster,

navigate to its **VMs** tab, select **Show / Hide Columns** > **EVC Mode**.

## CREATE AND CONFIGURE A VSPHERE DRS CLUSTER

This section describes how to create and configure a vSphere DRS cluster.

### Create a vSphere DRS Cluster

To create a vSphere DRS cluster, follow the procedure in the *Create a Cluster* section in this chapter and ensure that you choose to enable the DRS service. Use the remaining information in this section to configure the DRS cluster.

### Create a Resource Pool

You can use the following procedure to create a child resource pool in a DRS cluster.

1. In the vSphere Client, navigate to Hosts and Clusters, and right-click a DRS cluster in the inventory.
2. Select **New Resource Pool**.
3. Provide a name for the resource pool.
4. Optionally, select the **Scale Descendant's Shares** checkbox to enable scalable shares.  
(Enabling this option causes any child resource pools to use scalable shares, which scale dynamically when adding and removing virtual machines.)
5. Optionally, set **CPU** and **Memory Shares** to **low**, **normal**, **high**, or **custom** (default is normal). If you select custom, enter a numeric value

6. Optionally, set **CPU** and **Memory Reservation** to a numeric value (default is 0) and a unit of measure (MB, GB, MHz, or GHz).
7. Optionally, set **CPU** and **Memory Limit** to a numeric value (default is Unlimited) and a unit of measure (MB, GB, MHz, or GHz).
8. Optionally, set the **CPU** and **Memory Reservation Type** to **Expandable**
9. Click **OK**.

**Note**

When you create a child resource pool, the vSphere Client prompts you for resource pool attribute information. The system uses admission control to ensure that you do not allocate resources that are not available. If you choose **Scale Descendant's Shares**, then each descendant pool will also use scalable shares. You cannot change this behavior per child pool.

## Configure Advanced DRS Options

### Create Affinity / Anti-Affinity Rules

Table 10-2 provides some common use cases for VM-VM affinity and anti-affinity rules.



**Table 10-2** Use Cases for VM-VM Rules

Use Case	Rule Details
To improve application and communication performance for a multi-node application.	Use VM-VM affinity rules to ensure that sets of virtual machines that engage in significant data exchange reside on the same host, such that the data transfer occurs within the host system hardware and does not traverse the physical network infrastructure.
To improve application availability for a multi-node application.	Use VM-VM anti-affinity rules to ensure that sets of peer virtual machines reside on separate hosts, such that the failure of a single host does not result in the failure of all the peer application nodes.

You can use the following procedure to create a VM to VM affinity or anti-affinity rule.

### Create a VM-VM Affinity Rule

## **Procedure**

1. Browse to the cluster in the vSphere Client.
2. Click the **Configure** tab.
3. Under **Configuration**, click **VM/Host Rules**.
4. Click **Add**.
5. In the **Create VM/Host Rule** dialog box, type a name for the rule.
6. From the **Type** drop-down menu, select either **Keep Virtual Machines Together** (affinity) or **Separate Virtual Machines** (anti-affinity).
7. Click **Add**.
8. Select at least two virtual machines to which the rule will apply and click **OK**.
9. Click **OK**.

## **Configure Predictive DRS**

To configure Predictive DRS, you can use the following procedure.

1. In the vRealize Operations (vROps) GUI, locate the appropriate vCenter Server adapter instance.
2. Select the adapter, choose **Advanced Settings**
3. Set **Provide data to vSphere Predictive DRS** to **True**.
4. In the vSphere Client, select the cluster in the inventory pane.
5. Navigate to **Cluster > Services > vSphere DRS > Edit**
6. Check the **Predictive DRS** checkbox

# **CREATE AND CONFIGURE A VSPHERE HA CLUSTER**

This section describes how to create and configure a vSphere HA cluster.

## Create a vSphere HA Cluster

To create a vSphere HA cluster, follow the procedure in the *Create a Cluster* section in this chapter and ensure that you choose to enable the vSphere HA service. Use the remaining information in this section to configure the vSphere HA cluster.

## Configure Advanced vSphere HA Options

You can use the following procedures to add vSphere HA Advanced Options, as described in Table 4-9.

1. In the vSphere Client, select a vSphere HA cluster in the inventory pane.
2. Navigate to **Configure > vSphere Availability > Edit > Advanced Options.**
3. Click **Add**
4. Enter the name of the advanced option and the value.
5. Click **OK.**

Configure vSphere HA Admission Control



To configure Admission Control for a vSphere HA cluster, you can use the following procedure.

1. In the vSphere Client, select the vSphere HA cluster in the inventory pane.
2. Navigate to **Configure >vSphere Availability > Edit.**

3. Click **Admission Control** and set **Host failures cluster tolerates** to the maximum number of host failures you want the cluster to support.
4. Select one of the following options for **Define host failover capacity** by, as described in Table 4-8.
  - **Cluster Resource Percentage**
  - **Slot Policy (powered-on VMs)**
  - **Dedicated Host Failures**
  - **Disabled** (disables Admission Control)
5. Optionally, set the **Performance Degradation VMs Tolerate** to a percentage.
6. Click **OK**.

## Configure VMCP

To configure Virtual Machine Component Protection (VMCP) in a vSphere HA cluster, you can use the following procedure.

1. In the vSphere Client, select the cluster in the inventory pane.
2. Navigate to **Configure > vSphere Availability > Edit**
3. Set **Failures and Responses > Datastore with PDL** to one of the following
  - **Issue Events**
  - **Power off and restart VMs**
4. Set **Failures and Responses > Datastore with APD** to one of the following
  - **Issue Events**
  - **Power off and restart VMs - conservative restart policy**
  - **Power off and restart VMs - aggressive restart policy**

## Configure Virtual Machine and Application Monitoring

You can use the following procedure to turn on and configure virtual machine and application monitoring in a vSphere HA cluster.

1. In the vSphere Client, select the vSphere HA cluster in the inventory pane.
2. Navigate to **Configure > vSphere Availability > Edit**.
3. Select **Failures and Responses > VM Monitoring**.
4. Select **VM Monitoring** to turn on VMware Tools heartbeats.
5. Select **Application Monitoring** to turn on application heartbeats.
6. To set the heartbeat monitoring sensitivity, move the slider between **Low** and **High**, or select **Custom** and provide a custom value.
7. Click **OK**.

## Configure Proactive HA



To get started, you need to install a supported, vendor supplied vSphere Client plugin and register the Proactive HA Provider. When you turn on Proactive HA in a cluster, you can select from the list of providers for installed plugins that are monitoring every host in the cluster. You can use the following procedure to configure Proactive HA in a cluster.

1. Ensure the following prerequisites are met.
  - vSphere HA and DRS are enabled.

- To allow remediation actions, you need the Host.Config.Quarantine and Host.Config.Maintenance privileges.
2. In the vSphere Client, select the cluster in the inventory pane.
  3. Navigate to **Configure > vSphere Availability > Edit**.
  4. Select **Turn on Proactive HA**.
  5. Click **Proactive HA Failures and Responses**
  6. Set **Automation Level** to Manual or Automated
  7. Set Remediation to one of the following.
    - **Quarantine mode for all failures.**
    - **Quarantine mode for moderate and Maintenance mode for severe failure (Mixed).**
    - **Maintenance mode for all failures.**

## Configure vSphere Fault Tolerance

Before enabling vSphere Fault Tolerance (FT) for a virtual machine, you must prepare the hosts and cluster, by doing the following. Configure vSphere HA on the cluster. On each participating host, configure a vMotion port group, a VMkernel adapter enabled for vMotion, a Fault Tolerance Logging network, and a VMkernel adapter enabled for FT Logging.

To turn on FT for a virtual machine, you can use the following procedure.

- In the vSphere Client, right-click the virtual machine in the inventory pane.
- Select **Fault Tolerance > Turn On Fault Tolerance**.
- Click **Yes**.

- Select a datastore on which to place the Secondary VM configuration files and click **Next**.
- Select a host on which to place the Secondary VM and click **Next**.
- Review your selections and then click **Finish**

Before FT is turned on for a virtual machine, FT performs several validation steps related to the FT requirements listed in [Chapter 4, "Clusters and High Availability."](#) The virtual machine datastores and memory are replicated as FT is turned on. This may take several minutes, during which the virtual machine status does not appear as protected. When the replication completes and the state of the Secondary VM is synchronized with the Primary VM, the status changes to **Protected**.

To test FT failover for a virtual machine, right-click the virtual machine and select **Fault Tolerance > Test Failover**. Likewise, you can select **Fault Tolerance > Test Restart Secondary** to restart the Secondary VM.

## **MONITOR AND MANAGE VSPHERE RESOURCES**

You can use the vSphere Client Performance Graphs to view compute, storage, and network resource usage of virtual machines, hosts, and clusters. For a more granular look from the host perspective, you can use the ESXTOP utility. You can use vCenter Server alarms to bring attention to conditions and events that may call for human intervention, such as low resource availability on a cluster, host, or datastore. To bring multi-vCenter Server monitoring, predictive analysis, and intelligent operations to your environment, you can consider integrating vRealize Operations (vROps).

### **Metrics**

Performance metrics are organized into logical groups based on the object or object device, as shown in Table 10-3.

**Table 10-3** Metrics

Metric Group	Description
Cluster Services	Performance metrics per vSphere host clusters.
CPU	CPU utilization metrics per host, virtual machine, resource pool, or compute resource.
Datastore	Datastore utilization metrics
Disk	Disk utilization metrics per host, virtual machine, or datastore.
Memory	Memory utilization metrics per host, virtual machine, resource pool, or compute resource.
Network	Network utilization metrics per physical NIC, virtual NIC, and other network devices.
Power	Energy utilization metrics per host.
Storage Adapter	Data traffic metrics per host bus adapter (HBA).
Storage Path	Data traffic metrics per path.
System	Overall system availability metrics, such as the system heartbeat and uptime. These counters are available directly from hosts and from vCenter Server.
Virtual Disk	Disk utilization and disk performance metrics for virtual machines.
Virtual Flash	Virtual flash metrics.
Virtual Machine Operations	Virtual machine power and provisioning operations metrics in a cluster or data center.
vSphere Replication	Virtual machine replication metrics.

Disk metrics include I/O performance, such as latency and read/write speeds, and utilization metrics for storage as a finite resource.

The value obtained for memory utilization is one of the following:

- For virtual machines, memory refers to the guest physical memory, which is the virtual memory the hypervisor presents to the guest as physical memory.
- For hosts, memory refers to the machine memory, which is the physical memory in the host system.

## vSphere Client Performance Charts

The vSphere Client Performance Charts enable you to view performance metrics in different types of charts,

depending on the selected object and metric type, as described in [Table 10-4](#).

**Table 10-4** Performance Chart Types

Chart Type	Description
Line chart	Displays metrics for a single inventory object, where data for each metric is represented by a separate line. For example, a network chart for a host can contain one line showing the number of packets received, and another line showing the number of packets transmitted.
Bar chart	Displays metrics for objects, where each bar represents metrics for an object. For example, a bar chart can display metrics for datastores, where each datastore is represented as a bar. Each bar displays metrics based on the file type, such as virtual disk or snapshot.
Pie chart	Displays metrics for a single object, where each slice represents a category or child object. For example, a datastore pie chart can display the amount of storage space occupied by each virtual machine or by each file type.
Stacked Chart	Displays metrics for child objects. For example, a host's stacked CPU usage chart displays metrics for the ten virtual machines on the host that are consuming the most CPU. The <b>Other</b> amount displays the total CPU usage of the remaining virtual machines.

Overview and advanced performance charts are available for datacenter, cluster, host, resource pool, vApp, and virtual machine objects. Overview performance charts are also available for datastores and datastore clusters. Performance charts are not available for network objects. Charts are organized into views, which you can use to see related data together on one screen. You can specify the time range or data collection interval. Advanced charts contain more information than overview charts. You can print, configure, and export (PNG, JPEG, or CSV formats) advanced charts.

## Overview Performance Charts

You can use the vSphere Client to examine the overview performance charts for data centers, clusters, datastores (and datastore clusters), hosts, resource pools, vApps, and virtual machines.

To view a performance chart, you can use the following procedure

1. In the vSphere Client, select an appropriate object in the inventory pane.

2. Navigate to **Monitor > Performance**.
3. Select a view.
4. Select a predefined or custom time range.

**Table 10-5** contains the available performance chart views by object type.

**Table 10-5** Views by Object Type

Object Type	View List Items
Data center	<b>Clusters:</b> Thumbnail CPU and memory charts for each cluster, and stacked charts for total datacenter CPU and memory. <b>Storage:</b> Space utilization charts for each datastore by file type.
Datastore and datastore cluster	<b>Space:</b> Space utilization charts by datastore, by file type and by virtual machine. <b>Performance:</b> Disk performance (latency, throughput, and queuing) charts for the datastore (or datastore cluster, when Storage DRS is enabled) by virtual machine, by virtual disk, and by file type.
Cluster	<b>Home:</b> CPU and memory charts for the cluster. <b>Resource Pools &amp; Virtual Machines:</b> Thumbnail charts for resource pools and virtual machines, and stacked charts for total cluster CPU and memory usage. <b>Hosts:</b> Thumbnail charts for each host, and stacked charts for total cluster CPU, memory, disk usage, and network usage.
Host	<b>Home:</b> CPU, memory, disk, and network charts for the host. <b>Virtual Machines:</b> Thumbnail charts for virtual machines, and stacked charts for total CPU usage and total host memory usage.
Resource Pool	<b>Home:</b> CPU and memory charts for the resource pool. <b>Resource Pools &amp; Virtual Machines:</b> Thumbnail charts for resource pools, and virtual machines and stacked charts for total resource CPU and memory usage.
vApps	<b>Home:</b> CPU and memory charts for the resource pool. <b>Resource Pools &amp; Virtual Machines:</b> Thumbnail charts for resource pools, and virtual machines and stacked charts for total vApp CPU and memory usage.
Virtual Machine	<b>Storage:</b> Space utilization charts for the virtual machine by file type and by datastore. <b>Fault Tolerance:</b> CPU and memory charts that display metrics for the fault-tolerant primary and secondary virtual machines. <b>Home:</b> CPU, memory, network, and host thumbnail charts, and disk performance charts for the virtual machine.

**Note**

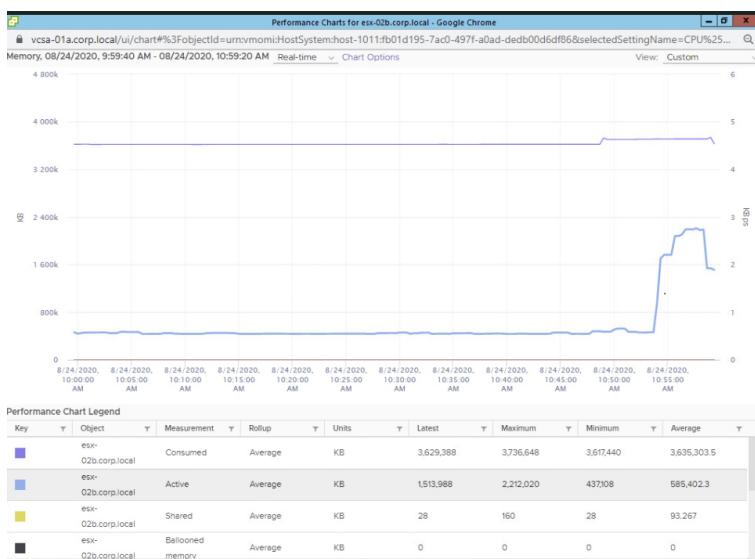
When Storage I/O Control is disabled, the values for the Storage I/O Normalized Latency metrics are zeros.

## Advanced Performance Charts

For more granularity, you can use advanced performance charts, or create your own custom charts. Advanced performance charts are especially useful when overview performance charts do not provide sufficient data for troubleshooting a specific issue. Advanced performance charts include the following features.

- Customizable: You can change and save chart settings
- More information. You can include data counters that are not supported in other performance charts. You can hover a data point to see details at that point.
- Exportable: You can save the image to a file or spreadsheet. You can export the data to a spreadsheet.

**Figure 10-1** is example advanced performance chart that includes memory metrics for a virtual machine.



**Figure 10-1** Sample Advanced Performance Chart

You can use the following procedure to access an advanced performance chart.

1. In the vSphere Client, select an appropriate object in the inventory pane.
2. Navigate to **Monitor > Performance**.
3. Click **Advanced**.
4. Optionally, select an appropriate view from **View** dropdown list.

5. Optionally, click the Popup Chart icon to open the chart in a separate window.
6. Click **Chart Options**.
7. In **Chart Metrics**, select an appropriate metric group.
8. Select a **Timespan**. If you choose **Custom Interval**, then select one of the following.
  - **Last**: Specify the number of hours, days, weeks, or months.
  - **From**: Specify beginning and ending times.
9. In **Target Objects**, select the appropriate inventory objects. (Optionally, use the **All** or **None** buttons)
10. Select an appropriate **Chart Type**.
11. In **Counters**, select the data counters to display in the chart. (Optionally, use the **All** or **None** buttons)
12. Optionally, click **Save Options As** and save your settings as a custom chart.

**Note**

Pop-up charts are useful for maximizing the available real estate for a chart and for comparing two separate charts side by side,

**Note**

For the stacked graph type, the following applies.

- You can use only one measurement unit.
- Per-virtual-machine stacked graphs are available only for hosts.
- You can click on a counter's description name to display details, such as whether the selected metric can be stacked per virtual machine.

After creating a custom chart, the chart is added to the View dropdown list. You can now use the chart in the same manner that you would any pre-built view.

You can use the following procedure to delete a custom chart.

1. In the vSphere Client, select an appropriate object in the inventory pane.
2. Navigate to **Monitor > Performance**.
3. Select **Advanced > Chart Options**.
4. Select the chart and click **Delete Options**.

You can use the following procedure to save data from an advance performance chart to a file either in a graphic format or in comma-separated values (CSV) format.

1. In the vSphere Client, select an object in the inventory pane.
2. Navigate to **Monitor > Performance**.
3. Click **Advanced**.
4. Optionally, select a view, or change chart options, until you are satisfied with the chart.
5. Click the **Export** icon.
6. Select one of the following options.
  - **To PNG:** Exports a bitmap image to PNG format.
  - **To JPEG:** Exports a bitmap image to JPEG format.
  - **To CSV:** Exports text data to CSV format.
  - **To SVG:** Exports a vector image to SVG format.
7. Provide a file name and location.
8. Click **Save**.

## **Troubleshooting and Optimizing Performance**

Table 10-6 provides the likely cause and potential solution for some example symptoms based on vSphere

performance metrics.

**Table 10-6** CPU Performance Analysis

Symptoms	Likely Causes	Potential Solutions
Host: Consistently High CPU Usage	The host has insufficient CPU resources to meet the demand.	Add the host to a DRS cluster.  Increase the number of hosts in the DRS cluster.
Virtual Machine: CPU usage is above 90%. CPU ready is above 20%. Application performance is poor	Too many virtual CPUs running on the host.  Storage or network operations are placing the CPU in a wait state.  The Guest OS generates too much load for the CPU.	Migrate one or more virtual machines to other hosts.  Upgrade the physical CPUs of the host  Upgrade ESXi to the latest version.  Enable CPU-saving features such as TCP Segmentation Offload, large memory pages, and jumbo frames.  Increase the amount of memory allocated to the virtual machines, which may improve cached I/Os and reduce CPU utilization.  Reduce the number of virtual CPUs assigned to virtual machines.  Verify VMware Tools is installed.  Compare the CPU usage of troubled virtual machines with that of other virtual machines on the host or in the resource pool. (Hint: use a stacked graph)
Host: Memory usage is	The host has insufficient memory	Verify VMware Tools is installed and the

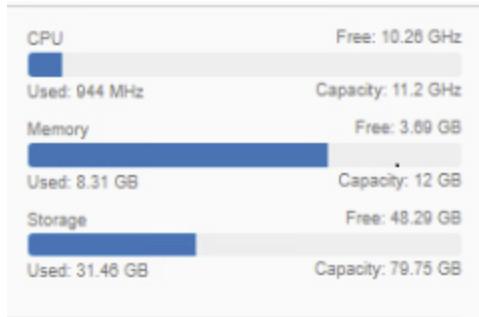
		<p>Balloon Driver is enabled for all virtual machines.</p> <p>Reduce the memory size of oversized virtual machines.</p> <p>Reduce the memory reservation of virtual machines, where it is set higher than needed.</p> <p>Add the host to a DRS cluster.</p> <p>Increase the number of hosts in the DRS cluster.</p> <p>Migrate one or more virtual machines to other hosts.</p> <p>Add physical memory to the host</p>
<p>Virtual Machine: Swapping is occurring. (Memory usage may be high or low.)</p> <p>Virtual Machine: Memory usage is high.</p> <p>Guest OS: Memory usage is high. Paging is occurring.</p>	<p>The guest OS is not provided sufficient memory by the virtual machine</p>	<p>Increase the memory size of the virtual machine.</p>
<p>Virtual Machine: CPU Ready is low.</p> <p>Guest OS: CPU Utilization is high.</p>	<p>The guest OS is not provided sufficient CPU resources by the virtual machine</p>	<p>Increase the virtual machine's number of CPUs.</p> <p>Migrate the virtual machine to a host with faster CPUs.</p>
Datastore: Space utilization is high.	<p>Snapshot files are consuming a lot of datastore space.</p> <p>Some virtual machines are provisioned with more storage space than required.</p> <p>The datastore has insufficient storage space to meet the demand.</p>	<p>Delete or consolidate virtual machine snapshots.</p> <p>Convert some virtual disks to thin provisioned.</p> <p>Migrate one or more virtual machines (or virtual disks) to other datastores.</p> <p>Add the datastore to a Storage DRS datastore</p>

		<p>cluster.</p> <p>Add datastores with available space to the datastore cluster.</p> <p>Add more storage space to the datastore.</p>
Disk: Device latency is greater than 15 ms.	Problems with the storage array.	<p>Migrate the virtual machines to datastores backed by other storage arrays.</p>
Disk: VMkernel latency is greater than 4 ms. Queue latency is greater than zero.	<p>The maximum throughput of storage device is not sufficient to meet the demand of the current workload.</p>	<p>Migrate the virtual machines to datastores backed by storage devices (LUNs) with more spindles.</p> <p>Balance virtual machines and their disk IO across the available physical resources. Utilize Storage DRS I/O balancing.</p> <p>Add more disks (spindles) to the storage device backing the datastore.</p> <p>Configure the queue depth and cache settings on the RAID controllers. Adjust the <b>Disk.SchedNumReqOutstanding</b> parameter.</p> <p>Configure multipathing.</p> <p>Increase the memory size of the virtual machine to eliminate any guest OS paging. Increase the guest OS caching of disk I/O.</p> <p>Ensure that no virtual machine swapping or ballooning is occurring.</p> <p>Defragment guest file systems.</p> <p>Use eager zeroed thick provisioned virtual disks.</p>
Network: Packets dropped is greater than zero. Latency is high. Transfer rate is low.	<p>The maximum throughput of physical network adapter is not sufficient to meet the demand of the current workload.</p> <p>Virtual machine network resource shares are too few.</p>	<p>Install VMware Tools on each virtual machine and configure the guest OS to use the best performing network adapter driver (such as vmxnet3).</p> <p>Migrate virtual machines to other hosts or to</p>

	<p>Network packet size is too large, which results in high network latency. Use the VMware AppSpeed performance monitoring application or a third-party application to check network latency.</p> <p>Network packet size is too small, which increases the demand for the CPU resources needed for processing each packet. Host CPU, or possibly virtual machine CPU, resources are not enough to handle the load.</p>	<p>other physical network adapters.</p> <p>Verify all NICs are running in full duplex mode.</p> <p>Implement TCP Segmentation Offload (TSO) and Jumbo Frames.</p> <p>Assign additional physical adapters as uplinks for the associated port groups.</p> <p>Replace physical network adapters with high bandwidth adapters.</p> <p>Place sets of virtual machines, who communicate regularly with each other on the same ESXi host.</p>
Empty performance charts	<ul style="list-style-type: none"> <li>• Some metrics are not available for pre-ESXi 5.0 hosts</li> <li>• Data is deleted when you remove or add objects to vCenter Server.</li> <li>• Performance charts data for inventory objects that were moved to a new site by VMware vCenter Site Recovery Manager is deleted from the old site and not copied to the new site.</li> <li>• Performance charts data is deleted when you use VMware vMotion across vCenter Server instances.</li> <li>• Real-time statistics are not available for disconnected hosts or powered off virtual machines.</li> <li>• Non-real-time statics are rolled up at specific intervals. For Example, 1-Day statistics might not be available for 30 minutes after the current time, depending on when the sample period began.</li> <li>• The 1-Day statistics are rolled up to create one data point every 30 minutes. If a delay occurs in the roll-up operation, the 1-Week statistics might not be available for 1 hour after the current time. It takes 30 minutes for the 1-Week collection interval, plus 30 minutes for the 1-Day collection interval.</li> <li>• The 1-Week statistics are rolled up to create one data point every two hours. If a delay occurs in the roll-up operations, the 1-Month statistics might not be available for 3 hours. It takes 2 hours for the 1-Month collection interval, plus 1 hour for the 1-Week collection interval.</li> <li>• The 1-Month statistics are rolled up to create one data point every day. If a delay occurs in the roll-up operations, the statistics might not be available for 1-day and 3 hours. It takes one day for the past year collection interval, plus 3 hours for the past month collection interval. During this time, the charts are empty.</li> </ul>	<p>Upgrade hosts to a later version of ESXi.</p> <p>Allow time for data collection on recently objects that were recently added, migrated, or recovered to the vCenter Server.</p> <p>Power on all hosts and allow time for real-time statistics to collect.</p> <p>Allow time for the required rollups for non-real-time statistics.</p>

## Monitor and Manage Cluster Resources

On a Summary tab for a vSphere DRS cluster you can see the Capacity, Used, and Free metrics for CPU, Memory, and Storage resources in the upper right corner as shown in Figure 10-2.

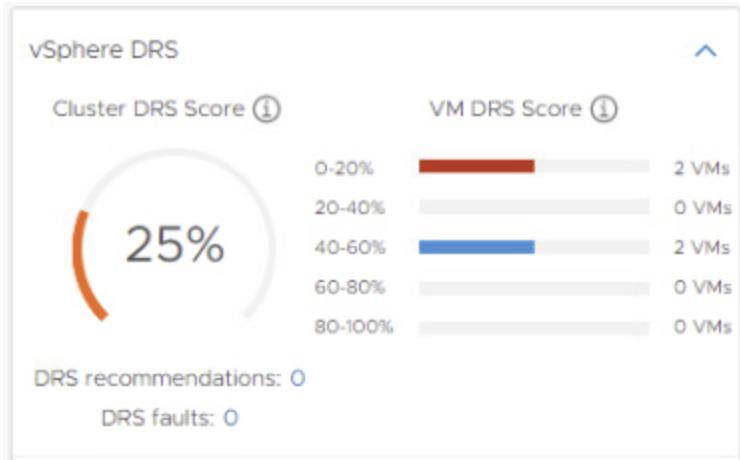


**Figure 10-2** DRS Cluster Resource Usage

To examine the CPU and memory usage more closely, you can navigate to **Monitor > vSphere DRS and select CPU Utilization or Memory Utilization.**

These pages show a bar graph, where each bar represents the total resource (CPU or memory) usage of a specific host and each bar is split into sections representing the resource usage of individual virtual machines. Likewise you can select **Monitor > vSphere DRS > Network Utilization** to examine the network utilization of each host in the cluster.

The **Summary** tab shows the vSphere **DRS Score**, the number of **DRS recommendations**, and the number of **DRS faults**, as shown in Figure 10-3.



**Figure 10-3** Sample DRS Score

If DRS is in manual mode, you can click on the number of DRS Recommendations on the summary tab, which is a link that takes you to the DRS Recommendations page. On the DRS Recommendations page, you can view the current recommendations, select those that you want to apply, and click the **Apply Recommendations** button. Each recommendation includes a description, such as which virtual machine to migrate to which host, and a reason, such as balance average memory loads.

Optionally, you can click the **Run DRS Now** button to make DRS perform its analysis and potentially generate new recommendations.

## Monitor and Manage Resource Pool Resources

To view resource pool configuration details, you can select a DRS cluster in the inventory pane and navigate to **Hosts > Resource Pools**. On that page you will see all the resource pools that are direct children of the cluster. For each pool, you will see its **CPU** and **memory** resource settings, including **Reservation**, **Limit**, **Shares Setting** (such as Low or Custom), **Shares Value** (numeric share value), and **Allocation Type** (Expandable or non-Expandable). You can click on the name of a resource pool, which is a link to the pool's

**Summary** page, which shows the current capacity, usage, and free compute resources for the resource pool. The summary page also shows the number of virtual machines, powered on virtual machines, child resource pools, and vApps in the pool.

For more detail, you can navigate to **Monitor > Utilization** or to **Monitor > Resource Allocation** and select **CPU**, **Memory**, or **Storage**. For both CPU and memory resources, the Utilization page shows the resource configuration, the consumed, the active, and the worst-case allocation. The Utilization page also shows a break down of **Guest Memory**, including metrics for **Active Guest Memory**, **Swapped**, **Compressed**, and **Ballooned**.

You can use Overview and Advanced Performance Charts with resource pools. When you see undesired behavior, you can edit the settings of an existing resource pool to change the pool's CPU and memory shares, reservations, and limits. For example, consider a scenario where you configure two resource pools in a cluster with 100 GHz CPU capacity. In one pool with 40 virtual machines, you set CPU Shares to High. In the other pool, with 8 virtual machines, you set CPU shares to Normal. You see in the performance charts that the virtual machines in the pool with the 40 virtual machines have greater CPU Ready values than the virtual machines in the other pool. You realize that although you used higher CPU shares for the first pool, the virtual machines are experiencing more CPU contention than virtual machines in the second pool. To correct this, you could take one of the following actions.

- Increase the CPU shares on the first pool using a custom value.
- Change the CPU shares on the second pool to Low.

- Set an appropriate CPU Reservation on the first pool.
- Set an appropriate CPU Limit on the second pool.
- Change the configuration to use Scalable Shares.

## Monitor and Manage Host Resources and Health

You can use the vSphere Client to monitor the state of host hardware components, such as CPUs, memory, fans, temperature, voltage, power, network, battery, storage, cable (interconnect), software components, watchdog, and PCI devices. To view the host hardware health status with the vSphere Client, you can use the following procedure.

1. In the vSphere Client, select host in the inventory pane.
2. Navigate to **Monitor > Hardware Health**.
3. Select the type of information to view.
  - Sensors
  - Storage Sensors
  - Alerts and Warnings
  - System Event Log

The host health monitoring tool presents data gathered using Systems Management Architecture for Server Hardware (SMASH) profiles. The information displayed depends on the sensors available on your server hardware.

**Note**

You can also set alarms to trigger when the host health status changes

If you participate in the Customer Experience Improvement Program (CEIP), then you can configure

Skyline Health to perform online health checks. If CEIP is not enabled, then the Internet connectivity check is unavailable. You can use the following procedure to configure Skyline Health.



1. In the vSphere client, select a vCenter Server or a host in the inventory pane.
2. Select **Monitor > Skyline Health**.
3. Expand **Online Health Connectivity** category and select one of the following options.
  - **CEIP:** Verifies CEIP is enabled for the vCenter Server
  - **Online health connectivity** (Internet check): Verifies vCenter Server to vmware.com connectivity via HTTPS / 443
  - **Advisor:** (Included in Production and Premier Support contracts) Provides additional features such as automatic support log bundle transfer with Log Assist.
  - **Audit CEIP Collected Data:** Allows you to view data collected and sent for CEIP.
  - **Number of Online health checks performed successfully**
4. Expand the following categories and examine the related health warnings
  - **Compute Health Checks**
  - **Network Health Checks**
  - **Security Health Check**
  - **Storage Health Checks**
  - **General Health Checks**
5. Click **Rest** to run the health checks immediately.

6. Optionally, if issues are discovered, click the **Ask VMware** button to request a knowledge base article that describes the how to resolve the issue.

## Monitor and Manage Virtual Machine Resources

Table 10-7 contains some of the key metrics for monitoring virtual machines

**Table 10-7** Virtual Machine Metrics

Metric	Unit	Description
CPU Usage	%	Indicates the CPU workload for the virtual machine.
CPU Ready Time	ms	Indicates the amount of time a VCPU is ready to work (has a workload and is ready to be scheduled) but is waiting to be scheduled on hardware. High CPU Ready Time is a sign of CPU contention.
Memory Consumed	KB	Indicates the amount of physical memory currently backing the virtual machine.
Memory Active	KB	Indicates the amount of consumed memory that is actively being read or written by the guest OS.
Memory Swap In Rate	KBps	Indicates the amount of memory read from the virtual machine's swap file over time.
Disk Usage	KBps	Indicates the disk throughput.
Virtual Disk Read Latency	ms	Indicates the average amount of time for a read operation to complete.
Network Usage	KBps	Indicates the amount of data transmitted and received over time.
Network Transmit packets dropped	number	Indicates the number of packets transmitted to the network that were dropped.

## Shares, Limits, Reservations

You can set the CPU and memory shares, reservation, and limit on a virtual machine using the following procedure.

1. In the vSphere Client, right-click your virtual machine in the inventory.
2. Right-click and select **Edit Settings**.
3. Edit the **CPU Resources**
4. Set the **Shares, Reservation, and Limit**
5. Edit the **Memory Resources**
6. Set the **Shares, Reservation, and Limit**
7. Click **OK**.

The relative priority represented by each share changes whenever additional, sibling virtual machine are powered on or powered off. Likewise, each share's relative priority changes whenever the shares on siblings are increased or decreased. This affects all virtual machines in the same resource pool.

For example, consider the following scenario.

- All virtual machines have the same number of vCPUs
- Two virtual machines, each run in a resource pool with CPU Limit set to 8GHz.
- The virtual machines are CPU bound (they are demanding more CPU resources than they are receiving).
- Their CPU shares are set to **Normal**
- You should expect each virtual machine's Performance Chart to show CPU Utilization is 4GHz each.
- When you power on a third CPU-bound sibling virtual machine with CPU shares value set to **High**, you should expect to see the new virtual machine uses 4GHz and the first two machines drop to 2GHz each.

To understand the impact of shares, consider another scenario, where a set of sibling virtual machines are frequently CPU bound and are utilizing all the resources in their parent resource pool. During these periods of CPU contention in the resource pool, you see significantly high CPU Ready Time on each of the virtual machines. You are only concerned about improving the performance of one specific virtual machine, so you increase its CPU Shares. The CPUs Ready Time for that machine should decrease during periods of CPU

contention, while the CPU Ready Time of its siblings should rise.

To guarantee a specific amount of resources to always be available to a running virtual machine, even when the physical server is heavily loaded, you can set its CPU or memory reservation. The vCenter Server or ESXi host allows you to power on a virtual machine only if there are enough unreserved resources to satisfy the virtual machine's reservation. Likewise, your attempts to increase the reservation on a running virtual machine (or a resource pool) will succeed only if there are enough unreserved resources to satisfy the request. In the previous scenario, if you want to ensure that a virtual machine always receives access to at least 1 GHz, regardless of the number or resource settings of siblings, you should set its CPU reservation to 1 GHz.

**Note**

The default CPU and memory reservation for a virtual machine is zero, meaning that its guest OS is not guaranteed to any specific amount of either resource. Instead, with default settings, shares would be applied during periods of compute resource contention.

You can set limits for CPU, memory, and storage I/O for a virtual machine to establish an upper bound (maximum) amount of resources that can be allocated to the virtual machine. The host never allocates more than the limit, even when there are unused resources on the system. By default, the limits are set to unlimited, which means the virtual machine's configured memory becomes its effective limit. Using limits has the following benefits and drawbacks.

- **Benefits:** If you are concerned that the performance of a virtual machine may deteriorate as you add virtual machines to the cluster, you could set limits on the virtual machine to simulate having fewer available resources and measure its performance.

- **Drawbacks:** You may be wasting idle resources because the system prevents virtual machines from exceeding the limits that you set, even when the system is underutilized, and idle resources are available.

**Note**

If you want to reduce the risk that a virtual machine may consume excessive resources and impact the performance of other virtual machines, you can consider setting low shares on the virtual machine. Low shares decrease the virtual machine's access to the resource during periods of resource contention, while never preventing the virtual machine from using idle resources.

## Admission Control

When you power on a virtual machine, the system checks the amount available unreserved CPU and memory resources. It determines whether it can guarantee the reservation for the virtual machine. This process is called admission control. If enough unreserved CPU and memory are available (or if there is no reservation), the virtual machine is powered on. Otherwise, an **Insufficient Resources** warning appears.

**Note**

Each virtual machine, including those with no user-specified memory reservation, may have some reservation for its memory overhead. The memory overhead reservation is considered by admission control.

**Note**

When the vSphere DPM feature is enabled and some hosts are in standby mode, their unreserved resources are considered available for admission control. If a virtual machine cannot be powered on without these resources, vSphere DPM makes a recommendation to power on one or more standby hosts.

## VMware Tools and Microsoft Windows Perfmon

When VMware Tools is installed, VMware provides performance counters that enable you to view data within Windows guest OS using the Microsoft Windows Perfmon utility. VMware provides virtual machine-specific performance counter libraries for the Windows

Perfmon utility, which enables administrators to accurately examine virtual machine usage data and guest OS usage data within the same pane of glass.

For a Windows virtual machine, where VMware Tools is installed, you can use the following procedure to examine VMware specific statistics in the Windows Perfmon utility.

1. Logon to Windows and click Start > Run
2. Enter **Perfmon** and press **Enter**.
3. In the Performance dialog box, click **Add**.
4. In the **Add Counters** dialog box, select **Use local computer counters**.
5. Select a performance object, whose name begins with **VM** (a virtual machine performance object)
6. Select the counters that you want to display for that object.
7. If the performance object has multiple instances, select the instances you want to display.
8. Click **Add**.
9. Examine the data for the selected performance object.
10. Click **Close**

## **Latency Sensitivity**

If you have a latency sensitive application, such as Voice Over IP (VOIP) or a media player application, you can edit the virtual machine's settings and to set **VM Options > Latency Sensitivity** to **High**. With this setting, you should ensure that all the virtual machine's configured CPU and memory are reserved. With this setting, the system effectively gives exclusive physical CPU access to each virtual CPU. If the virtual machine is in a DRS cluster, DRS will automatically create a VM-Host soft affinity rule.

## Impact of Virtual Machine Configurations



The specific settings you make for a virtual machine can impact its performance, as summarized in [Table 10-8](#).

**Table 10-8** Impact of Virtual Machine Configurations

Configuration	Impact
Compute oversize / undersize	If the compute size of the virtual machine is over sized, then it may result in wasted resources. If it is undersized, the virtual machine may experience poor performance.
Virtual disk oversize / undersize	If the size of the virtual disk is over sized, then it may result in wasted resources. If it is undersized, the virtual machine may experience a denial of service.
VMDK provisioning types	If the virtual disk is thin provisioned, then you may be maximizing the use of your storage space, while decreasing the virtual machine's performance and increasing its risk of denial of service.
Resource reservations	If a resource is reserved, you may be improving and guaranteeing the guest OS performance, while reducing the density of virtual machines on the resource.
Independent disks	If a virtual disk is set to independent mode, then you are prevented from taking snapshots of it. If it is set to <b>Independent – Nonpersistent</b> , then all changes are discarded when you power off or reset the virtual machine.
Guest OS Type	The choice for the guest OS type during the virtual machine creation directly impacts the type of virtual devices that are used in the virtual machine.
VMware Tools version	The VMware Tools version impacts the set of device drivers it provides to the guest OS.
Permissions	The permissions set on a virtual machine impacts who can use (power on, open a console), who can modify (change virtual hardware settings), and who can manage (set permissions, migrate) the virtual machine.

## Other Virtual Machine Resource Management Features

You can configure virtual machines to support SRIOV, VGPU, RDMA, and Configure VMs to Support DirectPath I/O Passthrough as discussed in [Chapter 14](#).

## ESXTOP

ESXTOP is a utility that provides a real time, detailed look at resource usage from the ESXi Shell. You can run ESXTOP in interactive, batch, or replay mode. You must have root user privileges. RESXTOP is a similar tool that can be installed and run from a Linux server and connected to ESXi hosts.

By default, when you issue the command `esxtop`, the utility opens in interactive mode to show the CPU panel, where statistics for each virtual machine and other groups are displayed in separate rows. To see just virtual machines statistics, you can press the shift-V (capital V) key. Each column provides CPU statistics, such as %USED, %WAIT, %RDY, %CSTP, and %SWPWT. To see statistics for the multiple worlds that comprise a virtual machine, you can press the E key and enter the virtual machine's ID. [Figure 10-4](#) shows an example of an ESXTOP CPU panel, displaying only virtual machines statistics with one virtual machine (GID 33791) expanded.

1:24:45pm up 1:31, 562 worlds, 3 VMs, 4 vCPUs; CPU load average: 0.12, 0.14, 0.19															
PCPU USED(%):		11 11 AVG: 11		PCPU UTIL(%):		11 11 AVG: 11									
GID	NAME	NWLD	%USED	%RUN	%SYS	%WAIT	%VMWAIT	%RDY	%IDLE	%OVRLF	%CSTP	%MLMTD	%SWPWT		
24851	kms-01b	10	12.86	12.92	0.06	984.53	0.31	2.84	185.43	0.07	0.00	0.00	0.00		
33791	vms	1	0.08	0.01	0.07	99.97	-	0.01	0.00	0.00	0.00	0.00	0.00		
33791	Network-135	1	0.00	0.00	0.00	99.98	-	0.00	0.00	0.00	0.00	0.00	0.00		
33791	c_135915	1	0.09	0.10	0.00	99.85	-	0.14	0.00	0.00	0.00	0.00	0.00		
33791	vmx-vthread-135	1	0.00	0.00	0.00	99.89	-	0.00	0.00	0.00	0.00	0.00	0.00		
33791	vmx-filtPoll:w1	1	0.00	0.00	0.00	99.98	-	0.00	0.00	0.00	0.00	0.00	0.00		
33791	vmx-ske:w10	1	0.01	0.01	0.00	99.98	-	0.00	0.00	0.00	0.00	0.00	0.00		
33791	vmx-svga:w10	1	0.00	0.00	0.00	99.99	-	0.00	0.00	0.00	0.00	0.00	0.00		
33791	vmx-vcpu-0:w10	1	1.55	1.55	0.00	96.95	0.17	1.50	96.78	0.02	0.00	0.00	0.00		
33791	LSI-135915:0	1	0.00	0.00	0.00	99.99	-	0.00	0.00	0.00	0.00	0.00	0.00		
33780	app-01b	9	1.04	1.00	0.03	897.71	0.80	1.19	97.11	0.00	0.00	0.00	0.00		

**Figure 10-4** Sample ESXTOP CPU Panel

You can change the view from the CPU panel to other panels using keystrokes. For example, you can press the M key for the memory panel, the V key for the virtual machine storage panel, or the N key for the network panel. [Table 10-9](#) contains a description of some of the key statistics available for each panel.

**Table 10-9** Key ESXTOP Panels and Metrics

Panel	Statistic	Description
CPU	%USED	Percentage of physical CPU core cycles used by the virtual machine.
CPU Panel	%RUN	Percentage of total time scheduled for the virtual machine without accounting for hyperthreading, system time, co-stopping, and waiting. $\%RUN = 100\% - \%RDY - \%CSTP - \%WAIT$
CPU	%RDY	Percentage of time the virtual machine was ready to run but was not provided CPU resources on which to execute. Indicator of CPU contention on the host.
CPU	%WAIT	Percentage of time the virtual machine spent in the blocked or busy wait state, including idle time. %WAIT includes %SWPWT.
CPU	%CSTP	Percentage of time a virtual machine spends in a ready, co-deschedule state. Indicator that the virtual machine's multiple CPUs are in contention.
CPU	%SWPWT	Percentage of time a virtual machine spends waiting for the host to swap memory.
Memory Panel	MEMSZ	Amount of physical memory allocated to a virtual machine. $\text{MEMSZ} = \text{GRANT} + \text{MCTLsz} + \text{SWCUR} + \text{"never touched"}$
Memory Panel	GRANT	Amount of guest physical memory mapped to a virtual machine
Memory Panel	CNSM	Amount of the memory consumed by the virtual machine. $\text{CNSM} = \text{GRANT} - \text{shared memory}$
Memory Panel	SWCUR	Amount of swapped memory by the virtual machine.
Memory Panel	SWR/s	Rate at which the host swaps in memory from disk for the virtual machine.
Memory Panel	OVHD	Amount of memory used for virtual machine overhead, which is memory charged to the virtual machine that is not used by the guest OS.
Virtual Machine Storage Panel	READS/s	Number of read commands issued per second
Virtual Machine Storage Panel	WRITES/s	Number of write commands issued per second.
Virtual Machine Storage Panel	MBREAD/s	Megabytes read per second.
Virtual Machine Storage Panel	LAT/rd	Average latency (in milliseconds) per read.
Network Panel	PKRRX/s	Number of packets received per second.
Network Panel	MbTX/s	MegaBits transmitted per second.
Network Panel	%DRPTX	Percentage of transmit packets dropped. Indicates the physical network adapter cannot meet the demand, perhaps due to load from other virtual machines.
Network Panel	%DRPRX	Percentage of receive packets dropped. Indicates that insufficient CPU resources are available for network processing.

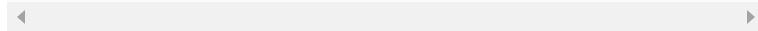
**Note**

The network panel contain a row for each NIC in a virtual machine, rather than row for each virtual machine. The E and shift-V keystrokes are not applicable to the network panel.

You can use the **-b** argument to run ESXTOP in a batch mode, where you collect statistics in a CSV file, which you can later manipulate with other tools, such as Microsoft Perfmon or Excel. For example, you can use the following command to collect statistics in a file named **mydata.csv**.

---

```
esxtop -b > mydata.csv
```



You can use ESXTOP in replay mode, where it uses pre-collected data rather than real time data. To collect the data, you should run **vm-support** in snapshot mode, specifying the data collection interval and duration (in seconds), as shown in the following example.

```
vm-support -S -d 3600 -I 5
```

After collecting the data, you must unpack and decompress the resulting tar file. Then, you can run ESXTOP in replay mode, providing the path to the data file, as shown here.

```
esxtop -R vm-support_dir_path
```

## VIMTOP

VIMTOP is a tool you can run in the vCenter Server appliance to see resource usage for services running in the appliance. It is like ESXTOP, but displays services, such as vCenter Server, Certificate Manager, vPostgres, and ESXi Agent Manager, rather than virtual machines and ESXi worlds. You can use VIMTOP to identify which service is using the most compute, disk, or network resources whenever vCenter Server is running poorly.

## vCenter Server Management Interface

In the vCenter Server Management Interface (VAMI) you select **Monitor** to view the resource usage of the vCenter Server. To see compute usage graphs, select **Monitor > CPU and Memory**. To see the usage of each storage partition, select **Monitor > Disks**. To use a graph where you can select and view specific network metrics, select **Monitor > Network**.

You can navigate to **Monitor > Database** to view the database utilization of alarms, events, tasks, and statistics. Here, you can also view the overall space utilization of the database and database log.

## EVENTS, ALARMS, AND AUTOMATED ACTIONS

A configurable events and alarms subsystem exists in vSphere that tracks events throughout vSphere and stores the data in log files and in the vCenter Server database. It enables you to specify the conditions under which alarms are triggered. Alarms can change state from normal (green) to warning (yellow) to alert (red) depending on changing conditions. Triggered alarms can automatically launch alarm actions.

### Events

Events are simply recorded incidents (something that occurred), such as user actions or system actions, that occurred involving a host or any object managed by vCenter Server. The following list includes a few examples.

- A license key expires
- A virtual machine is migrated
- A virtual machine is powered on
- A host connection is lost

Event data includes details such as who generated it, when it occurred, and what type of event it is. Table 10-10 describes the types of events

---

**Table 10-10** Event Types

Type	Description
Audit	Data concerning events which are tracked because it is crucial for the security framework. The data includes action details, such as who did it, when it occurred, and the IP address of the user.
Information	Describes that the operation completed successfully.
Warning	Indicates a potential risk to the system which needs to be addressed. This event does not terminate the process or operation.
Alert	Indicates that a fatal problem has occurred in the system and terminates the process or operation.

## View Events in the vSphere Client

You can use the following procedure to view events in the vSphere Client

1. In the vSphere Client. Select an object in the inventory pane.
2. Navigate to Monitor > **Events**.
3. Select an event to see the details.
4. Use the column headings to sort the events, show columns, hide columns, and filter the events.

## View the System Event Log

To view the system events, which are recorded in the vCenter Server database, you can use the following procedure.

1. Logon to the vSphere Client as a user with the **Global.Diagnostics** privilege.
2. Select the vCenter Server in the inventory pane.
3. Click **Monitor**, and click **Hardware Health**.
4. Click **System Event Log**.
5. Optionally, you can click **Export**.

## Stream Events to a Remote Syslog Server

You can enable remote streaming, such that the vCenter Server will stream newly generated events to a remote

syslog server. In the syslog server, the events have the following format.

```
<syslog-prefix> : Event [eventId] [partInfo] [created
```

Messages that are longer than 1024 characters split into multiple syslog messages.

**Note**

In an environment with no more than 30 hosts, you can configure hosts to send log files to a vCenter Server rather than storing them to a local disk. This feature is intended for smaller environments with stateless ESXi hosts. For all other cases, VMware recommends that you use a dedicated log server.

As an alternative to streaming events, you can forward events. When you forward events, the events are sent to a remote server rather than recorded.

You can use the following procedure to forward vCenter Server logs to a remote syslog server.

1. Logon to the vCenter Server Management Interface (VAMI) as root.
2. Select **Syslog**.
3. In the **Forwarding Configuration** section, click **Configure**.
4. In the **Create Forwarding Configuration** pane, enter the server address of the destination host.  
The maximum number of supported destination hosts is three.
5. Select a **Protocol** (TLS, TCP, RELP, or UDP) to use.
6. Provide a **Port** number
7. Optionally, add more destination servers
8. Click Save.
9. Optionally, click **Send Test Message**.

You can configure the writing of events to the vCenter Server streaming facility. Streaming events is disabled by default. You can use the following procedure to stream events to a remote syslog server.

1. In the vSphere Client, select the vCenter Server in the inventory pane.
2. Navigate to **Configure > Settings > Advanced Settings**.
3. Click **Edit**.
4. Enable the `vpxd.event.syslog` option.

## Alarms

Alarms are notifications that are activated in response to an event, a set of conditions, or the state of an inventory object. Table 10-11 contains the elements that are used in an alarm definition

**Table 10-11** Alarm Definition Elements

Element	Description
Name	Name (label) that is used to identify that alarm
Description	Text that useful for understanding the purpose of alarm
Targets	The type of object that is monitored by the alarm
Alarm Rules	A set of rules that define the alarms triggers, severity, and actions
Last Modified	The date of the most recent change to the alarm definition

For example, you might want to monitor the memory usage of all virtual machines in a specific vSphere cluster. In the vSphere Client, you can select the cluster in the inventory, create an alarm for the cluster, set the alarm's Targets to virtual machine, and configure rules with triggers base on memory usage.

**Note**

You can enable, disable, and modify alarms only from the object at which the alarm is defined. For example, if you defined a virtual machine memory alarm on a cluster, you cannot change the alarm at the individual virtual machine level.

## View and Acknowledge Triggered Alarms

To view triggered alarm, you can use the following procedure.

1. In the vSphere Client, select an object in the inventory pane
2. Navigate to **Monitor > Issues and Alarms**.
3. Click **Triggered Alarms**.
4. Optionally, select an alarm and click **Acknowledge**

You can acknowledge an alarm to let other users know that you are taking ownership of the issue and to prevent the alarm from sending more email messages. The alarm, however, is still visible in the system.

**Note**

After you acknowledge an alarm in the vSphere Client, its alarm actions are discontinued. Alarms are not cleared or reset when acknowledged.

To clear an alarm (reset its state to normal), you need the **Alarm.Set Alarm Status** privilege. You can select a triggered alarm and choose **Reset to green**.

## Create Alarm Definitions

To create or configure an alarm, you must use a user account with the **Alarms.Create alarm** or **Alarms.Modify alarm** privilege. To create an alarm, you can use the following procedure.

1. In the vSphere client, select an object in the inventory pane.
2. Navigate to **Configure > More > Alarm Definitions**.
3. Click **Add**

4. Provide the **Name**, **Description**, **Target Type**, and **Target**.
5. Click **Next**.
6. Create an Alarm Rule, by specifying the following for each rule.
  - Conditions: Trigger, Arguments, Operator, Threshold
  - Severity
  - Actions: Send email notifications, Send SNMP traps, Run Script
7. Optionally click **Add Another Rule**, **Duplicate Rule**, or **Remove Rule**
8. Click **Next**.
9. Specify **Alarm Reset Rules** by enabling the **Reset the alarm to green** option and providing details, such as arguments, operators, and actions.
10. Click **Next**
11. Click **Enable this Alarm**

## Alarm Actions

Alarm actions are operations that are automatically triggered by alarms. Table 10-12 provides details on available alarm actions.

**Table 10-12** Alarm Actions

---

Action	Details
Send Email Notification	Provide the recipient email address. Requires that you first configure the <b>Mail</b> settings for your vCenter Server. You must set the <b>Primary Receiver URL</b> to the DNS or IP address of your SNMP receiver. You should set the <b>Receiver port</b> to an appropriate value between 1 and 65535 and set the <b>Community string</b> to an appropriate community identifier.
Send SNMP Traps	Requires that you first configure the <b>SNMP receivers</b> settings for your vCenter Server. You must set the <b>Mail.server</b> to the DNS or IP address of your SMTP gateway. You must set <b>Mail.sender</b> to the email address of the sender.
Run Scripts	Provide the full pathname of the command or script, formatted into a single string. The execution will occur on the vCenter Server Appliance.
Advanced Actions	Only applicable to alarms that target virtual machines and hosts. Example host actions include <b>Enter maintenance mode</b> and <b>Exit Maintenance mode</b> . Example virtual machine actions include <b>Migrate VM</b> and <b>Reboot guest on VM</b> .

## Advanced Use Cases for Alarms

You can create custom alerts with notifications for many purposes, such as the following

- Something failed or disconnected (such as host connection failure or VASA provider disconnected).
- Something is not performing well (such as excessive CPU Ready Time, Memory Swapping, disk latency, or packets dropped).
- Poor health (such as vSAN Health, Key Management Server Health, vCenter HA Cluster Health).

## LOGGING IN VSphere

This chapter is intended to ensure that you understand logging in vSphere components and related products and that you are prepared to implement logging.

### ESXi Logs

Table 10-13 contains details on most of the ESXi log files, including the location and purpose of each. You should get familiar with each of these and learn which logs are useful for various troubleshooting scenarios. For example, when troubleshooting virtual machine issues,

the only directly useful logs are **vmkernel**, **vmkwarning**, **hostd**, and the specific virtual machine's log files. When troubleshooting issues related to the connection between an ESXi host and the vCenter Server, the **vpxa** log is most useful.

**Table 10-13** ESXi Log Files

Component	Location	Purpose
VMkernel	/var/log/vmkernel.log	Data related to virtual machines and ESXi.
VMkernel warnings	/var/log/vmkwarning.log	Data related to virtual machines.
Vmkernel summary	/var/log/vmksummary.log	Data related to uptime and availability statistics for ESXi
ESXi host agent	/var/log/hostd.log	Data related to the agent that manages and configures the ESXi host and its virtual machines.
vCenter agent	/var/log/vpxa.log	Data related to the agent that communicates with vCenter Server.
ESXi Shell	/var/log/shell.log	Data related to each command typed into the ESXi Shell as well as shell events.
Authentication	/var/log/auth.log	Data related to events authentication eventd for the local system.
System Messages	/var/log/syslog.log	Contains all general log messages and can be used for troubleshooting.
Virtual Machines	vmware.log located in the same folder as the virtual machine configuration file.	Data related to virtual machine power events, system failure information, tools status and activity, time sync, virtual hardware changes, vMotion migrations, machine clones, and more.
Trusted Infrastructure Agent	/var/run/log/kmxa.log	Data related to the Client Service on the ESXi Trusted Host
Key Provider Service	/var/run/log/kmxsd.log	Data related to the vSphere Trust Authority Key Provider Service.
Attestation Service	/var/run/log/attestd.log	Data related to the vSphere Trust Authority Attestation Service
ESX Token Service	/var/run/log/esxtokend.log	Data related to the vSphere Trust Authority ESX Token Service
ESX API Forwarder	/var/run/log/esxapiadapter.log	Data related to the vSphere Trust Authority API forwarder.
Quick Boot	/var/log/loadESX.log	Data related to restarting an ESXi host through Quick Boot

You can use the ESXi Host Client to examine the logs on a specific ESXi host by navigating to Monitor > Logs and selecting a specific log file. You can scroll through the log and search for specific text. You can select a log, click **Actions**, and choose **Open the in new window or Generate a support bundle**.

Likewise, you can use the ESXi Direct Console User Interface (DCUI) to view System Logs. In the DCUI, select **View System Logs**. and select the log you want.

You can use the Enter key (or space bar) to scroll through the log messages and press the forward slash (/) key to begin a search.

If you have the **Global.Diagnostics** privilege, then you can also use vSphere Client to export a host's system logs, by applying the following procedure.

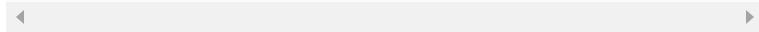
1. In the vSphere Client, right-click an ESXi in the inventory pane.
2. Click **Export System Logs**.
3. Select the appropriate objects
4. Optionally select **Gather performance data**.
5. Optionally, provide a **Password for encrypted core dumps**
6. Click **Export Logs**
7. Monitor the status of the **Downloading log bundles** task in the **Recent Tasks** pane.
8. When completed, the file is located in the default location. On a Windows desktop, the location is the Downloads folder and the file name begins with VMware-vCenter-support.

**Note**

In Step 3, you can select or deselect entire categories, such as **System**, **Virtual Machines**, and **Storage**. You can also select or deselect specific objects within each category, such as **Logs** and **CoreDumps**.

You can collect ESXi log files using the /usr/bin/vm-support command, which generates a file named in the following format.

esx-date-unique-xnumber.tgz



## vCenter Server Logs

The main logs in a vCenter Server appliance are located at `/var/log/vmware`. The most important logs are in the `vpxd` subdirectory. Some other sibling subdirectories include `vsan-health`, `vsphere-ui`, and `vpostgres`.

## Upload System Logs to VMware

To export system logs from the vCenter Server and all its hosts, you can use the previous procedure, but begin by selecting the vCenter Server instead of a specific host. In the wizard, you can select which hosts to include and you can optionally select **Include vCenter Serer and vSphere UI Client logs**.

You can export a vCenter Server instance's support bundle using the URL displayed on the DCUI home screen (<https://FQDN:443/appliance/support-bundle>).

Alternatively, you can run the `vc-support.sh` script in the vCenter Server appliance Bash shell to collect the support bundle.

You can directly upload a log package to an open VMware Service Request, using the following procedure.

1. In the vSphere Client, navigate to **Administration > Support**
2. Click **Upload File to Service Request**.
3. Provide a Service Request ID.
4. Click **Choose File**, select the appropriate log bundle, and click **OK**.

## Log Levels

The default log level setting is **Info**, where errors, warnings, and informational level are logged. You can change the log level to lower levels, such as **Verbose**, which is useful for troubleshooting and debugging, but

not recommended for normal use in production environments. You can use the vSphere Client to change the logging level by selecting the vCenter Server, selecting **Configure > Settings > General > Edit** and setting the **Logging Settings** to the appropriate level, as described in Table 10-14.

**Table 10-14** vCenter Server Logging Options

Logging Option	Description
None (Disable logging)	No vCenter Server logging occurs.
Error (Errors Only)	The vCenter Server collects only error entries into its log files.
Warning (Warning and Errors)	The vCenter Server collects warning and error entries into its log files.
Info (Normal logging)	The vCenter Server collects information, warning and error entries into its log files.
Verbose (Verbose)	The vCenter Server collects verbose, information, warning and error entries into its log files.
Trivia (Extended verbose)	The vCenter Server collects trivia, verbose, information, warning and error entries into its log files.

Although, setting the logging level to verbose or trivia may be beneficial for troubleshooting, doing so for long durations could cause noticeable vCenter Server performance degradation. VMware recommends that you use these levels in rare cases, while actively troubleshooting, and that you reset the logging level immediately afterwards. Changes to the logging level are persisted in the vCenter Server configuration file `/etc/vmware-vpx/vpxd.cfg`. You can make additional changes to logging behavior by editing the Advanced Settings of a vCenter Server. For example, you can use the vSphere Client to edit the following settings, which impact log size, retention, rotation, and compression.

- config.log.level
- config.log.maxFileNum
- config.log.maxFileSize
- config.log.compressOnRoll

**Note**

By default, vCenter Server vpxd log files are rolled up and compressed into .gz files. You can turn off compression for vpxd log files, by adding the `log.compressOnRoll` key with the value false to the vCenter Server Advanced Settings.

## Configure Syslog on ESXi Hosts

You can use the following procedure to configure the syslog service for a host.

1. In the vSphere Client, select a host in the inventory pane.
2. Navigate to **Configure > System > Advanced System Settings**.
3. Click **Edit**.
4. Filter for **syslog**.
5. To set up logging globally for the following options, select the option and enter the value.
  - **Syslog.global.defaultRotate**: Maximum number of logs to keep when rotating logs.
  - **Syslog.global.defaultSize**: Size (KB) of log, before triggering a log rotation.
  - **Syslog.global.LogDir**: Directory in a VMFS or NFS datastore to store logs specified in the format **[datastore] /path**. For example, to store logs in the `/vmfs/volumes/VMFS-01/systemlogs` folder, specify `[VMFS-01]/systemlogs`
  - **Syslog.global.logDirUnique**: Enabling this option creates a subdirectory for the host at the specified path, which is useful when more than one hosts uses the same shared datastore for logging.
  - **Syslog.global.LogHost**: Remote syslog host and port to which message are forwarded. For example, to forward to a server named syslogsvr-

1 using port 1514, specify `ssl://syslogsvr-1:1514`.

6. Optionally, select specific log names and change the number of rotations and log size for just that specific log.

7. Click **OK**.

You can control how log files are maintained for virtual machines. A new log file is created each time you power on or resume a virtual machine, or whenever the file size exceeds the **vmx.log.rotateSize** value, unless the value is 0 (default). VMware recommends saving 10-log files, each one limited to no less than 2MB. If you need logs for a longer time span, you can set **vmx.log.keepOld** to 20.

You can use the following procedure to change the number of log files for a single virtual machine.

1. In the vSphere Client, select a host or a virtual machine in the inventory pane.
2. Right-click the virtual machine and click **Edit Settings**.
3. Select **VM Options > Advanced**
4. Click **Edit Configuration**.
5. Add or edit the **vmx.log.keepOld** parameter to the appropriate number.
6. Click **OK**.

**Note**

To set this value for all virtual machines on a specific host, edit the `/etc/vmware/config` file and add or edit a line like the following.

```
vmx.log.keepOld = "10"
```

You can modify the `/etc/vmware/logfilters` file on a host to change its logging behavior. In this file you can add an entry specifying the following options.

- **numLogs:** The maximum number of log entries before the specified log messages are filtered and ignored. Use 0 to filter and ignore all the specified log messages.
- **Ident:** Specifies one or more system components to apply the filter.
- **logRegexp:** Specifies a case-sensitive phrase to filter the log messages by their content.
- Add the following line to the `/etc/vmsyslog.conf` file: **enable\_logfilters = true**
- Run the =command, **esxcli system syslog reload**

## Log Insight

To collect and analyze vSphere data using vRealize Log Insight (vRLI), you first must deploy vRLI, then you can follow this procedure.

1. In the vRLI web interface, navigate to the **Administration** tab.
2. Click **Integration**, > **vSphere**.
3. Provide hostname and credentials to connect to a vCenter Server.
4. Click **Test Connection**.
5. If you use an untrusted SSL certificate, click **Accept** in the dialog.
6. Click **Save**.
7. Use the vRLI web interface to configure the data collection from vCenter.

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, [Chapter 15, "Final Preparation,"](#) and the exam simulation questions on the CD-ROM.

## REVIEW ALL KEY TOPICS

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 10-15](#) lists a reference of these key topics and the page numbers on which each is found.

**Table 10-15** Key Topics for Chapter 10

Key Topic Element	Description	Page Number
Procedure	Add a Host Using Quickstart	
Table 10-2	Use Cases for VM - VM Rules	
Procedure	Configure vSphere HA Admission Control	
Section	Configure Proactive HA	
Section	Overview Performance Graph	
Section	Impact of Virtual Machine Configuration	
Procedure	Configure Skyline Health	

## COMPLETE THE TABLES AND LISTS FROM MEMORY

Print a copy of Appendix B, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix C, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

## DEFINE KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary:

COU Ready Time

ESXTOP

VIMTOP

Performance Charts

## Glossary

**CPU Ready Time:** CPU Ready Time is a metric that indicates the amount of time a VCPU is ready to work (has a workload and is ready to be scheduled) but is waiting to be scheduled on hardware. High CPU Ready Time is a sign of CPU contention.

**ESXTOP :** ESXTOP is a utility that provides a real time, detailed look at resource usage from the ESXi Shell.

**VIMTOP :** VIMTOP is a tool you can run in the vCenter Server appliance to see resource usage for services running in the appliance.

**Performance Charts:** The vSphere Client Performance Charts enable you to view performance metrics in different types of charts, depending on the selected object and metric type

## REVIEW QUESTIONS

1. You are creating a resource pool in vSphere DRS cluster. Which of the following is a default setting?
  - a. The Memory Limit is disabled.
  - b. The CPU Shares are 0
  - c. The Memory Reservation is 0
  - d. The CPU Reservation is normal.

2. You want to configure Predictive DRS in your vSphere Cluster. Which of the following is a requirement?

- a. Set DRS to **Fully Automated**
- b. In the cluster, set **Provide data to vSphere Predictive DRS** to True.
- c. In the **vRealize Operations**, set **Provide data to vSphere Predictive DRS** to True.
- d. In the **vRealize Automation**, set **Provide data to vSphere Predictive DRS** to True.

3. You are configuring a vSphere HA cluster and do now want it to automatically reserve resources for failure. What setting should you use?

- a. Set **Cluster Resource Percentage** to 0.
- b. Set **Cluster Resource Percentage** to 100.
- c. Set **Define host failover capacity to Dedicated Host Failures**
- d. Set **Define host failover capacity to Disabled**

4. You want to use a command line tool that shows real time CPU statistics for the services running in the vCenter Server. Which should you choose?

- a. vimtop
- b. esxtop
- c. Performance Charts
- d. vCenter Server Management Interface

5. You are examining vSphere logs. Which of the following logs are in the same folder as the virtual machine configuration file?

- a. vpxa.log

b. `vmkssummary.log`

c. `auth.log`

d. `vmware.log`

# **Chapter 11. Manage Storage**

**[This content is currently in development.]**

**This content is currently in development.**

# **Chapter 12. Manage vSphere Security**

**This chapter covers the following subjects:**

- Configure and Manage Authentication and Authorization
- Configure and Manage vSphere Certificates
- General ESXi Security Recommendations
- Configure and Manage ESXi Security
- Other Security Management

This chapter contains information related to VMware  
2V0-21.20 exam objectives 1.10, 1.11, 4.1, 4.1.1, 4.1.2, 4.3,  
4.3.1, 4.3.2, 4.3.3, 4.10, 4.11, 4.11.1, 4.13, 7.7, 7.

This chapter covers the procedures for managing security  
in a vSphere environment.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess  
whether you should study this entire chapter or move  
quickly to the “Exam Preparation Tasks” section.

Regardless, the authors recommend that you read the  
entire chapter at least once. Table 12-1 outlines the major  
headings in this chapter and the corresponding “Do I  
Know This Already?” quiz questions. You can find the  
answers in Appendix A, “Answers to the ‘Do I Know This  
Already?’ Quizzes and Review Questions.”

**Table 12-1** “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Configure and Manage Authentication and Authorization	1, 2
Configure and Manage vSphere Certificates	3, 4
General ESXi Security Recommendations	5, 6
Configure and Manage ESXi Security	7, 8
Other Security Management	9, 10

- 1.** You are responsible for multiple vSphere environments. What must you do to enable the use of Enhanced Linked Mode in vSphere 7.0?
  - a.** Associate two vCenter Servers with the same external PSC.
  - b.** Map the external PSC of one vCenter Server to the embedded PSC of another vCenter Server.
  - c.** Configure vCenter Server HA
  - d.** Connect two vCenter Servers to the same SSO domain.
  
- 2.** You are configuring permissions in a vSphere environment. When editing an existing permission, which of the following properties can you change?
  - a.** Role
  - b.** Privilege
  - c.** User
  - d.** Object
  
- 3.** You are managing certificates in your vSphere environment. By default, what types of certificates are in VECS? (pick two)
  - a.** ESXi Certificates
  - b.** Machine SSL Certificates
  - c.** Trusted Root Certificates

- d. None of the above**
- 4.** You are responsible for performing certificate management for your ESXi hosts. Which of the following privileges do you need?
  - a. Certificates.Manage Certificates**
  - b. Host.Manage Certificates**
  - c. Manage.Certificates**
  - d. Certificates.Manage.Host**
- 5.** You are enabling direct ESXi access using local accounts. To change the password requirements, such as minimum length, which of the following steps should you take?
  - a. Select Single Sign On > Configuration**
  - b. Configure Lockdown Mode**
  - c. Use the Set-PasswordControl cmdlet**
  - d. Configure Security.PasswordQualityControl**
- 6.** You want to enable passthrough for a network device on your ESXi host. You see an orange icon is associated with device. Which of the following actions should you do?
  - a. Reboot the host**
  - b. Ignore the icon, select the device and click OK.**
  - c. Navigate to Configure > Services and restart a specific service**
  - d. Give up. The device is not compatible for passthrough.**
- 7.** You want to configure your ESXi's acceptance level such that you cannot install VIBs signed at

or below the **PartnerSupported** level, but you can install VIBs signed at higher levels. Which option should you choose?

- a. VMwareCertified**
- b. VMwareAccepted**
- c. PartnerSupported**
- d. CommunitySupported**

**8.** You want to enable UEFI Secure Boot. To determine if your ESXi host supports Secure Boot, which of the following steps should you take?

- a. Use the following command**

```
/usr/lib/vmware/secureboot/bin/secur  
eBoot.py -c
```

- b. Check for compliance using a host profile.**

- c. Check for compliance using Life Cycle Manager**

- d. Use the Security Profile section in the vSphere Client.**

**9.** You need to use encryption in your vSphere environment. Which of the following should you use to configure a trust relationship to **Make KMS Trust vCenter?**

- a. In the vSphere Management Interface, choose Configuration > Key Management Servers.**

- b. vSphere Client, select the vCenter Server and choose Configuration > Key Management Servers.**

- c. In the vSphere Management Interface, choose Configuration > Encryption**

- d. vSphere Client, select the vCenter Server and choose Configuration > Encryption.**

**10.** You want to configure vSphere Trust Authority.  
Which of the following is a necessary step?

  - a. Create the Trusted Key Provider on the trusted cluster**
  - b. Import the Trusted Key Provider to the trusted authority cluster.**
  - c. Configure the Trusted Key Provider for the trusted hosts on the trusted cluster**
  - d. Configure the Trusted Key Provider for the hosts on the trusted authority cluster**

## **CONFIGURE AND MANAGE AUTHENTICATION AND AUTHORIZATION**

This section describes configuration and management tasks related to vSphere authentication and authorization. Authentication tasks involve vCenter Single Sign-on (SSO) and authorization involves permissions.

### **Manage SSO**

As explained in previous chapters, you can use the built-in identify provide vCenter Single Sign-On (SSO) and external identity providers for vSphere authentication. SSO includes the Security Token Service (STS), an administration server, the vCenter Lookup Service, and the VMware Directory Service (vmdir). The VMware

Directory Service is also used for certificate management.

Chapter 8, "vSphere Installation," provides the following procedures

- Adding and editing identity sources.
- Adding the vCenter Appliance to an Active Directory domain.
- Configure SSO password, lockout, and token Policies

This section provides procedures for enabling Windows Session Authentication (SSPI) and managing STS. This section also describes how to implement and use Enhanced Linked Mode.

**Note**

The lockout policy applies only to user accounts, not to system accounts such as administrator@vsphere.local.

## **Enable SSO with Windows Session Authentication**

To enable Windows Session Authentication (SSPI), you can use the following procedure.

**Step 1.** Prepare an Active Directory domain and its trusts in an SSO trusted manner as described in VMware KB 2064250.

**Step 2.** Join the vCenter Server to the Active Directory domain as described in Chapter 8.

**Step 3.** Install the Enhanced Authentication Plug-In.

**Step 4.** Instruct vSphere Client users to select the **Use Windows Session Authentication** checkbox during login.

**Note**

If you use federated authentication with Active Directory Federation Services, the Enhanced Authentication Plug-in only applies if vCenter Server is the identity provider.

## Manage Service Token Service (STS)

The vCenter Single Sign-On Security Token Service (STS) is a Web service that issues, validates, and renews security tokens. It uses a private key to sign tokens and publishes the public certificates. SSO manages the certificates that are used by STS for signing and stores the certificates (the signing certificates) in VMware Directory Service (vmdir). You can use the following procedure to generate a new STS signing certificate.

**Step 1.** Create a top-level directory.

**Step 2.** Copy the **certool.cfg** file into the new directory.

**Step 3.** Modify the **certool.cfg** file to use the local vCenter Server IP address and hostname.

**Step 4.** Generate the key (`/usr/lib/vmware-vmca/bin/certool --genkey`)

**Step 5.** Generate the certificate (`/usr/lib/vmware-vmca/bin/certool --gencert`)

**Step 6.** Create a PEM file with the certificate chain and private key.

**Note**

The certificate is not external-facing and is valid for 10 years. Only replace this certificate if required by your company's security policy.

To use a company required certificate or to refresh a certificate that is near expiration, you can use the PEM file from the previous procedure and the **sso-config** utility command to refresh the STS certificate, such as in the following example.

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vs
```

## Enhanced Linked Mode

To join vCenter Server systems in Enhanced Linked Mode, connect them to the same SSO domain. For example, during the deployment of a vCenter Server, choose to join the SSO domain of a previously deployed vCenter Server.

When implementing Enhanced Linked Mode, you should ensure that you properly synchronize the time settings of the new appliance to match that of the previously deployed appliance. For example, if you are using the vCenter Server GUI Installer to deploy two new vCenter Server appliances joined in Enhanced Linked Mode to the same ESXi host, you can configure each to synchronize the time settings with the host.

You can use a single vSphere Client window to manage multiple vCenter Server systems that are joined with Enhanced Linked Mode. Enhanced Linked Mode provides the following features for vCenter Server:

- You can log in to all linked vCenter Server systems simultaneously.
- You can view and search the inventories of all linked vCenter Server systems.
- Roles, permission, licenses, tags, and policies are replicated across linked vCenter Server systems.

**Note**

Enhanced Linked Mode requires the vCenter Server Standard licensing level.

## Users and Groups

By default, immediately following installation, only the `localos` and the SSO domain (`sphere.local` by default) identity sources are available. [Chapter 8](#) describes how to add identity sources, such as a native Active Directory (Integrated Windows Authentication) domain, an OpenLDAP directory service, or Active Directory as an LDAP Server. It also describes how to create users and groups in the SSO domain.

**Note**

After creating a user or group, you cannot change its name.

When using the procedure in [Chapter 8](#) to add members to a group in the SSO domain, you can add users from identity sources.

In some cases, you may wish to manage multiple, independent vSphere environments having similar, but separate SSO domains and users. In such scenarios, you can export SSO users using this procedure.

**Step 1.** Log onto the vSphere Web Client

**Step 2.** Select **Home > Administration**.

**Step 3.** Select **Single Sign On > Users and Groups**

**Step 4.** Select the **Users** tab

**Step 5.** click the **Export List** icon in lower right corner

You can use a similar procedure to export SSO groups, except that you choose **Groups** in Step 4.

## Privileges and Roles

To create a role in vCenter Server using the vSphere Client, you can use this procedure.

**Step 1.** Click **Menu >Administration > Roles**

**Step 2.** Click the Create role action (+) button.

**Step 3.** Provide a name for the role.

**Step 4.** Select the desired privileges.

**Step 5.** Click **OK**.

After creating custom roles, you can use the roles when assigning permissions in the same manner as you use the vCenter Server system roles and sample roles.

To clone a sample role or custom role in the vSphere Client, select the role at **Administration > Roles**, click the **Clone role action** icon and provide a name for the new role. To edit a sample role or custom role in the vSphere Client, select the role at **Administration > Roles**, click the **Edit role action** icon and modify the set of privileges in the role

## Permissions

To set a permission using the vSphere Client, you can use the following steps.

**Step 1.** Select the object in the inventory

**Step 2.** Click the **Permissions** tab

**Step 3.** Click the Add Permission icon

**Step 4.** Select a user or group form the **User** drop-down menu

**Step 5.** Select a role from the **Role** drop-down menu

**Step 6.** Optionally, select Propagate to children

**Step 7.** Click **OK**

By assigning a different role to a group of users on different objects, you control the tasks that those users can perform in your vSphere environment. For example,

to allow a group to configure memory for the host, select that host and add a permission that grants a role to that group that includes the **Host.Configuration.Memory Configuration** privilege.

## Global Permissions

In some cases, you may assign a global permission and choose not to propagate to child objects. This may be useful to provide a global functionality, such as creating roles. To assign a global permission, you should use the vSphere Client with a user account that has the **Permissions. Modify permission** privilege on the root object of all inventory hierarchies. Select **Administration > Global Permissions > Manage** and use the **Add Permission** icon (plus sign). Use the dialog to select the desired user group (or user) and role.

**Note**

By default, the administrator account in the SSO domain, such as **administrator@vsphere.local**, can modify global permissions, but the vCenter Server appliance root account cannot.

**Note**

Be careful when applying global permission. Decide if you genuinely want the permission to apply to all solutions and to all objects in all inventory hierarchies.

## Edit Permissions

If you wish to modify an existing permission, you can edit the permission and change role assignment. You cannot change the object, user, or user group in the permission, but you can change the role. If this is not adequate, then remove the permission and create a new permission with the correct settings. This work must be done as a user with sufficient privileges to change permissions on the associated object.

The biggest challenge in editing permissions may be locating the permission, so it can be modified. If you know the object on which the permission was created, then you can select the object in the vSphere Client inventory, select **Configure > Permissions**, right-click the permission and choose **Change Role**. Select the appropriate role and click **OK**.

If you do not already know which permission to modify or on which object the permission is assigned, you may need to investigate. Begin by selecting an object in the inventory on which you know the applied user permissions are incorrect. Select **Manage > Permissions** to discover all the permissions that apply to the object. Use the **Defined in** column to identify where each applied permission is defined. Some of the permissions may be assigned directly on the object and some may be assigned to ancestor objects. Determine which permissions are related to the issue and where they are assigned.

## CONFIGURE AND MANAGE VSPHERE CERTIFICATES

You can use the vSphere Client and vSphere Certificate Manager to view and manage certificates. With the vSphere Client you can perform the following tasks.

- View trusted root certificates and machine SSL certificates.
- Renew or replace existing certificates.
- Generate a custom Certificate Signing Request (CSR) for a machine SSL certificate.

For each certificate management task, you should use the administrator account in the SSO domain (**vsphere.local** by default)

## vSphere Client Certificate Management

You can use the following procedure to explore and take actions on the certificate stored in a VMware Endpoint Certificate Store (VECS) instance.

**Step 1.** In the vSphere Client, navigate to Home > Administration > Certificates > Certificate Management.

**Step 2.** If the system prompts you, enter the credentials of your vCenter Server.

**Step 3.** The **Certificate Management** page shows the certificate types in the VMware Endpoint Certificate Store (VECS). By default, the types are:

- Machine SSL Certificates
- Trusted Root Certificates

**Step 4.** For more details, click **View Details** for the certificate type.

**Step 5.** For the Machine SSL Certificates, you can choose from the following **Actions**

- Renew
- Import and replace certificate
- Generate CSR

**Step 6.** For Trusted Root Certificates, you can choose **Add**.

**Note**

To replace all VMCA-signed certificates with new VMCA-signed certificates, choose the Renew action for the Machine SSL certificates.

If you replace the existing certificate, you can remove the old root certificate if you are sure it is no longer in use.

By default, vCenter Server monitors all certificates in VECS and raises an alarm for any certificate that will expire in 30 days or less. You can change the 30 day threshold by modifying vCenter Server's advanced setting **vpxd.cert.threshold**.

## Using Custom Certificates

To set up your environment to use custom certificates, you need to generate CSRs for each machine and each solution user and replace certificates when you receive them. You can generate the CSRs using the vSphere Client or Certificate Manager. You can use the vSphere Client to upload both the root certificate and the signed certificates that are returned from the CA.

You can use the following procedure to generate a CSR for custom certificates.

**Step 1.** Verify that you meet the *Certificate Requirements* in Chapter 7, "vSphere Security."

**Step 2.** Use the vSphere Client to Home > Administration > Certificates > Certificate Management.

**Step 3.** If prompted, enter the credentials of your vCenter Server.

**Step 4.** In the Machine SSL Certificate section, for the certificate you want to replace, click **Actions** > **Generate Certificate Signing Request (CSR)**.

**Step 5.** Enter your certificate information and click Next.

**Step 6.** Copy or download the CSR.

**Step 7.** Click **Finish**.

**Step 8.** Provide the CSR to your Certificate Authority.

Alternatively, you can use the vSphere Certificate Manager utility from the vCenter Server shell to generate the CSR, by using the following command, selecting option 1 and providing the certificate information.

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

After your CA processes the CSR, you can use the following procedure to add the custom certificates.

**Step 1.** Use the vSphere Client to Home > Administration > Certificates > Certificate Management.

**Step 2.** If the system prompts you, enter the credentials of your vCenter Server.

**Step 3.** In the Machine SSL Certificate section, for the certificate that you want to replace, click **Actions > Import and Replace Certificate**.

**Step 4.** From the following options, select the last option, and click **Next**.

- Replace with VMCA
- Replace with certificate generated from vCenter Server
- Replace with external CA certificate (requires private key)

**Step 5.** Upload the certificates and click **Replace**

**Step 6.** Wait for vCenter Server services to restart.

## Manage ESXi Certificates

Initially, in vSphere 6.0 or later, ESXi hosts boot with an autogenerated certificate. When the host is added to a vCenter Server system, it is provisioned with a certificate

signed by the VMware Certificate Authority (VMCA). You can view and manage ESXi certificates using the vSphere Client or the `vim.CertificateManager` API in the vSphere Web Services SDK. You cannot use the vCenter Server certificate management CLIs to view or manage ESXi certificates.

## Change the Certificate Mode

You can change the ESXi certificate mode from VMCA mode to Custom Certificate Authority mode or to Thumbprint mode. In most cases, mode switches are disruptive and not necessary. If you do require a mode switch, review the potential impact before you start. You should only use the thumbprint mode for debugging.

**Note**

Thumbprint mode was used in vSphere 5.5 and should not be used in later versions, unless necessary, because some services may not work. Also, in this Thumbprint mode, vCenter Server only checks the certificate format, not its validity. Even expired certificates are accepted.

To perform certificate management for ESXi, you must have the **Certificates.Manage Certificates** privilege.

For example, if you wish to use custom certificates instead of VMCA to provision ESXi hosts, you need to edit the vCenter Server `vpxd.certmgmt.mode` advanced option. From the vSphere client you can use this procedure to change the certificate mode.

**Step 1.** Select the vCenter Server and click **Configure**.

**Step 2.** Click Advanced Settings, and click Edit.

**Step 3.** In the Filter box, enter `certmgmt` to display only certificate management keys.

**Step 4.** Change the value of `vpxd.certmgmt.mode` to `custom` and click **OK**.

**Step 5.** Restart the vCenter Server service

## Using Custom ESXi Certificates



You can switch the certificate mode from VMCA to a different root CA using these steps.

**Step 1.** Obtain the certificates from the trusted CA..

**Step 2.** Place the host or hosts into maintenance mode and disconnect them from vCenter Server.

**Step 3.** Add the custom CA's root certificate to VECS.

**Step 4.** Deploy the custom CA certificates to each host and restart services on that host.

**Step 5.** Change the Certificate Mode to Custom CA mode. (as described in the previous procedure)

**Step 6.** Connect the host or hosts to the vCenter Server system.

### Switch Back to VMCA Mode

If you are using the custom CA mode, you can switch back to VMCA mode using this procedure.

**Step 1.** Remove all hosts from the vCenter Server system.

**Step 2.** On the vCenter Server system, remove the third-party CA's root certificate from VECS.

**Step 3.** Change the Certificate Mode to VMCA mode.  
(See the Change the Certificate Mode procedure)

**Step 4.** Add the hosts to the vCenter Server system.

### Certificate Expiration

For ESXi 6.0 and later, you can use the vSphere Client to view information, including expiration, for all certificates that are signed by VMCA or a third party CA. In the vSphere Client, select the host and navigate to **Configure > System > Certificate**. Here you can examine the **Issuer**, **Subject**, **Valid From**, **Valid To**, and **Status** fields. The value of the **Status** field may be **Good**, **Expiring**, **Expiring Shortly**, **Expiration Imminent**, or **Expired**.

A yellow alarm is raised if the certificate's status is **Expiring Shortly** (less than 8 months). A red alarm is raised if the certificate's status is **Expiration Imminent** (less than two months).

By default, each time a host reconnects to vCenter Server, it renews any host certificates whose status is **Expired**, **Expiring immediately**, or **Expiring**. If the certificate is already expired, you must disconnect the host and reconnect it. To renew or fresh the certificates, you can use the following procedure.

**Step 1.** In the vSphere Client, select the host in the navigation pane.

**Step 2.** Navigate to **Configure > System > Certificate**.

**Step 3.** Click one of the following options.

- **Renew:** Retrieves a fresh signed certificate for the host from VMCA.
- **Refresh CA Certificates:** Pushes all certificates in the VECS TRUSTED\_ROOTS store to the host.

**Step 4.** Click **Yes**.

## GENERAL ESXI SECURITY RECOMMENDATIONS

In Chapter 7, you learned that vSphere has built-in security features and that you can take additional steps to harden ESXi. The following items are additional security measures recommended by VMware..

- Limit access to the Direct Console User Interface (DCUI), the ESXi Shell, and SSH. If you allow access to these items, which have privileged access to certain ESXi components, ensure that only trusted users have access and that timeouts are set.
- Do not directly access ESXi hosts that are managed by vCenter Server. Although it may be possible to access the host via DCUI, SSH, ESXi Shell, API or VMware Host Client, you should not normally do so. Instead, use the vSphere Client (or vSphere Web Client) or API connected to vCenter Server to manage the ESXi. Host.
- Only use the DCUI for troubleshooting. Likewise, only use root access to the ESXi Shell for troubleshooting.
- When upgrading ESXi components, only use VMware sources. Although the host runs several third-party packages, VMware only supports upgrades to those packages from VMware sources. Check third-party vendor sites and the VMware knowledge base for security alerts.
- You should follow the VMware security advisories at <http://www.vmware.com/security/>.
- Configure ESXi hosts with host profiles, scripts, or some other automation.

## Configure ESXi Using Host Profiles

You can use host profiles to set up standard, secured configurations for your ESXi hosts and automate compliance.

You can consider any setting that is applied by a host profile to be important to ensuring that your hosts are secured. Some settings, like direct ESXi permissions, may be obvious. Other settings, like NTP settings may not be obvious, but time synchronization issues impact integration with Active Directory which impacts user authentication. Network settings, like physical NIC speed, could impact the ability of the host to connect to the proper management network.

As covered in [Chapter 8](#), host profiles can be used to apply many host configuration settings, including security measures, such as ESXI level permissions. You can use the vSphere Client to configure a host profile for a reference host and apply the host profile to a set of hosts. You can also use host profiles to monitor hosts for host configuration changes. You can attach the host profile to a cluster to apply it to all hosts in the cluster. The high level steps are:

**Step 1.** Set up the reference host to specification and create a host profile.

**Step 2.** Attach the profile to a host or cluster.

**Step 3.** Apply the host profile from the reference host to other hosts or clusters

To ensure that an ESXi host is properly configured according to your standards, you can check for its compliance to its attached host profile. You can use the results to identify non-compliant settings on the host and remediate with the host profiles settings. You can use these steps to check compliance.

**Step 1.** Navigate to Host Profiles main view.

**Step 2.** Right click a host profile.

**Step 3.** Click Check Host Profile Compliance

The compliance status is for each ESXi host is Compliant, Unknown, or Non-compliant. Non-compliant status indicates specific inconsistency between the profile and the host, which you should remediate. Unknown status indicates that the compliance of the host is not known, because it could not be verified. A common root cause is that the host is disconnected. You should resolve the issue and re-check compliance.

## Use Scripts to Manage Host Configuration Settings

Another means to establish a standard, secured configuration for ESXi hosts in your vSphere environment is to use vSphere PowerCLI, ESXCLI, or custom code leveraging the vSphere API.

**Note**

Starting with vSphere 7.0, the vSphere CLI package is end of life. Its capabilities are supported with more API centric tools such as ESXCLI and Perl SDK.

From the ESXi Shell, you can use the ESXCLI command set to configure the host and to perform administrative tasks. ESXCLI provides a collection of namespaces as a mechanism for an administrator to quickly discover the precise command necessary for a specific task. For example, all the commands to configure networking exist in the **esxcli network** namespace, and all the commands to configure storage exist in the **esxcli storage** namespace. Each namespace is further divided into child namespaces that comprise various functions performed under the parent namespace. For example, the **esxcli storage** parent namespace contains a **core** namespace that deals with storage adapters and devices and a **nmp** namespace that deals with path selection and storage array types. Therefore, a typical ESXCLI command is composed of multiple namespaces, where each additional namespace is used to narrow the scope of

the command, ending with the actual operation to be performed.

To identify the proper ESXCLI command to perform a specific task, you can begin by entering **esxcli** at the command prompt in the ESXi Shell. Because it is not a command by itself, just the entry point to the namespace hierarchy, the results will show the first level of the namespace hierarchy. The first level of available namespaces includes **device**, **esxcli**, **fcoe**, **graphics**, **hardware**, **iscsi**, **network**, **nvme**, **rdma**, **sched**, **software**, **storage**, **system**, **vm**, and **vsan**. You can use the brief description of each namespace shown in the results to identify which namespace is most likely to serve your need. Press the up-arrow key on the keyboard to retrieve the last entered namespace and add the name for the next namespace. You can continue reviewing namespaces until you discover the command you need.

For example, if you are seeking a command to list all standard virtual switches, you could enter **esxcli network** to learn that it contains several namespaces, including one named **vswitch**. Likewise, could then enter **esxcli network vswitch** and learn that its namespaces are **standard** and **dvs**. Going further, you could learn that the **esxcli network vswitch standard** namespace contains the **list**. You can conclude that the command you need is **esxcli network vswitch standard list**. A few other sample ESXCLI commands are shown in Table 12-2,

**Table 12-2** Sample ESXCLI commands

Commands	Purpose and Details
<b>esxcli system account add</b>	Create a ESXi host local user account
<b>esxcli system account set</b>	Configure an ESXi host local user account
<b>esxcli system account list</b>	List ESXi host local user accounts
<b>esxcli system account remove</b>	Delete an ESXi host local user accounts
<b>esxcli network ip dns server list</b>	List the host's DNS servers.
<b>esxcli network nic list</b>	List the ESXi host physical network adapters
<b>esxcli system settings advanced get /UserVars/ESXiShellTimeOut</b>	Display the shell interactive timeout for the host.

Likewise, you can use PowerCLI to manage and configure a vSphere environment. When connecting to a vCenter Server environment, the functionality scope of PowerCLI is similar to the functionality scope of using the vSphere Client with the vCenter Server. Table 12-3 describes a few popular PowerCLI commands.

**Table 12-3** Sample PowerCLI commands

Command	Purpose	Example
<b>Connect-VIServer</b>	Connect to a vCenter Server	Connect-VIServer vc01 -User administrator@vsphere.local  Connects to a vCenter Server named vc01 as user administrator@vsphere.local
<b>Get-VMHost</b>	Retrieve information about one or more ESXi hosts	Get-VMHost -Location MyDC Retrieves details about all ESXi hosts in a datacenter named MyDC.
<b>Set-VMHost</b>	Change a setting or state of an ESXi host.	Set-VMHost -VMHost Host -State "Disconnected" Disconnects the host from vCenter Server

If you want to develop code using other tools, you may want to get familiar with vSphere REST APIs. To do so, you can browse to the FQDN of your vCenter Server and select **Browse vSphere REST APIs**. In vCenter Server 7.0, this link takes you to the **Developer Center > API Explorer** in the vSphere Client. Here you can learn how to make GET and POST calls to query and modify the state and configuration of your ESXi hosts and other vSphere objects.

## ESXi Passwords and Account Lockout

For direct ESXi host access, you can use local root account and additional user accounts that you create directly on the host. When setting a password on these accounts, you must comply with or modify the predefined requirements. ESXi uses the Linux PAM module `pam_passwdqc` for password management and control. You can change the required length, change character class requirement, and allow pass phrases using the `Security.PasswordQualityControl` advanced option.

**Note**

The default requirements for ESXi passwords can change from one release to the next. You can check and change the default password restrictions using the **Security.PasswordQualityControl** advanced option.



One step to harden an ESXi host is to harden the password required to use its predefined, local administrator account, which is called root. By default, the ESXi host enforces passwords for its local user accounts, which may be used to access the host via the Direct Console User Interface (DCUI), the ESXi Shell, Secure Shell (SSH) or the vSphere Client. Starting with ESXi 6.0, the default password policy must contain characters from at least three character classes (of the four character classes, which are lowercase letters, uppercase letters, numbers and special characters) and must be at least seven characters long.

**Note**

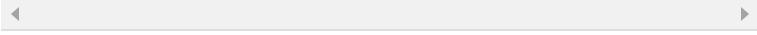
An uppercase character that begins a password and a number that ends a password do not count toward the number of used character classes. The password cannot contain a dictionary word or part of a dictionary word.

For example, **xQaT3!A** is a an acceptable password, because it contains 4 character classes and 7 characters. But, **Xqate!3** is not an acceptable password, because it only contains two character classes as the leading **X** and ending **3** do not count toward the number of used character classes. You can modify the ESXi password requirements using the ESXi host **Security.PasswordQualityControl** advanced option. You can set **Security.PasswordQualityControl** to configure the ESXi host to accept pass phrases, which it does not accept by default. The key to changing the password and pass phrase requirements is understanding the syntax and functionality of the

**Security.PasswordQualityControl** parameter,  
whose default value is

---

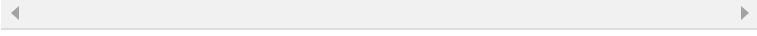
```
retry=3 min=disabled,disabled,disabled,7,7
```



The first part of the value used for this parameter identifies the number of retries allowed for the user following a failed attempt to logon. In the default value, **retry=3** indicates that three additional attempts are permitted following a failed logon. The remainder of the value can be abstracted as

---

```
min=N0,N1,N2,N3,N4
```



where:

- $N_0$  is the minimum number of accepted characters for passwords that contain characters from only one class or disabled to disallow passwords that contain characters from only one class.
- $N_1$  is the minimum number of accepted characters for passwords that contain characters from only two classes or disabled to disallow passwords that contain characters from only two classes.
- $N_2$  is the minimum number of accepted characters for pass phrases or disabled to disallow passphrases. Additionally, to require a passphrase, append passphrase= $N$  to the end of the value, where  $N$  specifies the minimum number of words, separated by spaces, in the passphrase.
- $N_3$  is the minimum number of accepted characters for passwords that contain characters from only three classes or disabled to disallow passwords that contain characters from only three classes.

- $N_4$  is the minimum number of accepted characters for passwords that contain characters from all four classes.

For example, to require a passphrase with a minimum of 16 characters and 3 words, set the Security.PasswordQualityControl to

```
retry=3 min=disabled,disabled,16,7,7,passphrase=3
```

The password requirements in ESXi 6.0 are implemented by pam\_passwdqc. For more details, see the man pages for pam\_passwdqc.

In vSphere 6.x, account locking is supported for access through SSH and through the vSphere Web Services SDK. The Direct Console Interface (DCUI) and the ESXi Shell do not support account lockout. By default, a maximum of ten failed attempts is allowed before the account is locked. The account is unlocked after two minutes by default. You can modify the lockout behavior using the host's advanced options:

- **Security.AccountLockFailures**: Maximum number of failed login attempts before a user's account is locked. Zero disables account locking.
- **Security.AccountUnlockTime**: Number of seconds that a user is locked out.

## SSH and ESXi Shell Security

You can use SSH to remotely log in to the ESXi Shell and perform troubleshooting tasks for the host. SSH configuration in ESXi is enhanced to provide a high security level. VMware does not support Version 1 SSH protocol and uses Version 2 protocol exclusively. SSH supports only 256-bit and 128-bit AES ciphers for your connections.

The ESXi Shell is disabled by default on ESXi hosts. If necessary, you can enable local and remote access to the shell. But, to reduce the risk of unauthorized access, you should only enable the ESXi Shell when troubleshooting. If the ESXi Shell or SSH is enabled and the host is placed in lockdown mode, accounts on the Exception Users list who have administrator privileges can use these services. For all other users, ESXi Shell or SSH access is disabled. Starting with vSphere 6.0, ESXi or SSH sessions for users who do not have administrator privileges are closed.

If the ESXi Shell is enabled, you can still log in to it locally, even if the host is running in lockdown mode. To enable local ESXi Shell access, enable the ESXi Shell service. To enable remote ESXi Shell access, enable the SSH service.

**Note**

The root user and users with the Administrator role can access the ESXi Shell. Users who are in the Active Directory group ESX Admins are automatically assigned the Administrator role. By default, only the root user can run system commands (such as `vmware -v`) by using the ESXi Shell.

You can use the following procedure to enable the ESXi Shell.

**Step 1.** In the vSphere Client, select the host in the navigation pane.

**Step 2.** Navigate to Configure > Services.

**Step 3.** Select **ESXi Shell** and click **Start**.

**Step 4.** Optionally, select Edit Startup Policy and select one of the following options.

- Start and stop manually
- Start and stop with host
- Start and stop with port usage

## **Step 5.** Click OK

You can use a similar procedure to control local and remote access to the ESXi Shell by configuring the startup policy for DCUI and SSH services.

To increase security, you can set ESXi Shell Timeout. The availability timeout setting is the amount of time that can elapse before you must log in after the ESXi Shell is enabled. After the timeout period, the service is disabled, and users are not allowed to log in. To set the timeout, you can use this procedure.

**Step 1.** Browse to the host in the vSphere Web Client inventory.

**Step 2.** Click Configure.

**Step 3.** Under System, select Advanced System Settings.

**Step 4.** Select UserVars.ESXiShellTimeOut and click Edit.

**Step 5.** Enter the idle timeout setting.

**Step 6.** You must restart the SSH service and the ESXi Shell service for the timeout to take effect.

**Step 7.** Click OK

Likewise, you can set a timeout for idle ESXi Shell sessions. The idle timeout is the amount of time that can elapse before a user is logged out of an idle interactive session. You can control the amount of time for both local and remote (SSH) session from the Direct Console Interface (DCUI) or from the vSphere Web Client using the following procedure.

**Step 1.** Browse to the host in the vSphere Web Client inventory.

**Step 2.** Click Configure.

**Step 3.** Under System, select Advanced System Settings.

**Step 4.** Select

**UserVars.ESXiShellInteractiveTimeOut**, click the **Edit** icon, and enter the timeout setting.

**Step 5.** Restart the ESXi Shell service and the SSH service for the timeout to take effect.

**Step 6.** If the session is idle, users are logged out after the timeout period elapses.

An SSH key can allow a trusted user or script to log in to a host without specifying a password. You can upload the authorized keys file for the root user, a RSA key, or a RSA public key to a host. To upload a RSA public key to a host, you can use the following `vifs` command.

```
vifs --server hostname --username username --put file
```

To upload an RSA key or root user authorized key files, use the same command change the target to  
**/host/ssh\_host\_rsa\_key** or  
**/host/ssh\_root\_authorize\_keys**, respectively.

## PCI and PCIe Devices and ESXi

You can use the VMware DirectPath I/O feature to pass through a PCI or a PCIe device to a virtual machine, but this results in a potential security vulnerability. This could be triggered when buggy or malicious code, such as a device driver, is running in privileged mode in the guest OS. So, you should use PCI or PCIe passthrough to a virtual machine *only* if a trusted entity owns and administers the virtual machine. Otherwise, you risk that the host may be compromised by the following:

- The guest OS might generate an unrecoverable PCI or PCIe error
- The guest OS might generate a Direct Memory Access (DMA) operation that causes an IOMMU page fault on the ESXi host.
- If the operating system on the ESXi host is not using interrupt remapping, the guest OS might inject a spurious interrupt into the ESXi host on any vector

To enable passthrough for a network device on a host, you can use the following procedure.

**Step 1.** In the vSphere Client, select the host in the navigation pane.

**Step 2.** Navigate to Configure > Hardware > PCI Devices and click Edit

**Step 3.** Select a device with a green icon and click **OK**

**Note**

An orange icon indicates the status of the device has changed and you must reboot the host before you can use the device.

## Disable the Managed Object Browser

The managed object browser (MOB) provides you with a means to explore the VMkernel object model. Starting with vSphere 6.0 the MOB is disabled by default to avoid malicious configuration changes or actions. You can enable and disable the MOB manually. VMware recommends that you do not enable MOB in production systems.

To enable the MOB using the vSphere Client, you can use the following procedure.

**Step 1.** In the vSphere Client, select the host in the inventory.

**Step 2.** In the right pane, click the **Configuration** tab.

**Step 3.** Select System > Advanced Settings and click **Edit**.

**Step 4.** Select `Config.HostAgent.plugins.solo.enableMob` and set its value to `true`

## ESXi Networking Security Recommendations

Chapter 7 provides VMware general network security recommendations for vSphere. Concerning each ESXi host, you can summarize the network isolation into the following categories.

- vSphere Infrastructure networks: Isolate these networks for their specific functions, such as vMotion vSphere Fault Tolerance, storage and vSAN. In many cases you may not need to route these networks outside a single rack.
- Management Network: This network carries client API, and third-party software traffic. Isolate this network such that it is only accessible by the appropriate administrators and systems. Consider using a jump box or a virtual private network (VPN).
- Virtual machine networks: May involve many networks, each with unique isolation requirements. Consider using virtual firewall solutions, such as NSX.

## ESXi Web Proxy Settings

If you configure a Web proxy, consider the following.

- Do not use certificates that use a password or pass phrases. ESXi does not support Web proxies with passwords or pass phrases, which are also known as encrypted keys.
- If you want to disable SSL for vSphere Web Services SDK connections, you can change the connection from HTTPS to HTTP. You should only consider this if you have a fully trusted environment, where firewalls are in place and transmissions to and from the host are fully isolated.
- Most internal ESXi services are accessible only through port 443. Port 443 acts as a reverse proxy for ESXi. You can change the configuration to allow direct HTTP connections, but should only consider it for a fully trusted environment.
- During upgrades, the certificate remains in place.

## **vSphere Auto Deploy Security Considerations**

If you use vSphere Auto Deploy, consider the networking security, boot image security, and potential password exposure through host profiles.

Secure the Auto Deploy network as you would secure the network for any PXE-based deployment method. Auto Deploy transfers data over SSL, but it does not check the authenticity of the client or of the Auto Deploy server during a PXE boot.

The boot image includes host's public and private SSL key and certificate. If Auto Deploy rules are set up to provision the host with a host profile or host customization, then the boot image includes the host profile and host customization. The root password and user passwords in the host profile and host customization are hashed with SHA-512. Other

passwords, such as those to setup Active Directory using the host profile, are not protected. You can use vSphere Authentication Proxy to avoid exposing Active Directory passwords.

Ideally, you should completely isolate the Auto Deploy network.

## Control CIM Access

Common Information Model (CIM) is an open standard that defines a framework for agent-less, standards-based monitoring of ESXi host hardware resources. The framework consists of a CIM broker and a set of CIM providers. Hardware vendors, including server manufacturers and hardware device vendors, can write providers that monitor and manage their devices. VMware writes CIM providers that monitor server hardware, ESXi storage infrastructure, and virtualization-specific resources. These lightweight providers run inside the ESXi host and perform specific management tasks.

Instead of using root credentials, create a less-privileged vSphere user account to provide to remote applications that access the CIM interface. The required privilege for the user account is **Host.CIM.Interaction**.

Use the VIM API ticket function to issue a session ID (ticket) to the user account to authenticate to CIM. Ensure the account is granted permission to obtain CIM tickets.

When you install a third-party CIM VIB, the CIM service starts. If you need to manually enable the CIM service, you can use the following command.

```
esxcli system wbem set -e true
```

You can use the API SDK of your choice to call **AcquireCimServicesTicket** to return a ticket that you can use to authenticate the user with vCenter Server using CIM-XML port 5989 or WS-Man port 433 APIs.

## CONFIGURE AND MANAGE ESXi SECURITY

This section provides procedures for securing ESXi.

### Configure ESXi Firewall

By default, the ESXi firewall is configured to block incoming and outgoing traffic, except traffic for services that are enabled in the hosts' security profile. The firewall also allows Internet Control Message Protocol (ICMP) pings. Prior to opening any ports on the firewall, you should consider the impact it may have for potential attacks and unauthorized user access. You can reduce this risk by configuring the firewall to only allow communication on the port with authorized networks. To modify the firewall's rule set, you can use the vSphere Client to modify the host's security profile using this procedure.



**Step 1.** In the vSphere Client, select the host in the inventory pane.

**Step 2.** Navigate to Configure > System > Firewall.

**Step 3.** Select the appropriate service name, such as the incoming SSH Server (TCP 22) or the outgoing DNS client (TCP / UDP 53), and click **Edit**.

**Step 4.** Examine the rule set. Change the state of any rule by selecting the rule (place a check in the rule's box) to enable the rule or de-select the rule to disable.

**Step 5.** Optionally, for some services, you can uncheck the **Allow connections from any IP address box** and enter specific IP addresses in the accompanying text box to restrict use to only those IP addresses.

**Step 6.** Click **OK**.

When specifying specific IP addresses in Firewall settings, you can use the formats used in the following examples.

- 192.168.10.0/24
- 192.168.11.2, 2001::1/64
- fd3e:29a6:oa79:e462::/64

The NFS Client firewall rule set behaves differently than other rule sets. ESXi configures NFS Client settings when you mount or unmount an NFS datastore. When you mount an NFS v3 datastore, the following events occur.

- If the nfsClient rule set is disabled, ESXi enables the rule set, sets **allowedAll** to FALSE, and adds the NFS Server IP address to the list of allowed IP addresses.
- If the nfsClient rule set is enabled, ESXi adds the NFS Server IP address to the list of allowed IP addresses but does not change the state of the rule set or **allowedAll**.

When you mount an NFS v4.1 datastore, the following events occur.

- ESXi enables the nfs41client rule set, sets **allowedAll** to TRUE.

When you remove or unmount an NFS v3 datastore from a host, ESXi removes the IP address from the list of allowed IP addresses. When you remove or unmount the last NFS v3 datastore, ESXi stops the nfsClient rule set. Unmounting an NFS v4.1 datastore does not impact the firewall.

The ESXi software firewall is enabled by default. It should never be disabled while running production virtual machines. In rare cases, such as a temporary troubleshooting measure, you can disable the ESXi firewall using the **esxcli network firewall set --enabled false** command.

## Customize ESXi Services

Several optional services that are provided in an ESXi host are disabled by default. VMware disables these services to provide strong security out of the box. In a default installation, you can modify the status of the following services from the vSphere Client.

- **Running Services:** Direct Console UI, Load-Based Teaming Daemon, CIM Server, VMware vCenter Agent
- **Stopped Services:** ESXi Shell, SSH, attestd, kmxd, Active Directory Service, NTP Daemon, PC/SC Smart Card Daemon, SNMP Server, Syslog Server, X.Org Server

In some circumstances, you may wish to configure and enable these services. A good example of an optional service that you may decide to configure and enable in most environments is NTP, because solid time synchronization is vital for many services. For another example, you may wish to temporarily enable Secure Shell (SSH) service while troubleshooting. To enable,

disable, and configure these services, you can use the following procedure.

**Step 1.** In the vSphere Client, select the host in the navigation pane.

**Step 2.** Navigate to Configure > Services.

**Step 3.** Select a service that you wish to modify and click **Start**, **Stop** or **Restart** to immediately change the state of the service

**Step 4.** To change the behavior permanently, click **Edit Startup Policy** and choose from the following options:

- **Start and stop with port usage.**
- **Start and stop with host.**
- **Start and stop manually.**

**Step 5.** Click **OK**.

## Use Lockdown Mode

In vSphere 5.0 and earlier, only the root account can log into the DCUI on an ESXi host that is in lockdown mode.

In vSphere 5.1 and later, you can add a user to the `DCUI .Access` advanced system setting to grant the user access to the DCUI on a host that is in lockdown mode, even if the user is not granted the Administrator role on the host. The main purpose of this feature is to prepare for catastrophic failures of vCenter Server.

vSphere 6.0 and later includes an `Exception Users` list, whose main purpose is to support the use of lockdown mode, but still support service accounts, which must logon directly to the ESXi host. User accounts in the `Exception Users` list, who have administrator privileges can logon to the DCUI and ESXi Shell.

As described in Chapter 7, you can place a host in normal lockdown mode, strict lockdown mode, or normal mode.

To change the lockdown mode setting, you can use the followings procedure.

**Step 1.** In the vSphere Client, select an ESXi host in the navigation pane.

**Step 2.** Navigate to Configure > Security Profile.

**Step 3.** In the **Lockdown Mode** panel, click the **Edit** button.

**Step 4.** Click **Lockdown Mode** and choose either **Normal** or **Strict**.

**Step 5.** Click **OK**.

By default, the root account is included in DCUI.Access. You could consider removing the root account from DCUI.Access and replacing it with another account for better auditability.

Table 12-4 provides details for the behavior of an ESXi host in lockdown mode.

---

**Table 12-4** ESXi Lockdown Mode Behavior

Service	Normal Mode	Normal Lockdown Mode	Strict Lockdown Mode
vSphere Web Services API	All users, based on permissions	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
CIM Providers	Users with administrator privileges on the host	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)	vCenter (vpxuser) Exception users, based on permissions vCloud Director (vslauser, if available)
Direct Console UI (DCUI)	Users with administrator privileges on the host, and users in the DCUI.Access advanced option	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	DCUI service is stopped.
ESXi Shell (if enabled)	Users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host
SSH (if enabled)	Users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host	Users defined in the DCUI.Access advanced option Exception users with administrator privileges on the host

## Manage the Acceptance Levels of Hosts and VIBs

VIBs are software packages that include a signature from VMware or a VMware partner. To protect the integrity of the ESXi host, do not allow users to install unsigned (community-supported) VIBs. An unsigned VIB contains code that is not certified by, accepted by, or supported by VMware or its partners. Community-supported VIBs do not have a digital signature. The host's acceptance level must be the same or less restrictive than the acceptance level of any VIB you want to add to the host. For example, if the host acceptance level is `VMwareAccepted`, you cannot install VIBs at the `PartnerSupported` level. You should use extreme

caution when allowing **CommunitySupported** VIBs.

The following list contains details on defined VIB acceptance levels.



- **VMwareCertified:** VIBs go through thorough testing equivalent to VMware in-house Quality Assurance testing, for the same technology. Only I/O Vendor Program (IOVP) program drivers are published at this level. VMware takes support calls for VIBs with this acceptance level.
- **VMwareAccepted:** VIBs go through testing that is run by a partner and verified by VMware. CIM providers and PSA plug-ins are among the VIBs published at this level. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
- **PartnerSupported:** VIBs that are published by a partner that VMware trusts. The partner performs all testing, but VMware does not verify. VMware directs support calls for VIBs with this acceptance level to the partner's support organization.
- **CommunitySupported:** VIBs that have not gone through any VMware-approved testing program and are not supported by VMware Technical Support or by a VMware partner.

To change the host acceptance level, you can use the following command.

---

```
esxcli --server=<server_name> software acceptance set
```

## Assign Privileges for ESXi Hosts

Typically, users should access vSphere via vCenter Server, where privileges are managed centrally. For use cases where some users access ESXi hosts directly, you can manage privileges directly on the host. The following roles are predefined directly in ESXi

- **Read Only:** Ability to view, not change assigned objects
- **Administrator:** Ability to change assigned objects
- **No Access:** No access to assigned objects. This role is the default role, which you can override.

In vSphere 6.0 and later, you can use the ESXCLI to manage local user accounts and to configure permissions on local and Active Directory accounts. You can connect directly to the ESXi host using the VMware Host Client and navigate to **Manage > Security & Users > Users** to create, edit, and remove local user accounts.

The following user accounts exists on an ESXi host that is not added to a vCenter System

- **root:** A user account that is created and assigned the Administrator role by default on each ESXi host
- **vpxuser:** A local ESXi user account that is created, managed, and used for management activities by vCenter Server.
- **dcui:** A user account that acts as an agent for the direct console and cannot be modified or used by interactive users.

**Note**

You can remove the access privileges for the root user. But you should first create another user account on the root level and assign it the Administrator role.

Much like vCenter Server, each ESXi host uses role-based permission for users who logon directly to the

ESXi host rather than accessing the host through vCenter Server. ESXi allows the creation of custom roles, but these roles are only applied when a user logs directly onto the host, such as when the user uses the VMware Host Client to connect to the host directly. In most cases, managing roles and permissions at the host level should be avoided or minimized. To create, edit, and remove roles, you can connect directly to an ESXi host using the VMware Host Client and navigate to **Manage > Security & users > Roles**.

## Use Active Directory to Manage ESXi Users

In scenarios where multiple users need to access multiple ESXi hosts directly (rather than accessing vCenter Server), you face challenges in synchronizing user names and passwords. To address the challenges, consider joining the hosts to Active Directory and assigning roles to specific AD users and groups. Then require users to provide their Active Directory credentials when logging directly to the host.

In scenarios where Active Directory users need to access an ESXi directly, you need to add the host to a directory service and apply permissions to those users. You can use the following steps to add an ESXi Host to an Active Directory domain.

**Step 1.** Verify that an Active Directory domain is available.

**Step 2.** Ensure that the host name of the ESXi host is fully qualified with the domain name that matches the domain name of the Active Directory forest. For example, if the Active Directory domain name is `mydomain.com` and the ESXi host name is `host-01`, then the host

fully qualified name is host-  
01.mydomain.com.

**Step 3.** Synchronize time between the ESXi host and domain controllers using NTP.

**Step 4.** Ensure the DNS is configured and ESXi host can resolve the host names of the Active Directory domain controllers.

**Step 5.** In the vSphere Client, select the ESXi host in the inventory pane.

**Step 6.** Navigate to Configure > Authentication Services

**Step 7.** Click Join Domain.

**Step 8.** In the dialog box, specify the domain and user credentials. Optionally, specify a proxy server.

**Step 9.** Enter a domain, either in the form *name.tld* or in the form *name.tld/container/path*, where *name.tld* is the domain name and */container/path* is an optional path to an organization unit, where the host computer object should be created. For example, you can use `domain.com/ou01/ou02`. to add the host to an organization unit named `ou02` that resides in an organization unit named `ou01` in a domain named `domain.com`.

**Step 10.** Click OK.

## Configure vSphere Authentication Proxy

You can use vSphere Authentication Proxy to add hosts to an Active Directory domain, instead of adding hosts to the domain explicitly. When vSphere Authentication Proxy is enabled, it automatically adds hosts that are being provisioned by Auto Deploy to the

Active Directory domain. You can also use vSphere Authentication Proxy to add hosts that are not provisioned by Auto Deploy.

To start the vSphere Authentication Proxy Service and add a domain, you can use the following procedure.

**Step 1.** Logon to the vCenter Server Management Interface (VAMI) as root.

**Step 2.** Select **Services > VMware vSphere Authentication Proxy**.

**Step 3.** Click **Start**.

**Step 4.** In the vSphere Client, select the vCenter Server in the inventory pane.

**Step 5.** Select **Configure > Authentication Proxy > Edit**.

**Step 6.** Enter the domain name and credentials of a user who can hosts to the domain

**Step 7.** Click **Save**.

Now, you can add a host to an Active Directory domain using the previously provided procedure, but this time, select the **Using Proxy Server** option.

## **Configure Smart Card Authentication for ESXi**

As an alternative to specifying a user name and password, you can use smart card authentication to log in to the ESXi Direct Console User Interface (DCUI) by using a Personal Identity Verification (PIV), Common Access Card (CAC) or SC650 smart card. In this case, the DCUI prompts for a smart card and PIN combination. To configure smart card authentication, you should setup the smart card infrastructure (AD domain accounts, smart card readers, smart card, etc.), configure ESXi to

join an AD domain that supports smart card authentication, use the vSphere Client to add root certificates, and follow these steps.



**Step 1.** In the vSphere Client, select the host in the inventory pane.

**Step 2.** Navigate to Configure > Authentication Services.

**Step 3.** In the Smart Card Authentication panel, click **Edit**.

**Step 4.** In the dialog box, select the **Certificates** page.

**Step 5.** Add trusted Certificate Authority (CA) certificates, for example, root and intermediary CA certificates, in the PEM format.

**Step 6.** Open the Smart Card Authentication page, select the **Enable Smart Card Authentication** check box, and click **OK**

## Configure UEFI Secure Boot for ESXi Hosts

Starting with vSphere 6.5, ESXi supports UEFI secure boot, which you can enable in the UEFI firmware. With secure boot enabled, a machine refuses to load any UEFI driver or app unless the operating system bootloader is cryptographically signed. In vSphere 6.5 and later, the ESXi bootloader contains and uses a VMware public key to verify the signature of the kernel and a small subset of the system that includes a secure boot VIB verifier that verifies each VIB packages installed on the host.

**Note**

You cannot perform a secure boot on ESXi servers that were upgraded by using ESXCLI commands because the upgrade does not update the bootloader.

You can use the following command to run the Secure Boot Validation script on an upgraded ESXi host to determine if it supports Secure Boot. The output is either Secure boot can be enabled or Secure boot CANNOT be enabled.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

To resolve issues with secure boot, you can follow these steps.

**Step 1.** Reboot the host with secure boot disabled.

**Step 2.** Run the secure boot verification script

**Step 3.** Examine the information in the  
`/var/log/esxupdate.log` file

## Securing ESXi Hosts with Trusted Platform Module

ESXi 6.7 can use Trusted Platform Modules (TPM) version 2.0 chips, which are secure cryptoprocessors that enhance host security by providing a trust assurance rooted in hardware. A TPM 2.0 chip attests to an ESXi host's identity. Host attestation is the process of authenticating and attesting to the state of the host's software at a given point in time. UEFI secure boot, which ensures that only signed software is loaded at boot time, is a requirement for successful attestation. The TPM 2 chip securely stores measurements of the software modules loaded in the ESXi host and vCenter Server remotely verifies. The automated high level steps of the attestation process are:

**Step 1.** Establish the trustworthiness of the remote TPM and create an Attestation Key (AK) on it.

**Step 2.** Retrieve the Attestation Report from the host.

**Step 3.** Verify the host's authenticity

To use TPM 2.0 chips, you should ensure your vSphere environment meets these requirements:

- vCenter Server 6.7
- ESXi 6.7 host with TPM 2.0 chip installed and enabled in UEFI
- UEFI Secure Boot enabled

Additionally, you should Ensure that the TPM is configured in the ESXi host's BIOS to use the SHA-256 hashing algorithm and the TIS/FIFO (First-In, First-Out) interface and not CRB (Command Response Buffer).

During the boot of an ESXi host with an installed TPM 2.0 chip, vCenter Server monitors the host's attestation status. The vSphere Client displays the hardware trust status in the vCenter Server's Summary tab under Security with the following alarms:

- Green: Normal status, indicating full trust.
- Red: Attestation failed

If the **Host secure boot was disabled** message appears in the vSphere Client, you must re-enable secure boot to resolve the problem. If the **No cached identity key, loading from DB** message appears, you must disconnect and reconnect the host.

## Secure ESXi Log Files

To increase the security of the host, take the following measures. (For details see Chapter 10, "Monitoring and

Managing Clusters and Resources.)

- Configure persistent logging to a datastore. By default, ESXi logs are stored in a in-memory file system that keeps only 24 hours of data and loses data during host reboot.
- Configure syslog to use remote logging from ESXi hosts to a central host, where you can monitor, search, and analyze logs from all hosts with a single tool.
- Query the syslog configuration to ensure the syslog server and port are valid.

## OTHER SECURITY MANAGEMENT

Managing vSphere security can involve other tasks, such as those described here.



### Key Management Server

In order to use encryption in vSphere, you must be running a Key Management Server (KMS) that has a trust relationship with vCenter Server. To add a KMS server to vCenter Server, you can use the following procedure.

**Step 1.** In the vSphere Client, select the vCenter Server in the inventory pane.

**Step 2.** Navigate to Configuration > Key Management Servers

**Step 3.** Click ADD

**Step 4.** Provide the server name, server address (FQDN), and server port.

**Step 5.** Optionally, provide other appropriate details, such as proxy details and user credentials

**Step 6.** If you are adding the first KMS server in a cluster, provide a cluster name

**Step 7.** Click the radius button next to the KMS server name

**Step 8.** In the Make vCenter Trust KMS window, click **TRUST**

**Step 9.** Click **MAKE KMS TRUST VCENTER**

**Step 10.** Select KMS Certificate and private key, and click **Next**.

**Step 11.** In the next window, next to KMS Certificate, click **Upload File** and open an available certificate PEM file.

**Step 12.** In the same window, next to KMS Private Key, click **Upload File** and open an available certificate PEM file.

**Step 13.** Click the **ESTABLISH TRUST** button

## Change Permission Validation Settings

Periodically, vCenter Server validates its user and group lists against the users and groups in the Windows Active Directory domain. It removes users and groups that no longer exist in the domain. You can change the behavior of this validation by using the vSphere Client edit the general settings of the vCenter Server and change the **Validation** and **Validation Period** options. If you want to disable the validation, deselect the **Validation > Enable** checkbox. If you want to adjust the frequency in which this validation is performed,

enter a value in the **Validation Period** text box to specify a time, in minutes, between validations.

## Configure and Manage vSphere Trust Authority (vTA)

With vSphere Trust Authority (vTA) you can do the following.

- Provide a hardware root of trust and remote attestation to ESXi hosts.
- Restrict the release of encryption keys to only attested ESXi hosts
- Centralize and secure the management of multiple key servers
- Enhance the level of encryption key management that is used to perform cryptographic operations on virtual machines.

With vTA, you can run workloads in secure environment where you detect tampering, disallow unauthorized changes, prevent malware, and verify the hardware and software stacks.

When you configure vTA, you enable The Attestation service and the Key Provider service on the ESXi host in the Trust Authority Cluster. The Attestation Service attests the state of the trusted ESXi hosts using a Trusted Platform Module (TPM) 2.0 chip as its basis for software measurement and reporting. The Attestation Service verifies that the software measurement signature can be attributed to a previously configured trusted TPM endorsement key (EK). The Key Provider Service removes the need for the vCenter Server and the ESXi hosts from requiring direct key server credentials. The Key Provider Service acts as a gatekeeper for the key servers, releasing keys only Trusted ESXi Trusted Hosts.

A Trusted ESXi host must contain a TPM. A TPM is manufactured with an EK, which is a public / private key pair, built into the hardware. You can configure the Attestation Service to trust all CA certificates where the manufacturer signed the TPM (the EK public key) or to trust the host's TOM CA certificate and EK public key.

**Note**

If you want to trust individual ESXi hosts, the TPM must include an EK certificate. Some TPMs do not.

You can use VMware PowerCLI to configure and manage vSphere Trust Authority. Alternatively, you could use vSphere APIs or the vSphere Client for at least some of the activities. To configure vTA, you can perform the following high-level tasks.

**Step 1.** On a Windows system with access to the vTA environment, install PowerCLI 12.0.0, Microsoft .NET Framework 4.8 or greater, and create a local folder.

**Step 2.** Add your user account to the TrustedAdmins groups on the vCenter Server managing the trust authority cluster and on the vCenter Server of the trusted cluster.

**Step 3.** Enable the Trust Authority State.

**Step 4.** Collect information about the trusted hosts in the trusted cluster (using Export-Tpm2CACertificate).

**Step 5.** Import the trusted host data to the trust authority cluster (New-TrustAuthorityPrincipal).

**Step 6.** Create the Trusted Key Provider on the trust authority cluster. (using New-TrustAuthorityKeyProvider)

**Step 7.** Export the trust authority cluster information from the trust authority cluster (using `Export-TrustAuthorityServicesInfo`).

**Step 8.** Import the trusted authority cluster data to the trusted cluster (using `Import-TrustAuthorityServicesInfo`).

**Step 9.** Configure the Trusted Key Provider for the trusted hosts on the trusted cluster (using `Register-KeyProvider` and `Set-KeyProvider`).

After configuring vTA, you can perform management operations, including those summarized in **Table 12-5**.

**Table 12-5** vTA Operations

Operation	Key steps
Start, stop, and restart vTA services.	In the vSphere Client, select the host, navigate to <b>Configure &gt; Services &gt; System</b> , and select <b>Restart, Start, or Stop</b> .
View trust authority hosts	In the vSphere Client, select the trusted cluster's vCenter Server, select <b>Configure &gt; Security &gt; Trust Authority</b> .
View vTA cluster state	In the vSphere Client, select the trust authority cluster's vCenter Server, select <b>Configure &gt; Trust Authority &gt; Trust Authority Cluster</b> .
Restart the Trusted Host service	In an SSH session, enter <code>/etc/init.d/kmxa restart</code> .
Add a trust authority host	Use PowerCLI to run <code>Add-TrustAuthorityVMHost</code> .
Add a trusted host	Use PowerCLI to run <code>Add-TrustedVMHost</code> .
Change the master key of a key provider	Use PowerCLI to run <code>Set-TrustAuthorityKeyProvider</code> .

Most of the vTA configuration and state information is stored on the ESXi hosts in the **ConfigStore** database. Backups of vCenter Server do not include vTA configuration. You can leverage the files that you exported during the configuration of vTA vSphere as your backup. If you need to restore vTA, use the exported files to reconfigure vTA.

## Securing Virtual Machines with Intel Software Guard Extensions (SGX)

You can enable vSGX on a virtual machine on an ESXi host that has compatible CPUs and SGX enabled in the BIOS. The virtual machine must use hardware version 17 or later (set Compatibility to **ESXi 7.0 and later**) and a supported guest OS (Linux, 64 bit Windows 10 or later, or 64 bit Windows Server 2016 or later). To enable vSGX, configure the following hardware settings.

- Select the **Security Devices > SGX > Enable** checkbox.
- Set VM Options > Boot Options > Firmware to **EFI**.
- Set the **Enter Enclave Page Cache (EPC) size** and select **Flexible Launch Control (FLC)** mode.

To enable vSGX, the virtual machine must be powered off. You can enable vSGX as you provision a new virtual machine. To remove vSGX from a virtual machine, uncheck the **Security Devices > SGX > Enable** checkbox.

## Encrypt a Virtual Machine

You can use the following procedure to create a new, encrypted virtual machine

**Step 1.** Establish a trusted connection with the KMS and select a default KMS.

**Step 2.** Create an encryption storage policy, or plan to use the bundled sample, VM Encryption Policy.

**Step 3.** Ensure that you have the Cryptographic operations.Encrypt new privileges.

**Step 4.** If the host encryption mode is not enabled, ensure you have the **Cryptographic operations.Register host** privilege.

**Step 5.** In the vSphere Client, launch the New Virtual Machine wizard.

**Step 6.** In the wizard, provide the following settings to encrypt the virtual machine.

- Compute resource settings: Select a compatible cluster or host. ESXi 6.5 or later is required.
- In the Select Storage settings, select **Encrypt this virtual machine**, select the storage policy (from step 2), and select an appropriate datastore.
- Virtual machine hardware compatibility: Select **ESXi 6.5 and later**.
- Customize hardware settings: Optionally, select **VM Options > Encryption** and select virtual disks to exclude from encryption.

**Step 7.** Complete the wizard and click **Finish**.

To encrypt an existing virtual machine, you can use the following procedure.

**Step 1.** Establish a trusted connection with the KMS and select a default KMS.

**Step 2.** Create an encryption storage policy, or plan to use the bundled sample, VM Encryption Policy.

**Step 3.** Ensure that you have the **Cryptographic operations**.**Encrypt new** privileges.

**Step 4.** If the host encryption mode is not enabled, ensure you have the **Cryptographic operations**.**Register host** privilege.

**Step 5.** Ensure the virtual machine is powered off.

**Step 6.** In the vSphere Client, right-click the virtual machine and **select VM Policies > Edit VM Storage Policies**.

**Step 7.** Select the storage policy (from step 2)

**Step 8.** Optionally, select **Configure per disk** and set encryption as needed for each virtual disk

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

## SUMMARY

You have now read the chapter covering security management for vSphere. You should now use information in the following sections to complete your preparation for Objectives 7.4, 7.5, 7.12.

## REVIEW ALL THE KEY TOPICS

Table 12-6 provides a reference to each of the key topics identified in this chapter. Take a few moments to review each of these specific items.

**Table 12-6** Key Topics

Key Topic Element	Description	Pages
Figure 12-1	vSphere Inventory Hierarchy	
List	Sample Roles	
Paragraph	ESXi password requirements	
Procedure	General Networking Security Recommendations	
Procedure	Modify ESXi firewall rule set	
Paragraph	Lockdown mode levels	
List	VIB acceptance levels	
Procedure	Add a KMS Server to vCenter Server	

## COMPLETE THE TABLES AND LISTS FROM MEMORY

Print a copy of Appendix C, “Memory Tables,” (found on the CD), or at least the section for this chapter, and complete the tables and lists from memory. Appendix D, “Memory Tables Answer Key,” also on the CD, includes completed tables and lists to check your work.

## Definitions of Key Terms

Define the following key terms from this chapter and check your answers in the glossary.

vCenter Single Sign-On Security Token Service (STS)

Certificate Manager

managed object browser (MOB)

Common Information Model (CIM)

vSphere Installation Bundles (VIBs)

## Glossary

**STS:** vCenter Single Sign-On Security Token Service (STS) is a Web service that issues, validates, and renews security tokens.

**Certificate Manager:** Certificate Manager is a command line utility that you can use to generate Certificate Signing Requests (CSRs) and replace certificates for machine and solution users.

**MOB:** The managed object browser (MOB) is a web-based interface that provides you with a means to explore the VMkernel object model.

**CIM:** Common Information Model (CIM) is an open standard that defines a framework for agent-less, standards-based monitoring of ESXi host hardware resources. The framework consists of a CIM broker and a set of CIM providers.

**VIB:** vSphere Installation Bundles (VIBs) are ESXi software packages, created and signed by VMware and

its partners, that contains solutions, drivers, CIM providers, and applications.

## ANSWER REVIEW QUESTIONS

- 1.** You want to add a global permission. Which of the following privileges do you need?

  - a. Permissions.Modify permission**  
privilege on the vCenter root object
  - b. Permissions.Modify permission**  
privilege on the global root object
  - c. Permissions.Add permission** privilege on the vCenter root object
  - d. Permissions.Add permission** privilege on the global root object
- 2.** A yellow alarm is raised due to a hosts' certificate expiration date. Which of the following is a true statement concerning the state of the certificate?

  - a.** The certificate is expired
  - b.** The certificate will expire in less than 2 months
  - c.** The certificate will expire between 2 and 6 months
  - d.** The certificate will expire between 2 and 8 months
- 3.** You set the `Security.PasswordQualityControl` parameter to `retry=3 min=disabled,disabled,disabled,7,7`. With this setting, which of the following statements is true?.

  - a.** You cannot use pass phrases.

- b.** Your password can use just a single character class.
    - c.** Your password must have at least two character classes and 7 letters.
    - d.** Vmware1 is an acceptable password.
- 4.** You configured an ESXi host with a TPM 2.0 chip and enabled UEFI Secure Boot. During the boot, you get this message: No cached identity key, loading from DB. What should you do?
  - a.** Reinstall ESXi
  - b.** Reboot ESXi
  - c.** Re-enable Secure Boot
  - d.** Disconnect the host from the vCenter Server and reconnect.
- 5.** You want to have a backup in case you ever need to restore vSphere Trusted Authority. What should you do?
  - a.** Keep a copy of the files that you exported while configuring vTA
  - b.** In the vSphere Client, choose Backup vTA Configuration
  - c.** Clone the vCenter Server
  - d.** Use the vCenter Server File Backup feature.

# Chapter 13. Manage vSphere and vCenter Server

This chapter covers the following topics:

- [vCenter Server Backup](#)
- [Upgrade to vSphere 7.0](#)
- [Using vSphere Lifecycle Manager](#)
- [Manage ESXi Hosts](#)
- [Monitor and Manage vCenter Server](#)

This chapter contains information related to VMware 2V0-21.20 exam objectives 1.8, 4.4, 4.6, 4.8, 4.11, 4.12, 4.16.1, 5.2, 5.7, 7.10, 7.11, 7.11.1, 7.11.2, 7.11.3, 7.11.4, 7.11.5

[vCenter Server Backup](#)

[Upgrade to vSphere 7.0](#)

[vCenter Server Data Transfer](#)

[Upgrade vCenter Server Appliance](#)

[Migrate vCenter Server for Windows to vCenter Server Appliance](#)

[Upgrade ESXi and Virtual Machines](#)

[Using Update Planner](#)

[Using vSphere Lifecycle Manager](#)

[About VMware Update Manager](#)

[Update Manager Download Service \(UMDS\)](#)

[Baselines and Images](#)

[ESXi Quick Boot](#)

ESXi Firmware Updates

Hardware Compatibility Checks

Export and Import Cluster Image

Backup and Restore Scenarios

Upgrade Virtual Machines

Manage ESXi Hosts

Monitor and Manage vCenter Server

Monitor and Manage vCenter Server with the VAMI

Monitor and Manage vCenter Server with the vSphere Client

Common vCenter Server Management Tasks

Configure Statistics Collection Settings

Verifying SSL Certificates for Legacy Hosts

Update the vCenter Server

Patching with VAMI

Patching with vCenter Server Appliance Shell

Manage the vCenter HA Cluster

Repoint a vCenter Server to Another Domain

This chapter covers topics related to managing vCenter Server and vSphere components.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section. Regardless, the authors recommend that you read the

entire chapter at least once. **Table 13-1** outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 13-1** “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
vCenter Server Backup	1, 2
Upgrade to vSphere 7.0	3, 4
Using vSphere Lifecycle Manager	5-7
Manage ESXi Hosts	8
Monitor and Manage vCenter Server	9, 10

- 1.** You want to backup your vCenter Server. Which one of the following approaches is valid?
  - a.** Use the vSphere Client to perform a file-based backup
  - b.** Use the vSphere Client to perform an image-based backup
  - c.** Use the vCenter Server Management Interface to perform a file-based backup -\*
  - d.** Use the vCenter Server Management Interface to perform an image-based backup
- 2.** You want to backup your vCenter Server. Which one of the following options is not valid?
  - a.** SCP
  - b.** FTP
  - c.** HTTP
  - d.** HTTPS
- 3.** You want to upgrade a vSphere 6.7 environment to vSphere 7.0. Which one of the following is the appropriate order?

- a.** Virtual machines, ESXi, vCenter Server,
  - b.** ESXi, vCenter Server, virtual machines.
  - c.** vCenter Server, ESXi, virtual machine hardware, VMware Tools
  - d.** vCenter Server, ESXi, VMware Tools, virtual machine hardware
- 4.** You plan to upgrade a Windows based vCenter Server to vCenter Server appliance 7.0 and want to transfer data in the background. Which of the following can be included in the background transfer?
  - a.** Configuration data only
  - b.** Configuration data and performance data.
  - c.** Historical and performance data
  - d.** Data from the embedded database.
- 5.** You are preparing to use Lifecycle Manager. Which one of the following is the smallest, installable software package (metadata and binary payload) for ESXi?
  - a.** An Update
  - b.** An Upgrade
  - c.** A Patch
  - d.** A VIB
- 6.** You want to enable Quick Boot for the hosts in your vSphere Cluster. In the vSphere Client, where should you navigate?
  - a. Menu > Lifecycle Manager**
  - b. Menu > Host and Clusters > DRS cluster settings**

- c. Menu > Host and Clusters > HA Cluster settings**
  - d. Menu > Host and Clusters > ESXi host settings**
7. You want to use Lifecycle Manager to update ESXi Firmware. Which of the following is a requirement?
- a. Firmware baselines**
  - b. VMware provided add-on**
  - c. Vendor provided plug-in**
  - d. Vendor provided baselines**
8. You want to manage the services running in an ESXi host. Which of the following actions are not available using the Host Client?
- a. Start a service**
  - b. Stop a service.**
  - c. Remove a service**
  - d. Change a service's policy**
9. You are using examining the Health State in the vCenter Server Management Interface (VAMI). What color indicates an Alert, where one or more components may be degraded?
- a. Red**
  - b. Orange**
  - c. Yellow**
  - d. Gray**
10. You are repointing a vCenter Server to an existing domain. Which one of the following is not a valid resolution setting involving conflicts?

**a.** Delete

**b.** Copy

**c.** Skip

**d.** Merge

## VCENTER SERVER BACKUP

To provide backup and recovery protection for your vCenter Server, you can use the integrated file-based backup feature. Alternatively, you can perform image-based backups using the vSphere API.

The vCenter Server Management Interface (VAMI) provides a file-based backup feature for the vCenter Server. If you need to restore the vCenter Server, you can use the vCenter Server Installer to deploy a new vCenter Server Appliance and to restore the database and configuration from the file-based backup. You can configure the backup to stream the data to a target using FTP, FTPS, HTTP, HTTPS, SFTP, NFS, or SMB.

When planning the vCenter Server backup, you should consider the following details.

- When a vCenter Server High Availability cluster is involved in a backup, only the primary vCenter Server is backed up.
- Protocol Considerations:
  - FTP and HTTP are not secure protocols.
  - Backup servers must support at least of 10 simultaneous connections for each vCenter Server

- You must have read and write permissions on the backup target.
- FTPS only supports explicit mode
- HTTP or HTTPS requires WebDAV on the backup Web server
- To support an HTTP proxy server, you can use only FTP, FTPS, HTTP, or HTTPS.
- You can use IPv4 or IPv6 URLs for the vCenter Server and file backup, but mixed IP versions between the backup server and the vCenter Server is unsupported.
- The vCenter Server Management API is required to restore from NFS or SMB based backups.
- After a restore completes, the following configurations are restored.
  - Virtual machine resource settings
  - Resource pool hierarchy and setting
  - Cluster-host membership
  - DRS configuration and rules
- The state of various vSphere components may change following a restore, depending on changes that were made since the backup. For example, the following items may be impacted.
  - Storage DRS datastore cluster configuration and membership.
  - Standby mode for some ESXi hosts where DPM is used.
  - Distributed switch configuration. (Consider exporting the switch configuration prior to restoring vCenter Server)
  - Content libraries and library items.
  - The registration of virtual machines on ESXi hosts. (Some virtual machines may be orphaned)

or missing from the vCenter Server inventory).

- The host membership of a vSphere HA cluster  
(The vCenter Server may be out of sync with the actual, current membership).
- Security patches may be missing following a restore (you should re-apply the missing patches).

If you have prepared a supported target server, then you can use the following procedure to schedule a file-based backup of the vCenter Server.

Step 1. Log onto the vCenter Server Management

Interface (`https://vCenterFQDN:5480`) as root.

Step 2. Click **Backup > Configure**.

Step 3. Enter the backup location details.

- **Backup Location:** Provide the protocol, port, server address, and folder.
- **Backup Server Credentials:** Provide the username and password with write privileges.

Step 4. Configure the schedule and time.

Step 5. Optionally, provide an encryption password.

Step 6. Provide a number of backups to retain or select **Retain all backups**.

Step 7. Optionally, select **Stats, Events, and Tasks** to backup historical data.

Step 8. Click **Create**.

You can use the VAMI to manually backup a vCenter Server by selecting **Backup > Backup Now**.

## Key Topic

To restore a vCenter Server, launch the vCenter Server Installer (described in [Chapter 8, "vSphere Installation"](#)) on your desktop (Windows, Linux, or Mac) and use the following procedure.

Step 1. In the Home page, click **Restore**.

Step 2. On the next page, click **Next**.

Step 3. Accept the license agreement and click **Next**.

Step 4. Provide the backup location and credentials for the backup file to be restored and click **Next**.

Step 5. Review the backup information and click **Next**.

Step 6. Continue using the wizard to provide connection details (FQDN, credentials, and certificate information) for the ESXi host or vCenter Server to which the appliance will be restored.

Step 7. When prompted in the wizard, provide a name and a root password for the vCenter Server appliance.

Step 8. Select a deployment size (from Tiny to X-Large).

Step 9. Select the storage size (from Default to X-Large).

Step 10. Select a datastore, provide virtual disk and network settings for the appliance.

Step 11. On the Ready to Complete Stage 1 page, click **Finish**.

Step 12. When the OVA deployment finishes, click **Continue** to proceed with stage 2.

Step 13. Continue navigating the wizard, until it prompts you for Single Sign-on credentials.

Step 14. Provide the credentials and click **Validate and Recover**.

Step 15. On the **Ready to complete** page, review the details, click **Finish**, and click **OK**

**Note**

If a restore fails, power off and delete the partially restored VM. Then try to restore the VM again.

**Note**

You must power off the active, passive, and witness nodes in a vCenter Server High Availability Cluster prior to restoring. You must reconstruct the cluster after the completion of a successful restore operation.

If you prefer to use an image-based backup, you can leverage the vSphere API. For image-based backups you should consider the following.

- You must ensure the vCenter Server uses a fully qualified domain name (FQDN) with correct DNS resolution, or configure its hostname to be an IP address.
- If DHCP is used, you must configure the restored vCenter Server's IP address back to the original value.
- Ensure all vSphere component clocks are synchronized.
- The set of restored configurations for image-based restore is identical to the file-based restore.
- The impact to the state of vSphere components following an image-based restore is nearly

identical to the impact of a file-based restore.

To perform an image-based backup or recovery of vCenter Server, you must use a third-party product or custom code.

## UPGRADE TO VSphere 7.0

This section provides details for upgrading a vSphere environment to vSphere 7.0. For information on installing a new vSphere 7.0 environment, see [Chapter 8](#).

To upgrade a vSphere 6.5 or 6.7 environment to vSphere 7.0, you should upgrade the major components in the following order.

1. vCenter Server
2. ESXi hosts
3. Virtual machines - VMware Tools
4. Virtual machines - virtual machine hardware

**Note**

For vCenter Server 6.0 and earlier, you should upgrade to 6.5 or 6.7, then upgrade to 7.0.

You should backup vCenter Server prior to upgrading it. For details, see the *vCenter Server Backup* section in this chapter.

Upgrading your environment to use vCenter Server 7.0 requires you to either upgrade an existing vCenter Server appliance or migrate from an existing Windows based vCenter Server. When you upgrade or migrate a vCenter Server that uses an external Platform Services Controller (PSC), you converge the PSC into a vCenter Server appliance.

Prior to upgrading to vCenter Server 7.0, you should consider its compatibility with other vSphere components,

as summarized in Table 13-2.

**Table 13-2** vCenter Server 7.0 Compatibility

Component	Compatibility
vCenter Server appliance	You can upgrade vCenter Server appliance 6.5 and 6.7 to 7.0, except for specific build combinations that violate the back-in-time restrictions identified in VMware KB 67077
vCenter Server for Windows	You can migrate vCenter Server for Windows 6.5 and 6.7 (with or without an embedded PSC) to a vCenter Server 7.0 appliance.
vCenter Server database	vCenter Server 7.0 uses PostgreSQL for the embedded database. It does not support external databases.
ESXi hosts	vCenter Server 7.0 requires ESXi host version 6.5 or later.
Host Profiles	vCenter Server 7.0 requires Host Profiles version 6.0 or later.
VMFS	vCenter Server 7.0 supports VMFS3 and later, but can only create VMFS5 and VMFS6 datastores.
Virtual machines and VMware Tools	Review the ESXi Upgrade documentation for specific upgrade options, which are dependent on your current versions.
Auto Deploy	If you currently use Auto Deploy, when you upgrade to vCenter Server 7.0, VMware recommends you use Auto Deploy to upgrade hosts to ESXi 7.0.
vSphere Distributed Switch (vDS)	Upgrade to version to vDS 6.0 before upgrading vCenter Server.
Network I/O Control (NIOC)	Upgrade to NIOC version 3 before upgrading vCenter Server.
vSAN	VMware recommends you synchronize versions of vCenter Server and ESXi, to avoid potential faults.
vSAN disk version	Supported versions and paths may be impacted by the current version and upgrade history. See VMware Knowledge Base 2145267
Legacy Fault Tolerance (FT)	If you use Legacy FT on any virtual machines, you must turn off or upgrade the Legacy FT feature prior to vCenter Server upgrade or migration.

## vCenter Server Data Transfer

If you migrate a Windows based vCenter Server or upgrade a vCenter Server with an External PSC, you will need to transfer data to the embedded PostgreSQL database in the target vCenter Server appliance. At a minimum, you must transfer configuration data. You can choose whether you want to transfer historical data and performance metrics data. Specifically, you can choose one of the following options.

- **Configuration data** - Minimizes downtime during the upgrade)
- **Configuration and historical data** – You can choose to transfer historical data (usage statistics, tasks, and events) during the upgrade (impacting the downtime) or in the background following the upgrade.

- **Configuration, historical, and performance data** – You can transfer the configuration data during the upgrade and transfer the remaining data in the background following the upgrade.

**Note**

The option to transfer data in the background following an upgrade is only applicable to scenarios where the source vCenter Server uses an external database.

You can monitor the background data transfer using the vCenter Server Management Interface. You can pause and cancel the data transfer.

## Upgrade vCenter Server Appliance

You should address following prerequisites prior to upgrading a vCenter Server appliance to version 7.0



- Ensure the clocks of all the vSphere components are synchronized.
- Ensure the system meets the minimum hardware and software components.
- Ensure that the target ESXi host is not in lockdown, maintenance, or standby mode.
- Ensure that the target ESXi host is not part of a fully automated DRS cluster.
- Verify port 22 is open on the source vCenter Server appliance and port 443 is open on the ESXi host on which the source vCenter Server appliance is running.
- Verify that the source appliance has sufficient free space to accommodate data that is used for the upgrade.

- If the source vCenter Server uses an external database, determine its size and ensure that you account for it in the size of the new appliance.
- Ensure that network connectivity exists between the vCenter Server or ESXi that hosts the source vCenter Server appliance and the new vCenter Server appliance.
- If you plan to set the system name to a FQDN, ensure that forward and reverse DNS records are created.

Upgrading a vCenter Server appliance is a two stage process. The first stage is to deploy the OVA. The second phase is to transfer the data and configure the vCenter Server appliance. For a vCenter Server with an external PSC, you can use the following procedure for the first stage.

**Step 1.** Launch the vCenter Server Installer (GUI) and select **Upgrade**.

**Step 2.** Review the upgrade process on the first wizard page and click **Next**.

**Step 3.** Accept the license agreement and click **Next**.

**Step 4.** Provide the following information for the source vCenter Server and click **Connect**.

- Provide the address, HTTPS port, SSO credentials, and root password for the source vCenter Server.
- Provide the address, HTTPS port, and credentials for a user with administrative privileges for the ESXi host (or vCenter Server) that is hosting the source vCenter Server.

**Step 5.** Follow the wizard prompts to accept the certificate and accept the plan to converge the

source vCenter Server and external PSC into a single vCenter Server appliance

Step 6. Follow the wizard prompts to provide the following information for the target environment that will host the new vCenter Server appliance.

- If you are connecting to a vCenter Server, provide the address, HTTPS port, SSO credentials, and root password for the vCenter Server. Select a datacenter and an ESXi host (or cluster).
- If you are connecting to an ESXi host, provide the address, HTTPS port,, and credentials for a user with administrative privileges for the ESXi host.

Step 7. Follow the wizard to configure the new vCenter Server Appliance with the following information

- Virtual machine name
- Root user password
- Deployment size (Tiny to X-Large, as described in [Table 1-10](#))
- Storage size (Default to X-Large, as described in [Table 1-11](#))
- Datastore
- Temporary network used to transfer data from the source vCenter Server to the new vCenter Server.

Step 8. Click **Finish**.

Step 9. Click **Continue** to proceed to Stage 2.

**Note**

The identical Stage 1 procedure can be used when upgrading a vCenter Server Appliance with an embedded PSC, except the wizard will not prompt you to accept the plan to converge an external PSC.

For a vCenter Server with an external PSC, you can use the following procedure for the second stage.

Step 1. Review the stage 2 details and click **Next**.

Step 2. Wait for the pre-upgrade check to finish and respond to any of the following messages.

- Errors: Read the message, click **Logs** to obtain a support bundle, and troubleshoot. You cannot proceed with the upgrade until errors are corrected.
- Warnings: Read the messages and click **Close**.

Step 3. Specify the replication technology by choosing one of the following options

- **This is the first vCenter Server in the topology that I want to converge.**
- **This is a subsequent vCenter Server**  
(Also provide the IP address and HTTPS port of the partner vCenter Server)

Step 4. On the **Select upgrade data** page, choose the types of data transfer as described in the *vCenter Server Data Transfer* of this chapter.

Step 5. Complete the wizard and wait for the transfer and setup operations to complete.

Step 6. Decommision the source external PSC.

**Note**

The Stage 2 procedure to upgrade a vCenter Server Appliance with an embedded PSC is similar, but instead of being prompted for the replication technology, you are prompted (again) for information for connecting to the source vCenter Server and host environment (vCenter Server or ESXi host where the source vCenter Server resides).

## Migrate vCenter Server for Windows to vCenter Server Appliance



Migrating a vCenter Server for Windows to vCenter Server Appliance includes the following unique requirements.

- If the vCenter Server service is running as a user other than the Local System account, ensure the account is a member of the **Administrators** group and has the **Log on as a service**, **Act as part of the operating system**, and **Replace a process level token** permissions.
- Verify the vCenter Server and PSC certificates are valid and reachable.
- Verify the network connection to the domain controller is functioning.
- Verify that neither the source vCenter Server nor the PSC instance are using a DHCP IP address as the system name.

When you migrate vCenter Server for Windows to vCenter Server Appliance, the installer performs an environment pre-check that includes the following items.

- Sufficient storage space in source server.
- Validity and compatibility of SSL certificates and system names.
- Network connectivity, ports, and DNS resolution.
- Database connectivity

- Proper credentials and privileges for the Single Sign-on and Windows administrator accounts.
- NTP server validation

The following limitations apply when you migrate vCenter Server for Windows to vCenter Server Appliance 7.0.

- Local Windows OS users and groups are not migrated to the guest OS (Photon OS) of the new appliance. You should remove any vCenter Server permissions to local Windows users prior to the migration.
- At the end of the migration, the source vCenter Server is turned off and any solutions that are not migrated become unavailable. You should leave the source vCenter Server powered off to avoid network ID conflicts with the target vCenter Server appliance.
- The migration of Windows based vCenter Server instances that use custom ports for services other than Auto Deploy, Update Manager, vSphere ESXi Dump Collector, or HTTP reverse proxy (RHTTP) is not supported.
- Only one network adapter setting is migrated to the target vCenter Server appliance. If the source uses multiple IP addresses, you can select which IP address and network adapter settings to migrate.

To migrate a Windows based vCenter Server with an embedded PSC to vCenter 7.0, you can use the following procedure.

Step 1. Run the VMware Migration Assistant on the Windows server that runs vCenter Server. Leave it open during the migration.

- a. Download and mount the vCenter Server Installer
- b. Logon to Windows as an administrator.
- c. Double-click on VMware-Migration-Assistant.exe.
- d. Leave the Migration Assistant running until the migration is complete.

**Step 2.** Migrate the vCenter Server instance to an appliance.

- a. Using the Stage 1 procedure for upgrading a vCenter Server appliance, as a guide, launch the vCenter Server GUI installer, but choose **Migrate** rather than Upgrade.
- b. Provide connection information for the source Windows based vCenter Server.
- c. Provide information on the target server (vCenter Server or ESXi host) to deploy the vCenter Server appliance.
- d. Provide appliance information, such as root password, compute deployment size, storage deployment size, and datastore.
- e. Configure the temporary network used to transfer data from the source vCenter Server to the new vCenter Server and select **Continue to Stage 2**.
- f. In Stage 2, provide credentials for the single sign-on administrator and for the Windows system. If the Windows system is connected to an Active Directory domain, provide credentials for an appropriate domain user.
- g. Complete the wizard. Click **Finish** on the **Ready to Complete** page.

- h. Click **OK** to confirm the shutdown of the source Center Server
- i. Monitor the data transfer and configuration process.

**Note**

If the Windows based vCenter Server uses an external Update Manager, run the Migration Assistant on the Update Manager machine before running it on the vCenter Server.

To migrate a Windows based vCenter Server to vCenter 7.0 with an external PSC, you can use the previous procedure as a guide, but you should run the VMware Migration Assistant in the Windows based PSC prior to running it in the vCenter Server. You should also decommission the source external PSC following the migration.

## Upgrade ESXi and Virtual Machines

After upgrading to vCenter Server 7.0, you can use Lifecycle Manager to upgrade ESXi hosts and virtual machines, as described in the *Using vSphere Lifecycle Manager* section in this chapter.

## Using Update Planner

You can use the Update Planner to examine available vCenter Server updates and upgrades. You can produce interoperability reports for associated VMware products with your source (current) and target vCenter Server versions. You can generate pre-update reports to help ensure your system meets the minimum software and hardware requirements. The report identifies potential upgrade issues and provides potential remedy actions. To use Update Planner, you must join the VMware Customer Experience Improvement Program (CEIP)

You can use the following procedure to perform an interoperability check of VMware products within your

environment against the current vCenter Server version.

Step 1. In the vSphere Client, select a vCenter Server in the inventory pane.

Step 2. Select **Monitor > Interoperability**.

Step 3. Review the Product Interoperability report, which should contain all the available products in your environment

Step 4. If a VMware product in your environment is not automatically detected, you can use the following steps to manually add it to the list and regenerate the interoperability report.

- a. For each missing product, click **Add Product** and select the VMware product and version.
- b. Click **Done**.
- c. Regenerate the report and review that the product list.

Step 5. Click **Export** to save the report as a comma-separated values (CSV) file.

You can use the following steps to create an interoperability report on the compatibility of your environment's VMware products against a target version of vCenter Server.

Step 1. In the vSphere Client, select a vCenter Server in the inventory pane.

Step 2. Select **Updates > Update Planner**

Step 3. Select a target vCenter Server version (major upgrade or minor update).

Step 4. Click **Generate Report > Interoperability**.

Step 5. Review the Product Interoperability report, which should contain all the available products in your environment

Step 6. If a VMware product in your environment is not automatically listed, undetected, you can use the following steps to manually add it and regenerate the interoperability report.

- a. For each missing product, click **Add Product** and select the VMware product and version.
- b. Click **Done**.
- c. Regenerate the report and review that the product list.

Step 7. Click **Export** to save the report as a comma-separated values (CSV) file.

You can use the following steps to run pre-checks and generate reports providing pre-update information. The report identifies potential problems that might prevent the completion of a software upgrade or update. It includes a list with actions that you must address to ensure a successful upgrade of vCenter Server.

Step 1. In the vSphere Client, select a vCenter Server in the inventory pane.

Step 2. Select **Updates > Update Planner**

Step 3. Select a target vCenter Server version (major upgrade or minor update).

Step 4. Click **Generate Report > Pre-Update Checks**.

Step 5. Click **Export** to save the report as a comma-separated values (CSV) file.

Step 6. Optionally, click **Open Appliance Management or Download ISO**.

Step 7. You can use the vCenter Server Management Interface to perform administrative tasks to apply patches and updates, after you address issues identified in the report

## USING VSphere LIFECYCLE MANAGER

In vSphere 7.0, you have choices for methods and tools to facilitate the deployment and lifecycle management of ESXi host. You can use an ESXi installer image or VMware vSphere Auto Deploy to deploy hosts. Using vSphere Auto Deploy can result in hosts deployed in stateless mode. Using an ESXi installer image results in hosts deployed in stateful mode. Depending on the deployment method, you can use a variety of tools and methods for host updates and upgrade. For example, you can use Update Manager baselines, ESX Image Builder CLI, ESXCLI, or vSphere Auto Deploy. In any case, the ESXi image may change at runtime due to some solution installing software automatically or a service changing a setting.

VMware vSphere Life Cycle Manager provides simple, centralized lifecycle management for ESXi hosts and clusters using of images and baselines. Specifically, lifecycle management of a vSphere cluster refers to tasks such as installing and updating host firmware and ESXi. In vSphere 7.0, vSphere Lifecycle Manager encompasses and enhances the functionality that Update Manager provided for earlier vSphere releases. It is a service that runs in vCenter Server and is automatically enabled in the vSphere Client. It can work in an environment with direct access to the Internet or access via a proxy server. It can also work with Update Manager Download Service

(UMDS) in a secured network with no access to the Internet. In such cases, you use the Update Manager Download Service (UMDS) to download updates to the vSphere Lifecycle Manager depot, or you import them manually.

[Chapter 8](#) provides information on Lifecycle Manager implementation.

In vSphere 7.0, vSphere Lifecycle Manager enables you can use images or baselines. An image represents a desired software specification to be applied to all hosts in a cluster. An image is a description of which software, drivers, and firmware to run on a host. You can apply a single image to all hosts in a cluster to ensure consistency. Updates to software and firmware occur in a single workflow. The use of images with vSphere Lifecycle Manager enables new functionalities, including image recommendations, automated firmware updates, and hardware compatibility checks.

You can use baselines in vSphere 7.0, much like you could in previous vSphere versions to perform the following tasks.

- Upgrade ESXi 6.5 and 6.7 hosts.
- Patch ESXi 6.5, 6.7, and 7.0 hosts.
- Install and update third-party software on ESXi hosts.

Starting with vSphere 7.0, you can use vSphere Lifecycle Manager images to perform the following tasks to a set of hosts at the cluster level

- Install a desired ESXi version on each host.
- Install and update third-party software on each ESXi
- Update the firmware of each ESXi host.

- Update and upgrade each ESXi hosts in a cluster.
- Check the hardware compatibility of each host against hardware compatibility lists, such as VMware Compatibility Guide (VCG) and a host and vSAN Hardware Compatibility List (vSAN HCL).

You can start using Lifecycle Manager images as you create a cluster. Otherwise, you can switch from using baselines to images later. After switching the cluster to use images, you cannot revert the cluster back to using baselines. But, you could move the hosts to another cluster, which uses baselines. If you setup an image for a cluster and remediate all the hosts in the cluster, then all standalone VIB and non-integrated agents are deleted from the hosts.

vSphere Lifecycle Manager involves several components, including a service named vSphere Lifecycle Manager that runs in vCenter Server and uses the embedded vCenter Server PostgreSQL database. It communicates with agents running in each ESXi host.

vSphere Lifecycle Manager uses a Desired Stated model based on images that represent both the target software and target configuration of the host. The use of images requires all hosts to be ESXi 7.0 or later, be stateful, and from the same hardware vendor.

**Note**

In vSphere 7.0, vSphere Lifecycle Manager images are not supported for clusters with Kubernetes enabled or NSX installed. You can manage such clusters using baselines and baseline groups. You cannot enable vSphere with Kubernetes or install NSX-T on a cluster that is managed with an image.

You can leverage vSphere Lifecycle Manager for VMware Tools and virtual machine hardware upgrade operations on virtual machines running on ESXi 6.5, ESXi 6.7, and ESXi 7.0 hosts.

To get started using vSphere Life Cycle Manager, in the vSphere Client you can navigate to **Menu > Lifecycle Manager** (which is called the Lifecycle Manager home view) and select a vCenter Server. Here you can configure Lifecycle Manager using the **Settings** tab. Table 13-3 provides a description of the available settings for Lifecycle Manager remediation.

**Table 13-3** Lifecycle Manager Remediation Settings

Setting	Details
Quick Boot	You can enable Quick Boot to skip the hardware reboot during remediation.
Cluster Settings	You can disable vSphere Distributed Power Management (DPM), HA admission control, and FT for the entire cluster during remediation.
VM Power State	You can power-off, suspend, or leave alone the power state of running VMs during remediation.
VM Migration	You can migrate or leave alone powered off and suspended VMs during remediation.
Maintenance Mode Failures	You can control the number of retries and the delay between retries in the case that a host fails to enter maintenance mode.
PXE booted hosts	You can allow the installation of software for solutions on the PXE booted ESXi hosts
Removable media devices	You can automatically disconnect all virtual machine removable media devices prior to remediation and automatically reconnect afterwards.

When working with images, the following settings are applicable: Quick boot, VM power state, VM migration, maintenance mode failures, HA admission control, and DPM

When working with baselines, the following settings are applicable: Quick boot, VM power state, VM migration, maintenance mode failures, PXE booted hosts, and Removable media devices

You can perform the following set of tasks from the Lifecycle Manager home view.

- Browse the vSphere Lifecycle Manager depot.
- Trigger the synchronization of updates with the configured online depots.
- Trigger the synchronization of hardware compatibility data.

- Import offline depots manually.
- Import ISO images to use for the creation of upgrade baselines.
- Create and manage baselines and baseline groups.
- Configure the default vSphere Lifecycle Manager download source.
- Add a URL to an online depot to the list of download sources.
- Enable or disable downloading from a download source.
- Configure host remediation settings.
- Configure virtual machine rollback settings

## About VMware Update Manager

In vSphere 7.0, VMware Update Manager (VUM) is rebranded as vSphere Lifecycle Manager, which includes new features, such as the ability to provide ESXi lifecycle management at a cluster level.

## **Update Manager Download Service (UMDS)**

VMware vSphere Update Manager Download Service (UMDS) is an optional module of vSphere Lifecycle Manager, whose primary function is to download data when Lifecycle Manager does not have Internet connectivity. You can configure a Web server on the UMDS to automatically export the downloads to make them available to Lifecycle Manager. Alternatively, you can export the data from UMDS to a portable media drive. UMDS and Lifecycle Manager must be of the same version and update release.

UMDS is a 64-bit Linux application and is bundled with the vCenter Server 7.0 appliance. You can use that

bundle to install UMDS on a separate Linux system. You cannot upgrade UMDS on a Linux system. Instead, you can uninstall UMDS, perform a fresh installation, and continue using an existing patch store. To install UMDS, you can use the following procedure.

Step 1. Logon to a supported Linux system, such as Ubuntu (14.04, 18.04, 18.04 LTS, or 20.04 LTS) or Red Hat Enterprise Linux (7.4, 7.5, 7.7, or 8.1).

Step 2. For Red Hat Enterprise 8.1, install the libnsl package version 2.28 or later.

Step 3. Verify you have administrative privileges.

Step 4. Open a command shell.

Step 5. Copy the VMware-UMDS-7.0.0-build\_number.tar.gz to the Linux server.

Step 6. Run the vmware-install.pl script.

Step 7. When prompted, accept the EULA, select an installation directory, provide proxy settings, and specify the directory for storing patches.

To connect UMDS to third party vendor websites, you can use the following command.

```
vmware-umds -S --add-url https://web1.vendor1.com/ind
```

To export data from UMDS to a specific location that serves as a shared repository for vSphere Lifecycle Manager, you can use the following command, where repositoryPath represents a valid path to the shared repository.

```
vmware-umds -E -export-store repositoryPath
```

## Baselines and Images

vSphere Lifecycle Manager supports the use of baselines and baselines groups that are available in previous vSphere releases for host patching and upgrade operations. It supports multiple types of baselines, including pre-defined baselines, recommendation baselines, extension baselines, and custom baselines.

Pre-defined baselines cannot be edited or deleted. To examine the pre-defined baselines in the vSphere Client, select Menu > **Lifecycle Manager > Baselines**. The pre-defined baselines are categorized as host security patches, critical host patches, and non-critical host patches.

Recommendation baselines, which are predefined baselines generated by vSAN, appear by default when the vSAN cluster members are ESXi 6.0 Update 2 and later. You can use recommendation baselines to update the cluster with recommended critical patches, drivers, updates, and supported ESXi version for vSAN. You can create a baseline group containing multiple recommendation baselines, but only if you do not include other baseline types in the group. The vSAN recommendation baselines are typically refreshed every 24 hours for Lifecycle Manager instances with Internet access.

Custom baselines are those that you create. Patch baselines can be dynamic or fixed. With dynamic baselines, you specify the criteria for patches to be automatically included in the baseline. You can manually include or exclude patches from dynamic baselines. With fixed baselines, you manually select the patches to include.

You can use the following procedure to create a dynamic baseline. It requires that you have the **VMware**

**vSphere Lifecycle Manager.Manage Baselines**  
privilege.



Step 1. In the vSphere Client, select **Menu > Lifecycle Manager**

Step 2. If necessary, select the vCenter Server system in the **Lifecycle Manager** menu.

Step 3. Select **Baselines > New > Baseline**.

Step 4. In the wizard, provide the following baseline information and click **Next**.

- a. Name and (optionally) description
- b. Type: Upgrade, Patch, or Extension

Step 5. On the **Select Patches Automatically** page, set the criteria for adding patches to the baseline.

- a. Select automatic update check box.
- b. On the **Criteria** tab, specify the values for the following options to restrict which patches are included in the baseline, then click **Next**.
  - **Patch Vendor**
  - **Product (you can use an asterisk at the end to allow any version number)**
  - **Severity**
  - **Category**
  - **Release Date (you can specify a date range)**

- c. On the **Matched** tab, optionally deselect patches that matched the criteria, but you wish to permanently exclude.
- d. On the **Excluded** and **Select** tabs, you can view patches are excluded and which patches are included.

Step 6. On the **Select Patches Manually** page, you can optionally select specific patches, from the set of patches that do not meet the criteria for automatic inclusion, to include in the baseline.

Step 7. On the **Summary** page, click **Finish**

Extensions baselines contain additional (VMware or third party) software modules for hosts, such as device drivers. You can install additional modules using extension baselines and update the modules using patch baselines.

**Note**

In vSphere 7.0, the vendor name of VMware for inbox components has changed from **VMware, Inc** to **VMware**. If you filter the components by **VMware**, the results contain both **VMware, Inc** for 6.x patches and **VMware** for 7.0 patches.

If your user has the **View Compliance Status** privilege, you can use the **Updates** tab for a selected object to view the object's compliance with baselines or images. You can select a host or cluster that is managed with baselines and click on **Updates > Baselines**. From there, you can do the following tasks.

- Check the compliance of hosts or clusters against baselines and baseline groups.
- Attach and detach baselines and baseline groups to hosts or clusters.
- Perform a remediation pre-check.

- Stage patches or extensions to prepare for remediation.
- Check the compliance of ESXi hosts against an image.
- Remediate hosts against baselines and baseline groups.
- Remediate hosts that are part of a vSAN cluster against system-managed baselines.

You can select a cluster that is managed with an image and click on **Updates > Images**. From there, you can do the following tasks.

- Export, import, and edit the image used by the cluster.
- Upgrade the firmware of the ESXi hosts in the cluster.
- Check for and examine recommended images for the cluster.
- Check for hardware compatibility for a selected ESXi version against the vSAN HCL
- Check the compliance of the ESXi hosts against the image.
- Run a remediation pre-check.
- Remediate the ESXi hosts against the cluster's image.

You can select a host, then select **Updates > Hosts > Hardware Compatibility** to check the host hardware against the *VMware Compatibility Guide*. You can select a host, then select **Updates > Hosts** and then select **VMware Tools** or **VM Hardware** to check and upgrade the VMware Tools version and virtual hardware version of the virtual machines.

**Table 13-4** provides definitions of vSphere Life Cycle Manager terms.

**Table 13-4** Lifecycle Manager Definitions

Term	Definition
Update	A software release that makes small changes to the current version, such as vSphere 7.0 U1, 7.0 U2, and so on.
Upgrade	A software release that introduces major changes to the software. For example, you can upgrade from vSphere 6.5 to 6.7 and 7.0.
Patch	A small software update that provides bug fixes or enhancements to the current version of the software, such as 7.0a, 7.0 U1a, and so on.
VIB	A vSphere Installation Bundle (VIB) is the smallest, installable software package (metadata and binary payload) for ESXi.
VIB metadata	An XML file that describes the contents of the VIB, including dependency information, textual descriptions, system requirements, and information about bulletins.
Standalone VIB	A VIB that is not included in a component.
Depot	The hosted version of updates provided by VMware, OEMs, and third-party software vendors, containing the metadata and the actual VIBs.
Offline bundle/Offline depot	An archive (ZIP file) that contains VIBs and metadata that you use for offline patching and updates. A single offline bundle might contain multiple base images, vendor add-ons, or components.
OEM	Original Equipment Manufacturer (OEMs) are VMware partners, for example Dell, HPE, VMware Cloud on AWS.
Third-party software providers	Providers of I/O filters, device drivers, CIM modules, and so on.

**Note**

During a synchronization of a depot, vSphere Lifecycle Manager downloads only the VIB metadata.

In earlier vSphere releases, VIBs are packaged into bulletins. In vSphere 7.0, VIBs are packaged into components, which are created by VMware, OEMs, and third-party software providers. A component is much like a bulletin with extra metadata containing the component name and version. VMware bundles components together into fully functional ESXi images. OEMs bundle components into add-ons that they deliver via the VMware online depot as offline bundles. Third party vendors create and ship drivers packaged as components.

vSphere Lifecycle Manager can consume bulletins and components. It lists the available components as

bulletins when baselines are used to manage a host or cluster. When images are used, vSphere Lifecycle Manager only works with components.

The ESXi base image, which is the ESXi image that VMware provides with each release of ESXi, is a complete of components that can boot up a server. Base images have friendly names, have a unique version that corresponds to the ESXi release, and are hosted in the VMware online depot. Alternatively, you can download an ESXi installer ISO file and an offline bundle (ZIP file) that contains the ESXi version from my.vmware.com.

A vendor add-on is a collection of components that you can use to customize an ESXi image with OEM content and drivers. You cannot use vendor add-ons on their own. You can use a vendor add-on to add, update, or remove components that are part of the ESXi base image. You can use the vSphere Client to view the list of components that a vendor add-on adds to or removes from an ESXi base image.

Prior to vSphere 7.0, OEMs create custom images by merging their content with the stock VMware provided image. OEMs released custom images in accordance with the major and update releases of vSphere. Starting with vSphere 7.0, in addition to releasing custom ISO images and offline bundles, OEMs can release ZIP files that contain only the vendor add-on. This approach decouples the release cycle of OEMs from the release cycle of VMware.

vSphere Lifecycle Manager can consume software updates delivered as an online depot, as an offline depot, or as an installable ISO image. An online depot is a hosted version of the software updates. Starting with vSphere 7.0, the default, VMware online depot provides hosts vendor add-ons. The default depot also contains VMware certified, ESXi-compatible I/O device drivers.

You can use the vSphere Client to access third-party online depots containing additional components.

Offline bundles are ZIP files that contains the software metadata and the respective VIBs. Starting with vSphere 7.0, OEMs can distribute add-on.zip files that contain the delta between the OEM custom image and the base image that VMware provides.

A baseline is a set of bulletins. Patch baselines, extension baselines, and upgrade baselines contain patch bulletins, extension bulletins, and ESXi images, respectively. You can attach baselines to hosts, check compliance of the host with its associated baseline, and remediate (update) the hosts using the baseline.

You can classify baselines depending on the following.

- Update type: patch baselines, extension baselines, and upgrade baselines.
- Content: Fixed or dynamic.
- Predefined, recommendation, or custom baselines.
- Predefined host patches: Host Security Patches, Critical Host Patches, and Non-Critical Host Patches.

You cannot modify or delete the predefined baselines. You can use the predefined baselines to create custom patch, extension, and upgrade baselines. Recommendation baselines are baselines generated automatically by vSAN. You can use recommendation baselines only with vSAN clusters.

A baseline group is a set of non-conflicting baselines, which you can apply as a single entity. Host baseline groups can contain a single upgrade baseline plus patch and extension baselines. For efficiency, you can attach and apply baselines and baseline groups to container

objects (such as folders, vApps, and clusters), rather than to the individual, underlying objects (virtual machines and hosts).

To check the cluster compliance against an image, you can select the cluster, select **Updates > Hosts > Image** and click the **Check Compliance** button. When you check a cluster's compliance with a Lifecycle Manager image, one of the following four compliance states are identified for each member host.

- Compliant: The host's image matches the image applied to the cluster.
- Non-Compliant: The host's image does not match the image applied to the cluster. Some potential causes are differences in the ESXi version, the firmware version, or the set of components. Another potential cause is the host contains a standalone VIB.
- Incompatible: The cluster's image cannot be applied to the host. Some potential reasons are the host's ESXi version is later than the version in the image, the host has insufficient RAM, or the host hardware is incompatible with the cluster's image.
- Unknown: No compliance state information is available, perhaps because the host was recently added, or the cluster's image was edited.

## ESXi Quick Boot

You can use Quick Boot with vSphere Lifecycle Manager to optimize the host patching and upgrade operations. When Quick Boot is enabled, vSphere Lifecycle Manager skips the hardware reboot (the BIOS or UEFI firmware reboot), which reduces the time a host spends in maintenance mode and reduces the risk of failures during.

Starting with vSphere 6.7, Quick Boot is supported on a limited set of hardware platforms and drivers. Quick Boot is not supported on ESXi hosts that use TPM or on ESX 6.7 hosts that use passthrough devices. To determine if your system is compatible with Quick Book, you can run the following command in the ESXi Shell.

```
/usr/lib/vmware/loadesx/bin/loadESXCheckCompat.py
```

To enable Quick Boot you can use the following procedure.

Step 1. In the vSphere Client, navigate to **Menu >**

**Lifecycle Manager**

Step 2. In the **Lifecycle Manager** dropdown menu, select a vCenter Server.

Step 3. Select **Settings > Host Remediation > Images.**

Step 4. Click **Edit.**

Step 5. In the **Edit Cluster Settings** window, select the **Quick Boot** checkbox

Step 6. Click **Save.**

## **ESXi Firmware Updates**

You can use Lifecycle Manager images to perform firmware updates on cluster member hosts. Firmware updates are not available for clusters that are managed with baselines. To apply firmware updates, you must use a vendor-provided firmware and drivers add-on in the image. Firmware updates are available in a special vendor depot that you access through a vendor-specific hardware support manager plug-in that registers itself as a vCenter Server extension.

The hardware support manager enables you to select a firmware add-on to include in an image and the firmware versions to be installed on the hosts. During remediation, vSphere Lifecycle Manager requests the selected hardware support manager to update the firmware on the hosts in accordance with the firmware add-on specified in the image.

In vSphere 7.0, you can deploy hardware support manager plug-ins from Dell and HPE. Dell's plug-in, which you deploy as an appliance, is part of the Dell OpenManage Integration for VMware vCenter Server (OMIVV). HPE's plug-in, which you deploy as an appliance, is part of the HPE iLO Amplifier management tool. You should follow the vendor's specific deployment and configuration documentation. The main steps are:

Step 1. Deploy and power on the virtual appliance

Step 2. Register it as a vCenter Server extension

Step 3. Use the plug-in's UI in the vSphere Client.

You can use the following procedure to manage the firmware on cluster member hosts that are managed with a single image.

Step 1. In the vSphere Client, select the cluster in the inventory pane.

Step 2. Examine the cluster member hosts and verify they from the same vendor.

Step 3. Select the cluster and click **Updates > Hosts > Image**.

Step 4. In the **Image** card, click **Edit**.

Step 5. In the Edit Image card, click Firmware and Drivers Addon > Select.

Step 6. In the dialog box, select a hardware support manager.

Step 7. Select a firmware add-on from the provided list and review the right panel, which contains information, such as whether the selected add-on contains the necessary drivers for the ESXi versions in the cluster.

Step 8. Click **Select**.

Step 9. In the **Image** card, validate and save the image, which triggers a compliance check against the new image.

Step 10. In the **Image Compliance** card, review the results.

Step 11. If any host in the cluster has firmware that is non-compliant with the new image firmware, remediate the respective host or the cluster, using the following steps.

- a. Optionally, in the **Image Compliance** card, click **Run Pre-Check** for the cluster or for a selected host.
- b. In the **Image Compliance** card, initiate remediation.
- c. To remediate all hosts in the cluster, click the **Remediate All** button. If the remediation of a single host fails, the remediation for the cluster is aborted.
- d. Alternatively, to remediate a single host, click the vertical ellipsis icon for the host and select **Remediate**.

**Note**

The host vendor must match the selected hardware support manager vendor. Otherwise, a compliance check will report that the hosts that are from a different vendor or report an incompatibility. Firmware remediation fails.

## Hardware Compatibility Checks

You can use vSphere Lifecycle Manager to automate the process of validating the hardware compliance against the VMware Compatibility Guide (VCG) and vSAN Hardware Compatibility List (vSAN HCL) based on ESXi version. Hardware compatibility checks for vSAN cluster member hosts use the vSAN HCL for the I/O devices used by vSAN and the VCG for all other devices.

To check the hardware compatibility for a cluster, select the cluster, click **Updates > Hosts > Hardware compatibility**, and click **Run Checks**.

## Export and Import Cluster Image

You can export a cluster image from one vCenter Server instance and import it to another vCenter Server instance. You can use the following procedure to export the image.

Step 1. In the vSphere Client, select the cluster in the inventory pane.

Step 2. Click **Updates > Hosts > Image**.

Step 3. Click the horizontal ellipsis icon and select **Export**.

Step 4. In the **Export Image** dialog box, select a file format, and click **Export**.

If you intend to use the image in another vCenter Server, export it as a JSON file and as a ZIP file. You can import both the JSON file and the ZIP file to the target vCenter Server system.

You can use the following procedure to import a cluster image.

Step 1. In the vSphere Client, select the cluster in the navigation pane.

Step 2. Click **Updates > Hosts > Image**.

Step 3. Click the horizontal ellipsis icon and select **Import**.

Step 4. In the **Import Image** dialog box, select a JSON file and click **Next**.

Step 5. Optionally, use the Edit Image card to modify the following image elements

- ESXi Version
- Vendor Add-On
- Firmware and Drivers Add-On
- Components

Step 6. Resolve any issues with conflicting components or unresolved dependencies.

Step 7. Optionally, click **Validate**.

Step 8. Click **Save**.

## Backup and Restore Scenarios

After switching a cluster from using baselines to using images, if you restore the vCenter Server from a backup made prior to the switch, the restored cluster reverts to being managed by baselines.

If you restore a vCenter Server back to a point in time prior to when you used Lifecycle Manager to remediate a cluster with a new image containing new components, then a compliance check on the cluster reveals the hosts are incompatible. In this case, Lifecycle Manager expected the hosts to be using a different image. To fix

this, you should upgrade the cluster to the new image and remediate.

## Upgrade Virtual Machines

You can use vSphere Lifecycle Manager to upgrade VMware Tools and the virtual machine hardware version of multiple virtual machines in a folder, vApp, host, or cluster. You can upgrade a virtual machine regardless of its power state and let Lifecycle Manager change the power state of the virtual machine as needed and return it to its original state when ready. To upgrade VMware Tools, Lifecycle Manager will power on the virtual machine. To upgrade the virtual machine hardware, Lifecycle Manager will power off the virtual machine.

You can use the following procedure to upgrade the hardware for a set of virtual machines using vSphere Life Cycle Manager.

Step 1. In the vSphere client, select a virtual machine container object, such as a folder or cluster.

Step 2. Navigate to **Updates > Hosts > VM Hardware**

Step 3. Select the specific virtual machines to upgrade

Step 4. Click Upgrade to Match Host

Step 5. Optionally, use the **Scheduling Options** to configure the upgrade as a scheduled task

Step 6. Optionally, use Rollback Options and configure the following options.

a. Select or deselect the **Take snapshot of VMs** check box. (enabled by default)

b. Select a period for keeping the snapshots, either indefinitely or for a fixed period.

- c. Provide a snapshot name
- d. Optionally, provide a description.
- e. Optionally, select the checkbox to include the virtual machine memory in the snapshot.

#### Step 7. Click Upgrade to Match Host

You can use the same procedure to upgrade VMware Tools, except you should choose **Upgrade VMware Tools to Match Host** in step 4. On the VMware Tools page, you can choose **Set Auto Update**. Optionally, you can use a virtual machine's **Updates** tab to turn on the **Automatically upgrade on reboot** feature.

For more information concerning VMware Tools and virtual machine hardware, such as procedures for interactive installation, host compatibility, and log levels, see [chapter 14](#).

## MANAGE ESXI HOSTS

In some cases, such as when you are performing host maintenance and troubleshooting activities, you may want to restart the management agents on an ESXi host. To do so using the Direct Console User Interface (DCI), select **Troubleshooting > Restart Management Agents** menu options. This operation restarts all installed management agents and services that are running in `/etc/init.d` on the ESXi host. Typically, these agents include `hostd`, `ntpd`, `sfcbd`, `s1pd`, `wsman`, and `vobd`. When you restart the management agents, current users of the vSphere Client and Host Client lose connectivity to the host.

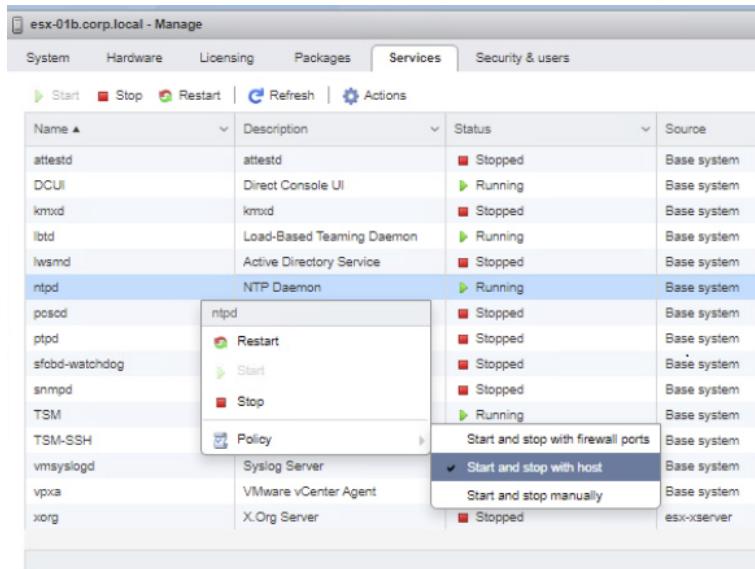
When troubleshooting network connectivity with a host, you can choose **Test Management Network** in the host's DCUI, which automatically pings the host's

configured default gateway, pings the DNS server, and attempts to resolve its hostname. You can specify additional addresses for the ping tests. To restore network connectivity for a host or to renew a DHCP lease, you can choose **Restart the Management networking** in the host's DCUI.

In rare situations such as the following, you may want to restore a standard switch to an ESX host, which you can do with the **Restore Standard Switch** option in the DCUI.

- The distributed switch used for management is not functioning.
- You need to restore the host connection to vCenter, which uses a distributed switch.
- You do not want vCenter Server to manage the host and want to ensure the management connection does not use a distributed switch.

You can use the Host Client interface to manage the host's services. To get started, logon to the Host Client as the root user or other user with local administrator privileges and navigate to **Manage > Services**. Here you can examine the state of each ESXi service. To change the state of a service, right-click on the service and select **start**, **stop**, or **reset**. You can also change a service's startup policy, such that it automatically starts with the host or associated firewall ports, or is only started manually, as illustrated in [Figure 13.1](#). You can perform similar operations using the vSphere Client by selecting the host and navigating to **Configure > System > Services**.



**Figure 13-1** Managing Host Services in the Host Client

To manage firewall rules on an ESXi host, you can select the host in the vSphere Client and navigate to

**Configure > System > Firewall.**, as illustrated in Figure 13.2. Here you can view the currently allowed incoming and outgoing firewall services. The details for each service include the service name, the associated TCP ports, the associated UDP ports and the allowed IP addresses. To make changes, you can use the **Edit** button to view all the currently defined services, select the services you want to allow, and optionally restrict the available IP addresses for the service. To perform similar operations in the Host Client, navigate to **Networking > Firewall rules**.

Service name	TCP ports	UDP ports	Allowed IP addresses
CIM Secure Server	5989	--	All
CIM Server	5988	--	All
CIM SLP	427	427	All
DHCP Client	--	68	All
DHCPv6	546	546	All
DVSsync	--	8301, 8302	All
Fault Tolerance	8300	--	All
iofiltervp	9080	--	All
NFC	902	--	All
SNMP Server	--	161	All
SSH Server	22	--	All
VMotion	8000	--	All
vSphere Web Access	80	--	All
vSphere Web Client	443, 902	--	All

**Figure 13-2** Firewall Rules in the vSphere Client

In the vSphere Client you can right-click on a specific host and choose from a set of available actions. For example, to address a vCenter Server connection to a host, you can choose **Connection > Disconnect**, wait for the task to complete, then choose **Connection > Connect**. To remove a host from the vCenter Server inventory, you can choose **Remove from Inventory**, which requires you to first enter maintenance mode.

If you want to perform maintenance activities on a host, such as upgrading its hardware, you can choose **Maintenance Mode > Enter Maintenance Mode**. Following the completion of a maintenance activity, you can select **Maintenance Mode > Exit Maintenance Mode**. To test a host's ability to be used with Distributed Power Management (DPM), you can choose **Power > Enter Standby Mode**.

The following list are some of the other action items that you can select for a host in the vSphere client. Details for these tasks are provided elsewhere in this book.

- Certificates: Renew certificates or Refresh CA certificates
- Host Profiles: Attach, Detach, Extract, or Change Host Profile, or Remediate
- Export System Logs
- Assign License
- Settings
- Move To
- Add Permission

# MONITOR AND MANAGE VCENTER SERVER

You can use the vSphere Client and the vCenter Server Management Interface (commonly called the VAMI) to configure, monitor, and manage components and resource usage of the vCenter Server Appliance.

The *VIMTOP* and *VAMI* sections in [Chapter 10](#), "Monitoring and Managing Clusters and Resources," provide information about monitoring the resource usage of the services and database running in the vCenter Server appliance. If database resources are low, you can consider adjusting the statistics interval, statistics level, task retention, and event retention settings. If you determine that the appliance is low on disk space, you can add more space. To increase the disk space for a vCenter Server 7.0 appliance, you can use the following procedure.

Step 1. Use the vSphere Client (or Host Client) to navigate the vSphere environment that is hosting the vCenter Server appliance.

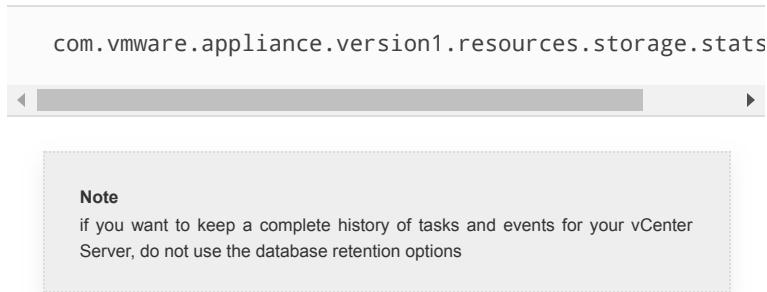
Step 2. Select the vCenter Server appliance (virtual machine), edit its settings, and increase the size of affected virtual disk.

Step 3. Use SSH to connect to the vCenter Server as the root user.

Step 4. Run the following command

```
com.vmware.appliance.system.storage.resize
```

Optionally, to see the impact of the command, you can use the following command to examine the total and used storage (in Kilobytes) before and after step 4.



## Monitor and Manage vCenter Server with the VAMI

You can use the vCenter Server Management Interface (often referred to as the VAMI) to monitor and manage specific components of your vCenter Server.

To access the VAMI, use a web browser to connect to `https://vCenter-FQDN:5480`. By default, you can logon using the root account and the password that was set during the vCenter Server deployment.

**Note**  
If you are using Internet Explorer, verify that TLS 1.0, TLS 1.1, and TLS 1.2 are enabled in the security settings.

After logging into the VAMI as root, you can perform any of the tasks described in [Table 13-5](#).

**Table 13-5** Tasks in vCenter Server Management Interface

Task	Steps / Details
View vCenter Server health status.	<p>Click <b>Summary</b></p> <p>Examine the color of the <b>Overall Health</b> badge.</p>
Reboot vCenter Server	<p>Click <b>Summary</b></p> <p>Click <b>Actions &gt; Reboot</b> and click <b>Yes</b></p>
Shutdown vCenter Server	<p>Click <b>Summary</b></p> <p>Click <b>Actions &gt; Shutdown</b> and click <b>Yes</b></p>
Create a Support Bundle	<p>Click <b>Summary</b></p> <p>Click <b>Actions &gt; Create Support Bundle</b> and save the bundle to your desktop.</p>
Monitor CPU and memory use of vCenter Server	<p>Click <b>Monitor</b></p> <p>Click the <b>CPU &amp; Memory</b> tab and use the <b>date range</b> dropdown menu to specify a timeframe.</p>
Monitor disk use of vCenter Server	<p>Click <b>Monitor</b></p> <p>Click the <b>Disk</b> tab.</p>
Monitor network use of vCenter Server	<p>Click <b>Monitor</b></p> <p>Click the <b>Network</b> tab and use the <b>date range</b> dropdown menu to specify a timeframe.</p> <p>Examine the graph grid and use the provided table to select a packet or transmit byte rate to monitor.</p>
Monitor database use of	Click <b>Monitor</b>

vCenter Server	<p>Click the <b>Database</b> tab and use the <b>date range</b> dropdown menu to specify a timeframe.</p> <p>At the base of the graph, select specific database components to include in the graph.</p>
Enable or disable each type of vCenter Server access.	<p>Click <b>Access</b></p> <p>Configure each of the following options.</p> <p><b>Enable SSH login.</b></p> <p><b>Enable DCUI</b></p> <p><b>Enable Console CLI</b></p> <p><b>Enable Bash Shell</b></p>
Configure network settings for vCenter Server	<p>Click <b>Networking</b></p> <p>Click <b>Edit</b> and fill in the following networking details</p> <p>DNS settings</p> <p>IPv4 settings</p> <p>IPv6 settings</p> <p>Proxy server settings</p> <p>When configuring a proxy server, you can enable HTTPS, FTP, and HTTP options. You should provide the proxy server's IP address or host name, user credentials, and a port number.</p>
Configure the firewall rules for the vCenter Server	<p>Click <b>Firewall</b></p> <p>Examine the existing set of rules and choose from the following commands to change the rule set.</p> <p><b>Add</b></p> <p><b>Edit</b></p> <p><b>Delete</b></p> <p><b>Reorder</b></p> <p>For each rule, include the appropriate NIC, IP address, subnet, and action (<b>Accept</b>, <b>Ignore</b>, <b>Reject</b>, or <b>Return</b>).</p>
Configure the time settings for the vCenter Server	Click <b>Time</b>

	<p>Click <b>Time Zone</b> &gt; <b>Edit</b> and select the appropriate time zone.</p> <p>Click <b>Time Synchronization</b> &gt; <b>Edit</b> and select the <b>Mode</b> to <b>Disable</b>, <b>Host</b>, or <b>NTP</b>.</p>
Start, stop, and restart a Service in the vCenter Server	<p>Click <b>Services</b></p> <p>Select a service and click <b>Start</b>, <b>Stop</b>, or <b>Restart</b>.</p>
Configure settings for updating vCenter Server	<p>Click <b>Update</b></p> <p>Click <b>Settings</b>, set the options for automatic update checking, and set the repository to default or to a custom (HTTPS or FTPS) URL. Optionally provide credentials if a custom repository is used.</p> <p>Click <b>Check Updates</b> to manually check for updates.</p>
Change the root user password in vCenter Server	<p>Click <b>Administration</b></p> <p>Click <b>Password</b> &gt; <b>Change</b>. Set the password and the password expiration details. If you set the password to expire, provide the number of days and an address for the email warning.</p>
Configure log forwarding on the vCenter Server	<p>Click <b>Syslog</b></p> <p>Click <b>Configure</b> (or <b>Edit</b>, if you previously configured syslog hosts), enter up to three destination hosts in the Create Forward Configuration pane, set the <b>Protocol</b> and <b>Port</b>.</p> <p>Protocol options:</p> <ul style="list-style-type: none"> <li>TLS – Transport Layer Security</li> <li>TCP – Transmission Control Protocol</li> <li>RELP – Reliable Event Logging Protocol</li> <li>UDP – User Datagram Protocol</li> </ul>
Configure and schedule backups of the vCenter Server	<p>Click <b>Backup</b></p> <p>Click <b>Backup</b> &gt; <b>Backup Now</b> to initiate a backup or click <b>Backup</b> &gt; <b>Configure</b> to schedule backups.</p> <p>Use the <b>Activity</b> table to monitor backups.</p>

Table 13-X provides a description for each of the possible color (icons) for the Health Status badge.

**Table 13-X** Health States

Color	Description
Green	Good. All components are healthy
Yellow	Warning. One or more components may become overloaded soon.
Orange	Alert. One or more components may be degraded. Non-security patches may be available.
Red	Critical. One or more components may be in an unusable state and vCenter Server may become unresponsive soon. Security patches may be available.
Gray	Unknown. No data is available.

**Note**

When responding to an alert, you should begin by examining the details in the Health Messages pane.

You can use the following procedure to reconfigure the FQDN, IP Address, or the Primary Network Identifier (PID) of the vCenter Server.

Step 1. Log in to the VAMI using your administrator SSO credentials.

Step 2. Click Networking > Network Settings > Edit.

Step 3. Select the appropriate NIC and click **Next**.

Step 4. In the **Edit Settings** pane, change the host name and IP address. Click **Next**.

Step 5. In the **SSO Credentials** pane, provide the administrator SSO credentials. (You must provide the credentials for the administrator account in the SSO domain such as administrator@vsphere.local)

Step 6. In the Ready to Complete pane, click Finish.

Step 7. Monitor the progress in the task bar and wait to be redirected to the new IP address.

Step 8. Log in using your administrator SSO credentials.

Step 9. On the **Networking** page, verify the new host name and IP address.

Step 10. Re-register all deployed plugins

Step 11. Regenerate all custom certificates

Step 12. If vCenter Server HA was enabled, reconfigure vCenter HA

Step 13. If Active Directory was enabled, reconfigure Active Directory

Step 14. If Hybrid Link mode was enabled, reconfigure Hybrid Link with Cloud vCenter Server

**Note**

If you set an IP address as a system name during the deployment of the appliance, you can later change the primary network identifier to a fully qualified domain name. If vCenter High Availability (HA) is enabled, you must disable the vCenter HA setup before reconfiguring the primary network identifier.

## Monitor and Manage vCenter Server with the vSphere Client

You can use the vSphere Client to monitor and manage specific components of your vCenter Server.

### Common vCenter Server Management Tasks

Using the vSphere Client, you can logon, select your vCenter Server in the inventory and then perform any of the tasks in Table 13-6.

**Table 13-6** Management Tasks in vSphere Client

---

Task	Steps / Details
Assign a license to your vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Select <b>Settings &gt; Licensing &gt; Assign License</b></p> <p>Select an existing license or enter a new license key</p> <p>Requires the <b>Global.Licenses</b> privilege</p>
Configure statistics settings for vCenter Server	See the <i>Configure Statistics Collection Settings</i> section in this chapter.
Configure runtime settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; Runtime Settings</b> and configure the following settings.</p> <ul style="list-style-type: none"> <li>• <b>vCenter Server unique ID:</b> A valid number from 0 through 63 (default value is randomly generated)</li> <li>• <b>vCenter Server managed address:</b> Can be IPv4, IPv6, a fully qualified domain name, an IP address, or another address format.</li> <li>• <b>vCenter Server name:</b> Name of the vCenter Server system (should match the vCenter Server DNS name)</li> </ul> <p>Requires the <b>Global.Settings</b> privilege</p>
Configure user directory settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; User Directory</b> and configure the following, which will be applied to vCenter Server Single Sign-On identity sources.</p> <ul style="list-style-type: none"> <li>• <b>User directory timeout:</b> Timeout in seconds for directory server connection</li> <li>• <b>Query Limit:</b> Must be enabled to set a query limit size</li> <li>• <b>Query limit size:</b> Maximum numbers of queries.</li> <li>• <b>Validation:</b> Enable to have vCenter Server validate (synchronize) known users against the directory server.</li> <li>• <b>Validation period:</b> Number of minutes between validation executions.</li> </ul> <p>Requires the <b>Global.Settings</b> privilege</p>
Configure Mail Sender Settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; Mail</b> and configure the following.</p> <ul style="list-style-type: none"> <li>• <b>Mail server:</b> SMTP server information</li> <li>• <b>Mail sender:</b> Full Email address (including domain name) of the sender</li> </ul>

	Requires the <b>Global.Settings</b> privilege
Configure SNMP Settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; SNMP receivers</b> and configure the following for one or more receivers.</p> <ul style="list-style-type: none"> <li>• <b>Enable receiver:</b> Use to enable or disable a receiver</li> <li>• <b>Primary receiver URL:</b> Hostname or IP address of the SNMP receiver</li> <li>• <b>Receiver port:</b> Port number (between 1 and 65535) of the receiver</li> <li>• <b>Community String:</b> The community identifier</li> </ul> <p>Requires the <b>Global.Settings</b> privilege</p>
View Port Settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; Ports</b> and examine the ports used by the Web service.</p>
Configure timeout settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; Timeout Settings</b> and configure the following...</p> <ul style="list-style-type: none"> <li>• <b>Normal:</b> Timeout for normal operations</li> <li>• <b>Long:</b> Timeout for long operations</li> </ul> <p>Restart the vCenter Server system</p> <p>Requires the <b>Global.Settings</b> privilege</p>
Configure logging settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; Logging settings</b> and select one of the following logging options.</p> <ul style="list-style-type: none"> <li>• <b>None (Disable logging)</b></li> <li>• <b>Error (Errors only)</b></li> <li>• <b>Warning (Errors and warnings)</b></li> <li>• <b>Info (Normal logging)</b></li> <li>• <b>Verbose (Verbose)</b></li> <li>• <b>Trivia (Extended verbose)</b></li> </ul> <p>Requires the <b>Global.Settings</b> privilege</p>
Configure database settings for vCenter Server	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Settings &gt; General &gt; Edit &gt; Database</b> and configure the following.</p> <ul style="list-style-type: none"> <li>• <b>Maximum connection</b></li> <li>• <b>Task retention (days)</b></li> <li>• <b>Event retention (days)</b></li> </ul> <p>To limit the database growth and save storage space, you can configure the database to periodically discard task and event information.</p>
Verify SSL certificates	See the Verify SSL Certificates for Legacy Hosts procedure.

	<p>for legacy hosts.</p> <p>Configure advanced settings for vCenter Server (which are kept in the entries to the <code>vpxd.cfg</code> file),</p>	<p>Select the <b>Configure</b> tab.</p> <p>Navigate to <b>Advanced Settings &gt; Edit Settings</b>. Add or modify advanced settings entries, providing a <b>Name</b> and <b>Value</b> for each entry. (Cannot delete entries).</p> <p>If necessary, restart the vCenter Server system</p> <p>Only use <b>Advanced Settings</b> when instructed to do so by VMware. Requires the <b>Global.Settings</b> privilege.</p>
Send a message to users logged into vCenter Server	Select the <b>Configure</b> tab.	<p>Navigate to <b>Settings &gt; Message of the Day</b>, click <b>Edit</b>, and enter a message, such as a maintenance announcement or request for users to log out.</p>
Start, stop, and restart the services (nodes) in the vCenter Server	<p>Navigate to <b>Administration &gt; System Configuration</b></p> <p>Select a node and click <b>Reboot Node</b>.</p> <p>Requires your user account to be a member of the <b>SystemConfiguration.Administrators</b> group.</p>	
View the health status of vCenter Server services and nodes.	<p>Navigate to <b>Administration &gt; Deployment &gt; System Configuration</b></p> <p>Examine the health status badge for each service and node. See Table 13-X for explanation of health status badges.</p> <p>Requires your user account to be a member of the <b>SystemConfiguration.Administrators</b> group.</p>	
Export a Support Bundle	<p>Navigate to <b>Administration &gt; Deployment &gt; System Configuration</b></p> <p>Select a node, click <b>Export Support Bundle</b>, select the services that you want to include from the two available categories (cloud infrastructure and virtual appliance) and click <b>Export Support Bundle</b>.</p> <p>Requires your user account to be a member of the <b>SystemConfiguration.Administrators</b> group.</p>	

## Configure Statistics Collection Settings

vCenter Server and ESXi use data counters, organized in metric groups, to collect data statistics. A data counter is a unit of information that is relevant to a specific inventory object or device. For example, the disk metric group includes separate data counters for collecting disk read rate, disk write rate, and disk usage data. Statistics for each counter are rolled up at specific collection intervals. Each data counter consists of several attributes that are used to determine the statistical value collected.

Collection levels determine the number of counters for which data is gathered during each collection interval. Collection intervals determine the time period during which statistics are aggregated, calculated, rolled up, and archived in the vCenter Server database. Together, the collection interval and collection level determine how much statistical data is collected and stored in your vCenter Server database.

You can configure statistical data collection intervals to set the frequency at which statistic queries occur, the length of time statistical data is stored in the database, and the type of statistical data that is collected. To configure a statistical interval, you can logon to the vSphere Client as a user with **Performance.ModifyIntervals** privilege and use the following procedure

Step 1. In the vSphere Client, select the vCenter Server instance in the inventory pane.

Step 2. Select the **Configure > Settings**

Step 3. Select **General > Edit**.

Step 4. To enable a statistics interval, select its checkbox.

Step 5. Set the following interval attributes using the provided dropdown menus.

- **Interval Duration:** The time interval in which statistics data is collected.
- **Save For:** The amount of time to keep statistics in the database.
- **Statistics Level:** The level of statistic data to be collected (1 to 4).

Step 6. (**Optional**) In **Database Size**, provide the following items and examine the estimated database size and number of rows.

- Number of Physical Hosts.
- Number of Virtual Machines.

Step 7. Click **Save**.

Table 13-7 contains the details for the default data collection intervals.

**Table 13-7** Collection Intervals

Collection Interval (Archive Length)	Collection Frequency	Default Behavior
1 Day	5 Minutes	<p>Real-time (20s) statistics are rolled up to create one data point every 5 minutes. The result is 288 data points every day.</p> <p>You can change the interval duration and archive length of the 1-Day collection interval by configuring the statistics settings.</p>
1 Week	30 Minutes	<p>1-Day statistics are rolled up to create one data point every 30 minutes. The result is 336 data points every week.</p> <p>You cannot change the default settings of the 1-Week collection interval.</p>
1 Month	2 Hours	<p>1-Week statistics are rolled up to create one data point every 2 hours. The result is 360 data points every month</p> <p>You cannot change the default settings of the 1-Month collection interval.</p>
1 Year	1 Day	<p>1-Month statistics are rolled up to create one data point every day. The result is 365 data points each year.</p> <p>You can change the archive length of the 1-Year collection interval by configuring the statistics settings.</p>

The default statistics level for all statistic intervals is 1. You can set the statistics level to a value between 1 and 4 inclusively. The lower the level is, the fewer number of statistics counters are used. Level 4 uses all statistics counters, but it typically only used for debugging purposes. When setting a statistics level for a specific statistics interval, you must use a value less than or equal to the statistics level for the preceding statistics interval. Table 13-7 provides a summary of the metrics that are included for each statistics level.

**Table 13-7** Statistics Levels

Level	Metrics	Best Practice
1	Cluster Services: all metrics  CPU: cpurentitlement, totalmhz, usage (average), usagemhz  Disk: capacity, maxTotalLatency, provisioned, unshared, usage (average), used  Memory: consumed, mementitlement, overhead, swapinRate, swapoutRate, swapused, totalmb, usage (average), vmmemctl (balloon)  Network: usage (average), IPv6  System: heartbeat, uptime  Virtual Machine Operations: numChangeDS, numChangeHost, numChangeHostDS	Use for long-term performance monitoring when device statistics are not required.
2	Level 1 metrics plus the following  CPU – idle, reservedCapacity  Disk – All metrics, excluding numberRead and numberWrite  Memory – All metrics, excluding memUsed and maximum and minimum rollup values.  Virtual Machine Operations – All metrics	Use for long-term performance monitoring when device statistics are not required but you want to monitor more than the basic statistics.
3	Level 1 and Level 2 metrics plus the following  Metrics for all counters, excluding minimum and maximum rollup values.  Device metrics	Use for short-term troubleshooting or when device statistics are required.  Due to the large quantity of data, use for the shortest (Day or Week) collection interval that suits your use case.
4	All metrics supported by the vCenter Server, including minimum and maximum rollup values.	Same best practice as Level 3, except only use Level 4 when you require metrics rollup values that are not available in Level 3.

**Note**

If you increase the collection level, you may need to allocate more storage and system resources to avoid a decrease in the performance.

## Verifying SSL Certificates for Legacy Hosts

You can configure vCenter Server and the vSphere Client to check for valid SSL certificates before connecting to a host for operations such as adding a host or making a remote console connection to a virtual machine. vCenter Server 5.1 and vCenter Server 5.5 always connect to ESXi hosts using SSL thumbprint certificates. Starting with vCenter Server 6.0, VMware Certificate Authority signs the SSL certificates by default.

You can instead replace certificates with certificates from a third-party CA. Thumbprint mode is supported only for legacy hosts. To configure SSL certificate validation, you can use the following procedure.

Step 1. In the vSphere Client, select the vCenter Server object in the inventory.

Step 2. Navigate to Configure > Settings > General.

Step 3. Click **Edit** and select **SSL settings**.

Step 4. Determine the host thumbprint for each legacy host that requires validation.

- a. Log in to the direct console
- b. Select **System Customization > View Support Information** on the **System Customization** and examine the thumbprint that displayed in the right column.

Step 5. Compare each host thumbprint with the thumbprint listed in the vCenter Server SSL settings dialog box.

Step 6. If the thumbprints match, select the check box for the host. Non-selected hosts will be disconnected after you click **Save**.

Step 7. Click **Save**.

## Update the vCenter Server

You can use the VAMI or the vCenter Server appliance shell to install patches.

### Patching with VAMI

To update a vCenter Server appliance, you may want to first stage the patches to the appliance, using the following procedure.

Step 1. Logon as root to the VAMI

Step 2. Click **Update**

Step 3. Click **Check Updates** and select one of the following sources.

a. Check URL

b. Check CDROM

Step 4. Optionally, choose **Run Pre-check**

Step 5. In the staging options section, click **Stage**.

**Note**

Other staging options include **Stage and Install**, **Unstage**, and **Resume**

If you choose to use the **Check URL** option, the vCenter Server uses the configured VMware repository URL. The default VMware repository URL requires Internet access. If your vCenter Server is not connected to the Internet or if required by your security policy, you can configure a custom repository URL for your vCenter Server patches using the following procedure.

Step 1. Download the vCenter Server appliance patch

ZIP file from VMware's website

(<https://my.vmware.com/web/vmware/downloads>).

Step 2. On a local Web server, create a repository directory under the root

Step 3. Extract the ZIP file into the repository director

Step 4. Logon as root to the VAMI

Step 5. Select Update > Settings

Step 6. Set the **Repository settings**: Choose **use specified repository**, provide the URL and

(optionally) the user credentials.

**Step 7. Click **OK**.**

After staging the patches to the vCenter Server, you can install the patches using the following procedure.

**Step 1. Logon as root to the VAMI**

**Step 2. Ensure the patches are staged, or use the staging procedure, but for the staging options, select **Stage and Install**.**

**Step 3. Click Update**

**Step 4. Select the range of patches to apply and click Install**

**Step 5. Read and accept the End User License Agreement (EULA)**

**Step 6. Wait for installation to complete, then click **OK****

**Step 7. If a reboot is required, click **Summary > Reboot**.**

**Note**

You should only perform the previous procedure during a maintenance period because the services provided by the vCenter Server become unavailable during the patch installation. As a precaution, you should also back up the vCenter Server prior to patching.

To configure vCenter Server to schedule automatic checks for available patches in the configured repository URL, you can use the following procedure.

**Step 1. Logon as root to the VAMI**

**Step 2. Verify the correct repository URL is set and available.**

**Step 3. Click Update > Settings**

**Step 4. Select Check for Updates Automatically**  
and set the day and time (in UTC) to check for available patches

### Patching with vCenter Server Appliance Shell

An alternate method for patching vCenter Server is the use its shell. For patching purposes, you should logon to the shell as a user with the Super Administrator role and use the commands in [Table 13-8](#) as needed.

**Table 13-8** Commands for Patching

Purpose	Command / Utility
View the full list of patches and software packages installed in the vCenter Server appliance, in chronological order.	<code>software-packages list --history</code>
View details about a specific patch.	<code>software-packages list --patch <i>patch_name</i></code>
Configure the vCenter Server to use a custom repository URL.	<code>update.set --currentURL <i>http://webserver/repo</i> [--username <i>username</i>] [--password <i>password</i>]</code>
Configure the vCenter Server to use the default VMware repository URL.	<code>update.set --currentURL default</code>
Enable automatic checks for vCenter Server appliance patches in the current repository.	<code>update.set --CheckUpdates enabled [--day <i>day</i>] [--time <i>HH:MM:SS</i>]</code>
Stage the patches from an attached ISO image.	<code>software-packages stage --iso</code>
Stage the patches from the current repository URL.	<code>software-packages stage --url</code>
Stage the patches from the repository URL that is not currently configured in the vCenter Server.	<code>software-packages stage --url <i>URL_of_the_repository</i></code>
Install the staged patches.	<code>software-packages install -staged</code>
Install patches directly from an attached ISO image.	<code>software-packages install --iso</code>
Install patches directly from the configured repository URL.	<code>software-packages install -url</code>
Install patches directly from a repository URL that is not currently configured in the vCenter Server.	<code>software-packages install --url <i>URL_of_the_repository</i></code>
Reboot the vCenter Server following a patch installation.	<code>shutdown reboot -r "patch reboot"</code>

**Note**

To stage only third party patches, include the `--thirdParty` option with the `software-packages stage` command. To directly accept the End User License Agreement (EULA), include the `--acceptEulas` option.

## Manage the vCenter HA Cluster

During normal operation, the vCenter HA cluster mode is **Enabled**, such that it is protecting vCenter Server from hardware and software failures. When the cluster detects the failure of the Active node, the Passive node attempts an automatic **failover**, such that the Passive node becomes the Active node. You can choose to perform a manual failover by choosing the **Initiate Failover** option in the vCenter HA settings in the vSphere Client. When performing a manual failover, you can choose to synchronize first or to force the failover without synchronization.

You can change the vCenter HA cluster mode to **Maintenance** when preparing to perform some maintenance activities. If the Passive or Witness nodes are unavailable (or recovering from a failure), a vCenter HA cluster mode may be disabled, such that the Active node continues as a standalone vCenter Server. When the cluster is operating in either **Maintenance** or **Disabled** mode, an Active node can continue serving client requests even if the Passive and Witness nodes are lost or unreachable.

To change the vCenter HA cluster mode, you can select the Active node in the vSphere Client, select **Configure** > **Settings** > **vCenter HA** > **Edit**, and change the option. You can choose **Enable vCenter HA**, **Maintenance Mode**, **Disable vCenter HA**, or **Remove vCenter HA cluster**.

You can use the following procedure to perform backup and restore operations on a vCenter HA cluster.

Step 1. Use the Active Node's VAMI to obtain a File-Based Backup up the Active vCenter Server node. (Do not back up the Passive node or Witness node.)

Step 2. Before you begin the restore operation, power off and delete all vCenter HA nodes and remove

the cluster configuration.

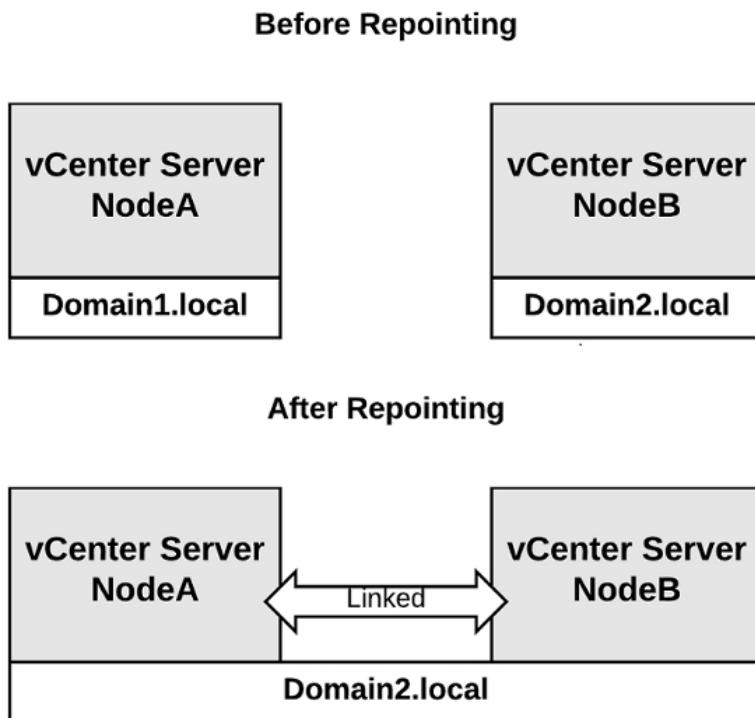
Step 3. Restore the Active node from the backup.

Step 4. The Active node is restored as a standalone vCenter Server.

Step 5. Reconfigure vCenter HA

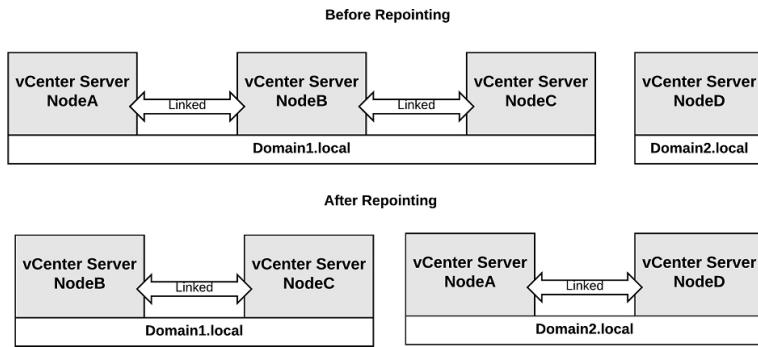
## Repoint a vCenter Server to Another Domain

You can repoint a vCenter Server from one SSO domain to another existing domain. The steps in the procedure depends on if the vCenter Server is the only node in the source domain and if it is being repointed to a new or an existing domain. Figure 13.3 illustrates repointing a vCenter Server (Node A) from a single-node domain to an existing domain.



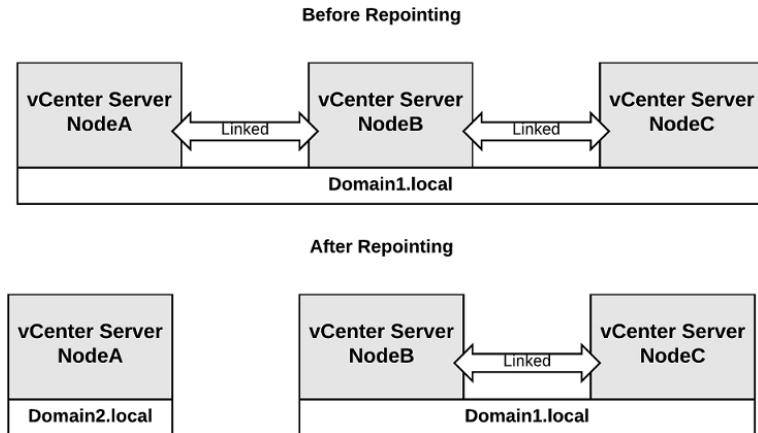
**Figure 13-3** Repoint vCenter to an Existing Domain

Figure 13.4 illustrates repointing a vCenter Server (Node A) from a multi-node domain to an existing domain.



**Figure 13-4** Repoint vCenter from a Multi-Node Domain

Figure 13.5 illustrates repointing a vCenter Server (Node A) from a multi-node domain to a new domain that is created with the repoint command.



**Figure 13-5** Repoint vCenter to a New Domain

If the source domain contains multiple (linked) vCenter Servers, then the repointing process involves additional steps to shut down the vCenter Server and unregister it from the source domain. If the vCenter Server is repointed a new domain, then you do not need to run a pre-check or supply the replication partner parameters. Repointing is only supported with vCenter Server 6.7 Update 1 and later. You should backup each node prior to repointing. To repoint a vCenter Server to another domain, you can use the following procedure.

Step 1. If multiple vCenter Servers exist in the source domain:

- a. Shut down the chosen vCenter Server.
- b. To unregister the chosen vCenter Server from the source domain, log into one of the other nodes in the source domain and run the following command, where the username and password are credentials for the source SSO domain administrator account.

```
cmsso-util unregister --node-pnid Target_vCenter_FQDN
```

- c. Power on the chosen vCenter Server.

Step 2. Ensure the chosen vCenter Server is powered on.

Step 3. If joining an existing domain:

- a. Ensure that a target replication partner (a vCenter Server in the existing domain) is powered on.
- c. Optionally run the following pre-check mode command from the chosen vCenter Server, which fetches tagging and authorization (roles and privileges) data and checks for conflicts between the source and destination.

```
cmsso-util domain-repoint -m pre-check --src-emb-admi
```

The pre-check writes the conflicts to the /storage/domain-data directory.

- d. Optionally, check conflicts and apply one of the following resolutions to all conflicts or separately to each conflict.

- **Copy:** Create a duplicate copy of the data in the target domain.
- **Skip:** **Skips copying the data in the target domain.**
- **Merge:** **Merges the conflict without creating duplicates.**

The default resolution mode for Tags and Authorization conflicts is **Copy**.

Step 4. Run the following execute command, which applies any pre-check data and either repoints the chosen vCenter Server to the existing domain or creates a new domain for repointing. If the chosen vCenter Server is being pointed a new domain, then you do not need to supply the replication partner parameters.

```
cmsso-util domain-repoint -m execute --src-emb-admin
```

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, [Chapter 15, "Final Preparation,"](#) and the exam simulation questions on the CD-ROM.

## REVIEW ALL KEY TOPICS

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 13-9](#) lists a reference of these key topics and the page numbers on which each is found.

**Table 13-9** Key Topics for Chapter 13

Key Topic Element	Description	Page Number
Procedure	Restore vCenter Server	
Table 13-2	vCenter Server 7.0 Compatibility	
List	Prerequisites for Upgrading vCenter Server Appliance	
Section	Migrate vCenter Server for Windows to vCenter Server	
Table 13-3	Lifecycle Manager Remediation Settings	
Procedure	Create a Dynamic Baseline	
Procedure	Enable Quick Boot	
Table 13-5	Management Tasks Using the VAMI	
Table 13-6	Management Tasks Using the vSphere Client	

## DEFINE KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary:

VMware vSphere Life Cycle Manager

Image

VMware vSphere Update Manager Download Service (UMDS)

Base Image

Add-on

Baseline

## Glossary

**VMware vSphere Life Cycle Manager:** VMware vSphere Life Cycle Manager is a service, which runs in vCenter Server, that provides simple, centralized lifecycle management for ESXi hosts and clusters using images and baselines.

**Image:** In vSphere Lifecycle Manager, an image is a description of which software, drivers, and firmware to run on a host.

**UMDS:** VMware vSphere Update Manager Download Service (UMDS) is an optional module of vSphere Lifecycle Manager, whose primary function is to

download data when Lifecycle Manager does not have Internet connectivity.

**Base Image:** The ESXi base image, which is the ESXi image that VMware provides with each release of ESXi, is a complete of components that can boot up a server.

**Add-on:** In vSphere Lifecycle Manager, A vendor add-on is a collection of components that you can use to customize an ESXi image with OEM content and drivers.

**Baseline:** In vSphere Lifecycle Manager, a baseline is a set of bulletins.

## REVIEW QUESTIONS

- 1.** You need to restore the vCenter Server from a file-based backup. Which of the following will not be restored?
  - a.** Resource pool hierarchy and setting
  - b.** vSphere DRS Cluster state
  - c.** Cluster-host membership
  - d.** vSphere DRS DRS configuration and rules
  
- 2.** You plan to upgrade a Windows based vCenter Server to vCenter Server appliance 7.0 and want to transfer data in the background. Which of the following can be included in the background transfer?
  - a.** Configuration data only
  - b.** Configuration data and performance data.
  - c.** Performance data
  - d.** Data from the extended database

**3.** You are configuring remediation setting for Lifecycle Manager. Which of the following settings are only available when working with baselines?

- a.** PXE booted hosts and removable media devices
- b.** Quick boot and VM Power State
- c.** VM Migration and VM Power State
- d.** VM Migration and Maintenance Mode Failures.

**4.** Your vCenter Server is offline and the distributed switch for an ESXi host management network is not functioning. Which one of the following steps may fix the ESX management connectivity?

- a.** Use the Host Client to restart ESXi networking
- b.** Use the vSphere Client to restart ESXi networking
- c.** Use SSH to restart ESXi networking
- d.** In the DCUI, select Restore Standard Switch

**5.** You are repointing a vCenter Server to an existing domain. In which one of the following scenarios would you need to run a pre-check?

- a.** Multiple vCenter Servers exist in the target domain.
- b.** Multiple vCenter Servers exist in the source domain
- c.** A single vCenter Server exists in the target domain

- d.** A single vCenter Server exists in the source domain

# **Chapter 14. Manage Virtual Machines**

This chapter covers the following topics:

- Create and Configure Virtual Machines
- Manage Virtual Machines
- Advanced Virtual Machine Management
- Content Library

This chapter contains information related to VMware  
2V0-21.20 exam objectives 4.7, 5.6, 7.1, 7.2, 7.3, 7.6,  
7.11.4

This chapter provides details on managing virtual machines.

## **“DO I KNOW THIS ALREADY?” QUIZ**

The “Do I Know This Already?” quiz allows you to assess whether you should study this entire chapter or move quickly to the “Exam Preparation Tasks” section.

Regardless, the authors recommend that you read the entire chapter at least once. **Table 14-1** outlines the major headings in this chapter and the corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

**Table 14-1** “Do I Know This Already?” Section-to-Question Mapping

---

Foundation Topics Section	Questions
Create and Configure Virtual Machines	1,2,3
Manage Virtual Machines	4,5,6
Advanced Virtual Machine Management>	7,8
Content Library	9.10

- 1.** You are creating a virtual machine in your vSphere 7.0 environment and you want the virtual disk and NVDIMM devices to share the same PMem resources. Which of the following options should you choose?
- a.** In the memory settings, select PMem
  - b.** In the memory settings, select Standard
  - c.** In the Storage Type settings, select PMem
  - d.** In the Storage Type settings, select Standard
- 2.** You want to change the logging for the VMware Tools installation, such that `vminst.log` is sent to the host, but `vmmsi.log`. Which option should you choose?
- a. `vmx.log.guest.level = "warning"`**
  - b. `vmx.log.guest.level = "info"`**
  - c. `vmx.log.guest.level = "verbose"`**
  - d. `vmx.log.guest.level = "trivia"`**
- 3.** You want to deploy new virtual machines using Linked Clones. Which of the following should you use?
- a. vSphere API**
  - b. vSphere Client**
  - c. Host Client**
  - d. vCenter Management Interface**

- 4.** You are updating a virtual machine and want to use hardware version 14. Which of the following Compatibility Settings should you choose?
- a.** ESXi 7.0 and later
  - b.** ESXi 6.7 Update 2 and later
  - c.** ESXi 6.7 and later
  - d.** ESXi 6.5 and later
- 5.** You want to control the host compatibility for your virtual machines at various levels of the inventory. On which of the following objects can you set the **Default VM Compatibility** option?
- a.** Cluster
  - b.** VM folder
  - c.** Virtual machine
  - d.** template
- 6.** Which options should you choose to minimize the time required to create a virtual machine snapshot?
- a.** Snapshot the memory and quiesce the file system.
  - b.** Snapshot the memory, but do not quiesce the file system.
  - c.** Quiesce the file system, but do Not snapshot the memory
  - d.** Do not quiesce the file system or snapshot the memory
- 7.** You want to enable Microsoft virtualization-based security (VBS) for a Windows virtual machine in a vSphere environment. Which of the following is a requirement?

- a.** vSphere 7.0 or later
  - b.** virtual machine hardware version 17 or later
  - c.** IOMMU
  - d.** Windows 8 or later
- 8.** You are considering whether to use vGPUs for some of the virtual machines in your vSphere environment. Which of the following is not a common use case for vGPUs?
  - a.** Fast provisioning
  - b.** High end graphics in VDI
  - c.** Machine Learning
  - d.** Artificial Intelligence
- 9.** You are setting permissions for a vCenter Server. You want to ensure a specific user can manage the vCenter Server's content libraries and content but can only view content libraries belonging to other vCenter Servers. Which settings should you make?
  - a.** Grant the **Read Only** role as a global permission and the **Administrator** role on the vCenter Server
  - b.** Grant the **Content Library Administrator** role as a global permission and **Administrator** role on the vCenter Server
  - c.** Grant just the **Administrator** role on the vCenter Server
  - d.** Grant just the **Content Library Administrator** role on the vCenter Server
- 10.** You want to add items to the content library. Which of the following is not a valid choice?
  - a.** You can import a vApp

- b.** You can select a virtual machine and choose Clone to Template in Library.
- c.** You can import an ISO
- d.** You can migrate a virtual machine to the library.

## CREATE AND CONFIGURE VIRTUAL MACHINES

You can use the vSphere Client to create and manage virtual machines. The associated procedures are intuitive. The following sections summarize each procedure and provide some related details, such as the required privileges.

### Create a New Virtual Machine



The following list contains the required privileges for creating a virtual machine.

- **Virtual machine.Inventory.Create new** on the destination folder or data center.
- **Virtual machine.Configuration.Add new disk** on the destination folder or data center (when adding a new disk).
- **Virtual machine.Configuration.Add existing disk** on the destination folder or data center (when adding an existing disk).

- **Virtual machine.Configuration.Configure**  
**Raw device** on the destination folder or data center (when using a Raw Device Mapping (RDM) or SCSI pass-through device).
- **Virtual machine.Configuration.Configure**  
**Host USB device** on the destination folder or data center (when attaching a virtual USB device backed by a host USB device).
- **Virtual machine.Configuration.Advanced configuration** on the destination folder or data center (when configuring advanced virtual machine settings).
- **Virtual machine.Configuration.Change**  
**Swapfile placement** on the destination folder or data center (when configuring swap file placement).
- **Virtual machine.Configuration.Toggle disk change tracking** on the destination folder or data center (when enabling change tracking on the virtual machine's disks).
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.
- **Network.Assign network** on the network where the virtual machine will be connected.

To create a virtual machine, you can use the **New Virtual Machine** wizard and select **Create a new virtual machine**. In the wizard, you should provide all required information, including compute resource (host, cluster, or resource pool, or vApp), the storage type and location, virtual machine compatibility, guest OS, Windows Virtualization Based Security (for a Windows virtual machine), and hardware customization.

When selecting the **Storage Type** on a host that has PMem memory, you can select either the **Standard** or **PMem** radio button. If you chose PMem storage for a virtual machine, its default virtual disk, new virtual disk, and NVDIMM devices share the same PMem resources. You should adjust the size of newly added devices. The wizard alerts you if issues exist.

## Power on VM

To power on a virtual machine, you can right-click the virtual machine and choose **Power On**. Some likely causes of power-on failures are provided in the following list.

- Evaluation period (or license) has expired
- Insufficient permissions
- Insufficient storage space to create files, such as the swap file.
- Assigned MAC address conflicts with VMware reserved MACs
- Operation would violate admission control.

## Open Console to VM

To open a console to the virtual machine, you can use an integrated web-based console or the independent VMware Remote Console (VMRC). To use the integrated web-based console, you should ensure the virtual machine is powered, select it in the inventory pane, and either choose **Launch Web Console** in the vSphere Client or **open browser console** in the Host Client.

To use the VMRC to access a virtual machine, you should first ensure it is installed on your local system and, if necessary, prepare a proxy server. Then you can launch it from the vSphere Client or the VMware Host client. In the vSphere Client, select the virtual machine in the

inventory pane and select **Summary > Launch**

**Remote Console.** In the Host Client, select the virtual machine in the inventory pane and select **Console > Launch Remote Console.**

To configure a proxy server for VMware Remote Console, you can browse to `vmrc://settings` or use the menu if VMware Remote Console is already open. Choose **Preferences** in the appropriate menu as described in the following list.

- On Windows, select **VMRC > Preferences**.
- On macOS, select **VMware Remote Console > Preferences**.
- On Linux, select **File > Remote Console Preferences**.

The main steps are to select the **Enable proxy for remote virtual machine option** and to set the appropriate settings, such as the proxy server's hostname or IP (IPv4 or IPv6) address and port, and optionally provide user credentials. The specific steps depend on the OS type (windows, Linux, or macOS).

**Note**

In VMRC version 11.0, the `VMWARE_HTTPSPROXY` environment variable, which is used to set a proxy server in previous versions of VMRC, is ignored after applying the previous procedure. To use authentication with the proxy server, you must use the previous procedure instead of the environment variable.

## Install and Upgrade VMware Tools

You can install VMware Tools in the guest OS of your virtual machines to enable several features that improve manageability and smooth user interaction. To interactively install VMware Tools using the vSphere Client, you can right-click on a virtual machine, select **Guest OS > Install VMware Tools** and select **Mount**, which connects the virtual machine's first

virtual CD-ROM disk drive to the appropriate VMware Tools ISO file based on your guest operating system.. If autorun is configured in the guest OS, the VMware Tools installation may begin automatically. Otherwise, you may need to interactively launch the installer in the guest OS. For example, you may need to launch `d:\setup.exe` in a Windows 64 guest. In many cases, the default installation is adequate. If you need non-default components, such as the Guest Introspection Thin Agent driver, select **Custom** setup.

The open source implementation of VMware Tools for Linux is Open VM Tools.

Whenever a new VMware Tools version is available, such as following an ESXi upgrade, you should consider upgrading your virtual machines. You should always upgrade VMware Tools prior to upgrading the virtual machine hardware. You can use the same procedure as you used to install VMware Tools, except choose

### **Upgrade VMware Tools.**

Previous versions of vSphere allow you to use Update Manager to upgrade virtual machine hardware and VMware Tools. In vSphere 7.0, you can use the vSphere Client directly to upgrade the hardware and VMware Tools for a set of virtual machines in a container, such as a folder or cluster, as described in the *Upgrade Virtual Machines* section in [Chapter 13](#).

VMware Tools Lifecycle Management provides a simplified and scalable approach for installation and upgrade of VMware Tools. You can configure your virtual machine to automatically check for and apply VMware Tools upgrades each time you power on your virtual machine. Automatic Tools upgrade is not supported for Solaris or Netware guests. The prerequisites for automatic VMware Tools upgrade are that the virtual machines must be hosted by ESX / ESXi 3.5 or later,

must be managed by vCenter Server 3.5 or later, must be using VMware Tools shipped with ESX / ESXi 3.5 or later, and must be running a guest OS that is supported for ESX / ESXi 3.5 and vCenter Server 3.5 or later.

You can set the `vmx.log.guest.level` option as described in [Table 14-2](#) to control the use of log files for VMware Tools installation.

**Table 14-2** Installer Log Options

<b>Value</b>	<b>Description</b>
<code>vmx.log.guest.level = "off"</code>	Logging to host is disabled. (default value)
<code>vmx.log.guest.level = "error"</code>	<code>vminst.log</code> and <code>vmmsi.log</code> remain in the virtual machine and are not sent to the host.
<code>vmx.log.guest.level = "warning"</code>	<code>vminst.log</code> and <code>vmmsi.log</code> remain in the virtual machine and are not sent to the host.
<code>vmx.log.guest.level = "notice"</code>	<code>vminst.log</code> and <code>vmmsi.log</code> remain in the virtual machine and are not sent to the host.
<code>vmx.log.guest.level = "info"</code>	<code>vminst.log</code> is sent to the host but <code>vmmsi.log</code> remains in the virtual machine.
<code>vmx.log.guest.level = "verbose"</code>	<code>vminst.log</code> and <code>vmmsi.log</code> are sent to the host.
<code>vmx.log.guest.level = "trivia"</code>	<code>vminst.log</code> and <code>vmmsi.log</code> are sent to the host.

When using the `setup.exe` command to install VMware Tools, you can use the `/mg` or the `"LOGMODE=G"` options to control and suppress logging to the host. To suppress logging during automatic upgrades, you can set the `install-vmxGuestLogDisabled` parameter to `true` in the **tools.conf** file. To use the `tools.conf` file in some versions of Windows, you may need to create the file and deal with a hidden Application Data or Program Data file. To do so, you could open a text editor (such as Notepad) using **Run as administrator**. If you change the `tools.conf` file, you do not need to restart VMware Tools. By default, the tools service will check the config file every 5 seconds for changes.

## Shutdown Guest

To stop the virtual machine gracefully, you can right-click on a virtual machine, choose **Power > Shutdown Guest**. This operation, which requires that VMware Tools is running in guest OS, will safely stop the guest OS and power-down the virtual machine. If **Shutdown Guest** is not available for a virtual machine, a likely cause is that VMware Tools is not installed or not running.

## Clone a Virtual Machine

You can clone a virtual machine to a template. The following list contains the required privileges.

- **Virtual machine.Provisioning.Create** template from virtual machine on the source virtual machine.
- **Virtual machine.Inventory.Create from existing** on virtual machine folder where the template is created.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on all datastores where the template is created

To clone a virtual machine to template, right-click the virtual machine, select **Clone > Clone as Template**, and complete the wizard. In the wizard, provide a template name, folder, compute resource, and datastore.

**Note**

You cannot change the storage policy if you clone an encrypted virtual machine.

You can clone a virtual machine to a create a new virtual machine. The following list contains the required privileges.

## Key Topic

- **Virtual machine.Provisioning.Clone** virtual machine on the virtual machine you are cloning.
- **Virtual machine.Inventory.Create from existing** on the data center or virtual machine folder.
- **Virtual machine.Configuration.Add new disk** on the data center or virtual machine folder.
- **Resource.Assign virtual machine to resource pool** on the destination host, cluster, or resource pool.
- **Datastore.Allocate space** on the destination datastore or datastore folder.
- **Network.Assign network** on the network to which you assign the virtual machine.
- **Virtual machine.Provisioning.Customize** on the virtual machine or virtual machine folder (when customizing the guest operating system).
- Virtual machine.Provisioning.Read customization specifications on the root vCenter Server (when customizing the guest operating system).

You can clone a virtual machine to create a new virtual machine by right clicking the virtual machine and selecting **Clone > Clone to Virtual Machine**. In the wizard, you should provide all required information, such as name, compute resource, compatibility, and storage. The procedure is much like the procedure in the *Deploy Virtual Machine from Template* section in this chapter, including the option to customize the guest OS.

**Note**

You cannot use the vSphere Client to clone a virtual machine using linked clones or instant clones. You can do so with API calls.

If the source virtual machine has an NVDIMM device and virtual PMem hard disks, the destination host or cluster must have an available PMem resource. If the virtual machine has virtual PMem hard disks, but does not have an NVDIMM device, the destination host or cluster must have an available PMem resource.

Otherwise, all hard disks of the destination virtual machine will use the storage policy and datastore selected for the configuration files of the source virtual machine.

## Convert Between VM and Template

You can right-click a powered down virtual machine, choose **Template > convert to template**.

You can convert a template to a virtual machine. This is useful when you want to install new software and guest OS updates in the template. To do so, right-click the template and select **Convert Template to Virtual Machine**. You need the following privileges

- **Virtual machine.Provisioning.Mark as virtual machine** on the source template.
- **Resource.Assign virtual machine to resource pool** on the target resource pool

## Deploy Virtual Machine from Template

The following list contains the required privileges for deploying a virtual machine from a template.

- **Virtual machine.Inventory.Create from existing** on the data center or virtual machine folder.

- **Virtual machine.Configuration.Add new disk** on the data center or virtual machine folder.  
(when adding a new virtual disk).
- **Virtual machine.Provisioning.Deploy** template on the source template.
- **Resource.Assign virtual machine to resource pool** on the target host, cluster, or resource pool.
- **Datastore.Allocate space** on the target datastore.
- **Network.Assign network** on the target network.  
(when adding a new network card.)
- **Virtual machine.Provisioning.Customize** on the template or template folder (when customizing the guest operating system).
- **Virtual machine.Provisioning.Read customization specifications** on the root vCenter Server (when customizing the guest operating system)

To deploy a virtual machine from template, right-click the template and select **Clone Deploy from template**. In the wizard, you should provide all required information, such as name, compute resource, compatibility, storage, and guest customization options. The guest customization choices are **Select an existing specification**, **Create a specification** and **Create a specification from an existing application**.

## **Customize the Guest OS**

When you clone a virtual machine to template or to a new virtual machine, you have the option to customize the guest OS. Additionally, other scenarios may allow you to customize a guest OS. This section describes guest OS customization.

You can customize the guest OS to change the computer name, network settings, and guest OS licensing to prevent conflicts in the environment. During a cloning operation, you can provide the customization settings or select a pre-built customization specification.

Guest OS customization requires a supported guest OS installed on SCSI node 0:0 and VMware Tools. Windows guest customization requires ESXi version 3.5 or later. Linux guest customization requires Perl in the guest OS. To customize a Linux guest OS, you need to install VMware Tools 10.10.10 or later and enable the `enable-custom-scripts` option (disabled by default).

Optionally, you can create a custom application for vCenter Server to use to generate computer names and IP addresses during guest customization. To do so, create a custom script based on the sample reference script (`sample-generate-name-ip.pl`) found in VMware KB Article 2007557 and configure the associated vCenter Server advanced settings. For example, set `config.guestcust.name-ip-generator.program` to `c:\perl\bin\perl.exe` and set `config.guestcust.name-ip-generator.arg1` to `c:\sample-generate-name-ip.pl`.

You can use the following procedure to create a guest customization specification for Linux.



**Step 1.** In the vSphere Client, navigate to Menu > Policies and Profiles > VM Customization Specifications.

**Step 2.** Click the Create a new specification icon.

**Step 3.** On the **Name and target OS** page, enter a name and a description for the customization specification, select **Linux** as a target guest OS, and click **Next**.

**Step 4.** On the **Computer name** page, configure one of the following options for assigning the computer name.

- **Use the virtual machine name**
- **Enter a name in the Clone / Deploy wizard**
- **Enter a name** (For this option, enter a name in the provided box and optionally select **Append a numeric value** checkbox)
- **Generate a name using the custom application configured with vCenter Server.** (For this option, optionally enter a parameter to pass to the application.)

**Step 5.** Enter the **Domain Name** and click **Next**.

**Step 6.** Select the **Time Zone** and click **Next**.

**Step 7.** On the **Customization Script** page, you can optionally provide a script to run in the guest OS and click **Next**.

**Step 8.** On the **Network** page, you can choose one of the following options and click **Next**.

- **Use standard network settings** (use DHCP to assign IP configuration.)
- **Manually select custom settings** (vCenter Server will prompt the user to provide the IP configuration for each virtual NIC when using the guest customization specification)

**Step 9.** On the **DNS settings** page, enter the DNS server and domain settings.

**Step 10.** Complete the wizard and click **Finish**.

To create a guest customization specification for Windows, you can use the previous procedure with the following modifications.



- On the **Name and target OS** page, select **Windows** as a target guest OS and optionally select **Generate a new security identity (SID)**.
- On the **Set Registration Information** page, enter the virtual machine owner's name and organization and click **Next**.
- On the **Windows license** page, provide a Windows product key. For a Windows Server specification, either select the **Per Seat** option or configure the maximum concurrent connections for the **Per Server** option. Click **Next**.
- On the **Set Administrator Password** page, configure the password, optionally select **Automatically logon as Administrator** option, and click **Next**.
- On the **Networking** page, if you choose the **Manually select custom settings**, then use the **DNS tab** to provide DNS server details and click **WINS** to provides WINS details.
- On the **Set Workgroup or Domain** page, either provide a workgroup name or provide user credentials and a domain name, and click **Next**

Whenever you create a new virtual machine by deploying from template or by cloning, you can use the wizard to

select the **Customize the operating system** checkbox and select the appropriate specification. To customize an existing virtual machine, right-click the virtual machine in the inventory pane, select **Guest OS > Customize Guest OS** and select the appropriate specification.

As needed, you can manage guest customization specifications by navigating to **Menu > Policies and Profiles > VM Customization Specifications**. Here, you can import guest customization specifications. You can also select a specific specification and select one of the following actions.

- **Edit customization spec**
- **Duplicate customization spec**
- **Export customization spec**
- **Delete customization spec**

## Deploy OVF / OVA Templates

Another method for deploying virtual machines is to leverage Open Virtual Format (OVF) or Open Virtual Appliance (OVA) templates. You can use the vSphere Client to deploy an OVF or OVA template. You can export a virtual machine, virtual appliance, or vApp as an OVF or OVA template to create virtual appliances that can be imported by other users. Compared to other methods, using OVF to export and import virtual machines provides the following benefits.

- Compressed data (faster downloads and uploads)
- Validation of the OVF by vCenter Server prior to importing
- Encapsulation of multiple virtual machines.

OVA is essentially a single-file distribution of an OVF package. Prior to vSphere 6.5, the Client Integration

Plug-In is required to export and import OVF and OVA templates. Starting in vSphere 6.5, you can only export to OVF. Deploying a virtual machine from an OVF template is commonly referred to as deploying an OVF.

To deploy an OVF, you can use the following procedure.

**Step 1.** In the vSphere Client, right click on a cluster in the inventory pane.

**Step 2.** Select Deploy OVF Template.

**Step 3.** In Select OVF Template page, specify the path to the OVF file as a URL or local file and click **Next**.

**Step 4.** Use the wizard to provide information for the new virtual machine, such as name, folder, and compute resource.

**Step 5.** On the Review details page, verify the OVF template details, such as publisher, download size, and size on disk. Click **Next**.

**Step 6.** Complete the wizard by providing typical details for a new virtual machine, such as storage policy, storage location, and network configuration.

**Step 7.** Optionally customize the deployment properties on the **Customize template** page.

**Step 8.** Optionally, select a binding service provider on the **vService bindings** page.

**Step 9.** On the Ready to complete page, click Finish.

## MANAGE VIRTUAL MACHINES

This section covers reoccurring activities that you may perform regarding virtual machines.

## Configure Virtual Machine Hardware

When creating or upgrading a virtual machine, you can configure the virtual machine compatibility setting, which controls the ESXi versions on which the virtual machine can run. The compatibility setting controls which virtual machine hardware version is used. The main use cases for configuring the compatibility setting to a version earlier than the default for the host are to maintain compatibility with older hosts and to standardize virtual machine deployment in your environment. The main downside of configuring the compatibility setting to a version earlier than the default for the host is the virtual machine may not be able to use virtual hardware features supported by the host and may not achieve the best performance. [Table 14-3](#) describes virtual machine compatibility options.

**Table 14-3** Virtual Machine Compatibility Options

Compatibility Setting	Hardware Version
ESXi 7.0 and later	Hardware version 17
ESXi 6.7 Update 2 and later	Hardware version 15
ESXi 6.7 and later	Hardware version 14
ESXi 6.5 and later	Hardware version 13
ESXi 6.0 and later	Hardware version 11
ESXi 5.5 and later	Hardware version 10
ESXi 5.1 and later	Hardware version 9.
ESXi 5.0 and later	Hardware version 8
ESX/ESXi 4.0 and later	Hardware version 7
ESX/ESXi 3.5 and later	Hardware version 4

**Note**

ESXi 5.0 allows you to run virtual machines with ESX/ESXi 3.5 and later compatibility (hardware version 4), but does not allow you to create them.

The compatibility setting impacts the supported features for the virtual machine. [Table 14-4](#) contains some of the feature sets available in recent hardware versions.

**Table 14-4** Features by Recent Virtual Machine Hardware Versions

Feature	Ver 17	Ver 15	Ver 14	Ver 13	Ver 11
Maximum memory (GB)	6128	6128	6128	6128	4080
Maximum number of logical processors	256	256	128	128	128
Maximum number of cores (virtual CPUs) per socket	64	64	64	64	64
NVMe controllers	4	4	4	4	N
Maximum NICs	10	10	10	10	10
USB 3.1 SuperSpeedPlus	Y	N	N	N	N
Maximum video memory (GB)	4	2	2	2	2
Dynamic DirectPath	Y	N	N	N	N
PCI Hot add support	Y	Y	Y	Y	Y
Virtual Precision Clock device	Y	N	N	N	N
Virtual Watchdog Timer device	Y	N	N	N	N
Virtual SGX device	Y	N	N	N	N
Virtual RDMA	Y	Y	Y	Y	N
NVDIMM controller	1	1	1	N	N
NVDIMM device	64	64	64	N	N
Virtual I/O MMU	Y	Y	Y	N	N
Virtual TPM	Y	Y	Y	N	N
Microsoft VBS	Y	Y	Y	N	N

To control the default hardware compatibility for new virtual machines, you can set the **Default VM**

**Compatibility** setting at the host, cluster, or data center levels. The settings on a host override the settings on a cluster, which override the settings on the data center. To make the settings on a host or cluster, you must have **Host.Inventory.Modify cluster** privilege. To make the settings on a data center, you must have **Datacenter.Reconfigure datacenter** privilege.

You can upgrade the compatibility level of an existing virtual machine but should first upgrade VMware Tools. For example, you can select a virtual machine and use the **Compatibility > Schedule VM Compatibility Upgrade** option to upgrade the compatibility the next time you restart the virtual machine. Optionally, you can select **Only upgrade after normal guest OS**

**shutdown** to upgrade compatibility during regularly scheduled guest maintenance.

You can change the number of virtual CPUs used by a virtual machine. Specifically, you can set the number of cores and cores per socket. In ESXi 7.0, the maximum number of virtual CPU sockets is 128. To configure a virtual machine with more than 128 virtual CPUs, you must use multicore virtual CPUs.

By default, you cannot add CPU resources to a virtual machine when it is turned on. To change this behavior, you can enable the virtual machine's **CPU hot add** option, but the following conditions apply.



- For best results, use virtual machine compatibility set to ESXi 5.0 or later.
- Hot adding multicore virtual CPUs requires compatibility set to ESXi 5.0 or later.
- You cannot use hot adding to increase the number of virtual CPUs for a virtual machine with 128 virtual CPUs or less,
- You can use hot adding to increase the number of virtual CPUs for a virtual machine that already has more than 128 virtual CPUs.
- You can disable hot-add for virtual machines with guest operating systems that do not support CPU hot add.
- For virtual machines with compatibility set to **ESXi 4.x and later**, to support CPU hot add, set the **Number of cores per socket** to 1.

- Hot adding CPU resources to a virtual machine disconnects and reconnects all USB passthrough devices.

To enable CPU hot add, the following prerequisites apply.

- Latest VMware Tools version.
- Guest operating system that supports CPU hot add.
- Virtual machine compatibility is set to a minimum of **ESX/ESXi 4.x or later**.
- Virtual machine is turned off.
- Required privileges: Virtual Machine.Configuration.Settings

CPU identification (CPU ID) masks control the visibility of CPU features to guest OS. Masking CPU features can impact a virtual machine availability for migration using vMotion. For example, if you mask the AMD No eXecute (NX) or the Intel eXecute Disable (XD) bits, you prevent the virtual machine from using those features, but you allow the virtual machine to hot-migrate to hosts that do not include this capability

**Note**

Changing the CPU compatibility masks can result in an unsupported configuration. Do not manually change the CPU compatibility masks unless instructed to do so by VMware Support or a VMware Knowledge base article.

During specific management operations, such as creating a virtual disk, cloning a virtual machine to a template, or migrating a virtual machine, you can set the provisioning policy for the virtual disk file. You can use Storage vMotion or other cross datastore migrations to transform virtual disks from one format to another. The available virtual disk provisioning policies are described in [Table 14-5](#).

**Table 14-5** Virtual Disk Provisioning Policies

Provisioning policy	Description	Sample Use Case
Thick Provision Lazy Zeroed	All the provisioned space is allocated during creation. Data is zeroed on the first demand from the virtual machine.	Minimizes the risk of exhausting free datastore space.
Thick Provision Eager Zeroed	All the provisioned space is allocated and zeroed (erased) during creation	Required for some clustering features, such as Fault Tolerance.  Provides the best performance.
Thin Provision	Space is allocated and zeroed on demand, as needed, up to the provisioned space	Fastest method to provision and migrate virtual disks.

You can change a virtual disk from the thin format to thick format by navigating to **Datastore > Files** in the vSphere Client and choosing the **Inflate** action for the virtual disk file. The vSphere Client does not provide a deflate option. To change a virtual disk provisioning type from thick to thin, you can migrate the virtual machine storage and select the appropriate policy.

Creating and growing a virtual disk provisioned for Thick Provision Eager Zeroed may take significantly longer than a virtual disk provisioned for Thick Provision Lazy Zeroed.

You can configure virtual machines with virtual disks greater than 2 TB (large capacity virtual disks), but you must meet resource and configuration requirements. The maximum size for large capacity virtual disks is 62 TB. You should avoid using the maximum size, because some operations, such as those involving snapshot and linked clones, may not finish when the maximum amount of disk space is allocated to a virtual disk. Operations such as snapshot quiesce, cloning, Storage vMotion, and vMotion in environments without shared storage, can take significantly longer to finish. The following conditions and limitations apply to virtual machines with large capacity disks.

- You must use a guest OS that supports large capacity virtual hard disks.
- Target hosts for migration and clone operations must use ESXi 6.0 or later.

- NFS, vSAN, and VMFS5 or later datastores are supported.
- Fault Tolerance is not supported.
- BusLogic Parallel controllers are not supported.

To increase the size of a virtual disk, you need the following privileges.

- **Virtual machine.Configuration.Modify device settings** on the virtual machine.
- **Virtual machine.Configuration.Extend virtual disk** on the virtual machine.
- **Datastore.Allocate space** on the datastore.

To control how a virtual disk is impacted by snapshots, you can set the disk mode for a virtual disk to the settings described in [Table 14-6](#).

**Table 14-6** Virtual Disk Mode Settings

Disk mode	Description
Dependent	Included in snapshots.
Independent - Persistent	Not included in snapshots.  All data written are written permanently to disk.
Independent – Nonpersistent	Not included in snapshots.  Changes are discarded when you turn off or reset the virtual machine.

You can set shares for a virtual disk, which work much like CPU or memory shares for a virtual machine. The disk shares provide a relative priority for accessing the disk during periods of disk I/O contention for the underlying storage. The values **Low**, **Normal**, **High**, and **Custom** are compared to the sum of all shares of all virtual machines on the host. To control the maximum amount of disk I/O for a virtual disk, you can set the virtual disk's **Limit - IOPs** value. By default, the virtual disk is set for normal shares and unlimited IOPs.

You can add virtual disks to virtual machines, including new virtual disks, existing virtual disks, and Raw Device Mappings (RDMs). To add an RDM to a virtual machine, you need to use a account with the **Virtual machine.Configuration.Configure Raw device** privilege, select a target LUN, choose where to store the mapping file, choose a compatibility mode (physical or virtual), and select a disk mode. Disk modes are not available for RDMs using physical compatibility mode.

A storage controller is included by default when you create a virtual machine. You can add additional SCSI controllers (BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS, and VMware Paravirtual SCSI), AHCI, SATA, and NVM Express (NVMe) controllers. The following limitations apply to storage controllers.

- **ESXi 4.x and later compatibility** is required for LSI Logic SAS and VMware Paravirtual SCSI.
- **ESXi 5.5 and later compatibility** is required for AHCI SATA
- **ESXi 6.5 and later compatibility** is required for NVMe
- BusLogic Parallel controllers do not support large capacity disks.
- Disks on VMware Paravirtual SCSI controllers may not provide the expected performance if they have snapshots or if the host's memory is overcommitted.

Before changing the storage controller type, you should ensure the guest OS has the drivers for the target controller type, or the disks will become inaccessible. Likewise, in the following cases, adding storage controller types to a virtual machine that use BIOS firmware may cause boot problems and require you to fix by entering the BIOS setup.

- If the virtual machine boots from LSI Logic SAS or VMware Paravirtual SCSI, and you add a disk that uses BusLogic, LSI Logic, or AHCI SATA controllers.
- If the virtual machine boots from AHCI SATA, and you add BusLogic Parallel or LSI Logic controllers.

**Note**

Adding additional disks to virtual machines that use EFI firmware does not cause boot problems.

## Edit Virtual Machine Options

You can edit a virtual machine and use the **VM Options** tab for multiple purposes, such as setting VMware Tools scripts, controlling user access to the remote console, configuring startup behavior, and changing the virtual machine name, as summarized in Table 14-7.

**Table 14-7** Settings on the Virtual Machine Options Tab

Options	Description
General Options	Virtual machine name  View Only: Configuration file location, working location, guest OS type and version
VMware Remote Console Options	Locking behavior, simultaneous connections.
Encryption	Encryption settings.
Power Management	Suspend behavior.
VMware Tools	VMware Tools scripts behavior, VMware Tools upgrade settings, guest OS time synchronization settings
Boot Options	Boot delay, force entry into the BIOS or EFI setup screen.
Advanced	Acceleration and logging settings, debugging and statistics, swap file location, and latency sensitivity
Fibre Channel NPIV	Virtual node and port World Wide Names (WWNs).

A virtual machine name must be unique within the folder where the virtual machine is located. If you move a virtual machine to a different datastore folder or host that already has a virtual machine of the same name, you must change the virtual machine's name to keep it unique. Changing a virtual machine name impacts how the virtual machine is identified by vCenter Server and does not impact file (or folder) names or the guest OS.

After changing a virtual machine name, you can leverage Storage vMotion to migrate the virtual machine, which renames the associated files to match the new virtual machine name.

You can encrypt a virtual machine by editing its storage policies or by editing **VM Options**. Before encrypting a virtual machine, you must meet the following prerequisites.



- Establish a trusted connection with the KMS and select a default KMS.
- Create an encryption storage policy (or plan to use the sample VM Encryption Policy).
- Powered off the virtual machine
- Verify that you have the required privileges:
  - Verify you have the **Cryptographic operations.Encrypt** new privilege
  - If the host encryption mode is not enabled, then verify you have the **Cryptographic operations.Register host** privilege.

You can use the following procedure to encrypt a virtual machine.

**Step 1.** In the vSphere Client, right-click the virtual machine in the inventory pane

**Step 2.** Select **VM Policies > Edit VM Storage Policies** and use one of the following methods.

- Select an encryption storage policy to apply to the virtual machine and its virtual disks and click **OK**.

- Click **Configure per disk**, select the encryption storage policy for VM, select an encryption or other storage policies for each virtual disk, and click **OK**.

**Step 3.** If you prefer, you can encrypt the virtual machine, or both virtual machine and disks, from the **Edit Settings** menu in the vSphere Client.

- a. Right-click the virtual machine and select **Edit Settings**.
- b. Select the **VM Options** tab, and open **Encryption**. Choose an encryption policy. If you deselect all disks, only the VM home is encrypted.

**Step 4.** Click **OK**.

## Configure Guest User Mappings

You can enable guest OS access for some of your SSO user account to facilitate some administrative tasks, such as upgrading VMware Tools. You can use the following procedure to enroll SSO users to user accounts in guest operating systems by using SSO certificates. Subsequent guest management requests use an SSO SAML token to log in to the guest.

**Step 1.** In the vSphere Client, select a powered-on virtual machine in the inventory pane

**Step 2.** Click **Configure > Guest User Mappings** tab.

**Step 3.** Enter your user name and password and click **Log In**.

**Step 4.** In the **Guest User Mappings** pane, click the **Add** button.

**Step 5.** In the dialog box, select the SSO user.

**Step 6.** Specify a guest OS username and click **OK**.

## Edit OVF Details

You can use the following procedure to edit a virtual machine's OVF settings to customize the OVF environment, OVF transport, and boot behavior after OVF deployment. This information is preserved when you export the virtual machine as an OVF template.

**Step 1.** In the vSphere Client, select a virtual machine in the inventory pane.

**Step 2.** Click **Configure > Settings > vApp options**.

**Step 3.** Click the **Edit** button.

**Step 4.** If vApp options are not enabled, select the **Enable vApp options** check box.

**Step 5.** Click the **OVF Details** tab.

**Step 6.** Set the **OVF environment transport** option to one of the following.

- **ISO Image:** mounts an ISO image with the OVF template to the CD-ROM drive.
- **VMware Tools:** initializes the `guestInfo.ovfEnv` variable with the OVF environment document.

**Step 7.** Optionally, enable the Installation boot option and delay time in seconds, to automatically reboot the virtual machine after OVF deployment.

**Step 8.** Click **OK**

## Create and Manage Virtual Machine Snapshots

You can use virtual machine snapshots to capture the state and data of a virtual machine at a specific point in time. A snapshot preserves the following information.

- Virtual machine settings.
- Power state.
- Disk state.
- (Optional) Memory state.

To take a snapshot, you can right-click a virtual machine, select **Snapshots > Take Snapshot**, and provide a snapshot name. Optionally, you can provide a snapshot description and select **Snapshot the virtual machine's memory**. Also, you can optionally choose **Quiesce guest file system**. Quiescing the file system requires the virtual machine to be powered on, VMware Tools to be running, and **Snapshot the virtual machine's memory** to be deselected.

**Note**

To minimize the impact to a running virtual machine and to reduce the time required to take a snapshot, do not snapshot the memory state or quiesce the guest file system.

After creating a snapshot, you can use the Snapshot Manager to view the snapshot hierarchy of the virtual machine, which appears as a tree with branches, as illustrated in Figure 5.X. To open the Snapshot Manager, you can right-click the virtual machine and choose **Snapshots > Manage Snapshots**. In the Snapshot Manager, the snapshot that appears above the **You are here** icon is the parent snapshot. If you revert to a snapshot, that snapshot becomes the parent snapshot. If you take a snapshot of a virtual machine that already has at least one snapshot, the new snapshot is a child of the parent snapshot.

To revert a virtual machine to a specific snapshot, select the snapshot in the Snapshot Manager for the virtual machine and select **Revert To**. This requires you to have the **Virtual machine.Snapshot management.Revert to snapshot** privilege on the virtual machine.

When you revert the virtual machine to a snapshot, you return its virtual disks and settings to the state captured in the snapshot. If the snapshot includes the memory state, then reverting to the snapshot returns the virtual machine's memory to that state. You can revert the virtual machine to any available snapshot in the Snapshot Manager. Subsequent snapshots from this point create a new branch of the snapshot tree. When you revert to a snapshot, no snapshots are removed, but you lose the virtual machine's current disk state. In other words, all changes to disk data made since the last snapshot will be permanently lost. If you revert to a snapshot without memory state, the virtual machine will be in the powered off state.

You can delete a snapshot for a running virtual machine without disrupting its end users. Deleting a snapshot removes your ability to revert to that snapshot's state in the future. To delete a specific snapshot, select the snapshot in the Snapshot Manager for the virtual machine and select **Delete**. Optionally, to delete all snapshots, select **Delete All**.

If the virtual machine is in a state where it has no snapshots but has one or more delta disks contributing to the active state of the virtual machine, then you can consolidate its disks. In this state, you can right-click the virtual machine and select **Snapshots > Consolidate**. The system will merge the data from delta disks into the base disks and delete the delta disks. In normal conditions, your virtual machine will be in state where the **Consolidate** option is not available.

## Migrate Virtual Machines



To migrate a virtual machine using the vSphere Client, you can right-click the virtual machine in the inventory pane, choose **Migrate**, and complete the wizard. The details for completing the wizard are dependent on the migration type. The required privileges for each migration type are covered in [Chapter 5](#). You can use the **Recent Tasks** pane to monitor the progress of your migration.

To cold migrate a virtual machine, you can use the following procedure.

**Step 1.** In the vSphere Client, right-click a powered off virtual machine and select **Migrate**.

**Step 2.** Select one of the following migration types and click **Next**.

- a. **Change compute resource only**
- b. **Change storage only**
- c. **Change both compute resource and storage**
- d. **Migrate virtual machine(s) to a specific datacenter**

**Step 3.** If you select a migration type that includes a cross host migration, select the destination compute resource (host, cluster, resource pool, or vApp), verify no issues exist in the **Compatibility** panel, and click **Next**.

**Step 4.** If you select a migration type that includes a cross datastore migration, select the virtual disk format (**Same as Source**, **Thin**

**Provisioned, Thick Provisioned Lazy Zeroed, or Thick Provisioned Eager Zeroed**), select the appropriate policy in the **VM Storage Policy** menu and select the destination, as described here.

- a. To store all the virtual machines in a datastore, select the datastore and click **Next**.
- b. To store all the virtual machines in a Storage DRS cluster, select the cluster and click **Next**.
- c. To store the virtual machine configuration files and virtual disks in separate locations, click **Advanced** and configure the destination for the configuration files and each virtual disk. Click **Next**.

**Step 5.** For cross host migrations, select the destination network for the virtual machines and click **Next**. Alternatively, you can click **Advanced** to assign separate networks to individual virtual machine network adapters.

**Step 6.** Click **Finish**.

To perform a hot cross host (vMotion) migration, you can apply the previous cold migration procedure, with the following changes.

- Start with a powered on virtual machine.
- Select change compute resource only.
- You will not be prompted to select a destination datastore.
- Select either Schedule vMotion with high priority or Schedule Regular vMotion.

To perform a hot cross data store (Storage vMotion) migration, you can apply the previous cold migration procedure, with the following changes.

- Start with a powered on virtual machine.
- Select change storage only.
- You will not be prompted to select a destination host.

To perform a hot cross host and cross data store (vMotion without shared storage) migration, you can apply the previous cold migration procedure, with the following changes.

- Start with a powered on virtual machine.
- Select change both compute resource and storage.
- Select either Schedule vMotion with high priority or Schedule Regular vMotion.

## ADVANCED VIRTUAL MACHINE MANAGEMENT

This section covers topics related to the configuration and management of virtual machines that are not covered elsewhere in the book.

### Manage OVF Templates

To export a virtual machine into a self-contained OVF template, you can select the virtual machine and select **Actions > Template > Export OVF Template**. You must have the **vApp.Export** privilege. In the export wizard, you must provide a name and can optionally provide a description and configure advanced options. In the advanced options, you can include details concerning BIOS, UUID, MAC address, boot order, PCI slots, and other settings.

You can browse the VMware Virtual Appliance Marketplace to discover and download virtual appliances provided by VMware and VMware partners. The varying cost and licensing for each appliance are controlled by the provider.

## **Virtual Based Security**

Starting with vSphere 6.7, you can enable Microsoft virtualization-based security (VBS) on supported Windows guest operating systems. VBS is a Microsoft feature for Windows 10 and Windows Server 2016 operating systems that uses hardware and software virtualization to enhance system security by creating an isolated, hypervisor-restricted, specialized subsystem. Windows typically uses hashed credentials stored in memory, including Active Directory credentials, that may be subject to the Pass the Hash exploit. In VBS, you can enable a feature called Credential Guard that keeps account hash information outside the memory of the Windows instance, mitigating Pass the Hash. If the hardware TPM is not available or not enabled in the BIOS, then Windows will still use VBS and you can still enable Credential Guard, but the credentials will not be as secure.

On a traditional (non-virtual) Windows server, to prepare for VBS you should ensure its BIOS, firmware, and operating system are set to use UEFI firmware, Secure Boot, hardware virtualization (Intel VT / ADM-V), and IOMMU. You can enable VBS in the Windows operating system. When you reboot Windows, the Microsoft hypervisor will load and will leverage virtualization to bring up additional Windows components, including the credential management subsystem, in a separate memory space. All subsequent communication between Windows and Windows components are via RPC calls run through a Microsoft hypervisor-based communications channel.

In vSphere, to use VBS, you must use virtual hardware version 14 or later. The virtual machine must be set to use UEFI firmware, Secure Boot, hardware virtualization (Intel VT / ADM-V), and IOMMU. In the virtual machine settings, enable the **Virtualization Based Security** checkbox on the **VM Options** tab. Finally, you must enable VBS by editing the group policy.

Enabling VBS for the virtual machine does not automatically enable virtual TPM, but you can add a virtual TPM device. A virtual TPM doesn't have a hardware-based vault. Instead, the data that it secures is written to the NVRAM file, which is encrypted using VM Encryption, providing strong encryption and virtual machine portability.

## Manage VMs using PowerCLI

VMware PowerCLI is a command-line and scripting tool built on Windows PowerShell that provides cmdlets for managing and automating VMware products, including vSphere. You can install PowerCLI on a workstation or server in your vSphere environment and use PowerCLI to automate some aspects of your virtual machine management.

The main prerequisites for installing PowerCLI 12.0 on a Windows system are the presence of .NET Framework 4.7.2 or later and Windows PowerShell 5.1. For Linux and macOS systems, the requirements are .NET CORE 3.1 and PowerShell7. The main steps to install PowerCLI are to download the product to the system and run the following command in the PowerShell console.

---

```
Install-Module VMware.PowerCLI -Scope CurrentUser
```

In many cases, you will want to change the execution policy, which is set to the most secure policy by default

(Restricted). For example, to change the policy to RemoteSigned,, you can use the following command.

```
Set-ExecutionPolicy RemoteSigned
```

The Connect-VIServer cmdlet allows you to connect to a vCenter Server. The Get-VM cmdlet allows you to collect information about virtual machines. You can use the following commands to connect to a vCenter Server named server1.vsphere.local (using the administrator@vsphere.local account and the password “VMware1!”) and display information for all of its managed virtual machines.

```
Connect-VIServer -Server server1.vsphere.local -Protocol
```

```
Get-VM
```

To start a virtual machine named win-01, you can use the following commands.

```
Get-VM win-01 | Start-VM
```

You can use PowerCLI to create virtual machines from specifications provided in an XML file. The XML content could provide detailed specifications for multiple virtual machines. For example, you can use the following sample XML content, which represents the minimum specifications for two virtual machines named MyVM1 and MyVM2 each having a 100 GB virtual disk.

```
<CreateVM>
<VM>
  <Name>MyVM1</Name>
  <HDDCapacity>100</HDDCapacity>
</VM>
<VM>
```

```
<Name>MyVM2</Name>
<HDDCapacity>100</HDDCapacity>
</VM>
</CreateVM>
```

If you save the sample content to a file named MyVMs.xml, then you can use the following commands to read the file, parse the XML content into a variable, and create a virtual machine based on each specification.

```
[xml]$s = Get-Content myVM.xml
$s.CreateVM.VM | foreach {New-VM -VMHost $vmHost1 -Na
```

You can use PowerCLI to migrate virtual machines. Consider a scenario where you need to automate frequent, massive migrations of virtual machines between datastores to prepare for storage array upgrades. At the lowest level, you need a command that migrates a virtual machine to a specified datastore. For example, you can use the following command to migrate a virtual machine named MyVM1 to a datastore named DS2.

```
Get-VM MyVM1 | Move-VM -Datastore DS2
```

## Configure VMs to Support vGPUs

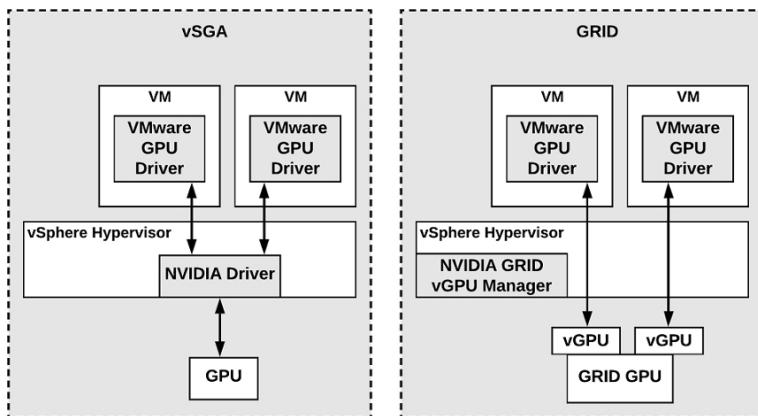
In vSphere 7.0, you can enable your virtual machines to use the processing power of available Graphic Processing Units (GPUs). GPUs are specialized processors developed for parallel processing, primarily for rendering graphical images. In vSphere, its main use case is to support high end graphics in virtual desktop infrastructure (VDI). Recently, the need to support artificial intelligence (AI) and machine learning (ML) has emerged has a major use case.

You can use GPUs in different manners in a vSphere environment. For AI/ML use cases, the GPU configuration choice is mostly impacted by size and complexity of the problem being solved. Likewise, for VDI, the GPU configuration choice is impacted by the end user graphics needs. The configuration involves either sharing GPUs with multiple virtual machines or dedicating some GPUs to specific virtual machines. [Table 14-8](#) summarizes the potential GPU configuration for specific AI / ML use cases.

**Table 14-8** Use Cases and GPU Configurations

GPU Configuration	Sample Use Cases	Details
GPU Sharing	ML Development and Testing	Good fit for small problems and for the ML inference phase
Dedicated GPU	Data Science	Commonly used for development and training in ML models
Dedicated Multiple GPUs per VM	Advanced, power ML users tackling large problems	Highest performing GPU model

For the VMware Horizon 7 VDI use case, depending on your hardware, you may have multiple options for sharing GPUs. For example, with NVIDIA hardware, you can choose to share GPUs using the NVIDIA vGPU (GRID) technology or the Virtual Shared Graphics Acceleration,(vSGA) technology. In the vSGA model, the vSphere hypervisor presents a virtual VMware SVGA 3D GPU to each virtual machine. In the GRID model, each hardware GPU presents multiple virtual GPUs that the hypervisor passes through to the virtual machines. In the GRID model, you can use a vGPU profile to assign a portion of the GPU hardware to a virtual machine. The vSGA model tends to be flexible and cost effective for supporting virtual desktops running office, video, and 2D CAD applications. But the performance of the GRID model may be preferred for virtual desktops running 3D modeling software. For a side by side comparison of the vSGA and GRID models, see [Figure 14.1](#).



**Figure 14-1** Comparison of the vSGA and GRID Models

The procedure to configure the GPU hardware, ESXi host, and virtual machine depend on your choice for GPU configuration. For example, you can use the following procedure to implement the GRID model using a vGPU profile (named `grid_p100-8a`) to allow a virtual machine to use up to 8 GB of the GPU's memory.

**Step 1.** Obtain the NVIDIA vGPU software and license.

**Step 2.** In the vSphere Client, select the ESXi host in the inventory pane.

**Step 3.** Navigate to Configure > Hardware > Graphics > Host Graphics

**Step 4.** Click Edit.

**Step 5.** Select the **Shared Direct** (Vendor shared passthrough graphics) option.

**Step 6.** Reboot the host and enter maintenance mode.

**Step 7.** In the ESXi Shell, enter the following command, but replace the path to represent the actual path to the downloaded VIB file.

```
esxcli software vib install -v /vmfs/volumes/ARL-ESX1
```

**Step 8.** Exit maintenance mode.

**Step 9.** Edit the virtual machine settings and select the option to add a new device.

**Step 10.** In the New PCI device dropdown, select NVIDIA GRID vGPU.

**Step 11.** In the **GPU Profile** dropdown, select an appropriate profile, such as **grid\_p100-8a**.

**Step 12.** In the virtual machine guest OS, install the appropriate NVIDIA vGPU driver.

## CONTENT LIBRARY

This section provides details for implementing and using content libraries to provide templates, ISOs, and other content across multiple vCenter Servers in a vSphere environment.

### Introduction to Content Library

A Content Library is a container objects for virtual machine templates, vApp templates, ISO images, and other files that you may want to share among multiple vCenter Servers in a vSphere environment. Content libraries allow you to share templates and other files in a manner that provides consistency, compliance, efficiency, and automation when deploying workloads at scale.

A content library contains and manages content in the form of library items. A single library item consists of one file or multiple files. For example, an OVF template is a set of files with the OVF, VMDK, and MF file extensions. When you upload an OVF template to the library, you upload the entire set of files, which the library represents as a single item.

When creating a content library, you can choose to create a local content library or a subscribed content library.

With a local library, you store and manage content in a single vCenter Server instance. After creating a local library, you can publish it to make it available for subscription. From another vCenter Server instance, you can create a subscribed content library with a subscription to the published library. With a subscribed library, you can control when to download the subscribed content, either immediately or as needed.

Historically, content libraries supported OVF templates but not standard virtual machine templates. Starting with vSphere 6.7 Update 1, content libraries support virtual machine templates in addition to OVF templates.

## Create a Content Library

You can use the vSphere Client to create a content library using the following procedure.

You must have one of the following privileges on the vCenter Server instance.

- Content library.Create local library
- Content library.Create subscribed library

You must have Datastore > Allocate space on the target datastore.

**Step 1.** Open the New Content Library wizard

**Step 2.** On the **Name and location** page, enter a name and select a vCenter Server instance for the content library. Click **Next**.

**Step 3.** On the **Configure content library** page, select the type of content library that you want to create and click **Next**.

- **Local content library:** A local content library is accessible only in the vCenter Server instance where you create it by default. Optionally, you can select **Enable publishing** to make the content of the library available to other vCenter Server instances
- **Subscribed content library:** Creates a content library that subscribes to published content library.

**Step 4.** On the **Add storage** page, select a storage location for the content library contents and click **Next**.

**Step 5.** On the **Ready to Complete** page, review the details and click **Finish**

## Publish a Content Library

You can publish an existing content library. For example, to publish an existing local, non-subscribed library, you can use the following procedure.

**Step 1.** Use the vSphere Client to navigate to **Content Libraries**.

**Step 2.** Right click on an existing content library and select **Edit Settings**

- a. Select the **Enable publishing** check box.
- b. Click the **Copy Link** button to copy the URL of your library that you can paste into the settings of a subscribed library.
- c. Select Enable user authentication for access to this content library and set a password for the library.

**Step 3.** Click **OK**.

**Note**

When you enable authentication for the content library, you effectively set a password on the static username `vcsp`, which you cannot change. It is a user account that is not associated with vCenter Single Sign-on or Active Directory.

## Subscribe to a Content Library

When using the previous procedure to create a subscribed content library, you must provide the following information.



**Step 1.** In the **Subscription URL** text box, enter the URL address of the published library.

**Step 2.** If authentication is enabled on the published library, select **Enable authentication** and enter the publisher password.

**Step 3.** Select a download method for the contents of the subscribed library: **immediately** or **when needed**.

**Step 4.** If prompted, accept the SSL certificate thumbprint. The SSL certificate thumbprint is stored on your system until you delete the subscribed content library from the inventory.

**Note**

The transfer service on the vCenter Server is responsible for importing and exporting content between the subscriber and the publisher, using HTTP NFC.

## Content Library Permissions

Content libraries are not direct children of the vCenter Server object in the vSphere inventory. Instead, content libraries are direct children of the global root. This means that permissions set on a vCenter Server do not

apply to content libraries even if they are set to propagate to child objects. To assign a permission on a content library, an Administrator must grant the permission to the user as a global permission. Global permissions support assigning privileges across solutions from a global root object

Consider the following scenarios.

- If a user is granted the `Read Only` role as a global permission and the `Administrator` role at a vCenter Server level, then the user can manage the vCenter Server's content libraries and content but can only view content libraries belonging to other vCenter Servers.
- If a user is granted the `Content Library Administrator` role as a global permission, the user can manage all content libraries and content in all vCenter Server instances.
- If a user is not granted any global permission but is granted the `Administrator` role at a vCenter Server level, the user cannot view or manage any libraries or content, including the vCenter Server's local content libraries.

vCenter Server provides a predefined, sample role, `Content Library Administrator`, that allows you to give users or groups the necessary privileges to manage selected content libraries. You can modify the role or use it as an example to create custom roles. If a user is assigned the `Content Library Administrator` role on a library, that user can perform the following tasks on that library.

- Create, edit, and delete local or subscribed libraries.
- Synchronize a subscribed library and synchronize items in a subscribed library.

- View the item types supported by the library.
- Configure the global settings for the library.
- Import items to a library.
- Export library items.

**Note**

You cannot set permissions on a content library directly

## Synchronization Options

When configuring the subscribing library, you can choose either to download all libraries' content immediately or download library content only when needed. The first option starts the full synchronization process immediately. It includes the full content, including the metadata and actual data. The latter option starts the synchronization process for just the metadata immediately. The metadata contains information about the actual content data, allowing users to view and select the associated templates and ISOs. In this case, the actual data is synchronized only as needed when subscribed library objects are demanded. The impact of the on-demand synchronization is that storage space may be saved for the subscribing library, but a delay may exist each time a library item is selected.

To enable automatic synchronization, select the option to **Enable automatic synchronization with the external library** in the subscribed library settings. Consider the fact that the automatic synchronization requires a lot of storage space, because you download full copies of all the items in the published library.

The content library synchronization method has an impact on VM provisioning time and datastore space usage. If an object is not already downloaded when you go to use it, you may have to wait while the subscribed

content library downloads it from the published library. To optimize VM provisioning time, consider setting the download method to **immediately**. To optimize datastore space usage, consider setting the download method to **when needed**.

## Add Items to the Content Library

You can import items such as OVA / OVF templates and vApps to a content library from your local machine or from a Web server. You can also import ISO images, certificates, and other files. You can add an item that resides on a Web server to a content library, or you can add items to a content library by importing files from your local file system.

You can import an OVF package to use as a template for deploying virtual machines and vApps. You can also import other types of files, such as scripts or ISO files. To import a file, right-click a content library, choose **Import Item**, select a file, and assign the **Item Name**.

You can also add content to the library by cloning VMs or templates to the library, as described in the following steps.

**Step 1.** In the vSphere Client, navigate to the virtual machine or template that you want to clone.

**Step 2.** Select one of the following cloning tasks.

- Right-click a virtual machine and select **Clone > Clone to Template in Library**.
- Right-click a VM template and select **Clone to Library**.

**Step 3.** Depending on the selection in the previous step, complete the cloning wizard. For example, if you selected a VM template and chose **Clone to Library**, then you can use the following

steps to create a new template in the content library.

- a. Select the **Clone as** option and choose to create a new template
- b. From the content libraries list, select the library in which you want to add the template.
- c. Enter a name and description for the template.
- d. (Optional) Select the configuration data that you want to include in the template. You can select to preserve the MAC-addresses on the network adapters and include extra configuration.
- e. Click **OK**.

## Deploy VMs Using the Content Library

You can deploy virtual machines from the VM templates in your content library using this procedure.

**Step 1.** Select Home > Content Libraries.

**Step 2.** Select a content library and click the **Templates** tab.

**Step 3.** Right-click a VM Template and select **New VM from This Template**.

**Step 4.** On the **Select name and location** page, enter a name and select a location for the virtual machine.

**Step 5.** (Optional) To apply a customization specification to your virtual machine, select the **Customize the operating system** checkbox and click **Next**.

**Step 6.** On the **Customize Guest OS** page, select a customization specification or create a new one, and click **Next**.

**Step 7.** On the Select a resource page, select a host, a cluster, a resource pool, or a vApp where to run the deployed VM template, and click **Next**.

**Step 8.** On the **Review details** page, verify the template details and click **Next**.

As mentioned in the section “How to Use This Book” in the Introduction, you have a couple of choices for exam preparation: the exercises here, [Chapter 15, "Final Preparation,"](#) and the exam simulation questions on the CD-ROM.

## REVIEW ALL KEY TOPICS

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 14-9](#) lists a reference of these key topics and the page numbers on which each is found.



**Table 14-9** Key Topics for Chapter 14

Key Topic Element	Description	Page Number
List	Permissions to create a virtual machine	
List	Permissions to clone a virtual machine	
Procedure	Create a Linux guest customization specification	
Procedure	Create a Windows guest customization specification	
List	Conditions for CPU hot add	
List	Requirements for virtual machine encryption	
Section	Migrate Virtual Machines	
Section	Configure VMs to Support vGPUs	
Procedure	Subscribe to a content library	

## DEFINE KEY TERMS

Define the following key terms from this chapter and check your answers in the glossary:

Microsoft virtualization-based security (VBS)

VMware PowerCLI

Content Library

Open Virtual Format (OVF) template

Open Virtual Appliance (OVA) template

Graphic Processing Unit (GPU)

## Glossary

**VBS:** Microsoft virtualization-based security (VBS) is a Microsoft feature for Windows 10 and Windows Server 2016 operating systems that uses hardware and software virtualization to enhance system security by creating an isolated, hypervisor-restricted, specialized subsystem.

**PowerCLI:** VMware PowerCLI is a command-line and scripting tool built on Windows PowerShell that provides cmdlets for managing and automating VMware products, including vSphere.

**Content Library:** A Content Library is a container objects for virtual machine templates, vApp templates, ISO images, and other files that you may want to share

among multiple vCenter Servers in a vSphere environment.

**OVF Template:** An Open Virtual Format (OVF) template is a set of files with the OVF, VMDK, and MF file extensions

**OVA Template:** An Open Virtual Appliance (OVA) is essentially a single-file distribution of an OVF package

**GPU:** A Graphic Processing Unit (GPU) is a specialized processor developed for parallel processing, primarily for rendering graphical images.

## REVIEW QUESTIONS

- 1.** Which of the following is a requirement for guest OS customization?
  - a.** ESXi 5.0 or later
  - b.** VMware Tools 11.0 or latter
  - c.** A supported guest OS installed on SCSI node 0:0
  - d.** A supported guest OS installed on any SCSI node
- 2.** You want to create a virtual machine that can use up to 4096 MB video memory. Which compatibility option should you choose?
  - a.** ESXi 7.0 and later
  - b.** ESXi 6.7 Update 2 and later
  - c.** ESXi 6.7 and later
  - d.** ESXi 6.5 and later
- 3.** You are snapshotting production virtual machines and want to minimize the impact to

users of the guest OS and its applications. Which option should you choose?

- a.** Snapshot the memory and quiesce the file system.
- b.** Snapshot the memory, but do not quiesce the file system.
- c.** Quiesce the file system, but do Not snapshot the memory
- d.** Do not quiesce the file system or snapshot the memory

**4.** In your vSphere 7.0 environment, you want to export a virtual machine for portability to other systems. Which approach should you use?

- a.** Export to OVF
- b.** Export to OVA
- c.** Export as a VM template
- d.** Export as a VMDK

**5.** You are configuring a subscribed content library. Which of the following is used to synchronize content?

- a.** HTTPS
- b.** HTTP NFC
- c.** FTP
- d.** SCP

# **Chapter 15. Final Preparation [This content is currently in development.]**

**This content is currently in development.**